International Mathematical Forum, Vol. 8, 2013, no. 20, 957 - 965
HIKARI Ltd, www.m-hikari.com

On the Exponential Diophantine Equation $a^{2x} + a^x b^y + b^{2y} = c^z$

Nobuhiro Terai

Division of Information System Design, Ashikaga Institute of Technology
268-1 Omae, Ashikaga, Tochigi 326–8558, Japan
terai@ashitech.ac.jp

Kei Takakuwa

Department of Mathematics, Faculty of Science, Gakushuin University
Mejiro, Toshima-ku, Tokyo 171–8588, Japan
takakuwa@math.gakushuin.ac.jp

Abstract

Let a, b, c be fixed positive integers satisfying $a^2 + ab + b^2 = c$ with $\gcd(a, b) = 1$. We show that the Diophantine equation $a^{2x} + a^x b^y + b^{2y} = c^z$ has only the positive integer solution $(x, y, z) = (1, 1, 1)$ under some conditions. The proof is based on elementary methods and Cohn's ones concerning the Diophantine equation $x^2 + C = y^n$.

Mathematics Subject Classification: 11D61

Keywords: exponential Diophantine equation, integer solution, Eisenstein numbers

1 Introduction.

Let a, b, c be primitive *Pythagorean numbers*, i.e., relatively prime positive integers satisfying $a^2 + b^2 = c^2$. Jeśmanowicz [J] conjectured that if a, b, c are primitive Pythagorean numbers, then the Diophantine equation

$$a^x + b^y = c^z$$

has only the positive integer solution $(x, y, z) = (2, 2, 2)$. Although Jeśmanowicz' Conjecture holds for many special Pythagorean numbers, this remains unsolved in general. (See Terai[Te1] and [Te2] for analogues to Jeśmanowicz' conjecture.)

On the other hand, we call $a,\ b,\ c$ *Eisenstein numbers* if a, b, c are positive integers satisfying $a^2+ab+b^2=c^2$. As another analogue to Jeśmanowicz' conjecture concerning Pythagorean numbers, in previous papers [TT] and [Te3], we proposed the following:

Conjecture 1. *Let a, b, c be fixed positive integers satisfying $a^2+ab+b^2=c^2$ with $\gcd(a,\ b)=1$. Then the Diophantine equation*

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

has only the positive integer solution $(x, y, z)=(1, 1, 2)$.

In this paper, as an analogue to Conjecture 1, we also propose the following:

Conjecture 2. *Let a, b, c be fixed positive integers satisfying $a^2+ab+b^2=c$ with $\gcd(a, b)=1$. Then equation (1) has only the positive integer solution $(x, y, z)=(1, 1, 1)$.*

Using the methods of Cohn[C1] and [C2] concerning the Diophantine equation $x^2+C=y^n$ as well as the ones in [TT], we show that the above Conjecture holds under some conditions. In fact, we establish the following:

Theorem 1. *Let a, b, c be fixed positive integers satisfying*

$$a=p^s, \quad b=2q^t, \quad c=a^2+ab+b^2 \tag{2}$$

with $c\not\equiv 0 \pmod 3$, where p, q are distinct odd primes and s, t are positive integers. Sppose that $q^t<10000$. Then equation (1) has only the positive integer solution $(x, y, z)=(1, 1, 1)$.

Theorem 2. *Let a, b, c be fixed positive integers satisfying*

$$a=m, \quad b=2, \quad c=a^2+ab+b^2 \tag{3}$$

with $c\not\equiv 0 \pmod 3$, where m is odd ≥ 3. Then equation (1) has only the positive integer solution $(x, y, z)=(1, 1, 1)$.

2 Lemmas.

We use the following Lemmas to show Theorems 1,2.

Lemma 1 ([TT]). *Eisenstein numbers a, b, c with $\gcd(a,\ b)=1$ and $a-b\equiv 1 \pmod 3$ are given as follows:*

$$a=u^2-v^2, \qquad b=v(2u+v), \qquad c=u^2+uv+v^2,$$

where u, v are positive integers such that $\gcd(u, v)=1$, $u>v$ and $u\not\equiv v \pmod 3$.

Lemma 2 (Nagell[N1]). *The Diophantine equation*

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

has only the positive integer solution $(x, y, n) = (18, 7, 3)$ *with* $n \geq 2$.

