Functiones et Approximatio
45.2 (2011), 207–229

JEŚMANOWICZ' CONJECTURE ON EXPONENTIAL DIOPHANTINE EQUATIONS

Takafumi Miyazaki

Abstract: Let (a, b, c) be a primitive Pythagorean triple such that $a^2 + b^2 = c^2$ with even b. In 1956, L. Jeśmanowicz conjectured that the equation $a^x + b^y = c^z$ has only the solution $(x, y, z) = (2, 2, 2)$ in positive integers. In this paper, we give various new results on this conjecture. In particular, we prove that if the equation has a solution (x, y, z) with even x, z then $x/2$ and $z/2$ are odd.

Keywords: exponential Diophantine equations, lower bounds for linear forms in logarithms of algebraic numbers, generalized Fermat equations, Pythagorean triples.

1. Introduction

Let $\mathbb{N}, \mathbb{Z}$ be the sets of positive integers and integers, respectively. Let a, b, c be relatively prime positive integers greater than 1. In this paper, we consider the solutions of the equation

$$a^x + b^y = c^z, \qquad x, y, z \in \mathbb{N}. \tag{1.1}$$

We say that this is an exponential Diophantine equation. A triple (a, b, c) is called a *primitive Pythagorean triple* if $a^2 + b^2 = c^2$. In the history of exponential Diophantine equations, the consideration of such triples is the oldest and celebrated problem. Sierpiński treated the case $(a, b, c) = (3, 4, 5)$ and showed that the corresponding equation (1.1) has only the solution $(x, y, z) = (2, 2, 2)$ (see [Si]). Continuing the work of Sierpiński, Jeśmanowicz showed in 1956 that the equation (1.1) has no solution other than $(x, y, z) = (2, 2, 2)$ for each of the cases $(a, b, c) = (5, 12, 13)$, $(7, 24, 25)$, $(9, 40, 41)$ and $(11, 60, 61)$, and he proposed the following (see [Je]).

Conjecture 1.1. *Let (a, b, c) be a primitive Pythagorean triple such that $a^2 + b^2 = c^2$. Then the equation (1.1) has only the solution $(x, y, z) = (2, 2, 2)$.*

2010 Mathematics Subject Classification: primary: 11D61; secondary: 11D41, 11J86

It is well-known that, for any primitive Pythagorean triple (a, b, c) such that $a^2 + b^2 = c^2$ with even b, there exist integers m, n such that

$$a = m^2 - n^2, \qquad b = 2mn, \qquad c = m^2 + n^2,$$

where $m > n > 0$, $\gcd(m, n) = 1$, $m \not\equiv n \pmod 2$. We will always consider the above expressions and the solutions of the equation

$$(m^2 - n^2)^x + (2mn)^y = (m^2 + n^2)^z, \qquad x, y, z \in \mathbb{N}. \tag{1.2}$$

A number of other special cases of Conjecture 1.1 have since been settled. After the work of Jeśmanowicz, Lu proved the conjecture when $n = 1$ (see [Lu]). In 1965, Dem'janenko extended earlier results in several papers ([Ko, Ko2], [Po]) by proving the conjecture to be true whenever $m - n = 1$ (see [De]) . In general, this problem has not yet been solved. For other known results, see [DC], [Le, Le2, Le3, Le4], [Miy], [Ta], [TA, TA2, TA3].

It is crucially important to know divisibility properties of solutions x, y, z, in particular, parities of them. There are some simple conditions to ensure evenness of x, y, z given by [Ca], [DC2] (also see Lemmas 2.1-2.3 below). We denote by α the 2-adic valuation of mn. Then, for the case $\alpha < 3$, we often observe that x, y, z are all even only under assumptions on m, n modulo 8. Most known results on Conjecture 1.1 concern the case $\alpha = 1$. In particular, if $\alpha = 1$ and x, y, z are all even, then it is easily seen that $y = 2$, and the conjecture holds (see [GL]). For example, we know from [Ca] that the case where $m \equiv 1 \pmod 8$ and $n \equiv 6 \pmod 8$ implies $(x, y, z) = (2, 2, 2)$. For the case $\alpha > 1$, see [DC2], [Miy].

In this paper, we give various new results concerning the case $\alpha > 1$. We will use some upper bounds for solutions of exponential equations from Scott [Sc], Mignotte [Mi], and a good upper bound which can be obtained under the assumption that x, y, z are all even.

To state our results, we introduce the following notation which has already been defined by the author in [Miy]. Note that we may assume that $n > 1$ by [Lu]. We define integers $\alpha \geqslant 1, \beta \geqslant 2, e = \pm 1$ and odd integers $i \geqslant 1, j \geqslant 1$ as follows.

$$\begin{aligned} &m = 2^\alpha i, && n = 2^\beta j + e && \text{if } m \text{ is even,} \\ &m = 2^\beta j + e, && n = 2^\alpha i && \text{if } m \text{ is odd.} \end{aligned} \tag{1.3}$$

In what follows, we consider the above forms of m, n. This preparation plays important roles to examine parities of three variables x, y, z.

First, by elementary considerations and an upper bound for exponential variables due to Scott, and Scott and Styer (see [Sc], [SS]), we prove the following.

Theorem 1.2. *Assume that m is even. If $2^{2\alpha-\beta-1} > i(2^\beta j + e)$, then Conjecture 1.1 holds. In particular, if m is a power of 2, then Conjecture 1.1 holds.*

Next, by results on generalized Fermat equations due to Poonen [Poo], Bruin [Br2], Darmon and Merel [DM] (see Lemmas 4.5 and 6.3 below), we prove the following result.

Theorem 1.3. *Assume that* $\alpha \geqslant 5, e = -1$ *and that* $3\alpha \leqslant \beta+1 \leqslant 2^{\alpha-3}$ *or* $\beta < \alpha$. *If* $\log \max(i,j) \leqslant 2^{\alpha-6}$, *then Conjecture 1.1 holds.*

The following result can be regarded as a more or less generalization of the results of Ko [Ko, Ko2], Podsypanin [Po], and Dem'janenko [De] which assert that the conjecture holds when $n+1 = m$. Note that $n+1 = m$ implies that $2\alpha \neq \beta+1$.

Theorem 1.4. *Assume that* $2\alpha \neq \beta+1, e = -1$ *and* $m \geqslant 23n$. *If* $n+1$ *is divisible by* $\prod_{p|m,\ p\neq 2} p$, *where* p *runs over all odd prime factors of* m, *then Conjecture 1.1 holds.*

Finally, using many results on generalized Fermat equations (see Section 6), we prove the main result of this paper.

Theorem 1.5. *Let* (x,y,z) *be a solution of* (1.2). *Assume that* x *and* z *are even. Put* $x = 2X, z = 2Z$ *with* $X, Z \geqslant 1$. *Then*

(i) X *and* Z *are odd.*
(ii) *If* $2\alpha = \beta + 1$, *then* $X = Z = 1$ *and* $y = 2$.

By (ii) in Theorem 1.5, we can generalize our previous result (Theorem 1.5 in [Miy]) as follows.

Corollary 1.6. *Let* m, n *be expressed as* (1.3). *Assume that* $\alpha \geqslant 2$. *Then Conjecture 1.1 holds if* m, n *are expressed as one of the following forms.*

$$\begin{aligned}
&m = 2^\alpha i, && n = 2^{2\alpha-1}j + 1, && \text{where } j \equiv 1 \pmod 4,\\
&m = 2^\alpha i, && n = 2^{2\alpha-1}j - 1, && \text{where } j \equiv -1 \pmod 4,\\
&m = 2^{2\alpha-1}j - 1, && n = 2^\alpha i, && \text{where } j \equiv -1 \pmod 4.
\end{aligned}$$

2. Sufficient conditions for evenness of solutions

It is crucially important to know divisibility properties of solutions for Conjecture 1.1, in particular, parities of them. In this section, we prepare some lemmas to determine parities of solutions. In what follows, let (x,y,z) be a solution of (1.2). Note that the following three lemmas have been used in many papers. For their proofs, see, for example, [Miy].

Lemma 2.1. x *is even if one of the following holds.*

(i) *There exists a divisor* d *of* m *such that* $d \not\equiv 1 \pmod 4$.
(ii) $n \equiv 2 \pmod 4$.

