# On the exponential Diophantine equation $a^x + b^y = c^z$

2012

Takafumi Miyazaki

Department of Mathematics and Information Sciences

Tokyo Metropolitan University

**Acknowledgments.** To start, the author would like to express his deepest gratitude to his supervisor Professor Hirofumi Tsumura for his constant support and encouragements. He is very grateful to Professor Nobuhiro Terai for his leading, endurance and many encouragements. Also he would like to thank for Professors Masaki Sudo, Isao Wakabayashi and Noriko Hirata-Kohno and Yasutsugu Fujita for their discussions, reading his papers carefully, giving useful comments and encouragements.

Finally, the author would like to my parents, family, and friends for their constant supports and encouragements.

# Contents

# Chapter 0

# Introduction

Let $\mathbb{N} = \{1, 2, 3, ...\}$ be the set of positive integers and $\mathbb{Z} = \{0, \pm 1, \pm 2, ...\}$ the set of integers. The study of the problem to ask whether a sum of two powers is a power or not is one of the main themes of number theory. In other words, it is to search the solutions of equation

$$X^x + Y^y = Z^z$$

where $X, Y, Z, x, y, z \in \mathbb{N}$. There are a very large number of works in cases where some of $X, Y, Z, x, y, z$ are variables. A good example is the (generalized) Fermat equation

$$X^n + Y^n = Z^n$$

where $X, Y, Z \in \mathbb{N}$ and $n$ is a fixed positive integer with $n \geq 2$. In this thesis we consider the problem in case where $x, y, z$ are variables.

Let $a, b, c$ be pair-wise relatively prime positive integers. Then we consider the exponential Diophantine equation

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

where $x, y, z \in \mathbb{N}$. This field has a long history. Originally this problem was considered for fixed triples $(a, b, c)$. Using congruences, the quadratic reciprocity law and factorizations in number fields, several authors determined complete solutions of (1) (cf. [Ha], [Ma], [Na], [Uc]). We consider the case where $a, b, c > 1$. By the theory of Diophantine approximations, we can examine the solutions of (1). By Baker's theory of linear forms in logarithms, we can obtain effectively computable upper bounds for the size of solutions of (1), which may be generally very large. According to [Hi], under certain assumptions on $a, b, c$, we have the following upper estimate:

$$\max(x, y, z) < 2^{288} \sqrt{abc} \log(abc)$$

for all solutions $(x, y, z)$ of (1). On the other hand, equation (1) can be regarded as a kind of unit equations. Let $N = N(a, b, c)$ be the number of solutions of (1). Mahler [Ma] first showed the finiteness of $N$. The theory of unit equations

gives upper bounds for $N$. In particular, using a result in [BS], we obtain an absolute upper bound:

$$N \leq 2^{36}.$$

In case where divisibility properties of $x, y, z$ are given, we may connect (1) to other Diophantine equations, in particular, generalized Fermat equations (cf. [Co, Ch.14]). We remark that these upper bounds above are generally not useful to determine the solutions of (1).

We generally observe that $N$ is very small. It seems no triple $(a, b, c)$ for which $N > 3$. The only known case for which $N = 3$ (at least as far as the author knows) is

$$3 + 5 = 2^3, \quad 3^3 + 5 = 2^5, \quad 3 + 5^3 = 2^7.$$

One of the main themes on exponential Diophantine equations is to show that $N$ is very small, such as $N \leq 3$, which is known to be true in case where $c$ is a prime ([Sc, Theorem 6]). For this purpose we should treat triples $(a, b, c)$ for which (1) has one solution $(x, y, z) = (p, q, r)$. In this direction there is a celebrated problem suggested by Terai [Te2]. In [Mi, Miy2] we proposed a modified version of it as follows.

**Conjecture 0.1.1** *Let $p, q, r$ be positive integers with $p, q, r \geq 2$, and let $a, b, c$ be pair-wise relatively prime positive integers such that $a^p + b^q = c^r$. Assume that $(a, b, c)$ is not any of the following cases (up to any change a into b):*

$$(2,\ 7,\ 3), \quad (2,\ 2^{p-2} - 1,\ 2^{p-2} + 1)\,;\ p \geq 3.$$

*Then (1) has the unique solution $(x, y, z) = (p, q, r)$.*

In what follows, we call Conjecture 0.1.1 Terai's conjecture. This is one of the most famous unsolved problems in the field of exponential Diophantine equations. Note that

$$2^5 + 7^2 = 3^4; \quad 2 + 7 = 3^2,$$
$$2^p + (2^{p-2} - 1)^2 = (2^{p-2} + 1)^2; \quad 2 + (2^{p-2} - 1) = 2^{p-2} + 1 \ (p \geq 3).$$

Terai's conjecture is the main theme in this thesis.

In Chapter 1, we consider Terai's conjecture in the case $p = q = r = 2$, which is just the conjecture of Jeśmanowicz [Je]. Jeśmanowicz' conjecture is a famous unsolved problem on Pythagorean numbers, also in the field of exponential Diophantine equations. We first introduce several known results on Jeśmanowicz' conjecture, and prove the results obtained in [Miy6].

In Chapter 2, we consider Terai's conjecture more generally. We first introduce several known results on the conjecture, and prove some of the results obtained in [Miy2, Miy3].

In Chapter 3, we consider an analogous problem of the conjecture of Jeśmanowicz. We prove the result obtained in [Miy4].

In Chapter 5, we give several results concerning upper bounds for solutions of (1) under certain assumptions. Furthermore, using them, we solve equations (1) in case where $a, b$ and $c$ are Fibonacci numbers.

# Chapter 1

# Jeśmanowicz' conjecture

## 1.1 Jeśmanowicz' conjecture

For positive integers $a, b, c$, we call $(a, b, c)$ a *Pythagorean triple* if $a^2 + b^2 = c^2$, and further *primitive* if $a, b, c$ are relatively prime. We know that Pythagorean triples appear in many mathematical subjects, especially, Diophantine equations. In 1956 Leon Jeśmanowicz [Je] proposed the following problem.

**Conjecture 1.1.1** *Let $(a, b, c)$ be a primitive Pythagorean triple such that $a^2 + b^2 = c^2$. Then (1) has the unique solution $(x, y, z) = (2, 2, 2)$.*

This is one of the most famous unsolved problems on Pythagorean numbers, also in the field of exponential Diophantine equations. For the most famous Pythagorean triple $(a, b, c) = (3, 4, 5)$, Sierpiński [Si] considered (1), that is,

$$3^x + 4^y = 5^z.$$

He proved that the above equation has the unique solution $(x, y, z) = (2, 2, 2)$ in positive integers $x, y$ and $z$. Later, Jeśmanowicz [Je] further showed similar results for each of the following equations:

$$5^x + 12^y = 13^z, \quad 7^x + 24^y = 25^z, \quad 9^x + 40^y = 41^z, \quad 11^x + 60^y = 61^z,$$

and he proposed his conjecture.

It is well-known that, for any primitive Pythagorean triple $(a, b, c)$ satisfying $a^2 + b^2 = c^2$ (we may assume that $b$ is even), we can write

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

where integers $m, n$ satisfy the condition

$$m > n > 0, \quad \gcd(m, n) = 1, \quad m \not\equiv n \pmod 2.$$

We will always consider the above expressions.

## 1.2 Results

In this section we introduce several known results on Conjecture 1.1.1.

After the work of Jeśmanowicz mentioned in the Section 1.1, Lu [Lu] showed

**Proposition 1.2.1** *If $n = 1$, then Conjecture 1.1.1 is true.*

We remark that $m$ may be any positive even integer if $n = 1$, and that $n = 1$ if and only if $c = a + 2$. Proposition 1.2.1 is the only result in which Conjecture 1.1.1 is true for fixed $n$.

Later, extending earlier results in several papers [Ko, Ko2, Po], Dem'janenko [De] proved

**Proposition 1.2.2** *If $c = b + 1$, then Conjecture 1.1.1 is true.*

Propositions 1.2.1 and 1.2.2 include the results of Sierpiński and Jeśmanowicz. Also they are crucially important since they are used in many earlier works. For other known results, see for example [Ca, DC, HY, Le, Miy].

The purpose in this chapter is to generalize both Propositions 1.2.1 and 1.2.2 by proving the following results.

**Theorem 1.2.1** *If $a \equiv \pm 1 \pmod{b}$, then Conjecture 1.1.1 is true.*

**Theorem 1.2.2** *If $c \equiv 1 \pmod{b}$, then Conjecture 1.1.1 is true.*

Both Theorems 1.2.1 and 1.2.2 are generalizations of Proposition 1.2.1. Indeed, if $n = 1$, then $m$ is even and $b = 2m$, so $a = m^2 - 1 \equiv -1 \pmod{b}$ and $c = m^2 + 1 \equiv 1 \pmod{b}$. Theorem 1.2.2 is also a generalization of Proposition 1.2.2.

From Theorem 1.2.1 we obtain the following corollary, which can be regarded as an analogue of Proposition 1.2.2.

**Corollary 1.2.1** *If $|b - a| = 1$, then Conjecture 1.1.1 is true.*

For the Pythagorean triples $(a, b, c)$ satisfying $a^2 + b^2 = c^2$ and $|b - a| = 1$, we can find a topic on them in Section "RIGHT TRIANGLES WHOSE LEGS DIFFER BY UNITY" in the famous book of Dickson "History of the Theory of Numbers": Vol. 2 (Chelsea) (see [Di, pp.181–183]). Some histories are written in it. For example, Fermat gave an easy method to find such triples (see Remark 1.4.1 below).

In the next section we prepare some lemmas for proving Theorems 1.2.1 and 1.2.2. It is crucially important to examine parities of exponential variables $x, y, z$ for Conjecture 1.1.1. Using the parameters introduced by the author in [Miy], we give useful lemmas to examine parities of $x$ and $z$. Further, we quote a well-known result on Diophantine equations due to Euler.