Lemma 3 (Nagell[N2]). *The Diophantine equation*

$$3x^2 + 1 = y^n$$

has no positive integer solutions x, y, n *with* y *odd and* n *odd* ≥ 3.

Lemma 4 (Ljunggren[L]). *The Diophantine equation*

$$3x^2 + 1 = 4y^n$$

has no positive integer solutions $x,\ y,\ n$ *with* $y > 1$ *and* $n \geq 3$.

Lemma 5 (Brown[B1], [B2]). *The Diophantine equation*

$$x^2 + 3^m = y^n$$

has only the positive integer solution $(x, y, m, n) = (10, 7, 5, 3)$ *with* $\gcd(x, y) = 1$, m *odd and* $n \geq 3$.

Lemma 6 (Cohn[C1]). *Let* C *be a positive integer with* $C = cd^2$, c *square-free and* $c \not\equiv 7 \pmod 8$. *If* p *is an odd prime and*

$$x^2 + C = y^p$$

for coprime integers $x,\ y$, *then either*

(a) *there exist integers* $a,\ b$ *with* $b \mid d$, $y = a^2 + cb^2$ *and* $\pm x + d\sqrt{-c} = (a + b\sqrt{-c})^p$*;or*

(b) $c \equiv 3 \pmod 8$, $p = 3$ *and there exist odd integers* $A,\ B$ *with* $B \mid d$, $y = (A^2 + cB^2)/4,\ \ \pm x + d\sqrt{-c} = \left(\dfrac{A + B\sqrt{-c}}{2}\right)^3$*;or*

(c) $p \mid h$, *the class number of the imaginary quadratic field* $\mathbf{Q}(\sqrt{-c})$*;or*

(d) $C = 3A^2 \pm 8,\ p = 3,\ x = A^3 \pm 3A$*;or*

(e) $C = 48D^6,\ p = 3,\ x = 4D^3$.

3 The Diophantine equation $X^2 + 3D^2 = Y^n$.

When $y = 1$, equation (1) can be written as

$$(a^x + D)^2 + 3D^2 = c^z,$$

where $b = 2q^t = 2D$. Hence we need the following Proposition to show Theorem 1.

Proposition 1. *Let $D = q^t < 10000$, where q is an odd prime and t is a positive integer. Then the Diophantine equation*

$$X^2 + 3D^2 = Y^n \tag{4}$$

has only the positive integer solutions $(X, Y, D, n) = (10, 7, 9, 3),\ (118, 7, 31, 5),\ (254, 7, 503, 7),\ (716, 19, 809, 5),\ (28724, 19, 4789, 7)$ *with* $\gcd(X, Y) = 1$ *and* $n \geq 3$.

Proof. When $D = 3^t$, it follows from Lemma 5 that equation (4) has only the positive integer solution $(X, Y, D, n) = (10, 7, 9, 3)$ with $\gcd(X, Y) = 1$ and $n \geq 3$.

Next consider the case $D = q^t < 10000$ with $q > 3$. If X is odd ,then taking (4) modulo 8 implies that $4 \equiv X^2 + 3D^2 = Y^n \equiv 0 \pmod 8$, which is impossible. Hence X is even and so n is odd. We may suppose that n is an odd prime, say $n = l$.

If $l = 3$, then Lemma 6 (b) shows that there exist odd integers $u,\ v$ such that

$$\pm X + D\sqrt{-3} = \left(\frac{u + v\sqrt{-3}}{2}\right)^3$$

with $v \mid D$ and $Y = (u^2 + 3v^2)/4$. Equating the imaginary parts yields

$$8D = 3v(u^2 - v^2),$$

which is impossible, because $D = q^t$ with $q > 3$.

Now suppose that $l > 3$. Then in view of Lemma 6 (a), there exist integers $u,\ v$ such that

$$\pm X + D\sqrt{-3} = (u + v\sqrt{-3})^l$$

with $Y = u^2+3v^2$. We observe that u is even, since Y and v are odd. Equating the imaginary parts yields

$$D = v \sum_{j=0}^{(l-1)/2} \binom{l}{2j+1} u^{l-(2j+1)} v^{2j} (-3)^j. \tag{5}$$

Since $D = q^t$, we have $v = \pm q^k$ with $0 \le k \le t$. We now have to distinguish three cases: (i) $k = 0$, (ii) $0 < k < t$, (iii) $k = t$.