In particular, $mn \equiv 2 \pmod 4$ *implies that* x *is even.*

Lemma 2.2. *Let* d *be a divisor of* $m + n$. *Then*

(i) *If* $d \equiv 7 \pmod 8$, *then* y *is even.*
(ii) *If* $d \equiv 3 \pmod 8$, *then* z *is even.*
(iii) *If* $d \equiv 5 \pmod 8$, *then* $y \equiv z \pmod 2$.

Lemma 2.3. *Let d be a divisor of $m-n$. If $d \equiv \pm 3 \pmod 8$, then $y \equiv z \pmod 2$.*

Next, we give some lemmas expressed by α, β, i, j in (1.3). For the case where m is even, substituting the upper expression in (1.3) into (1.2), we have

$$[2^{2\alpha}i^2 - (2^{2\beta}j^2 + 2^{\beta+1}ej + 1)]^x + 2^{(\alpha+1)y}k = [2^{2\alpha}i^2 + (2^{2\beta}j^2 + 2^{\beta+1}ej + 1)]^z, \quad (2.1)$$

where k is odd. Note that Lemmas 2.4 and 2.5 have essentially been proved in [Miy], but here we obtain more refined results.

Lemma 2.4. *Let (x, y, z) be a solution of (1.2). Then*

(i) *If $\alpha > 1, \alpha \neq \beta$ and $2\alpha \neq \beta + 1$, then $x \equiv z \pmod 2$.*
(ii) *If $2\alpha \neq \beta + 1$ and $y > 1$, then $x \equiv z \pmod 2$.*
(iii) *If $2\alpha = \beta + 1$, then $y > 1$, and x or z is even according to $j \not\equiv e \pmod 4$ or $j \equiv e \pmod 4$.*

Proof. We consider the case where m is even.

(i) Suppose that $x \not\equiv z \pmod 2$. By Lemma 2.1, we may assume that $2 \mid x$ and $2 \nmid z$. Considering (1.2) modulo $2^{2\alpha+1}$, we have

$$\begin{aligned}(2mn)^y &= (m^2+n^2)^z - (m^2-n^2)^x \\ &\equiv zm^2n^{2z-2} + n^{2z} + xm^2n^{2x-2} - n^{2x} \\ &\equiv m^2(zn^{2z-2} + xn^{2x-2}) + n^{2z} - n^{2x} \pmod{2^{2\alpha+1}}.\end{aligned} \quad (2.2)$$

Let ν_2 be the 2-adic valuation and let

$$A = m^2(zn^{2z-2} + xn^{2x-2}), \ B = n^{2z} - n^{2x}.$$

Then the 2-adic valuation of A is

$$\nu_2(A) = \nu_2(m^2) = \nu_2(2^{2\alpha}i^2) = 2\alpha$$

since $zn^{2z-2} + xn^{2x-2}$ is odd. On the other hand, the 2-adic valuation of B is

$$\nu_2(B) = \nu_2(n^{2|x-z|} - 1) = \nu_2(n^2 - 1) = \nu_2(2^{2\beta}j^2 \pm 2^{\beta+1}j) = \beta + 1,$$

where we used the facts that $x \not\equiv z \pmod 2, 2 \nmid n$ and $\beta > 1$. Since we assume that $2\alpha \neq \beta + 1$, we have from (2.2) that

$$\begin{aligned}(\alpha+1)y &= 2\alpha \qquad \text{if } \ 2\alpha < \beta + 1, \\ (\alpha+1)y &= \beta + 1 \qquad \text{if } \ 2\alpha > \beta + 1.\end{aligned}$$

These imply that $\alpha = 1, y = 1$ and $\alpha = \beta, y = 1$, respectively.

(ii) is clear by (i).

(iii) Assume that $2\alpha = \beta + 1$. Note that $\alpha > 1$ and $2\beta = 4\alpha - 2$. Considering (2.1) modulo $2^{4\alpha-2}$, we have

$$[(i^2 - ej)2^{2\alpha} - 1]^x + 2^{(\alpha+1)y}k \equiv [(i^2 + ej)2^{2\alpha} + 1]^z \pmod{2^{4\alpha-2}},$$

so

$$\pm(i^2 - ej)2^{2\alpha}x + f + 2^{(\alpha+1)y}k \equiv (i^2 + ej)2^{2\alpha}z + 1 \pmod{2^{4\alpha-2}},$$

where $f = \pm 1$. In particular, we see from this congruence that $f \equiv 1 \pmod 4$, so $f = 1$. By $\alpha > 1$, we also see that $y > 1$. Hence

$$\pm(i^2 - ej)x + 2^{\alpha(y-2)+y}k \equiv (i^2 + ej)z \pmod{2^{2\alpha-2}}.$$

This implies that

$$\pm(1 - ej)x \equiv (1 + ej)z \pmod 4$$

since $2 \nmid i$. Since j and e are odd, ej is also odd. Hence we have the wanted conclusion.

For the case where m is odd, we reach the wanted conclusion by a similar process. ■

The following is the key to the proof of (ii) in Theorem 1.5.

Lemma 2.5. *Assume that $2\alpha = \beta + 1$. Let (x, y, z) be a solution of (1.2) with even x, z. Put $x = 2X, z = 2Z$ with $X, Z \geqslant 1$. If $y > 3$, then X or Z is even.*

Proof. By (1.2), we have $(2mn)^y = DE$, where $D = (m^2+n^2)^Z+(m^2-n^2)^X, E = (m^2 + n^2)^Z - (m^2 - n^2)^X$. It is easily seen that $\gcd(D, E) = 2$ and $2^{(\alpha+1)y} \parallel DE$. Hence we have for the proper choice of the sign

$$(m^2 + n^2)^Z \pm (m^2 - n^2)^X \equiv 0 \pmod{2^{(\alpha+1)y-1}}.$$

Here we suppose that $y > 3$. Since $(\alpha + 1)y - 1 > 4\alpha - 2$, we have from the above congruence that $(m^2 + n^2)^Z \pm (m^2 - n^2)^X \equiv 0 \pmod{2^{4\alpha-2}}$. As seen in the proof of (iii) in Lemma 2.4, we see that this congruence leads to the wanted conclusion. ■

At the end of this section, we give a sufficient condition on evenness of solutions.

Lemma 2.6. *Assume that $2\alpha \neq \beta + 1$ and $e = -1$. Let (x, y, z) be a solution of (1.2) with $y > 1$. Then x, y, z are all even.*

Proof. Since $e = -1$, we see that $m \not\equiv 1 \pmod 4$. Hence, by Lemma 2.1, x is even. It follows from $2\alpha \neq \beta + 1, y > 1$ and (ii) in Lemma 2.4 that z is even.

Finally, we show that y is even. First assume that $\alpha \geqslant 3$ and $\beta \geqslant 3$, or $\alpha = \beta = 2$. Then we know that $m + n \equiv 7 \pmod 8$. Hence, by Lemma 2.2, y is even. Next, we consider the case $\alpha = 2$ and $\beta \geqslant 3$. Then $m - n \equiv \pm 3 \pmod 8$. Hence y is even by Lemma 2.3. In case $\alpha = 1$, it is easily seen that $m + n \equiv 5 \pmod 8$ or $m - n \equiv \pm 3 \pmod 8$. Therefore, y is even by Lemmas 2.2 and 2.3. ■

3. lower bounds for solutions

In this section, we give some lower bounds for solutions of (1.2) under some assumptions. First, considering the difference between α and β, we obtain the following lower bounds for $x \pm z$. These are used to prove Theorems 1.2 and 1.3.

Lemma 3.1. *Assume that* $3\alpha \leqslant \beta + 1$. *Let* (x, y, z) *be a solution of* (1.2) *with* $y > 2$. *Then* 2^α *divides* $x + z$.

Proof. We consider the case where m is even. Considering (2.1) modulo $2^{\beta+1}$, we have

$$(2^{2\alpha}i^2 - 1)^x + 2^{(\alpha+1)y}k \equiv (2^{2\alpha}i^2 + 1)^z \pmod{2^{\beta+1}}$$

for some odd integer k. Now we suppose that $y > 2$. By $3\alpha \leqslant \beta + 1$, we see from the above congruence that $(2^{2\alpha}i^2 - 1)^x \equiv (2^{2\alpha}i^2 + 1)^z \pmod{2^{3\alpha}}$. This implies that x is even and $-2^{2\alpha}xi^2 \equiv 2^{2\alpha}zi^2 \pmod{2^{3\alpha}}$, so $x + z \equiv 0 \pmod{2^\alpha}$.