In the remaining sections we prove Theorems 1.2.1 and 1.2.2. An important step in the proofs is to show that $x, y, z$ are all even. We observe that this yields sharp upper bounds for $x, y, z$. On the other hand, by congruence reductions, we can obtain congruence relations among the solutions, which yield sharp

lower bounds for hypothetical solutions. Finally we observe that hypothetical solutions lead to contradictions, and complete the proofs.

In what follows, we consider the equation

$$(m^2 - n^2)^x + (2mn)^y = (m^2 + n^2)^z \tag{1.2.1}$$

where $x, y, z \in \mathbb{N}$.

## 1.3 Preliminaries

In this section we prepare some lemmas for proving Theorems 1.2.1 and 1.2.2. First we give lemmas to examine parities of exponential variables $x$ and $z$. It is crucially important to know parities of $x, y, z$ for Conjecture 1.1.1.

The following notation have already been defined by the author in [Miy]. By Proposition 1.2.1, we may assume that $n > 1$. We define integers $\alpha, \beta, e$ ($\alpha \geq 1$, $\beta \geq 2$, $e = \pm 1$), and odd positive integers $i, j$ as follows:

$$\begin{aligned} &m = 2^\alpha i, \quad n = 2^\beta j + e \qquad \text{if } m \text{ is even,} \\ &m = 2^\beta j + e, \quad n = 2^\alpha i \qquad \text{if } m \text{ is odd.} \end{aligned} \tag{1.3.1}$$

In what follows, we consider the case where $2\alpha \neq \beta + 1$. The following two lemmas will be used to determine parities of exponential variables. In particular, Lemma 1.3.1 will play an important role in the proofs. For a non-zero integer $k$, we denote the 2-adic valuation by $\mathrm{ord}_2$.

**Lemma 1.3.1** *Let $(x, y, z)$ be a solution of (1.2.1). If $y > 1$, then $x \equiv z \pmod 2$.*

*Proof.* This is a direct consequence of [Miy, Lemma 3.1]. But, for the sake of completeness, we prove this lemma here.

Assume that $2\alpha \neq \beta + 1$. We consider the case where $m$ is even. As defined in (1.3.1), we put $m = 2^\alpha i$ and $n = 2^\beta j + e$.

Let $(x, y, z)$ be a solution of (1.2.1). It is easy to see that $x$ is even by taking (1.2.1) modulo 4. Suppose that $x \not\equiv z \pmod 2$, that is, $z$ is odd. Taking (1.2.1) modulo $2^{2\alpha+1}$, we have

$$\begin{aligned} (2mn)^y &= \left(m^2 + n^2\right)^z - \left(m^2 - n^2\right)^x \\ &\equiv m^2 n^{2z-2} z + n^{2z} + m^2 n^{2x-2} x - n^{2x} \\ &\equiv m^2 (n^{2z-2} z + n^{2x-2} x) + n^{2z} - n^{2x} \pmod{2^{2\alpha+1}}. \end{aligned}$$

Put

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

Then

$$(2mn)^y \equiv A + B \pmod{2^{2\alpha+1}}.$$

Since $n$ is odd and $x \not\equiv z \pmod 2$, we see that $n^{2z-2} z + n^{2x-2} x$ is odd, hence

$$\mathrm{ord}_2(A) = \mathrm{ord}_2(m^2) = \mathrm{ord}_2(2^{2\alpha} i^2) = 2\alpha,$$

$$\begin{aligned}\mathrm{ord}_2(B) &= \mathrm{ord}_2(n^{2|x-z|}-1)\\ &= \mathrm{ord}_2(n^2-1)\\ &= \mathrm{ord}_2\big(2^{2\beta}j^2+2^{\beta+1}ej\big)\\ &= \mathrm{ord}_2(2^{\beta+1}j)\\ &= \beta+1.\end{aligned}$$

Since $\mathrm{ord}_2((2mn)^y) = (\alpha+1)y$ and $2\alpha \neq \beta+1$, it follows that

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

This implies that $\alpha = 1$ and $y = 1$, or $\alpha = \beta$ and $y = 1$. Therefore, if $y > 1$, then $x \equiv z \pmod 2$. Similarly, we can prove the lemma for the case where $m$ is odd. □

**Lemma 1.3.2** *Let $(x, y, z)$ be a solution of* (1.2.1)*. If $x$ and $z$ are even, then $X \equiv Z \pmod 2$, where $X = x/2$ and $Z = z/2$.*

*Proof.* We consider the case where $2\alpha \neq \beta+1$. Let $(x, y, z)$ be a solution of (1.2.1). Assume that $x$ and $z$ are even. We can write $x = 2X$ and $z = 2Z$, where $X, Z \in \mathbb{N}$. We define even positive integers $D$ and $E$ by

$$D = (m^2+n^2)^Z + (m^2-n^2)^X, \quad E = (m^2+n^2)^Z - (m^2-n^2)^X.$$

Then $(2mn)^y = DE$ by (1.2.1). Since

$$(2mn)^y \geq D > m^2+n^2 > 2mn,$$

it follows that $y > 1$. It is easy to see that $\gcd(D, E) = 2$. Since $DE$ is (exactly) divisible by $2^{(\alpha+1)y}$, we see that the congruence

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

holds for the proper sign.

First, we consider the case where $2\alpha > \beta+1$. Then, since $(\alpha+1)y-1 > 2\alpha \geq \beta+2$, the above congruence can be reduced to $(m^2+n^2)^X \pm (m^2-n^2)^Z \equiv 0 \pmod{2^{\beta+2}}$. Substituting $\alpha, \beta$ expression in (1.3.1) into this congruence, we have $2^{\beta+1}ejX \equiv \pm 2^{\beta+1}ejZ \pmod{2^{\beta+2}}$. This implies that $X \equiv Z \pmod 2$ since $ej$ is odd.

Finally, we consider the case where $2\alpha < \beta+1$. Then, since $(\alpha+1)y - 1 \geq 2\alpha+1$ and $\beta+1 \geq 2\alpha+1$, it follows from the above congruence that $2^{2\alpha}i^2X \equiv \pm 2^{2\alpha}i^2Z \pmod{2^{2\alpha+1}}$. This implies that $X \equiv Z \pmod 2$ since $i$ is odd. □

The following is a classical well-known result due to Euler [Eu]. It is an analogue of the case $n = 3$ for Fermat's last theorem, and will be used in the proof of Theorem 1.2.1.

**Lemma 1.3.3** *The equation*

$$X^3 + Y^3 = 2Z^3$$

*has no integral solutions with* $\gcd(X, Y) = 1$ *and* $XYZ \notin \{0, \pm 1\}$.

*Proof.* For example, see [Na, pp.244–246], [Wa]. □

## 1.4 Proof of Theorem 1.2.1

In this section we prove Theorem 1.2.1. We consider the cases $a \equiv -1 \pmod{b}$ and $a \equiv 1 \pmod{b}$ separately.

### 1.4.1 The case $a \equiv -1 \pmod{b}$

In this section we prove that Conjecture 1.1.1 is true if $a \equiv -1 \pmod{b}$.

Assume that $a \equiv -1 \pmod{b}$, or

$$m^2 - n^2 = -1 + 2mnt, \tag{1.4.1}$$

where $t \in \mathbb{N}$. Then

$$m^2 \equiv -1 \pmod{n}, \tag{1.4.2}$$

$$n^2 \equiv 1 \pmod{m}. \tag{1.4.3}$$

By Proposition 1.2.1, we may assume that $n > 1$. First we prove an important lemma.

**Lemma 1.4.1** *With the notation in* (1.3.1)*, we have*

(i) $n \geq 4t$.

(ii) $m$ *is divisible by* $2t$. *In particular,* $m$ *is even and* $n$ *is odd.*

(iii) $2\alpha \neq \beta + 1$.

*Proof.* From (1.4.1) we see that $(U, V) = (m - nt, n)$ is a positive solution of the Pellian equation

$$U^2 - (t^2 + 1)V^2 = -1.$$

Since the fundamental solution of the above Pellian equation is $t + \sqrt{t^2 + 1}$, all of the pairs $(m, n)$ are given by $m = U_l + tV_l$, $n = V_l$, where positive integers $U_l, V_l$ are defined by

$$U_l + V_l \sqrt{t^2 + 1} = (t + \sqrt{t^2 + 1})^l \,;\ l \geq 1 \text{ odd}.$$

(i) Since $V_l = n > 1$, we see that $l \geq 3$, hence $n = V_l \geq V_3 = 4t^2 + 1$.

(ii) This follows from the facts that $U_1 + tV_1 = 2t$ and

$$U_{l+2} = (2t^2 + 1)U_l + 2t(t^2 + 1)V_l \equiv U_l \pmod{2t},$$
$$V_{l+2} = 2tU_l + (2t^2 + 1)V_l \equiv V_l \pmod{2t}.$$

(iii) As defined in (1.3.1), we put $m = 2^\alpha i$ and $n = 2^\beta j + e$. We know from (ii) that $2^\alpha i$ is divisible by $2t$, in particular, $\mathrm{ord}_2(2t) \le \alpha$ since $i$ is odd. It follows from (1.4.1) that

$$\begin{aligned}\beta + 1 &= \mathrm{ord}_2\big((n-1)(n+1)\big) \\ &= \mathrm{ord}_2\big(m(m-2nt)\big) \\ &= \alpha + \mathrm{ord}_2(m - 2nt).\end{aligned}$$

Hence it suffices to check that $\mathrm{ord}_2(m-2nt) \neq \alpha$. If $\mathrm{ord}_2(2t) < \alpha$, then $\mathrm{ord}_2(2nt) < \alpha$, so $\mathrm{ord}_2(m-2nt) = \mathrm{ord}_2(2nt) < \alpha$. If $\mathrm{ord}_2(2t) = \alpha$, then $\mathrm{ord}_2(m-2nt) = \alpha + \mathrm{ord}_2(i - n(2t/2^\alpha)) > \alpha$. Therefore, $2\alpha \neq \beta + 1$. □

By (i) in Lemma 1.4.1, we see that $m > n \ge 3$.