(i) $k = 0$. Then $v = \pm 1$ and so

$$\sum_{j=0}^{(l-1)/2} \binom{l}{2j+1} u^{l-(2j+1)}(-3)^j \pm D = 0. \tag{6}$$

Note that $l \mid (D \pm 1)$. Indeed, taking (6) modulo l implies that $D \equiv \pm(-3)^{(l-1)/2} \equiv \pm 1 \pmod{l}$. Hence if D is given, then l is bounded and (6) is a equation in u of degree $l-1$. When $D = q^t < 10000$, we can easily check, by a computer, that (6) has only the positive integer solutions $(D, l, u) = (31, 5, 2)$, $(503, 7, 2)$, $(809, 5, 4)$, $(4789, 7, 4)$ with u even. Therefore equation (4) has only the solutions listed above.

(ii) $0 < k < t$. Then

$$q^{t-k} = \pm \sum_{j=0}^{(l-1)/2} \binom{l}{2j+1} u^{l-(2j+1)}(-3q^{2k})^j.$$

Taking the above equation modulo q implies that $l = q$, and so $t - k = 1$. The minus sign can be rejected. Indeed, otherwise $q \equiv -qu^{q-1} \pmod{q^2}$, so $1 \equiv -u^{q-1} \equiv -1 \pmod{q}$, which is impossible. Consequently

$$q = \sum_{j=0}^{(q-1)/2} \binom{q}{2j+1} u^{q-(2j+1)}(-3q^{2k})^j. \tag{7}$$

Since u is even, we have $q \equiv 1 \pmod 4$. Suppose now that $2^m \| (q-1)$ with $m \ge 2$. We observe that the general term in the right-hand side of (7) has the following form:

$$\frac{q(q-1)}{(2j+1)(q-2j-1)} \cdot 2^{q-2j-1} \cdot \left(\frac{u}{2}\right)^{q-2j-1} \binom{q-2}{2j} (-3q^{2k})^j.$$

When $0 \le j < (q-1)/2$, the above term is divisible by 2^{m+1}, because the inequality $q - 2j - 1 < 2^{q-2j-1}$ holds. Therefore it follows from (7) that

$$q \equiv (-3q^{2k})^{(q-1)/2} \equiv 3^{(q-1)/2} q^{k(q-1)} \pmod{2^{m+1}}.$$

Using induction on m, we easily see that $3^{2^{m-1}} \equiv 1 \pmod{2^{m+1}}$ for all $m \ge 2$. Since $q \equiv 2^m + 1 \pmod{2^{m+1}}$, we have $q^2 \equiv 1 \pmod{2^{m+1}}$. Hence we conclude that $q \equiv 1 \pmod{2^{m+1}}$, which is impossible.

(iii) $k = t$. Then $v = \pm q^t = \pm D$. Hence equation (5) leads to

$$\frac{\alpha^l - \beta^l}{\alpha - \beta} = \pm 1,$$

where $\alpha = u \pm D\sqrt{-3}$ and $\beta = u \mp D\sqrt{-3}$. In view of Theorem of Cohn[C2] by means of [BHV], we see that the above equation has no solutions. ∎

4 Proof of Theorem 1.

Suppose that our assumptions are all satisfied. Let $(x,\ y,\ z)$ be a solution of (1). From (2), we see that $c \equiv 3 \pmod 4$.

We distinguish two cases: (i) $y = 1$, (ii) $y \geq 2$.

(i) $y = 1$. Then equation (1) can be written as

$$(a^x + D)^2 + 3D^2 = c^z. \tag{8}$$

Taking equation (8) modulo 4 implies that z is odd. Hence it follows from Proposition 1 that equation (8) has no solutions $x,\ z$ with $z \geq 3$ under our assumptions. We therefore conclude that equation (1) has only the positive integer solution $(x, y, z) = (1, 1, 1)$.