For the case where n is even, we reach the wanted conclusion by a similar process. ■

Lemma 3.2. *Assume that* $\beta \leqslant \alpha$. *Let* (x, y, z) *be a solution of* (1.2) *with* $y > 1$. *Then* $2^{2\alpha-\beta}$ *divides* $x - z$.

Proof. We consider the case where m is even. Let (x, y, z) be a solution of (1.2) with $y > 1$. Considering (2.1) modulo $2^{2\beta}$, we have

$$(\mp 2^{\beta+1}j - 1)^x \equiv (\pm 2^{\beta+1}j + 1)^z \pmod{2^{2\beta}}.$$

This implies that x is even and $x \equiv z \pmod{2^{\beta-1}}$. In particular, $x \equiv z \pmod 2$. Considering (1.2) modulo $2^{2\alpha+1}$, we have

$$\begin{aligned} 0 \equiv (2mn)^y &= (m^2 + n^2)^z - (m^2 - n^2)^x \\ &\equiv zm^2n^{2z-2} + n^{2z} + xm^2n^{2x-2} - n^{2x} \\ &\equiv m^2(zn^{2z-2} + xn^{2x-2}) + n^{2z} - n^{2x} \\ &\equiv n^{2z} - n^{2x} \pmod{2^{2\alpha+1}}, \end{aligned} \tag{3.1}$$

where $(zn^{2z-2} + xn^{2x-2}) \equiv z + x \equiv 0 \pmod 2$. By

$$\begin{aligned} \nu_2(n^{2z} - n^{2x}) &= \nu_2(n^{2|z-x|} - 1) \\ &= \nu_2(n^2 - 1) + \nu_2(z - x) = \beta + 1 + \nu_2(z - x), \end{aligned}$$

we have from (3.1) that

$$\begin{aligned} \nu_2(z - x) &= \nu_2(n^{2z} - n^{2x}) - (\beta + 1) \\ &\geqslant 2\alpha + 1 - (\beta + 1) = 2\alpha - \beta. \end{aligned}$$

For the case where m is odd, we reach the wanted conclusion by a similar process. ■

Next, we give a good bound for solutions under the assumption that $n+1$ is divisible by $\prod_{p|m,p\neq 2} p$, where p runs over all odd prime factors of m. It will be used in the proof of Theorem 1.4. For this we use the following elementary fact.

Lemma 3.3. *Let $d > 1$ and let u, v be non-zero relatively prime integers. Let p be a prime factor of $u - v$. If p is odd, or $p = 2$ and 4 divides $u - v$, then*

$$\nu_p(u^d - v^d) = \nu_p(u - v) + \nu_p(d).$$

Proof. For example, see p.11 in [Ri]. ■

Lemma 3.4. *Assume that $e = -1$ and $n+1$ is divisible by $\prod_{p|m,p\neq 2} p$. Let (x, y, z) be a solution of (1.2). Then*

(i) *If $y = 1$, then m divides $(n + 1)(z - x)$.*
(ii) *If z is even, then m^2 divides $(n + 1)(z - x)$.*

Proof. Assume that $e = -1$ and $n + 1$ is divisible by $\prod_{p|m,p\neq 2} p$. Let (x, y, z) be a solution of (1.2). By (i) in Lemma 2.1, x is even. We may assume that $x \neq z$.

(i) Suppose that $y = 1$. It is clear from (1.2) that z is odd. Let p be an odd prime factor of m such that $p^{\alpha_p} \parallel m$ with $\alpha_p \geqslant 1$. Then, by our assumption,

$$n + 1 \equiv 0 \pmod{p}. \tag{3.2}$$

On the other hand, we see from (1.2) that

$$A \equiv 0 \pmod{p^{\alpha_p}}, \tag{3.3}$$

where $A = n^{2z} - n^{2x}$. We want to know the p-adic valuation of A. By $\gcd(m, n) = 1$, p does not divide n. Hence

$$\nu_p(A) = \nu_p(n^{2|z-x|} - 1). \tag{3.4}$$

Note that $\nu_p(A) > 0$. Then, by $p \neq 2$ and (3.4), p must divide only either $n^{|z-x|} + 1$ or $n^{|z-x|} - 1$. It follows from $x \not\equiv z \pmod 2$ and (3.2) that p divides $n^{|z-x|} + 1$. Then, by (3.2) and Lemma 3.3, we have

$$\nu_p(A) = \nu_p(n^{|z-x|} + 1) = \beta_p + \gamma_p, \tag{3.5}$$

where $\beta_p = \nu_p(n + 1)$ and $\gamma_p = \nu_p(|z - x|)$. It follows from (3.3) and (3.5) that $\alpha_p \leqslant \beta_p + \gamma_p$. So, since p is any odd prime factor of m, we have

$$(n + 1)(z - x) \equiv 0 \pmod{\prod_{p|m,\ p\neq 2} p^{\alpha_p}}. \tag{3.6}$$

For the wanted conclusion, it remains to consider the case where m is even. We know that $2^\alpha \parallel m$. Since $e = -1$, we see that $n+1 \equiv 0 \pmod 4$. Hence, by Lemma 3.3 and as the previous arguments, we can observe that 2^α divides $(n+1)(z-x)$. It follows from (3.6) that m divides $(n+1)(z-x)$.

(ii) Assume that z is even. So $x-z$ is even. Note that $y>1$. Let γ_0 be the 2-adic valuation of $x-z$. Considering (1.2) modulo m^2, we have $n^{2x}\equiv n^{2z} \pmod{m^2}$, so $n^{2|z-x|}\equiv 1 \pmod{m^2}$ by $\gcd(m,n)=1$. Then

$$\begin{aligned} n^{2|z-x|}-1 &= (n^{|z-x|}+1)(n^{|z-x|}-1) \\ &= (n^{|z-x|}+1)(n^{\frac{|z-x|}{2}}+1)(n^{\frac{|z-x|}{2}}-1) \\ &= (n^{|z-x|}+1)(n^{\frac{|z-x|}{2}}+1)\cdots(n^{\frac{|z-x|}{2^{\gamma_0}}}+1)(n^{\frac{|z-x|}{2^{\gamma_0}}}-1) \\ &\equiv 0 \pmod{m^2}. \end{aligned}$$

From this we see that, for any odd prime factor p of m such that $p^{\alpha_p} \parallel m$ with $\alpha_p \geqslant 1$, $p^{2\alpha_p}$ divides $n^{\frac{|z-x|}{2^{\gamma_0}}}+1$ since $p \mid n+1$. Thus, by Lemma 3.3, we have

$$2\alpha \leqslant \nu_p(n^{\frac{|z-x|}{2^{\gamma_0}}}+1) = \nu_p(n+1)+\nu_p\left(\frac{|z-x|}{2^{\gamma_0}}\right) = \nu_p(n+1)+\nu_p(z-x).$$

For the wanted conclusion, it remains to consider the case where m is even. By $n+1\equiv 0 \pmod 4$, (3.1) and Lemma 3.3, we have

$$\begin{aligned} 2\alpha+1 &\leqslant \nu_2(n^{2|z-x|}-1) \\ &= \nu_2((n^{|z-x|}+1)(n^{\frac{|z-x|}{2}}+1)\cdots(n^{\frac{|z-x|}{2^{\gamma_0}}}+1)(n^{\frac{|z-x|}{2^{\gamma_0}}}-1)) \\ &= (\gamma_0+1)+\nu_2(n^{\frac{|z-x|}{2^{\gamma_0}}}+1) = \nu_2(z-x)+1+\nu_2(n+1). \end{aligned}$$

Therefore, $\nu_2(m^2) = 2\alpha \leqslant \nu_2(z-x)+\nu_2(n+1)$. Hence m^2 divides $(n+1)(z-x)$.

This completes the proof. ■

4. Upper bounds for solutions

In this section, we give some upper bounds for solutions of (1.2). These are used to prove Theorems 1.2-1.4. Let (x,y,z) be a solution of (1.2). First, assuming that x and z are even, we obtain a good upper bound for z. For this purpose, we use the following result due to Scott and Styer [SS]. It is based on Theorem 1.2 in [Sc], which was surprisingly proved only by an elementary argument on imaginary quadratic fields. Combining it with the class number formula, Scott and Styer deduced the following (see Theorem 3 in [SS]).