Let $(x, y, z)$ be a solution of (1.2.1). We prepare several lemmas.

**Lemma 1.4.2** *$x$ and $z$ are even.*

*Proof.* Taking (1.2.1) modulo $m$, we have $(-n^2)^x \equiv (n^2)^z \pmod m$. Then (1.4.3) yields $(-1)^x \equiv 1 \pmod m$. Hence $x$ is even since $m \ge 3$.

Taking (1.2.1) modulo $n$, we have $(m^2)^x \equiv (m^2)^z \pmod n$. Then (1.4.2) yields $(-1)^z \equiv 1 \pmod n$, hence $z$ is also even since $n \ge 3$. □

By Lemma 1.4.2, we can write $x = 2X$ and $z = 2Z$, where $X, Z \in \mathbb{N}$. Note that $y > 1$ as we observed in the proof of Lemma 1.3.2.

**Lemma 1.4.3** $4tX \equiv 4tZ \pmod{mn}$.

*Proof.* Taking (1.2.1) modulo $m^2$, we have $n^{4X} \equiv n^{4Z} \pmod{m^2}$ since $y > 1$. On the other hand, we know from (1.4.1) that $n^2 \equiv 1 - 2mnt \pmod{m^2}$. It follows that $(1-2mnt)^{2X} \equiv (1-2mnt)^{2Z} \pmod{m^2}$, hence

$$4mntX \equiv 4mntZ \pmod{m^2}.$$

Similarly, we can show that

$$4mntX \equiv 4mntZ \pmod{n^2}$$

by taking (1.2.1) modulo $n^2$. Since $\gcd(m, n) = 1$, we find that

$$4mntX \equiv 4mntZ \pmod{m^2n^2},$$

hence $4tX \equiv 4tZ \pmod{mn}$. □

We define positive even integers $D, E$ as follows:

$$(2mn)^y = DE, \tag{1.4.4}$$

where

$$\begin{aligned}D &= \left(m^2 + n^2\right)^Z + \left(m^2 - n^2\right)^X, \\ E &= \left(m^2 + n^2\right)^Z - \left(m^2 - n^2\right)^X.\end{aligned}$$

It is easy to see that $\gcd(D, E) = 2$, and

$$D \equiv 1 + (-1)^X, \quad E \equiv 1 - (-1)^X \pmod 4.$$

Also, we see from (1.4.2) and (1.4.3) that

$$D \equiv 1 + (-1)^X, \quad E \equiv 1 - (-1)^X \pmod m$$

and

$$D \equiv (-1)^Z + (-1)^X, \quad E \equiv (-1)^Z - (-1)^X \pmod n.$$

**Lemma 1.4.4** *$X$ and $Z$ are odd.*

*Proof.* By Lemma 1.3.2 and (iii) in Lemma 1.4.1, we see that $X \equiv Z \pmod 2$. Suppose that $X$ and $Z$ are even. Then

$$D \equiv 2 \pmod 4, \quad D \equiv 2 \pmod{mn}.$$

Hence (1.4.4) yields $D = 2$, which is clearly absurd. We conclude that $X$ and $Z$ are odd. □

By Lemma 1.4.4, we see that

$$E \equiv 2 \pmod 4, \quad E \equiv 2 \pmod m, \quad D \equiv -2 \pmod n.$$

It follows from (1.4.4) that

$$\begin{aligned} D &= (m^2 + n^2)^Z + (m^2 - n^2)^X = 2^{y-1} m^y, \\ E &= (m^2 + n^2)^Z - (m^2 - n^2)^X = 2n^y. \end{aligned}$$

**Lemma 1.4.5** *$y$ is even.*

*Proof.* We see that $(m^2 + n^2)^Z = (D + E)/2 = 2^{y-2} m^y + n^y$. Taking this modulo $m$, we have

$$n^y \equiv 1 \pmod m$$

by (1.4.3). If $y$ is odd, then the above congruence yields $n \equiv 1 \pmod m$ by (1.4.3). This is absurd since $m > n > 1$. Hence $y$ is even. □

By Lemma 1.4.5, we can write $y = 2Y$, where $Y \in \mathbb{N}$. Since $\{a^X, b^Y, c^Z\}$ forms a primitive Pythagorean triple, we can write

$$a^X = k^2 - l^2, \quad b^Y = 2kl, \quad c^Z = k^2 + l^2,$$

where integers $k, l$ satisfy the condition

$$k > l > 0, \quad \gcd(k, l) = 1, \quad k \not\equiv l \pmod 2.$$

Since $b < c < a^2$ and $a^X < c^Z < b^{2Y}$, it follows that

$$|X - Z| < Z < 2Y.$$

Since $(k+l)(k-l) = a^X$ and $\gcd(k+l, k-l) = 1$, we can write

$$k + l = u^X, \quad k - l = v^X,$$

where integers $u, v$ satisfy $u > v > 0$, $\gcd(u, v) = 1$ and $uv = a$. Note that $u, v$ are odd.

We will obtain a sharp upper bound for $Y$.

**Lemma 1.4.6** $Y \leq \dfrac{\log(a+1)}{\mathrm{ord}_2(b)\log 2}$.

*Proof.* Since $X$ is odd and $4kl = (k+l)^2 - (k-l)^2 = u^{2X} - v^{2X}$, it follows that

$$Y \,\mathrm{ord}_2(b) = \mathrm{ord}_2(2kl) = \mathrm{ord}_2\left(\frac{u^{2X} - v^{2X}}{2}\right) = \mathrm{ord}_2(u \pm v),$$

where we take the proper sign for which $\mathrm{ord}_2(u \pm v) \geq 2$. Since $u \pm v \leq u + v \leq uv + 1 = a + 1$, we obtain

$$Y = \frac{\mathrm{ord}_2(u \pm v)}{\mathrm{ord}_2(b)} \leq \frac{\log(a+1)}{\mathrm{ord}_2(b)\log 2}. \ \square$$

We are ready to complete the proof. If $X \neq Z$, then (i) in Lemma 1.4.1, Lemma 1.4.3 and Lemma 1.4.6 yield

$$m \leq m\left(\frac{n}{4t}\right) = \frac{mn}{4t} \leq |X - Z| < Z < 2Y \leq \frac{\log(a+1)}{\log 2} < \frac{2\log m}{\log 2},$$

which does not hold. Hence $X = Z$.

Since $X$ is odd and $b^{2Y} = c^{2X} - a^{2X}$, it follows that

$$\mathrm{ord}_2(b^{2Y}) = \mathrm{ord}_2(c^{2X} - a^{2X}) = \mathrm{ord}_2(c^2 - a^2) = \mathrm{ord}_2(b^2),$$

which gives $Y = 1$, so $X = Z = 1$. We conclude that Conjecture 1.1.1 is true if $a \equiv -1 \pmod{b}$.

**Example 1.4.1** As we observed in the proof of Lemma 1.4.1, we can obtain all of the pairs $(m, n)$ satisfying (1.4.1). For example, putting $l = 1$, we have pairs $(m, n) = (2t, 1)$ with $t \geq 1$, which is just Proposition 1.2.1. Putting $l = 3$, we have pairs $(m, n) = (8t^3 + 4t,\ 4t^2 + 1)$ with $t \geq 1$.

### 1.4.2 The case $a \equiv 1 \pmod{b}$

In this subsection we prove that Conjecture 1.1.1 is true if $a \equiv 1 \pmod{b}$. The proof will proceed as well as the preceding section.

Assume that $a \equiv 1 \pmod{b}$, or

$$m^2 - n^2 = 1 + 2mnt, \tag{1.4.5}$$

where $t \in \mathbb{N}$. Then

$$m^2 \equiv 1 \pmod{n}, \tag{1.4.6}$$

$$n^2 \equiv -1 \pmod{m}. \tag{1.4.7}$$

**Lemma 1.4.7** *With the notation in* (1.3.1)*, we have*
(i) *$n$ is divisible by $2t$. In particular, $m$ is odd and $n$ is even.*
(ii) $2\alpha \neq \beta + 1$.

*Proof.* From (1.4.5) we see that $(U, V) = (m - nt, n)$ is a positive solution of the Pellian equation

$$U^2 - (t^2 + 1)V^2 = 1.$$

Since the fundamental solution of the above Pellian equation is $2t^2 + 1 + 2t\sqrt{t^2+1}$, all of the pairs $(m, n)$ are given by $m = U_l + tV_l$, $n = V_l$, where positive integers $U_l, V_l$ are defined by

$$U_l + V_l\sqrt{t^2+1} = (2t^2 + 1 + 2t\sqrt{t^2+1})^l\,;\, l \geq 1.$$

(i) This follows easily from the above.
(ii) Similar to Lemma 1.4.1. □

By (i) in Lemma 1.4.7, we see that $m > n \geq 2$.
Let $(x, y, z)$ be a solution of (1.2.1). We prepare several lemmas.

**Lemma 1.4.8** *$z$ is even.*

*Proof.* Taking (1.2.1) modulo $m$, we have $(-n^2)^x \equiv (n^2)^z \pmod{m}$. Then (1.4.7) yields $(-1)^z \equiv 1 \pmod{m}$. Hence $z$ is even since $m > n \geq 2$. □

By Lemma 1.4.8, we can write $z = 2Z$, where $Z \in \mathbb{N}$. From Lemma 1.3.1 and (ii) in Lemma 1.4.7 we observe that $x$ is even if $y > 1$.