(ii) $y \geq 2$. Then it follows from (1) that z is even, say $z = 2Z$. By Lemma 1, we have

$$a^x = U^2 - V^2, \quad b^y = V(2U + V), \quad c^Z = U^2 + UV + V^2, \tag{E_1}$$

or

$$a^x = V(2U + V), \quad b^y = U^2 - V^2, \quad c^Z = U^2 + UV + V^2, \tag{E_2}$$

where U, V are positive integers such that $\gcd(U, V) = 1$, $U > V$ and $U \not\equiv V \pmod 3$.

First consider (E_1). Since a is a power of an odd prime and $\gcd(U, V) = 1$, we have $a^x = U + V,\ U - V = 1$ and so

$$3(2V + 1)^2 + 1 = 4c^Z.$$

Now Lemma 4 implies that $Z = 1$ or 2. We show that neither $Z = 1$ nor $Z = 2$ occurs.

When $Z = 2$, then it follows from Lemma 1 that

$$U,\ V = h^2 - k^2, \quad k(2h + k)\ ; \qquad c = h^2 + hk + k^2,$$

where $h,\ k$ are positive integers such that $\gcd(h, k) = 1$, $h > k$ and $h \not\equiv k \pmod 3$. Thus we obtain

$$U + V = h(2k + h) = a^x = p^{sx}.$$

This implies that $2k + h = p^{sx}$ and $h = 1$, which contradicts $1 \leq k < h$.

When $Z = 1$, we first suppose that $a < b$. Then $c = a^2 + ab + b^2 < 3b^2 < b^3$ from $3 < b$. From (1), we have

$$b^{2y} < a^{2x} + a^x b^y + b^{2y} = c^2 < b^6.$$

Since $y \geq 2$, we have $y = 2$. It follows from (1) and (2) that

$$a^x b^2 \equiv 2ab^3 \pmod{a^2},$$

so $x = 1$. Then $a^2 + ab^2 + b^4 = c^2 = (a^2 + ab + b^2)^2$, which is impossible.

Suppose that $a > b$. Then $c = a^2 + ab + b^2 < 3a^2 \leq a^3$ from $3 \leq a$. From (1), we have

$$a^{2x} < a^{2x} + a^x b^y + b^{2y} = c^2 < a^6,$$

so $x = 1, 2$. If $x = 2$, then it follows from (1) and (2) that

$$a^4 \equiv a^4 + 2a^3 b \pmod{b^2},$$

which is impossible. Hence we obtain $x = 1$. Then since $U = V + 1$ and $a = 2V + 1$, we have

$$3V^2 + 3V + 1 = U^2 + UV + V^2 = c = a^2 + ab + b^2 > a^2 = (2V + 1)^2 = 4V^2 + 4V + 1,$$

which is impossible.

Next consider (E_2). Since a is a power of an odd prime and $\gcd(U, V) = 1$, we have $V = 1$, $2U + V = a^x$ and so

$$U^2 + U + 1 = c^Z.$$

Now Lemma 2 implies that $Z = 1$. As above, we have $x = 1$. Then since $V = 1$ and $a = 2U + 1$, we have

$$U^2 + U + 1 = c = a^2 + ab + b^2 > a^2 = (2U + 1)^2 = 4U^2 + 4U + 1,$$

which is impossible. ∎

5 Proof of Theorem 2.

Suppose that our assumptions are all satisfied. Let (x, y, z) be a solution of (1). From (3), we see that $c \equiv 3 \pmod 4$.

We distinguish two cases: (i) $y = 1$, (ii) $y \geq 2$.

(i) $y = 1$. Then equation (1) can be written as

$$(a^x + 1)^2 + 3 = c^z. \tag{9}$$

Taking equation (9) modulo 4 implies that z is odd. Hence it follows from Lemma 5 that equation (9) has no solutions x, z with $z \geq 3$ under our assumptions. We therefore conclude that equation (1) has only the positive integer solution $(x, y, z) = (1, 1, 1)$.

(ii) $y \geq 2$. Then it follows from (1) that z is even, say $z = 2Z$. By Lemma 1, we have

$$a^x = U^2 - V^2, \qquad 2^y = V(2U + V), \qquad c^Z = U^2 + UV + V^2, \qquad (E_1)$$

or

$$a^x = V(2U + V), \qquad 2^y = U^2 - V^2, \qquad c^Z = U^2 + UV + V^2, \qquad (E_2)$$

where U, V are positive integers such that $\gcd(U, V) = 1$, $U > V$ and $U \not\equiv V \pmod 3$.