Lemma 4.1. *Let r be any odd positive integer, let A and B be relatively prime integers greater than 1, let PQ be the largest square-free divisor of AB, with P and Q chosen so that $(AB/P)^{1/2}$ is an integer. Then if there exists a positive integer Z such that*

$$A+B=r^Z,$$

we must have

$$Z < \frac{1}{2} Q P^{1/2} \log P$$

for $P \geqslant 3$ *and*

$$Z \leqslant \begin{cases} Q/2 & \text{when } P = 1, \\ (Q+1)/2 & \text{when } P = 2. \end{cases}$$

By this lemma, we show the following.

Lemma 4.2. *Let* (x, y, z) *be a solution of* (1.2) *with even* x, z. *Then*

$$z < \prod_{p \mid mn} p,$$

where p *runs over all prime factors of* mn.

Proof. Put $x = 2X, z = 2Z$ with $X, Z \geqslant 1$. Then, by (1.2), we have

$$(2mn)^y = DE, \tag{4.1}$$

where

$$D = (m^2+n^2)^Z + (m^2-n^2)^X, \ E = (m^2+n^2)^Z - (m^2-n^2)^X. \tag{4.2}$$

By $\gcd(D, E) = 2, 2^{(\alpha+1)y} \parallel DE$, (4.1) and (4.2), we have

$$\begin{aligned} &D = 2^{(\alpha+1)y-1} d^y, \ E = 2e^y \\ \text{or} \quad &E = 2^{(\alpha+1)y-1} d^y, \ D = 2e^y, \end{aligned} \tag{4.3}$$

where d and e are relatively prime odd positive integers such that

$$2^{\alpha+1} de = 2mn. \tag{4.4}$$

By (4.2) and (4.3), we have

$$2^{(\alpha+1)y-2} d^y + e^y = (m^2+n^2)^Z. \tag{4.5}$$

Applying Lemma 4.1 to (4.5), we see that

$$Z < \frac{1}{2} PQ, \tag{4.6}$$

where P, Q are positive integers such that PQ is the product of all prime factors of $2de$. Because of (4.4), PQ is the product of all prime factors of $2mn$, which coincides with $\prod_{p \mid mn} p$. So it follows from (4.6) that our assertion holds. ■

Next, we obtain a good upper bound for x by fixing y. For this we quote a result on lower bound for linear forms in the logarithms of two algebraic numbers due to Mignotte. The following is an immediate consequence of the corollary to Theorem 2 in [Mi] (also see [LMN]).

Lemma 4.3. *Consider the linear form*

$$\Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1,$$

where $b_1, b_2, \alpha_1 > 1, \alpha_2 > 1$ are positive integers. Let ρ, λ, a_1, a_2 be positive real numbers with $\rho \geqslant 4, \lambda = \log \rho$,

$$a_i \geqslant (\rho + 1) \log \alpha_i \quad (1 \leqslant i \leqslant 2)$$

and

$$a_1 a_2 \geqslant \max\{20, 4\lambda^2\}.$$

Further assume that h is a real number with

$$h \geqslant \max\left\{ 3.5, 1.5\lambda, \log\left(\frac{b_1}{a_2} + \frac{b_2}{a_1}\right) + \log\lambda + 1.4 \right\},$$

and put

$$\chi = \frac{h}{\lambda}, \qquad v = 4\chi + 4 + \frac{1}{\chi}.$$

If $\Lambda \neq 0$, then we may conclude that

$$\log|\Lambda| \geqslant -(C_0 + 0.06)(\lambda + h)^2 a_1 a_2,$$

where

$$C_0 = \frac{1}{\lambda^3}\left\{\left(2 + \frac{1}{2\chi(\chi+1)}\right)\left(\frac{1}{3} + \sqrt{\frac{1}{9} + \frac{4\lambda}{3v}\left(\frac{1}{a_1} + \frac{1}{a_2}\right) + \frac{32\sqrt{2}(1+\chi)^{3/2}}{3v^2\sqrt{a_1 a_2}}}\right)\right\}^2.$$

By this lemma, we show the following.

Lemma 4.4. *Let (x, y, z) be a solution of (1.2) with $y = 1$. Then we have an upper bound*

$$x < 4020 \log(m^2 + n^2).$$

Proof. The proof proceeds as Lemma 3 in [CD2]. Now we assume that

$$a^x + b = c^z, \tag{4.7}$$

where $a = m^2 - n^2, b = 2mn$ and $c = m^2 + n^2$. Put $\Lambda = z \log c - x \log a$. Then $\Lambda > 0$. First, we give a trivial upper bound for $\log \lambda$. By (4.7), we have

$$z \log c = \log(a^x + b) = x \log a + \log\left(1 + \frac{b}{a^x}\right) < x \log a + \frac{b}{a^x}.$$

Then

$$\log \Lambda < \log b - x \log a. \tag{4.8}$$

Next, applying Lemma 4.3 to Λ, we obtain a lower bound for $\log \Lambda$. In the notation of Lemma 4.3, we put $b_1 = x, b_2 = z, \alpha_1 = a, \alpha_2 = c$. We may take $a_1 = (\rho+1) \log a$

and $a_2 = (\rho+1)\log c$. Choosing $\rho = 4.69$, we see that $a_1 a_2 \geqslant \max\{20, 4\lambda^2\}$. We can let

$$h = \max\left\{ 3.5, \log\left(\frac{x}{\log c} + \frac{z}{\log a}\right) + u \right\},$$

where $u = 1.8353$. It is easily seen from (4.7) that

$$\frac{x}{\log c} < \frac{z}{\log a} < \frac{x+1}{\log c}. \tag{4.9}$$

We will treat the two possible choices for h in turn. If $h = 3.5$, then $\log(x/\log c + z/\log a) \leqslant 3.5 - u < 1.8$. Then, by (4.9), we have

$$\frac{2x}{\log c} < \frac{x}{\log c} + \frac{z}{\log a} < e^{1.8} = 6.049\cdots.$$

So our assertion holds. Next suppose that

$$h = \log\left(\frac{x}{\log c} + \frac{z}{\log a}\right) + u \geqslant 3.5.$$

We will find an upper bound for C_0. It is clear that $1/a_1 + 1/a_2$ and $1/(a_1 a_2)$ are both maximal in the case $(a, c) = (3, 5)$. From $\chi \geqslant 3.5/\lambda$ and $v/4 > 1 + \chi$ in Lemma 4.3, we have

$$\frac{1}{2\chi(\chi+1)} \leqslant \frac{\lambda}{\frac{24.5}{\lambda} + 7}$$

and

$$\begin{aligned}
\frac{4\lambda}{3v}\left(\frac{1}{a_1} + \frac{1}{a_2}\right) + \frac{32\sqrt{2}(1+\chi)^{3/2}}{3v^2\sqrt{a_1 a_2}} &< \frac{4\lambda}{3v}\left(\frac{1}{a_1} + \frac{1}{a_2}\right) + \frac{32\sqrt{2}(v/4)^{3/2}}{3v^2\sqrt{a_1 a_2}} \\
&= \frac{4\lambda}{3v}\left(\frac{1}{a_1} + \frac{1}{a_2}\right) + \frac{4\sqrt{2}}{3\sqrt{v a_1 a_2}} \\
&< \frac{\lambda}{3(\chi+1)(\rho+1)}\left(\frac{1}{\log 3} + \frac{1}{\log 5}\right) \\
&\quad + \frac{2\sqrt{2}}{3(\rho+1)\sqrt{(\chi+1)\log 3 \log 5}} \\
&< \frac{\lambda}{3(\frac{3.5}{\lambda}+1)(\rho+1)}\left(\frac{1}{\log 3} + \frac{1}{\log 5}\right) \\
&\quad + \frac{2\sqrt{2}}{3(\rho+1)\sqrt{(\frac{3.5}{\lambda}+1)\log 3 \log 5}}.
\end{aligned}$$

Thus $C_0 < 0.7507\cdots$. Then, using Lemma 4.3, we have

$$\log \Lambda > -26.25(h+\lambda)^2 \log a \log c. \tag{4.10}$$

Combining (4.8) with (4.10), we find

$$\frac{x}{\log c} < \frac{\log b}{\log a \log c} + 26.25(h+\lambda)^2. \tag{4.11}$$

We see from (4.9) that

$$h = \log\left(\frac{x}{\log c} + \frac{z}{\log a}\right) + u < \log\left(2t + \frac{1}{\log c}\right) + u, \tag{4.12}$$

where $t = x/\log c$. Since $c \geqslant 5, c \geqslant b$ and $a \geqslant 3$, it follows from (4.11) and (4.12) that

$$t < \frac{1}{\log 3} + 26.25\left(\log\left(2t + \frac{1}{\log 5}\right) + u + \lambda\right)^2.$$

This implies that $t < 4020$. This completes the proof of Lemma 4.4. ■

Finally, assuming that x, y, z are all even, we obtain a good upper bound for y, which is as strong as Lemma 4.4. To obtain it, we will use the following result on generalized Fermat equations.