**Lemma 1.4.9** *$x$ is even and $y > 1$.*

*Proof.* Suppose that $y = 1$. We will observe that this leads to a contradiction. Note that $x$ is odd. Taking (1.2.1) modulo $n^2$, we see from (1.4.5) that

$$(1 + 2mnt)^x + 2mn \equiv (1 + 2mnt)^z \pmod{n^2}.$$

Hence

$$2tx + 2 \equiv 2tz \pmod{n}.$$

Then (i) in Lemma 1.4.7 yields $2 \equiv 0 \pmod{2t}$, hence $t = 1$. Then $a = b + 1$ by (1.4.5), so $a^x + a - 1 = (2a^2 - 2a + 1)^Z$ by (1.2.1). Taking this modulo $a$, we have $2 \equiv 0 \pmod{a}$. This is clearly absurd. □

By Lemma 1.4.9, we can write $x = 2X$, where $X \in \mathbb{N}$. We define $D, E$ as in the preceding section. Similarly to the proof of Lemma 1.4.4, we may show that $X, Z$ are odd and $4tX \equiv 4tZ \pmod{mn}$. From (i) in Lemma 1.4.7 we see that $2X \equiv 2Z \pmod{m}$. Hence

$$X \equiv Z \pmod{2m},$$

since $m$ is odd and $X - Z$ is even. Furthermore, since

$$D \equiv 2 \pmod{4}, \quad D \equiv 2 \pmod{n}, \quad E \equiv -2 \pmod{m},$$

it follows that

$$\begin{aligned} D &= (m^2+n^2)^Z + (m^2-n^2)^X = 2m^y, \\ E &= (m^2+n^2)^Z - (m^2-n^2)^X = 2^{y-1}n^y. \end{aligned} \tag{1.4.8}$$

Then $(m^2+n^2)^Z = (D+E)/2 = m^y + 2^{y-2}n^y$. Taking this modulo $n$, we have

$$m^y \equiv 1 \pmod{n}$$

by (1.4.6).

Using a classical well-known result due to Euler (Lemma 1.3.3), we will show that $y$ is even. For this we need a little complicated arguments.

**Lemma 1.4.10** *$y$ is even.*

*Proof.* Suppose that $y$ is odd. We will observe that this leads to a contradiction. Then $m \equiv 1 \pmod{n}$ by (1.4.6). We can write $m = 1 + hn$, where $h \in \mathbb{N}$. Substituting this into (1.4.5), we have

$$np = 2(h-t),$$

where $p = -h^2 + 2th + 1$. Note that $p \neq 0$ and $h \neq t$. From (ii) in Lemma 1.4.7 we see that $h \equiv 0 \pmod{t}$. In particular, $h \geq 2t$. Then $np = 2(h-t) > 0$, so $0 < p = -h(h-2t) + 1$. This implies that $h = 2t$. Hence $p = 1$, $n = 2t$, $m = 1 + n^2$.

We consider the cases $n \not\equiv 0 \pmod 3$ and $n \equiv 0 \pmod 3$ separately.

First, we consider the case where $n \not\equiv 0 \pmod 3$. Since $n^2 \equiv 1 \pmod 3$, we see that $m \equiv 2 \pmod 3$ and $m^2 - n^2 \equiv 0 \pmod 3$. Taking the first equation in (1.4.8) modulo 3, we have $2^Z \equiv 2^{y+1} \equiv 1 \pmod 3$. This implies that $Z$ is even, which is absurd.

Finally, we consider the case where $n \equiv 0 \pmod 3$. Since $m = 1 + n^2$, it follows from (1.4.8) that

$$\begin{aligned} (1+n^2)^y + 2^{y-2}n^y &= (1+3n^2+n^4)^Z, \\ (1+n^2)^y - 2^{y-2}n^y &= (1+n^2+n^4)^X. \end{aligned}$$

Note that $y > 2$. Taking the above equations modulo $3n^2$, we have $(1+n^2)^X \equiv (1+n^2)^y \equiv 1 \pmod{3n^2}$. This implies that $X \equiv y \equiv 0 \pmod 3$. But, the second equation above can be rewritten as

$$(1+n^2)^y + (-1-n^2-n^4)^X = 2(2^{y/3-1}n^{y/3})^3,$$

which contradicts Lemma 1.3.3. We conclude that $y$ is even. □

By Lemma 1.4.10, we can write $y = 2Y$, where $Y \in \mathbb{N}$. Similarly to the proof of the preceding section, we may obtain the same upper bound for $Y$ as Lemma 1.4.6. As a result, we see that if $X \neq Z$, then

$$2m \leq |X - Z| < 2Y \leq \frac{\log(a+1)}{\log 2} < \frac{2\log m}{\log 2},$$

which does not hold. Hence $X = Z$. This leads to the desired conclusion as we observed in the preceding section. We conclude that Conjecture 1.1.1 is true if $a \equiv 1 \pmod b$, and complete the proof of Theorem 1.2.1.

**Example 1.4.2** As we observed in the proof of Lemma 1.4.7, we can obtain all of the pairs $(m, n)$ satisfying (1.4.5). For example, putting $l = 1$, we have pairs $(m, n) = (4t^2 + 1,\ 2t)$ with $t \geq 1$, so $m = n^2 + 1$ with even $n$.

**Remark 1.4.1** We remark on the Pythagorean triples $(a, b, c)$ satisfying $a^2 + b^2 = c^2$ and $b = a + 1$. According to [Di, pp.181–183] (also see [Si2]), Fermat gave an easy method to find such triples. He found that, from one right triangle $(a, a + 1, c)$, one sees that $(A, A + 1, C)$ is also one right triangle, where $A = 2c + 3a + 1$ and $C = 3c + 4a + 2$. Generally, for any Pythagorean triple $(a, b, c)$ satisfying $b = a+1$, since $a^2+(a+1)^2 = c^2$ or equivalently, $(2a+1)^2-2c^2 = -1$, we observe from the theory of the Pellian equations (as we have already observed before) that $a$ and $c$ are given by

$$(2a + 1) + c\sqrt{2} = (1 + \sqrt{2}\,)^{2k+1}\,;\ k \geq 1.$$

The first ten examples are in Table 1. These have already been given by A. Girard (c.f. [Di, pp.181]).

Table 1.1: Pythagorean triples $(a, b, c)$ satisfying $a^2 + b^2 = c^2$ and $b = a + 1$

| $a$ | $b$ | $c$ |
|---|---|---|
| 3 | 4 | 5 |
| 20 | 21 | 29 |
| 119 | 120 | 169 |
| 696 | 697 | 985 |
| 4059 | 4060 | 5741 |
| 23660 | 23661 | 33461 |
| 137903 | 137904 | 195025 |
| 803760 | 803761 | 1136689 |
| 4684659 | 4684660 | 6625109 |
| 27304196 | 27304197 | 38613965 |

## 1.5 Proof of Theorem 1.2.2

In this section we prove that Conjecture 1.1.1 is true if $c \equiv 1 \pmod{b}$. The proof will proceed as well as that of Theorem 1.2.1.

Assume that $c \equiv 1 \pmod{b}$, or

$$m^2 + n^2 = 1 + 2mnt, \tag{1.5.1}$$

where $t \in \mathbb{N}$. Then

$$\begin{aligned} m^2 &\equiv 1 \pmod{n}, \\ n^2 &\equiv 1 \pmod{m}. \end{aligned}$$

By Propositions 1.2.1 and 1.2.2, we may assume that $n > 1$ and $t > 1$.

From (1.5.1) we see that $(U, V) = (m - nt, n)$ is a positive solution of the Pellian equation

$$U^2 - (t^2 - 1)V^2 = 1.$$

Since the fundamental solution of the above Pellian equation is $t + \sqrt{t^2 - 1}$, all of the pairs $(m, n)$ satisfying (1.5.1) are given by $m = U_l + tV_l$, $n = V_l$, where positive integers $U_l, V_l$ are defined by

$$U_l + V_l \sqrt{t^2 - 1} = (t + \sqrt{t^2 - 1})^l \, ; \, l \geq 1.$$

From this we may show the following lemma.

**Lemma 1.5.1** *We have*

(i) *If $l$ is odd, then the same conditions in Lemma 1.4.1 hold.*

(ii) *If $l$ is even, then the same conditions in Lemma 1.4.7 hold.*

Let $(x, y, z)$ be a solution of (1.2.1). As we observed in the proof of Lemma 1.4.2, we may show that $x$ is even. Similarly to the proof of Lemma 1.4.9, we observe that if $y = 1$ then $t = 1$, which is absurd. Hence $y > 1$, so $z$ is even by Lemmas 1.3.1 and 1.5.1. In the case where $l$ is even, we may show that $y$ is also even as we observed in Lemma 1.4.5.

Next, we will show that $y$ is even in the case where $l$ is even as follows. Suppose that $y$ is odd. As we observed in Lemma 1.4.10, this leads to the existence of a positive integer $h$ such that $m = 1 + hn$. Substituting this into (1.5.1), we have

$$np = 2(t - h),$$

where $p = h^2 - 2th + 1$. Then $p \neq 0$ (since $t > 1$) and $h \neq t$. From (ii) in Lemma 1.5.1 we know that $n$ is divisible by $2t$, so $h$ is divisible by $t$. In particular, $h \geq 2t$. Then $p = h(h - 2t) + 1 > 0$, so $t - h = (np)/2 > 0$, which is clearly absurd. We conclude that $y$ is even.

Therefore, $x, y, z$ are all even. Similarly to the preceding sections, we can complete the remaining parts of the proof of Theorem 1.2.2.

**Example 1.5.1** Let $t$ be a positive integer with $t > 1$. As we observed at the beginning of this section, we can obtain all of the pairs $(m, n)$ satisfying (1.5.1). For example, putting $l = 1$, we have pairs $(m, n) = (2t, 1)$, which is just Proposition 1.2.1 ($t = 1$ corresponds to $(a, b, c) = (3, 4, 5)$). Putting $l = 2$, we have pairs $(m, n) = (4t^2 - 1, 2t)$, so $m = n^2 - 1$ with even $n \geq 2$ ($t = 1$ corresponds to $(a, b, c) = (5, 12, 13)$).