First consider (E_1). Then we have $V = 2$ and $2U + V = 2^{y-1}$ and so

$$(U + 1)^2 + 3 = c^Z.$$

Now Lemma 5 implies that $Z = 1$. We show that the case $Z = 1$ does not occur.

If $Z = 1$, then

$$c = U^2 + 2U + 4 = m^2 + 2m + 4,$$

so $U = m$. From $a^x = U^2 - V^2$, we have

$$m^x = m^2 - 4,$$

which is impossible, since m is odd ≥ 3.

Next consider (E_2). Then we have $U + V = 2^{y-1}$ and $U - V = 2$ and so

$$3(V + 1)^2 + 1 = c^Z.$$

Now Lemma 3 implies that $Z = 1,\ 2$. We show that neither $Z = 1$ nor $Z = 2$ occurs.

If $Z = 1$, then taking the above equation modulo 4 yields

$$c = c^Z \equiv 1 \pmod 4,$$

which is impossible, since $c \equiv 3 \pmod 4$.

If $Z = 2$, then it follows from Lemma 1 that

$$U + V = r(2s + r), \qquad c = r^2 + rs + s^2,$$

where r, s are positive integers such that $\gcd(r, s) = 1$, $r > s$ and $r \not\equiv s \pmod 3$. Since $r(2s + r) = 2^{y-1}$, we have $r = 2,\ s = 2^{y-3} - 1$. Then $c = s^2 + 2s + 4 = m^2 + 2m + 4$ and so $s = m$. Also $U = 2^{y-2} + 1 = 2s + 3 = 2m + 3$ and $V = U - 2 = 2m + 1$. In vew of $a^x = V(2U + V)$, we have

$$m^x = 12m^2 + 20m + 7,$$

which is impossible, since m is odd ≥ 3. ∎

References

[BHV] Yu. Bilu, G. Hanrot and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine Angew. Math. **539**(2001), 75–122.

[B1] E. Brown, *Diophantine equations of the form* $x^2 + D = y^n$, J. reine. angew. Math. 274/275(1975), 385–389.

[B2] E. Brown, *Diophantine equations of the form* $ax^2 + Db^2 = y^n$, J. reine. angew. Math. **291**(1977), 118–127.

[C1] J.H.E. Cohn, *The diophantine equation* $x^2 + C = y^n$, Acta Arith. **65**(1993), 367-381.

[C2] J.H.E. Cohn, *The diophantine equation* $x^2 + C = y^n$*, II*, Acta Arith. **109**(2003), 205–206.

[J] L. Jeśmanowicz, *Some remarks on Pythagorean numbers* (in Polish), Wiadom. Mat. 1(1955/1956), 196–202.

[L] W. Ljunggren, *Über die Gleichungen* $1+Dx^2 = 2y^n$ *und* $1+Dx^2 = 4y^n$, Det Kgl. Norske Videnskabers Selskab, Forhandl. Bd. 15, Nr. 30, Trondheim 1942.

[N1] T. Nagell, *Des équations indéterminées* $x^2+x+1 = y^n$ *et* $x^2+x+1 = 3y^n$, Norsk. Mat. Forenings Skrifter No. 2(1921), 12–14.

[N2] T. Nagell, *Contributions to the theory of a category of Diophantine equations of the second degree with two unkowns*, Nova Acta Soc. Sci. Upsal, Ser IV, (2), **16**(1955), 1–38.

[Te1] N. Terai, *The Diophantine equation* $x^2 + q^m = p^n$, Acta Arith. **63**(1993), 351–358.

[Te2] N. Terai, *Applications of a lower bound for linear forms in two logarithms to exponential Diophantine equations*, Acta Aith. **90**(1999), 17–35.

[Te3] N. Terai, *A remark on a conjecture concerning Eisenstein numbers*, Compt. Rend. Math. Rep. Acad. Sci. Canada **22**(2000), 105–110.

[TT] N. Terai and K. Takakuwa, *On a Diophantine equation concerning Eisenstein numbers*, Tokyo J. Math. **24**(2001), 429–439.

Received: March 5, 2013