Lemma 4.5 ([CD2] Lemma 10). *Suppose that $N \in \mathbb{N}$ with $N > 1$. Then the equation*

$$X^{2N} + Y^4 = Z^2, \qquad \gcd(X, Y) = 1, \qquad XYZ \neq 0$$

has no integral solution.

By this lemma, we show the following.

Lemma 4.6. *Let (x, y, z) be a solution of (1.2). If x, y, z are even, then*

$$y \leqslant \frac{4\log m}{(\alpha+1)\log 2}.$$

In particular, $y \leqslant 2\log m/\log 2$.

Proof. By our assumption, we can put $x = 2X, y = 2Y, z = 2Z$ with $X, Y, Z \geqslant 1$. Since $\{(m^2-n^2)^X, (2mn)^Y, (m^2+n^2)^Z\}$ forms a primitive Pythagorean triple, there exist integers s, t such that

$$(m^2-n^2)^X = s^2 - t^2, \tag{4.13}$$

$$(2mn)^Y = 2st, \tag{4.14}$$

$$(m^2+n^2)^Z = s^2 + t^2, \tag{4.15}$$

where $s > t > 0, \gcd(s,t) = 1, s \not\equiv t \pmod 2$. Using $s^2 + t^2 < (s^2-t^2)^2$ and $s^2 + t^2 < (2st)^2$, we see from (4.13)-(4.15) that

$$|X - Z| < Z < 2Y. \tag{4.16}$$

Since $s+t, s-t$ are relatively prime, by (4.13), we have

$$s+t=u^X, \qquad s-t=v^X, \tag{4.17}$$

where $u>v>0, \gcd(u,v)=1, uv=m^2-n^2$. Note that u,v are odd since m^2-n^2 is odd. Since $2^\alpha \parallel mn$, we have

$$2^{(\alpha+1)Y} \parallel (2mn)^Y = 2st. \tag{4.18}$$

As in [Miy] we conclude from Lemma 4.5 that if X is even, then $Y=1$, hence $X=Z=1$ in view of (4.16), which contradicts $2 \mid X$. Thus

$$2 \nmid X. \tag{4.19}$$

We see from (4.13) and (4.19) that $m^2-n^2 \equiv s^2-t^2 \pmod 4$. Hence $m \equiv s \pmod 2$ and $n \equiv t \pmod 2$. Now we assume that m and s are even. By (4.18), we see that $2s$ is exactly divisible by $2^{(\alpha+1)Y}$. Then, by (4.17), we have

$$2s = u^X + v^X = (u+v)w,$$

where $w = u^{X-1} - u^{X-2}v + \cdots + v^{X-1}$. Since u, v, X are odd, w is odd. It follows that $2^{(\alpha+1)Y}$ divides $u+v$. In particular,

$$2^{(\alpha+1)Y} \leqslant u+v \leqslant uv+1 = m^2-n^2+1 \leqslant m^2.$$

Hence the wanted conclusion holds. For the case where m is odd, we reach the wanted conclusion by a similar process. This completes the proof of Lemma 4.6. ■

5. Proofs of Theorems 1.2, 1.3 and 1.4

Proof of Theorem 1.2. Since m is even, we know from (1.3) that $m=2^\alpha i$ and $n=2^\beta j+e$. We assume that

$$2^{2\alpha-\beta-1} > i(2^\beta j+e). \tag{5.1}$$

Since $m>n$, we see from (5.1) that $\alpha>\beta$ and $2\alpha \neq \beta+1$. So, by Lemmas 2.1 and 2.4, we see that x and z are even. Then $y>1$, so we have

$$x \equiv z \pmod{2^{2\alpha-\beta}} \tag{5.2}$$

by Lemma 3.2. Put $x=2X, z=2Z$ with $X, Z \geqslant 1$. We can use the notations (4.1) and (4.2). Then, by Lemma 4.2, we have an upper bound

$$Z < \prod_{p \mid mn,\ p \neq 2} p = \prod_{p \mid i(2^\beta j+e)} p \leqslant i(2^\beta j+e). \tag{5.3}$$

Combining (5.2) and (5.3), we see that if $x \neq z$, then

$$2^{2\alpha-\beta-1} \leqslant |X-Z| < Z < i(2^\beta j+e), \tag{5.4}$$

where we used the fact that $X < 2Z$ (this is immediate from $E > 0$ in (4.2)). This contradicts (5.1). Hence $x = z$. If X is even, then we observe from (4.2) that $mn \mid E, \gcd(D, E) = 2, (2mn)^y = DE, D \equiv 2 \pmod 4$, and these imply that $D = 2$. But this is clearly absurd. Thus X is odd. Then, by (4.2), we can put $D = 2m^2F$ and $E = 2n^2G$, where F and G are integers. Further, we see from $2 \mid m, 2 \nmid X$ and Lemma 3.3 that

$$F = \frac{(m^2+n^2)^X + (m^2-n^2)^X}{2m^2} = \frac{(m^2+n^2)^X - (-m^2+n^2)^X}{(m^2+n^2)-(-m^2+n^2)}$$

is odd, and G is also odd since $\gcd(D, E) = 2$. Therefore, we obtain $\nu_2(DE) = \nu_2(4m^2n^2) = 2\nu_2(2mn)$. This gives that $y = 2$ since $DE = (2mn)^y$. Then $X = Z = 1$ by (4.16).

Finally, if m is a power of 2, then (5.1) is equivalent to $2^{2\alpha-\beta-1} > 2^\beta j + e$. This inequality always holds since $2^{2\alpha-\beta-1} \geqslant 2^\alpha = m > n = 2^\beta j + e$. This completes the proof of Theorem 1.2. ∎

To prove Theorem 1.3, we show the following.

Lemma 5.1. *Assume that m is even and that m, n are expressed as* (1.3) *with $\alpha \geqslant 3, e = -1$. Then Conjecture 1.1 holds if one of the following holds.*

(i) $3\alpha \leqslant \beta + 1$ *and* $(1/3)2^{\alpha-3}(\alpha+1)\log 2 > \alpha \log 2 + \log i$.
(ii) $\beta \leqslant \alpha$ *and* $2^{2\alpha-\beta-3}(\alpha+1)\log 2 > \alpha \log 2 + \log i$.

Proof. Let (x, y, z) be a solution of (1.2). First we show that x, y, z are all even. Since $e = -1$, x is even. Note that $2\alpha \neq \beta + 1$ holds under the conditions (i) or (ii). We know that $\alpha \geqslant 3$. Then $m - n \equiv 5 \pmod 8$ or $m + n \equiv 7 \pmod 8$ according to $\beta = 2$ or $\beta \geqslant 3$. By Lemmas 2.2 and 2.3, we see that $y \equiv z \pmod 2$ or y is even according to $\beta = 2$ or $\beta \geqslant 3$. So, to prove $y > 1$, it suffices to consider the case $\beta = 2$. Then, since $\alpha \geqslant 3$, we know that $\alpha \neq \beta$. Thus $x \equiv z \pmod 2$ by (i) in Lemma 2.4. Then z is even. Hence, $y > 1$. Since $2\alpha \neq \beta + 1, e = -1$ and $y > 1$, we see from Lemma 2.6 that x, y, z are all even.

(i) We see from Lemmas 3.1, 4.6 and by (4.16) that if $y > 2$, then

$$2^\alpha \leqslant x + z < 6y \leqslant \frac{24 \log m}{(\alpha+1)\log 2} = \frac{24(\alpha \log 2 + \log i)}{(\alpha+1)\log 2}.$$

Hence, by our assumption, y has to be 2. This leads to $x = z = 2$ by (4.16). So our assertion holds.

(ii) We see from Lemmas 3.2, 4.6 and by (4.18) that if $x \neq z$, then

$$2^{2\alpha-\beta} \leqslant |x - z| < 2y \leqslant \frac{8(\alpha \log 2 + \log i)}{(\alpha+1)\log 2}.$$

Hence, by our assumption, $x = z$. This leads to $x = y = z = 2$ as seen in the proof of Theorem 1.2. So our assertion holds. ∎

By a similar process, we can prove the following.