# Chapter 2

# Terai's conjecture

## 2.1 Results

Terai's conjecture (Conjecture 0.1.1) concerns all positive integers $p, q, r \geq 2$. But we should treat exponents $(p, q, r)$ which admit infinite number of triples $(a, b, c)$ satisfying $a^p + b^q = c^r$ ($a, b, c$ are relatively prime positive integers). By the works of Darmon-Granville [DG] and Beukers [Beu], we can observe that all of such $(p, q, r)$ are given by (we take $p \geq q$)

$$(p,q,r) = \begin{cases} (2,2,r);\ r \geq 2, \\ (p,2,2);\ p \geq 3, \\ (3,2,3), (3,3,2), (3,2,4), (4,2,3), (4,3,2), (3,2,5), (5,2,3), (5,3,2). \end{cases}$$

Further, for each $(p, q, r)$ above, all of the relatively prime positive integers $a, b, c$ satisfying $a^p + b^q = c^r$ are given by several polynomials in two integral variables with integral coefficients (see [Beu] and [Co, Ch.14]). Most known results on Terai's conjecture concern the first case above. For $r \geq 2$, we can find that all of the relatively prime positive integers $a, b, c$ satisfying $a^2 + b^2 = c^r$ are given by (cf. [Co, p.466])

$$a = |A|, \quad b = |B|, \quad c = m^2 + n^2, \tag{i}$$

where integers $m, n, A$ and $B$ satisfy the condition

$$m > n > 0, \quad \gcd(m, n) = 1, \quad m \not\equiv n \pmod 2$$

and $A + B\sqrt{-1} = (m + n\sqrt{-1})^r$. There are a number of partial results in this case. Many of them concern the case where $m \equiv 2 \pmod 4$ or $n = 1$. Some well-known results in the case $n = 1$ are as follows.

**Proposition 2.1.1** *Let $r = 2$, and let $a, b, c$ be given by* (i). *Assume that $n = 1$. Then Conjecture 0.1.1 is true.*

This is just Proposition 1.2.1 and it can be proved only by elementary considerations.

All of other known results on Conjecture 0.1.1 concern the case where $r \geq 3$ is odd (as far as the author knows). Historically, Terai first started to study such case and gave some partial results (see [Te, Te2]). After several works on the case $r \in \{3, 5\}$, Cao and Dong [CD2] succeeded in extending them as follows.

**Proposition 2.1.2** *Let $r \in \{3, 5\}$, and let $a, b, c$ be given by* (i)*. Assume that $n = 1$. Then Conjecture 0.1.1 is true, that is, for each positive even integer $m$, the equation*

$$(m^3 - 3m)^x + (3m^2 - 1)^y = (m^2 + 1)^z$$

*has the unique solution $(x, y, z) = (2, 2, 3)$ in positive integers $x, y$ and $z$, and the equation*

$$(m|m^4 - 10m^2 + 5|)^x + (5m^4 - 10m^2 + 1)^y = (m^2 + 1)^z$$

*has the unique solution $(x, y, z) = (2, 2, 5)$ in positive integers $x, y$ and $z$.*

In the proof of this result, Cao and Dong used results on lower bounds for linear forms in the logarithms and on generalized Fermat equations. The former are used to obtain sharp upper bounds for solutions and the latter are used to reduce divisibility properties of solutions.

Later, some authors started to consider infinite pairs $(r, m)$ and showed similar results under certain assumptions. In particular, Le [Lem3] gave the following which is one of the most progressive results in this direction (see also [Lem2, Lem5]).

**Proposition 2.1.3** *Let $r$ be a positive integer such that $r \equiv 5 \pmod 8$, and let $a, b, c$ be given by* (i)*. Assume that $m > r^2, r < 11500$ or $m > 2r/\pi, r > 11500$, and that $n = 1$. Then Conjecture 0.1.1 is true.*

In the proof of this result, Le used similar tools as those of Proposition 2.1.2, in addition, he appealed to a celebrated result on the existence of primitive divisors of Lucas and Lehmer sequences due to Bilu, Harnot and Voutier [BHV], where the additional method is similar to that of [HY]. By Proposition 2.1.3, we see, for each $r$ with $r \equiv 5 \pmod 8$, that Conjecture 0.1.1 is true if $n = 1$ except for finite number of $m$'s. Also see [CD, CM, Lem] and their references.

In this chapter we first give results concerning the case where $a, b, c$ are given by (i) as follows.

**Theorem 2.1.1** *Let $r$ be a positive integer such that $r \equiv 4 \pmod 8$, and let $a, b, c$ be given by* (i)*. Assume that $n = 1$. Then Conjecture 0.1.1 is true.*

**Theorem 2.1.2** *Let $r$ be a positive integer such that $r \equiv 6 \pmod 8$, and let $a, b, c$ be given by* (i)*. Assume that $m^2/\log(m^2+1) \geq r^3/\log 2$ and $n = 1$. Then Conjecture 0.1.1 is true.*

Note that exceptional cases of Terai's conjecture are essentially given by a family of triples $(a, b, c) = (2,\ 2^{p-2} - 1,\ 2^{p-2} + 1); p \geq 3$. In fact, letting $p = 5$, we have $(a, b, c) = (2, 7, 3^2)$. So we may think that they essentially come from the case where $p \geq 3$ and $q = r = 2$. For $p \geq 3$, we can find that all of

the relatively prime positive integers $a, b, c$ satisfying $a^p + b^2 = c^2$ are given by (cf. [Co, p.465])

$$a = m^2 - n^2, \quad b = \frac{(m+n)^p - (m-n)^p}{2}, \quad c = \frac{(m+n)^p + (m-n)^p}{2}, \quad \text{(ii)}$$

where integers $m, n$ satisfy the condition

$$m > n > 0, \quad \gcd(m, n) = 1, \quad m \not\equiv n \pmod 2,$$

or

$$a = 2mn, \quad b = |2^{p-2}m^p - n^p|, \quad c = 2^{p-2}m^p + n^p, \quad \text{(iii)}$$

where integers $m, n$ satisfy the condition

$$m > 0, \quad n > 0, \quad \gcd(m, n) = 1, \quad n \equiv 1 \pmod 2.$$

Finally we show results concerning the case where $a, b, c$ are given by (ii) or (iii) as follows.

**Theorem 2.1.3** *Let $p$ be a positive integer such that $p \geq 3$ and $p \equiv 1 \pmod 4$, and let $a, b, c$ be given by* (ii)*. Assume that $n = 1$. Then Conjecture 0.1.1 is true.*

**Theorem 2.1.4** *Let $p$ be a positive integer with $p \geq 3$, and let $a, b, c$ be given by* (iii)*. Assume that $n = 1$. Then Conjecture 0.1.1 is true, that is, for each positive integer $m$ with $m \geq 2$, the equation*

$$(2m)^x + (2^{p-2}m^p - 1)^y = (2^{p-2}m^p + 1)^z \quad \big(x, y, z \in \mathbb{N}\big)$$

*has the unique solution $(x, y, z) = (p, 2, 2)$. Furthermore, if $m = 1$, then all of the solutions of the above equation are given by*

$$(x, y, z) = \begin{cases} (3, t, 2), \ (1, t, 1);\ t \geq 1 & \text{if } p = 3, \\ (p, 2, 2), \ (1, 1, 1) & \text{if } p \geq 4. \end{cases}$$

## 2.2 generalized Fermat equations

Let $P, Q, R$ be non-zero pair-wise relatively prime integers, and let $p, q, r$ be positive integer with $p, q, r \geq 2$. Then the equation

$$PX^p + QY^q = RZ^r,$$

$$X, Y, Z \in \mathbb{Z}, \quad \gcd(X, Y, Z) = 1, \quad XYZ \neq 0$$

is called a *generalized Fermat equation*. As we know, the case where $P = Q = R = 1$ and $p = q = r = n \geq 3$ corresponds to Fermat's last theorem. In this case, Wiles proved that the equation has no solutions. After his work, the interest shifted to the above general equation. In these 20 years many authors have treated special cases of this equation. 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 [Beu, DG]).

In this section we quote many results on generalized Fermat equations. They play a prominent role in the proofs of Theorems 2.1.1 and 2.1.2. They will be used to reduce divisibility properties of exponential variables. In the case $P = Q = R = 1$, for a solution $(X, Y, Z)$ of the above mentioned generalized Fermat equation, we call it non-trivial if $XYZ \neq 0$ and primitive if $\gcd(X, Y, Z) = 1$.

The following two lemmas are classical and well-known results due to Euler and Fermat, respectively.

**Lemma 2.2.1** *The equation*

$$X^3 + Y^3 = 2Z^3$$

*has no integral solutions with* $\gcd(X, Y) = 1$ *and* $XYZ \neq 0, \pm 1$.

**Lemma 2.2.2** *The equation*

$$X^4 + Y^2 = Z^4$$

*has no non-trivial primitive integral solutions.*

**Lemma 2.2.3 ([Co] pp.484–485)** *The equation*

$$X^4 + Y^3 = Z^4$$

*has no non-trivial primitive integral solutions.*

The following two lemmas are given by Cao and Dong in [CD, CD2]. These are deeply based on the results due to Bruin [Br], Darmon and Merel [DM], Poonen [Poo].

**Lemma 2.2.4 ([CD] Theorem 3)** *Let $N$ be a positive integer with $N > 1$. Then the equation*

$$X^{2N} + Y^2 = Z^4$$

*has no non-trivial primitive integral solutions with* $X \equiv 0 \pmod 2$.

**Lemma 2.2.5 ([CD2] Lemma 10)** *Let $N$ be a positive integer with $N > 1$. Then the equation*

$$X^{2N} + Y^4 = Z^2$$

*has no non-trivial primitive integral solutions.*

By using Chabauty's method, Bruin [Br, Br2, Br3] established the following results.

**Lemma 2.2.6 ([Br])** *The equation*

$$X^6 + Y^2 = Z^4$$

*has no non-trivial primitive integral solutions.*

**Lemma 2.2.7 ([Br2])** *The equation*

$$X^3 + Y^3 = Z^4$$

*has no non-trivial primitive integral solutions.*

**Lemma 2.2.8 ([Br3])** *The equation*

$$X^2 + Y^5 = Z^4$$

*has no non-trivial primitive integral solutions other than* $(X, Y, Z) = (\pm 122, -3, \pm 11), (\pm 7, 2, \pm 3)$.