Lemma 5.2. *Assume that m is odd and that m, n are expressed as* (1.3) *with $\alpha \geqslant 3, e = -1$. Then Conjecture 1.1 holds if one of the following holds.*

(i) $3\alpha \leqslant \beta + 1$ *and* $(1/3)2^{\alpha-3}(\alpha+1)\log 2 > \beta \log 2 + \log j$.
(ii) $\beta \leqslant \alpha$ *and* $2^{2\alpha-\beta-3}(\alpha+1)\log 2 > \beta \log 2 + \log j$.

We are now ready to prove Theorem 1.3.

Proof of Theorem 1.3. Assume that $\alpha \geqslant 5, e = -1$ and

$$\log \max(i, j) \leqslant 2^{\alpha-6}. \tag{5.5}$$

We distinguish the cases where m is even or m is odd. Assume that $3\alpha \leqslant \beta + 1 \leqslant 2^{\alpha-3}$ or $\beta < \alpha$.

First, we consider the case where m is even. By (5.5), we have

$$\begin{aligned}(1/3)2^{\alpha-3}(\alpha+1)\log 2 &= (2^{\alpha-3}/3)\alpha \log 2 + (2^{\alpha-3}/3)\log 2 \\ &> \alpha \log 2 + \log i.\end{aligned}$$

Hence (i) holds in Lemma 5.1. If $\beta \leqslant \alpha$, then $2^{2\alpha-\beta-2} \geqslant 2^{\alpha-2} > (1/3)2^{\alpha-3}$. So (ii) also holds. Then, by Lemma 5.1, the theorem holds.

Next, we consider the case where m is odd. By (5.5), we see that if $3\alpha \leqslant \beta + 1 \leqslant 2^{\alpha-3}$, then

$$\begin{aligned}(1/3)2^{\alpha-3}(\alpha+1)\log 2 &\geqslant 2^{\alpha-2}\log 2 \\ &> 2^{\alpha-3} + 2^{\alpha-6} \\ &> \beta \log 2 + \log j,\end{aligned}$$

and that if $\beta \leqslant \alpha$, then

$$\begin{aligned}2^{2\alpha-\beta-3}(\alpha+1)\log 2 &\geqslant 2^{\alpha-4}(\alpha+1) \\ &= 2^{\alpha-4}\alpha + 2^{\alpha-4} \\ &> \beta \log 2 + \log j.\end{aligned}$$

The application of Lemma 5.2 completes the proof of Theorem 1.3. ■

Example 5.3. We give examples of Theorem 1.3. Let $\alpha \geqslant 7, \alpha > \beta \geqslant 2, i = 3$ and $j \in \{1, 3\}$. By Theorem 1.3, if m, n are relatively prime positive integers and expressed as the following form $m = 2^\alpha 3, n = 2^\beta j - 1$, then Conjecture 1.1 holds. For example, if $\alpha = 7$, then

$$m = 384,\ n \in \{7, 11, 23, 31, 47, 95, 191\}.$$

Let $\alpha \geqslant 9, 3\alpha \leqslant \beta + 1 \leqslant 2^{\alpha-3}$ and $i, j \in \{1, 3, 5, \ldots, [e^{2^{\alpha-6}}]\}$. By Theorem 1.3, if m, n are relatively prime positive integers and expressed as the following forms $m = 2^\beta - 1, n = 2^\alpha$, then Conjecture 1.1 holds. For example, we can take $\alpha = 9$ and $26 \leqslant \beta \leqslant 63$.

Proof of Theorem 1.4. Assume that $2\alpha \neq \beta + 1, e = -1, m \geqslant 23n$, and that $n+1$ is divisible by $\prod_{p|m,\ p\neq 2} p$. Let (x, y, z) be a solution of (1.2). We first show that $y > 1$. Suppose that $y = 1$. It is clear from (1.2) that $x > z$. Then, by (i) in Lemma 3.4, we have

$$m \leqslant (n+1)(x-z). \tag{5.6}$$

Since $(m^2 - n^2)^x < (m^2 + n^2)^z$, we have

$$\frac{x \log(m^2 - n^2)}{\log(m^2 + n^2)} < z. \tag{5.7}$$

This viewpoint is crucial in the proof. On the other hand, by Lemma 4.4, we know that

$$x < 4020 \log(m^2 + n^2). \tag{5.8}$$

Combining (5.6)-(5.8), we obtain

$$\begin{aligned} m &\leqslant (n+1)(x-z) \\ &< (n+1)x \left(1 - \frac{\log(m^2-n^2)}{\log(m^2+n^2)}\right) < 4020(n+1) \log\left(\frac{m^2+n^2}{m^2-n^2}\right). \end{aligned}$$

Since we may assume that $n > 1$, this gives

$$t < 4020 \left(\frac{n+1}{n}\right) \log\left(\frac{t^2+1}{t^2-1}\right) \leqslant 6030 \log\left(\frac{t^2+1}{t^2-1}\right),$$

where $t = m/n > 1$. This implies that $t < 23$, which contradicts $m \geqslant 23n$. Therefore, $y > 1$. Thus x, y, z are all even by Lemma 2.6, so, by Lemma 4.6, we have an upper bound

$$y \leqslant \frac{2 \log m}{\log 2}. \tag{5.9}$$

On the other hand, by (ii) in Lemma 3.4, we have a lower bound

$$m^2 \leqslant (n+1)|z - x| \tag{5.10}$$

if $x \neq z$. It follows from (4.16), (5.9) and (5.10) that if $x \neq z$, then

$$m^2 \leqslant (n+1)|z-x| < 2(n+1)y \leqslant \frac{4(n+1)\log m}{\log 2}.$$

It follows that

$$m \leqslant \frac{m^2}{n+1} \leqslant \frac{4 \log m}{\log 2}.$$

since $m > n$. This gives that $m \leqslant 16$, which contradicts $m \geqslant 23n \geqslant 23$. Thus $x = z$. This leads to $x = y = z = 2$ as seen before, and we complete the proof of Theorem 1.4. ∎

6. Generalized Fermat equations

Let A, B, C, p, q, r be integers such that $ABC \neq 0, \gcd(A, B, C) = 1$ and $p, q, r \geqslant 2$. Then the equation

$$AX^p + BY^q = CZ^r,$$
$$X, Y, Z \in \mathbb{Z}, \qquad \gcd(X, Y, Z) = 1, \qquad XYZ \neq 0$$

is called a *generalized Fermat equation*. As we know, the case where $A = B = C = 1$ and $p = q = r = n \geqslant 3$ corresponds to Fermat's last theorem. In this case, Wiles proved that the equation has no solution. After his work, the next interest moved to the above general equations. In these 15 years many authors have treated these equations and obtained results. Most of their methods are based on Wiles's method, or more sophisticated arguments in the theory of elliptic curves and modular forms (see, for example, [Be], [DG]).

In this section, we quote many results on generalized Fermat equations. They play prominent roles in our proof of Theorem 1.5. Mainly, they will be used to determine divisibility properties of exponential variables.

Lemma 6.1 ([DM]). *Let $l \geqslant 3$. Then the equation*

$$X^l + Y^l = 2Z^l, \qquad \gcd(X, Y) = 1, \qquad XYZ \neq 0, \pm 1$$

has no integral solution.

By using the results due to Poonen [Poo], Darmon and Merel [DM], Cao [Ca2] has shown the following (also see [Da]).

Lemma 6.2 ([Ca2], [Da]). *Let p be an odd prime number. Then the equation*

$$X^4 - Y^4 = Z^p, \qquad \gcd(X, Y) = 1, \qquad XYZ \neq 0$$

has no integral solution.

The following lemma is given by Cao and Dong in [CD]. It is based on the results due to Bruin [Br2], Poonen [Poo], Darmon and Merel [DM].

Lemma 6.3 ([CD] Theorem 3). *Suppose that $N \in \mathbb{N}$ with $N > 1$. Then the equation*

$$X^{2N} + Y^2 = Z^4, \qquad \gcd(X, Y) = 1, \qquad XYZ \neq 0,\ 2 \mid X$$

has no integral solution.

By using Chabauty method, Bruin [Br, Br2] established the following results.