The following was essentially given in [Beu]. Here we use the following formulation.

**Lemma 2.2.9 ([Co] pp.474–475)** *All the non-trivial primitive integral solutions of*

$$X^4 + Y^3 = Z^2$$

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

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

*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* $s \not\equiv 0 \pmod 3$,

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

*where* $s$ *is odd and* $t \not\equiv 0 \pmod 3$,

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

*where* $t$ *is odd and* $t \not\equiv 0 \pmod 3$,

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

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

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

*where $s \not\equiv t \pmod 2$ and $t \not\equiv 0 \pmod 3$,*

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

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

The following lemma plays an prominent role in the proof of Theorem 2.1.1.

**Lemma 2.2.10 ([Iv, Sik])** *Let $n$ be a prime number with $n \geq 7$, and let $\alpha$ be a positive integer with $\alpha \geq 2$. Then the equation*

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

*has no solutions in non-zero pair-wise relatively prime integers $X, Y, Z$ with $XY \neq 1$.*

## 2.3 Preliminaries

Let $r$ be a positive even integer, and let $a, b, c$ be given by (i). Assume that $n = 1$. Then

$$a = |A|, \quad b = |B|, \quad c = m^2 + 1,$$

where $m$ is a positive even integer, and integers $A, B$ are defined by

$$A = m^r - \binom{r}{2} m^{r-2} + \cdots + (-1)^{r/2-1} \binom{r}{r-2} m^2 + (-1)^{r/2},$$

$$B = \binom{r}{1} m^{r-1} - \binom{r}{3} m^{r-3} + \cdots + (-1)^{r/2} \binom{r}{r-3} m^3 + (-1)^{r/2+1} \binom{r}{r-1} m.$$

In this section we prepare some elementary but important lemmas for the proofs of Theorems 2.1.1 and 2.1.2. In what follows, we denote the Jacobi symbol by $\left(\frac{*}{*}\right)$.

**Lemma 2.3.1** *The following hold.*
(i) *If* $r \equiv 0 \pmod 4$, *then* $B \equiv 0 \pmod{2m(m^2-1)}$.
(ii) *If* $r \equiv 2 \pmod 4$, *then* $A \equiv 0 \pmod{m^2-1}$ *and* $B \equiv 0 \pmod{2m}$.

*Proof.* This follows from the definition of $A$ and $B$. □

We consider the equation

$$|A|^x + |B|^y = (m^2+1)^z \tag{2.3.1}$$

where $x, y, z \in \mathbb{N}$.

**Lemma 2.3.2** *Assume that* $r \equiv 4 \pmod 8$. *We write* $r = 4k$, *where* $k \in \mathbb{N}$ *is odd. Let* $(x, y, z)$ *be a solution of* (2.3.1). *Then the following hold.*
(i) *If* $A > 0$ *and* $m \equiv 2 \pmod 4$, *then* $x \equiv z \pmod 2$.
(ii) *If* $A > 0$ *and* $m \equiv 0 \pmod 4$, *then* $x$ *is even.*
(iii) *If* $A > 0$ *and* $m \equiv 4 \pmod 8$, *then* $x$ *and* $z$ *are even.*
(iv) *If* $A < 0$, *then* $x$ *is even.*
(v) *If* $A < 0$ *and* $m \not\equiv 0 \pmod 8$, *then* $x$ *and* $z$ *are even.*

*Proof.* By (i) in Lemma 2.3.1, we know that $b \equiv 0 \pmod{m^2-1}$. Note that $A \equiv 1 \pmod 4$. We observe that

$$\begin{aligned} A &= m^{4k} - \binom{4k}{2} m^{4k-2} + \cdots - \binom{4k}{4k-2} m^2 + 1 \\ &\equiv 1 - \binom{4k}{2} + \cdots - \binom{4k}{4k-2} + 1 \\ &\equiv \Re((1+\sqrt{-1})^{4k}) \\ &\equiv 4^k \cos(k\pi) \pmod{m^2-1}. \end{aligned}$$

Hence $a \equiv -\mathrm{sgn}(A) 4^k \pmod{m^2-1}$ since $k$ is odd. Then, taking (2.3.1) modulo $m^2-1$ and $m-1$, we have

$$\left(\frac{-\mathrm{sgn}(A)}{m^2-1}\right)^x = \left(\frac{2}{m^2-1}\right)^z, \quad \left(\frac{-\mathrm{sgn}(A)}{m-1}\right)^x = \left(\frac{2}{m-1}\right)^z,$$

respectively.

(i) Assume that $A > 0$ and $m \equiv 2 \pmod 4$. Then the first equality above shows that $(-1)^x = (-1)^z$ since $m^2 - 1 \equiv 3 \pmod 8$. Hence $x \equiv z \pmod 2$.

(ii) Assume that $A > 0$ and $m \equiv 0 \pmod 4$. Then the first equality above shows that $(-1)^x = 1$ since $m^2 - 1 \equiv 7 \pmod 8$. Hence $x$ is even.

(iii) Assume that $A > 0$ and $m \equiv 4 \pmod 8$. Then the second equality above shows that $(-1)^x = (-1)^z$ since $m - 1 \equiv 3 \pmod 8$. It follows from (ii) that $z$ is even.

(iv) Assume that $A < 0$. Then $a = -A \equiv -1 \pmod 4$. Note that $b \equiv 0 \pmod 4$ by (i) in Lemma 2.3.1. So, taking (1) modulo 4, we have $(-1)^x \equiv 1 \pmod 4$. Hence $x$ is even.

(v) By (iv) and similar observations in (i) and (iii), we can prove the desired conclusion. □

**Lemma 2.3.3** *Assume that $r \equiv 6 \pmod 8$. We write $r = 2l$, where $l \in \mathbb{N}$ and $l \equiv 3 \pmod 4$. Let $(x, y, z)$ be a solution of (2.3.1). Then the following hold.*

(i) *If $A > 0$, then $x$ is even.*

(ii) $B \equiv -2^l m \pmod{m^2 - 1}$.

*Proof.* (i) If $A > 0$, then

$$a = A = m^{2l} - \binom{2l}{2} m^{2l-2} + \cdots + \binom{r}{r-2} m^2 - 1 \equiv -1 \pmod 4.$$

Since $B \equiv 0 \pmod 4$ by (i) in Lemma 2.3.1 and $c \equiv 1 \pmod 4$, it follows from (2.3.1) that $(-1)^x \equiv 1 \pmod 4$. Hence $x$ is even.

(ii) From the definition of $B$, we have

$$\begin{aligned} B &= \binom{2l}{1} m^{2l-1} - \binom{2l}{3} m^{2l-3} + \cdots - \binom{2l}{2l-3} m^3 + \binom{2l}{2l-1} m \\ &\equiv \left( \binom{2l}{1} - \binom{2l}{3} + \cdots - \binom{2l}{2l-3} + \binom{2l}{2l-1} \right) m \\ &\equiv m \Im\big((1 + \sqrt{-1})^{2l}\big) \\ &\equiv 2^l m \sin(l\pi/2) \pmod{m^2 - 1}. \end{aligned}$$

Hence $B \equiv -2^l m \pmod{m^2 - 1}$ since $l \equiv 3 \pmod 4$. □

**Lemma 2.3.4** *Let $(x, y, z)$ be a solution of (2.3.1). Then the following hold.*

(i) *If $x$ and $z$ are even, then $x \leq 4y - 2$.*

(ii) *If $x, y$ and $z$ are even, then $(r/4)\max(x, y) < z < r \min(x, y)$.*

*Proof.* Since $\{a, b, c^{r/2}\}$ forms a primitive Pythagorean triple and $b$ is even, there exist positive integers $i$ and $j$ such that $a = i^2 - j^2$, $b = 2ij$ and $c^{r/2} = i^2 + j^2$. This implies that $a^2 > b$ and $\max(a, b) < c^{r/2} < \min(a^2, b^2)$.

(i) If $x$ and $z$ are even, then

$$a^{2y} > b^y = (c^{z/2} + a^{x/2})(c^{z/2} - a^{x/2}) \geq c^{z/2} + a^{x/2} > a^{x/2}.$$

This gives the desired conclusion.

(ii) Since $\{a^{x/2}, b^{y/2}, c^{z/2}\}$ forms a primitive Pythagorean triple and $b$ is even, there exist positive integers $s$ and $t$ such that

$$a^{x/2} = s^2 - t^2, \quad b^{y/2} = 2st, \quad c^{z/2} = s^2 + t^2.$$

From this we see that $c^{z/2} = s^2 + t^2 < \min\big((s^2 - t^2)^2, (2st)^2\big) = \min(a^x, b^y)$. Hence we have $c^{z/2} < \min(c^{rx/2}, c^{ry/2})$, which gives that $z < r \min(x, y)$. Further, since $c^{r/2} < \min(a^2, b^2)$, we see that $\max(a^x, b^y) < c^z < \min(a^{4z/r}, b^{4z/r})$, which gives that $(r/4)\max(x, y) < z$. □

## 2.4 Proof of Theorem 2.1.1

In this section we prove Theorem 2.1.1. Let $r$ be a positive integer such that $r \equiv 4 \pmod 8$, and let $a, b, c$ be given by (i). Assume that $n = 1$. In this case, $A$ and $B$ are given by

$$A = m^r - \binom{r}{2} m^{r-2} + \cdots - \binom{r}{r-2} m^2 + 1,$$
$$B = \binom{r}{1} m^{r-1} - \binom{r}{3} m^{r-3} + \cdots + \binom{r}{r-3} m^3 - \binom{r}{r-1} m.$$

We put $a = |A|$, $b = |B|$ and $c = m^2 + 1$.

Let $(x, y, z)$ be a solution of (2.3.1). We prepare several lemmas. First we dispose of the case $y = 1$.

**Lemma 2.4.1** *$y > 1$.*

*Proof.* Taking (2.3.1) modulo $m^3$, we have

$$-\frac{r}{2}(r-1)m^2 x + b^y \equiv m^2 z \pmod{m^3}.$$

Suppose that $y = 1$. Then

$$-\frac{r}{2}(r-1)m^2 x \pm rm \equiv m^2 z \pmod{m^3}.$$

It is clear from this congruence that $r$ is divisible by $m$, and

$$-\frac{r}{2}(r-1)x \pm \frac{r}{m} \equiv z \pmod{m}. \tag{2.4.1}$$

Toward a contradiction, we will show that $x$ and $z$ must be even. Note that $m$ is not divisible by 8 since $m$ divides $r$. Then, by Lemma 2.3.2, it suffices to consider the case where $m \equiv 2 \pmod 4$ and $x \equiv z \pmod 2$. In this case, $r/m$ is even, so we can observe from (2.4.1) that $z$ is even. Hence $x$ and $z$ must be even. Then $x = 2$ by (i) in Lemma 2.3.4. Hence $a^2 + b^2 = c^r$ and $a^2 + b = c^z$. This yields $b(b-1) = c^z(c^{r-z} - 1)$. So $c^z$ divides $b - 1$ since $\gcd(b, c) = 1$. In particular, $c^z \leq b - 1$ $(< b)$. But this is a contradiction since $a^2 + b = c^z$. □

**Lemma 2.4.2** *$x$ is even and $z$ is divisible by 4.*

*Proof.* From Lemma 2.4.1 we know that $y > 1$. Then $b^y \equiv 0 \pmod{4m^2}$ by (i) in Lemma 2.3.1. Taking (2.3.1) modulo $4m^2$, we have $-r(r-1)m^2 x/2 \equiv m^2 z \pmod{4m^2}$, so

$$-\frac{r}{2}(r-1)x \equiv z \pmod 4. \tag{2.4.2}$$

Hence $z$ is even since $r/2$ is even. Further, by (i), (ii) and (iv) in Lemma 2.3.2, we see that $x$ is also even. It follows from (2.4.2) that $z$ is divisible by 4. □

By Lemma 2.4.2, we can write $x = 2X$ and $z = 4Z$, where $X, Z \in \mathbb{N}$.

Next, we will prove that $y \leq 3$ if $y$ is odd. For this we will use many results on generalized Fermat equations quoted in the previous section. This step is crucial in the proof.

We define positive even integers $D, E$ as follows:

$$b^y = DE, \tag{2.4.3}$$

where

$$D = c^{2Z} + a^X, \quad E = c^{2Z} - a^X. \tag{2.4.4}$$

It is easy to observe that $\gcd(D, E) = 2$. Then, by (2.4.3) and (2.4.4), we can write

$$D = 2u^y,\ E = 2^{\alpha y - 1} v^y \quad \text{or} \quad D = 2^{\alpha y - 1} u^y,\ E = 2v^y, \tag{2.4.5}$$

where $u$ and $v$ are relatively prime positive odd integers, and $2^\alpha$ is the exact power of 2 in $b$. Note that $\alpha \geq 2$ by (i) in Lemma 2.3.1. By (2.4.4) and (2.4.5), we have

$$u^y + 2^{\alpha y - 2} v^y = c^{2Z} \quad \text{or} \quad 2^{\alpha y - 2} u^y + v^y = c^{2Z}. \tag{2.4.6}$$

We remark that

$$\alpha y - 2 \geq 2, \quad uv \neq 1.$$

If $uv = 1$, then $u = v = 1$. This implies that $2^{\alpha y - 2} = (c^Z + 1)(c^Z - 1)$. Since $c \equiv 1 \pmod 4$, so we have $c^Z + 1 = 2$, which is clearly absurd.

**Lemma 2.4.3** *If $y$ is odd, then $y = 3$.*

*Proof.* Suppose that $y$ is odd. Then we see from Lemmas 2.2.8, 2.2.10, 2.4.1 and (2.4.6) that $y$ must be a power of 3. Hence we can write $y = 3Y$, where $Y \in \mathbb{N}$, and

$$(c^Z)^4 + (-b^Y)^3 = (a^X)^2.$$

By Lemma 2.2.9, we find that

$$\begin{aligned} c^Z &= \pm(s^6 + 40s^3t^3 - 32t^6), \\ b^Y &= 8st(s^3 - 16t^3)(s^3 + 2t^3), \\ a^X &= \pm(s^6 - 176s^3t^3 - 32t^6)(s^6 + 32t^6), \end{aligned} \tag{2.4.7}$$

where $s$ and $t$ are non-zero relatively prime integers satisfying $s \equiv 1 \pmod 2$ and $s \not\equiv t \pmod 3$.

Here we suppose that $Y > 1$. Then we can write $Y = 3Y'$ where $Y' \in \mathbb{N}$ (since $y = 3Y$ is a power of 3). Rewriting the second equality in (2.4.7), we have

$$(b^{Y'}/2)^3 = st(s^3 - 16t^3)(s^3 + 2t^3). \tag{2.4.8}$$

Since the left-hand side of (2.4.8) is even and $s$ is odd, we see that $t$ is even. Let $g = \gcd(s^3 - 16t^3, s^3 + 2t^3)$. It is easy to see that $g = 1$ or $g \equiv 0 \pmod 3$, and that four factors $s, t, s^3 - 16t^3$ and $s^3 + 2t^3$ on the right-hand side of (2.4.8) are

pair-wise relatively prime if and only if $g = 1$. We claim that $g = 1$; suppose not. Then $s^3 + 2t^3$ is divisible by 3. But this leads to

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

which is absurd. Hence the claim is proved, that is, $g = 1$. It follows from (2.4.8) that $s^3 + 2t^3\,(\neq 0)$ is a perfect third power. But this contradicts Lemma 2.2.1. Therefore, $y = 3$. □

**Lemma 2.4.4** *$y \neq 3$.*

*Proof.* Suppose that $y = 3$. We will observe that this leads to a contradiction. By (i) in Lemma 2.3.4, we see that $X \in \{1, 2, 3, 4, 5\}$. By Lemmas 2.2.3 and 2.2.7, we find that $X \in \{1, 5\}$. We will dispose of the case $X = 5$.

Suppose that $X = 5$. Then, by the third equality in (2.4.7), we can write

$$(\pm a)^5 = FG, \tag{2.4.9}$$

where

$$F = s^6 - 176s^3t^3 - 32t^6, \quad G = s^6 + 32t^6. \tag{2.4.10}$$

It is easy to observe that $F$ and $G$ are relatively prime if and only if $F$ or $G$ is not divisible by 3. We claim that $F$ and $G$ are relatively prime. For this, it suffices to show that $F$ is not divisible by 3 if $G$ is divisible by 3. Suppose that $G$ is divisible by 3. Then, by (2.4.10) and $\gcd(s, t) = 1$, we have $s \not\equiv 0 \pmod 3$ and $t \not\equiv 0 \pmod 3$. So $s^2 \equiv t^2 \equiv 1 \pmod 3$, and $s^3t^3 \equiv st \equiv -1$ since $s \not\equiv t \pmod 3$. These imply that $F \equiv 1 + 176 - 32 \equiv 145 \equiv 1 \pmod 3$. Hence the claim is proved. It follows from (2.4.10) that $G\,(\neq 0)$ is a perfect fifth power.

To sum up, it suffices to show that the equation

$$S^6 + 32T^6 = U^5$$

has no integral solutions with $\gcd(S, T) = 1, STU \neq 0$ and $S \equiv 1 \pmod 2$. Suppose that there is such a solution $(S, T, U)$. Then, by a factorization in $\mathbb{Z}[\sqrt{-2}\,]$, we have

$$(S^3 + 4T^3\sqrt{-2}\,)(S^3 - 4T^3\sqrt{-2}\,) = U^5.$$

Since $S$ is odd (hence $U$ is odd), we can easily observe that two factors on the left-hand side of the above equality are relatively prime in $\mathbb{Z}[\sqrt{-2}\,]$. Then, since the ring $\mathbb{Z}[\sqrt{-2}\,]$ is a unique factorization domain, we can write

$$S^3 + 4T^3\sqrt{-2} = (I + J\sqrt{-2}\,)^5$$

for some non-zero relatively prime integers $I$ and $J$. This gives that

$$S^3 = I(I^4 - 20I^2J^2 + 20J^4), \tag{2.4.11}$$

$$4T^3 = J(5I^4 - 20I^2J^2 + 4J^4). \tag{2.4.12}$$

Since $S$ is odd, we see from (2.4.11) that $I$ is odd. So, by (2.4.12), $J$ must be divisible by 4. We will consider the cases $T \not\equiv 0 \pmod 5$ and $T \equiv 0 \pmod 5$ separately.

First we consider the case where $T \not\equiv 0 \pmod 5$. Then we can observe from (2.4.12) that

$$J = 4M^3, \quad 5I^4 - 20I^2J^2 + 4J^4 = N^3,$$

where $M$ and $N$ are non-zero relatively prime integers. From this, we have

$$N^3 + 16J^4 = 5I^4 - 20I^2J^2 + 20J^4 = 5(I^2 - 2J^2)^2,$$

so

$$N^3 + (4M^2)^6 = 5W^2,$$

where $W = I^2 - 2J^2$. So it suffices to show that the equation

$$x_1^3 + y_1^6 = 5z_1^2$$

has no integral solutions with $x_1y_1z_1 \neq 0$. If there is such a solution $(x_1, y_1, z_1)$, then it induces a rational point $(X_1, Y_1) = (x_1/y_1^2,\ z_1/25y_1^3)$ on the elliptic curve

$$Y_1^2 = X_1^3 + 125. \tag{2.4.13}$$

Since this is 900B1 in Cremona's tables [Cr], we find that elliptic curve (2.4.13) has no rational points other than $(X_1, Y_1) = (-5, 0)$ and the point at infinity. This implies that $z_1 = 0$, which is a contradiction.