Lemma 6.4 ([Br]). *The equation*

$$X^3 + Y^3 = Z^4, \qquad \gcd(X, Y) = 1, \qquad XYZ \neq 0$$

has no integral solution.

Lemma 6.5 ([Br2] Theorem 1.2). *The equation*

$$X^2 - Y^4 = Z^5, \qquad \gcd(X, Y) = 1, \qquad XYZ \neq 0$$

has no integral solution other than $(X, Y, Z) = (\pm 122, \pm 11, 3), (\pm 7, \pm 3, -2)$.

The following is essentially given by Zagier. We can also refer to [Ed]. Here we use the following formulation.

Lemma 6.6 ([Co] pp.474–475). *All the integral solutions of*

$$X^4 + Y^3 = Z^2, \qquad \gcd(X, Y) = 1, \qquad XYZ \neq 0$$

are given by the following parameterizations (s *and* t *are non-zero relatively prime integers):*

$$\begin{cases} X = \pm(s^2 - 2ts - t^2)(7s^4 + 20ts^3 + 24t^2s^2 8t^3 s + 4t^4), \\ Y = (s^2 + 2t^2)(s^2 + 4ts - 2t^2)(3s^2 + 4ts + 2t^2)(5s^2 + 8ts + 2t^2), \\ Z = 4s(s + 2t)(s^2 + ts + t^2)(s^4 + 4ts^3 + 16t^2s^2 + 24t^3 s + 12t^4) \\ \qquad \times(19s^4 - 4ts^3 + 8t^3 + 4t^2), \end{cases}$$

where s *is odd and* $s \not\equiv t \pmod 3$,

$$\begin{cases} X = \pm(3s^2 - t^2)(9s^4 + 18s^2t^2 + t^4), \\ Y = (9s^4 + 2s^2t^2 + t^4)(9s^4 - 30s^2t^2 + t^4), \\ Z = 4st(3s^2 + t^2)(3t^4 - 2s^2t^2 + 3s^4)(81s^4 - 6s^2t^2 + t^4), \end{cases}$$

where $s \not\equiv t \pmod 2$ *and* $3 \nmid s$,

$$\begin{cases} X = 6st(3s^4 + 4t^4), \\ Y = 9s^8 - 168s^4t^4 + 16t^8, \\ Z = \pm(3s^4 - 4t^4)(9s^8 + 408s^4t^4 + 16t^8), \end{cases}$$

where s *is odd and* $3 \nmid t$,

$$\begin{cases} X = 6st(12s^4 + t^4), \\ Y = 144s^8 - 168s^4t^4 + t^8, \\ Z = \pm(12s^4 - t^4)(144s^8 + 408s^4t^4 + t^8), \end{cases}$$

where t *is odd and* $3 \nmid t$,

$$\begin{cases} X = \pm(s^6 + 40s^3t^3 - 32t^6), \\ Y = -8st(s^3 - 16t^3)(s^3 + 2t^3), \\ Z = s^{12} - 176s^9t^3 - 5632s^3t^9 - 1024t^{12}, \end{cases}$$

where s *is odd and* $s \not\equiv t \pmod 3$,

$$\begin{cases} X = \pm(9s^6 + 18s^5t + 45s^4t^2 + 60s^3t^3 + 15s^2t^4 - 6st^5 - 5t^6), \\ Y = -2(3s^4 - 6s^2t^2 - 8st^3 - t^4)(3s^4 + 12s^3t + 6s^2t^2 + 4st^3 + 3t^4), \\ Z = \pm(-27s^{12} + 324s^{11}t + 1782s^{10}t^2 + 3564s^9t^3 \\ \quad +3267s^8t^4 + 2376s^7t^5 + 2772s^6t^6 + 3960s^5t^7 \\ \quad +4059s^4t^8 + 2420s^3t^9 + 726s^2t^{10} + 156st^{11} + 29t^{12}), \end{cases}$$

where $s \not\equiv t \pmod 2$ *and* $3 \nmid t$,

$$\begin{cases} X = \pm(17s^6 + 30s^5t - 15s^4t^2 + 20s^3t^3 + 15s^2t^4 + 6st^5 - t^6), \\ Y = 2(3s^4 - 8s^3t - 6s^2t^2 - t^4)(7s^4 + 4s^3t + 6s^2t^2 - 4st^3 - t^4), \\ Z = \pm(397s^{12} - 156s^{11}t + 2046s^{10}t^2 - 1188s^9t^3 \\ \quad -1485s^8t^4 + 2376s^7t^5 - 924s^6t^6 + 792s^5t^7 \\ \quad +99s^4t^8 - 44s^3t^9 - 66s^2t^{10} + 12st^{11} - 3t^{12}), \end{cases}$$

where $s \not\equiv t \pmod 2$ *and* $s \not\equiv t \pmod 3$.

The following lemma is a consequence of Theorem 1.2 in [BS], which is based on the theory of Galois representations and modular forms.

Lemma 6.7 ([BS] Theorem 1.2). *Suppose that* $n \geqslant 7$ *is prime. Then the equation*

$$X^n + 2^\alpha Y^n = Z^2$$

has no solution in nonzero pair-wise co-prime integers (X, Y, Z) *with* $XY \neq 1$ *and* $\alpha \geqslant 2$.

7. Proof of Theorem 1.5

Proof of Theorem 1.5. Let (x, y, z) be a solution of (1.2) with even x, z. Put $x = 2X, z = 2Z$ with $X, Z \geqslant 1$.

(i) We use the notation (4.1)-(4.3).
First, we consider the case $1 \leqslant y \leqslant 2$. Note that $D \geqslant 2m^2 > 2mn$, hence $y > 1$. If $y = 2$, then $X = Z = 1$ by (4.16).
Next, we will show that the case $y = 3$ does not hold. Suppose that $y = 3$. Then we see from (4.1) and (4.2) that

$$(2mn)^3 = DE \geqslant (m^2 + n^2)^Z,$$

so $Z < 3$. Further, since $c^2 = a^2 + b^2 < a^{2X} + b^3 = c^{2Z}$, we must have $Z = 2$. So we see from $X < 2Z = 4$ (which follows from (4.2) and $E > 0$), Lemmas 6.2 and 6.4 that $X = 1$. But this yields $a^2 + b^3 = c^4 = (a^2 + b^2)^2 > a^4 + b^4$, which is absurd.

Finally, we consider the case $y > 3$. Suppose that X or Z is even. We will reach a contradiction. By Lemmas 4.5 and 6.3, we see that y must be odd. We consider the case where X is even. By Lemma 6.2, we see that Z is odd. Then, by (4.2), (4.3) and $2 \nmid y$, we have

$$(-e)^y + 2^{(\alpha+1)y-2}d^y = ((m^2-n^2)^{X/2})^2$$

or

$$e^y + 2^{(\alpha+1)y-2}(-d)^y = ((m^2-n^2)^{X/2})^2.$$

Hence we see from Lemma 6.7 and $(\alpha+1)y - 2 \geqslant 2y - 2 \geqslant 2$ that y must be of the form $y = 3^\delta 5^\gamma$, where δ and γ are non-negative integers with $(\delta, \gamma) \neq (0, 0)$. Then we have a solution of the equation

$$A^4 + B^{3^\delta 5^\gamma} = C^2,$$

where $A = (m^2-n^2)^{X/2}, B = 2mn, C = (m^2+n^2)^Z$. It is immediate that the case $\gamma > 0$ does not hold by Lemma 6.5. Hence $\gamma = 0$, namely y is a power of 3. In particular, we can put $y = 9Y$ with $Y \geqslant 1$ since $y > 3$. From $2 \nmid A, B \equiv 0 \pmod 4, 2 \nmid C$ and by Lemma 6.6, we have

$$\begin{cases} A = \pm(s^6 + 40s^3t^3 - 32t^6), \\ B^{3Y} = -8st(s^3 - 16t^3)(s^3 + 2t^3), \\ C = s^{12} - 176s^9t^3 - 5632s^3t^9 - 1024t^{12}, \end{cases}$$

where s and t are non-zero relatively prime integers such that $s \not\equiv t \pmod 3$. We want to deduce a contradiction from this. The middle equality can be written as

$$(B^Y)^3 = -8st(s^3 - 16t^3)(s^3 + 2t^3). \tag{7.1}$$

Since the left-hand side of (7.1) is divisible by 16 and s is odd, we see that t must be even. Let $g = \gcd(s^3 - 16t^3, s^3 + 2t^3)$. It is easily seen that $g \in \{1, 3, 9\}$, and that the four factors $-8t, s, s^3 - 16t^3$ and $s^3 + 2t^3$ on the right-hand side of (7.1) are pair-wise relatively prime if and only if $g = 1$. First, we consider the case $g = 1$. Then, by (7.1), we see that $s^3 + 2t^3$ is a cube of a non-zero integer. But, by Lemma 6.1, this implies that $st = \pm 1$, which contradicts $2 \mid t$. Next, we consider the cases $g = 3$ or 9. Since s and t are relatively prime and now $s^3 + 2t^3$ is divisible by 3, we know that $3 \nmid st$. Hence

$$s^3 + 2t^3 \equiv s + 2t \equiv s - t \equiv 0 \pmod 3.$$

But this contradicts $s \not\equiv t \pmod 3$.

When we suppose that Z is even, we get a contradiction by a similar reasoning. This completes the proof of Theorem 1.5.

(ii) By Lemma 2.5 and the proof of (i), we obtain $(x, y, z) = (2, 2, 2)$. ■

Proof of Corollary 1.6. Let (x, y, z) be a solution of (1.2). Since $m \not\equiv 1 \pmod 4$, $2\alpha = \beta + 1$ and $ej \equiv 1 \pmod 4$, it follows from Lemmas 2.1 and 2.4 that x and z are even. Then, by (ii) in Theorem 1.5, we have $(x, y, z) = (2, 2, 2)$. ■

Acknowledgements. The author would like to thank Professor Hirofumi Tsumura for his valuable suggestions and many encouragements, and also thank the anonymous referee for his/her careful reading the manuscript and giving many useful comments. In addition, the author is grateful to Naoki Ogura for helping him with computations in Lemma 4.4.

References

[BS] M. A. Bennett and C. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56** (2004), 23–54.

[Be] F. Beukers, *The diophantine equation* $Ax^p + By^q = Cz^r$, Duke Math. J. **91** (1998), 61–88.

[Br] N. Bruin, *On powers as sums of two cubes*, ANTS IV, Leiden 2000, 169–184, Lecture Notes in Comput. Sci. 1838, Springer 2000.

[Br2] —, *Chabauty methods using elliptic curves*, J. Reine Angew. Math. **562** (2003), 27–49.

[Ca] Z. F. Cao, *A note on the Diophantine equation* $a^x + b^y = c^z$, Acta Arith. **91** (1999), 85–93.

[Ca2] —, *The Diophantine equations* $x^4 - y^4 = z^p$ *and* $x^4 - 1 = dy^q$, C. R. Math. Rep. Acad. Sci. Canada (1) **21** (1999), 23–27.

[CD] Z. F. Cao and X. L. Dong, *On the Terai-Jeśmanowicz conjecture*, Publ. Math. Debrecen, **61** (2002), 253–265.

[CD2] —, *An application of a lower bound for linear forms in two logarithms to the Terai-Jeśmanowicz conjecture*, Acta Arith. **110** (2003), 153–164.

[Co] H. Cohen, *Number Theory - Volume II: Analytic and Modern Tools*. Graduate Texts in Mathematics. Springer-Verlag, 2007.

[Da] H. Darmon, *The equation* $x^4 - y^4 = z^p$, C.R. Math. Rep. Acad. Sci. Canada. XV No. **6** (1993), 286–290.

[DG] H. Darmon and A. Granville, *On the equations* $z^m = F(x, y)$ *and* $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. **27** (1995), 513–543.

[DM] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's last Theorem*, J. Reine. Angew. Math. **490** (1997), 81–100.

[De] V. A. Dem'janenko, *On Jeśmanowicz' problem for Pythagorean numbers*, Izv. Vyssˇ. Učebn. Zaved. Mat. **48** (1965), 52–56 (in Russian).

[DC] M. -J. Deng and G. L. Cohen, *On the conjecture of Jeśmanowicz concerning Pythagorean triples*, Bull. Austral. Math. Soc. **57** (1998), 515–524.

[DC2] —, *A note on a conjecture of Jeśmanowicz*, Colloq. Math. **86** (2000), 25–30.

[Ed] J. Edwards, *A complete solution to* $X^2 + Y^3 + Z^5 = 0$, J. Reine Angew. Math. **571** (2004), 213–236.

[GL] Y. -D. Guo and M. -H. Le, *A note on Jeśmanowicz conjecture concerning Pythagorean numbers*, Comment. Math. Univ. St. Pauli **44** (1995), 225–228.

[Je] L. Jeśmanowicz, *Several remarks on Pythagorean numbers*, Wiadom. Mat. **1** (1955/56), 196–202 (in Polish).

[Ko] C. Ko, *On Pythagorean numbers*, J. Sichuan Univ. Nat. Sci. **1** (1958), 73–80 (in Chinese).

[Ko2] —, *On Ješmanowicz conjecture*, ibid. **2** (1958), 81–90 (in Chinese).

[LMN] M. Laurent, M. Mignotte and Y. Nesterenko, *Formes lineaires en deux logarithmes et determinants d'interpolation*, J. Number Theory **55** (1995), 285–321.

[Le] M. -H. Le, *A note on Ješmanowicz conjecture*, Colloq. Math. **69** (1995), 47–51.

[Le2] —, *On Ješmanowicz conjecture concerning Pythagorean numbers*, Proc. Japan Acad. Ser. A Math. Sci. **72** (1996), 97–98.

[Le3] —, *A note on Ješmanowicz' conjecture concerning Pythagorean triples*, Bull. Austral. Math. Soc. **59** (1999), 477–480.

[Le4] —, *A note on Ješmanowicz' conjecture concerning primitive Pythagorean triplets*, Acta Arith. **138** (2009), 137–144.

[Lu] W. T. Lu, *On the Pythagorean numbers* $4n^2-1, 4n$ *and* $4n^2+1$, Acta Sci. Natur. Univ. Szechuan **2** (1959), 39–42 (in Chinese).

[Mi] M. Mignotte, *A corollary to a theorem of Laurent-Mignotte-Nesterenko*, Acta Arith. **86** (1998), 101–111.

[Miy] T. Miyazaki, *On the conjecture of Ješmanowicz concerning Pythagorean triples*, Bull. Austral. Math. Soc. **80** (2009), 413–422.

[Po] V. D. Podsypanin, *On a property of Pythagorean numbers*, Izv. Vyssh. Uchebn. Zaved. Mat. **4** (1962), 130–133 (in Russian).

[Poo] B. Poonen, *Some Diophantine equations of the form* $x^n + y^n = z^m$, Acta Arith. **86** (1998), 193–205.

[Ri] P. Ribenboim, *Catalan's Conjecture: Are* 8 *and* 9 *the only Consecutive Powers ?* Boston, MA: Academic Press, 1994.

[Sc] R. Scott, *On the equations* $p^x - b^y = c$ *and* $a^x + b^y = c^z$, J. Number Theory **44** (2) (1993), 153–165.

[SS] R. Scott and R. Styer, *On* $p^x - q^y = c$ *and related three term exponential Diophantine equations with prime bases*, J. Number Theory **105** (2004), 212–234.

[Si] W. Sierpiński, *On the equation* $3^x + 4^y = 5^z$, Wiadom. Mat. **1** (1955/56), 194–195 (in Polish).

[Ta] K. Takakuwa, *A remark on Ješmanowicz conjecture*, Proc. Japan Acad. Ser. A Math. Sci. **72** (1996), 109–110.

[TA] K. Takakuwa and Y. Asaeda, *On a conjecture on Pythagorean numbers*, Proc. Japan Acad. Ser. A Math. Sci. **69** (1993), 252–255.

[TA2] —, *On a conjecture on Pythagorean numbers II*, Proc. Japan Acad. Ser. A Math. Sci. **69** (1993), 287–290.

[TA3] —, *On a conjecture on Pythagorean numbers III*, Proc. Japan Acad. Ser. A Math. Sci. **69** (1993), 345–349.

[Te] N. Terai, *Applications of a lower bound for linear forms in two logarithms to exponential Diophantine equations*, Acta Arith. **86** (1999), 17–35.

Address: Takafumi Miyazaki: Department of Mathematics and Information Sciences, Tokyo Metropolitan University, 1-1, Minami-Ohsawa, Hachioji, Tokyo 192-0397, Japan.

E-mail: miyazaki-takafumi@ed.tmu.ac.jp

Received: 20 July 2010