Finally we consider the case where $T \equiv 0 \pmod 5$. Then $S \not\equiv 0 \pmod 5$ since $\gcd(S, T) = 1$. In this case, we can observe from (2.4.11) and (2.4.12) that

$$I = K^3,\ I^4 - 20I^2J^2 + 20J^4 = L^3,$$
$$J = 100M^3,\ 5I^4 - 20I^2J^2 + 4J^4 = 5N^3,$$

where $K, L, M$ and $N$ are non-zero integers with $\gcd(K, L) = 1, \gcd(M, N) = 1$ and $L \not\equiv 0 \pmod 5$. From this, we have

$$L^3 + 80J^4 = I^4 - 20I^2J^2 + 100J^4 = (I^2 - 10J^2)^2,$$

so

$$L^3 + 125(20M^2)^6 = W^2,$$

where $W = I^2 - 10J^2$. So it suffices to show that the equation

$$x_2^3 + 125y_2^6 = z_2^2$$

has no integral solutions with $x_2y_2z_2 \neq 0$. But, if there is such a solution $(x_2, y_2, z_2)$, then it induces a rational point $(X_1, Y_1) = (x_2/y_2^2,\ z_2/y_2^3)$ on the elliptic curve (2.4.13) as seen before, and so we have the same contradiction.

Therefore, $x = 2X = 2$, so $a^2 + b^2 = c^r$ and $a^2 + b^3 = c^z$. This implies that $b^2(b-1) = c^r(c^{z-r} - 1)$. Hence $c^r$ divides $b-1$ since $\gcd(b, c) = 1$. In particular, $c^r \leq b - 1\ (< b)$. But this is absurd since $a^2 + b^2 = c^r$. □

We are ready to prove Theorem 2.1.1.

*Proof of Theorem 2.1.1.* Assume the hypothesis of Theorem 2.1.1. Let $(x, y, z)$ be a solution of (i). By Lemmas 2.4.1-2.4.4, we see that $x, y$ are even and $z$ is divisible by 4. Then $y = 2$ by Lemma 2.2.4. It follows from (i) in Lemma 2.3.4 that $x \in \{2, 4, 6\}$. Further, by Lemmas 2.2.2 and 2.2.6, we see that $x \notin \{4, 6\}$. Therefore, $x = 2$, so $z = r$. This completes the proof of Theorem 2.1.1. □

## 2.5 Proof of Theorem 2.1.2

In this section we prove Theorem 2.1.2. Let $r$ be a positive integer such that $r \equiv 6 \pmod 8$, and let $a, b, c$ be given by (i). Assume that $n = 1$. In this case, $A$ and $B$ are given by

$$A = m^r - \binom{r}{2} m^{r-2} + \cdots + \binom{r}{r-2} m^2 - 1,$$
$$B = \binom{r}{1} m^{r-1} - \binom{r}{3} m^{r-3} + \cdots - \binom{r}{r-3} m^3 + \binom{r}{r-1} m.$$

We put $a = |A|$, $b = |B|$ and $c = m^2 + 1$. In what follows, we consider the case where

$$\frac{m^2 \log 2}{\log(m^2+1)} \geq r^3. \tag{2.5.1}$$

Then

**Lemma 2.5.1** *We have $m > r^{1.5}$. In particular, $m > 2r/\pi$.*

*Proof.* This easily follows from (2.5.1). □

**Lemma 2.5.2** *Both $A$ and $B$ are positive, that is, $a = A$ and $b = B$.*

*Proof.* We define the real number $\theta$ $(0 < \theta < \pi/2)$ by

$$\tan\theta = \frac{1}{m}.$$

Since $A = c^{r/2}\cos(r\theta)$ and $B = c^{r/2}\sin(r\theta)$, it follows from Lemma 2.5.1 that

$$0 < r\theta = r \arctan\left(\frac{1}{m}\right) < \frac{r}{m} < \frac{\pi}{2}.$$

Hence $A$ and $B$ are positive. □

Let $(x, y, z)$ be a solution of (2.3.1). We prepare several lemmas.

**Lemma 2.5.3** *$x, y$ and $z$ are all even.*

*Proof.* Since $A > 0$ by Lemma 2.5.2, we see that $x$ is even by (i) in Lemma 2.3.3. It is easy to see that $m$ divides $r$ if $y = 1$ (as seen in the proof of Lemma 2.4.1). Hence $y > 1$ by Lemma 2.5.1. Then $z$ is even by (2.4.2). Finally we show that $y$ is even. In view of (2.3.1), (ii) in Lemma 2.3.1, (ii) in Lemma 2.3.3 and Lemma 2.5.2, we have

$$1 = \left(\frac{-2m}{m^2-1}\right)^y = (-1)^y.$$

Hence $y$ is even. □

Next we obtain sharp upper and lower bounds for $y$. By Lemma 2.5.3, we can write $x = 2X$, $y = 2Y$ and $z = 2Z$, where $X, Y, Z \in \mathbb{N}$. Since $\{a^X, b^Y, c^Z\}$ forms a primitive Pythagorean triple, we can write

$$a^X = s^2 - t^2, \tag{2.5.2}$$

$$b^Y = 2st, \tag{2.5.3}$$

$$c^Z = s^2 + t^2, \tag{2.5.4}$$

where integers $s, t$ satisfy the condition $s > t > 0$, $\gcd(s,t) = 1$ and $s \not\equiv t \pmod 2$.

**Lemma 2.5.4** *$X$ is odd.*

*Proof.* Suppose that $X$ is even. Then, by Lemma 2.2.5, we see that $Y$ must be 1, that is, $y = 2$. This forces $x = 4$ by (i) in Lemma 2.3.4. Then, by (2.4.2), we see that $z$ must be divisible by 4, which contradicts Lemma 2.2.2. □

We denote the 2-adic valuation by $\mathrm{ord}_2$. Put $\alpha = \mathrm{ord}_2(m)$. Then $\mathrm{ord}_2(b) = 2^{\alpha+1}$ since $r \equiv 2 \pmod 4$.

**Lemma 2.5.5** *We have*

$$Y = \frac{\mathrm{ord}_2(u+v)}{\alpha+1}$$

*for some integers $u$ and $v$ satisfying $u > v > 0$, $\gcd(u,v) = 1$ and $uv = a$. In particular,*

$$Y \le \frac{r\log(m^2+1)}{4\log 2}.$$

*Proof.* Since $\gcd(s,t) = 1$ and $s \not\equiv t \pmod 2$, we observe that $\gcd(s+t, s-t) = 1$. Then, by (2.5.2), we can write

$$s + t = u^X, \quad s - t = v^X, \tag{2.5.5}$$

where integers $u, v$ satisfy the condition $u > v > 0$, $\gcd(u,v) = 1$ and $uv = a$. Note that $u, v$ are odd since $a = A \equiv -1 \pmod 4$. By (2.5.2) and Lemma 2.5.4, we have $s^2 - t^2 \equiv -1 \pmod 4$. This implies that $s$ is even and $t$ is odd. Since $\mathrm{ord}_2(b) = 2^{\alpha+1}$, it follows from (2.5.3) and (2.5.5) that

$$(\alpha+1)Y = \mathrm{ord}_2(2s) = \mathrm{ord}_2((u+v)w),$$

where

$$w = \frac{u^X + v^X}{u+v} = u^{X-1} - u^{X-2}v + \cdots - uv^{X-2} + v^{X-1}$$

is an integer. Since $u, v$ and $X$ are all odd, we see that $w$ is odd, and so $(\alpha+1)Y = \mathrm{ord}_2(u+v)$, that is, $Y = \mathrm{ord}_2(u+v)/(\alpha+1)$. The second assertion follows from

$$\mathrm{ord}_2(u+v) \le \frac{\log(u+v)}{\log 2} \le \frac{\log(uv+1)}{\log 2} = \frac{\log(a+1)}{\log 2} \le \frac{\log(c^{r/2})}{\log 2}. \ \square$$

We obtain a lower bound for $Y$ by a usual congruence reduction.

**Lemma 2.5.6** *If $Y > 1$, then*

$$Y > \frac{m^2}{2r(2r-1)}.$$

*Proof.* Suppose that $Y > 1$. Then $b^{2Y} \equiv 0 \pmod{m^4}$ by (ii) in Lemma 2.3.1. Taking (2.3.1) modulo $m^4$, we have $-r(r-1)m^2X \equiv 2m^2Z \pmod{m^4}$, so

$$-r(r-1)X \equiv 2Z \pmod{m^2}. \tag{2.5.6}$$

In particular, $m^2 \leq r(r-1)X + 2Z$. We know from (ii) in Lemma 2.3.4 that $rX < 4Z$ and $Z < rY$. Hence

$$m^2 < 4Z(r-1) + 2Z = 2Z(2r-1) < 2r(2r-1)Y,$$

so the desired conclusion holds. □

We are ready to prove Theorem 2.1.2.

*Proof of Theorem 2.1.2.* Assume the hypothesis of Theorem 2.1.2. Let $(x, y, z)$ be a solution of (2.3.1). By Lemma 2.5.3, we can write $x = 2X$, $y = 2Y$ and $z = 2Z$, where $X, Y, Z \in \mathbb{N}$. Suppose that $y > 1$. Then, by Lemmas 2.5.5 and 2.5.6, we find that

$$\frac{2m^2}{r(2r-1)} < \frac{r\log(m^2+1)}{\log 2},$$

or

$$\frac{m^2\log 2}{\log(m^2+1)} < \frac{r^2(2r-1)}{2}.$$

But this contradicts (2.5.1). Hence $Y = 1$. Then taking (2.3.1) modulo $m^4$, we have $-r(r-1)m^2X + r^2m^2 \equiv 2m^2Z \pmod{m^4}$, so

$$r(r-1)X - r^2 + 2Z \equiv 0 \pmod{m^2}. \tag{2.5.7}$$

On the other hand, we see from (i) in Lemma 2.3.4 and Lemma 2.5.4 that $X \in \{1, 3\}$. Note that $Z < r$ by (ii) in Lemma 2.3.4. If $X = 3$, then, by (2.5.7), we must have $2r^2 - 3r + 2Z \equiv 0 \pmod{m^2}$ and $2r^2 - 3r + 2Z > 0$. Hence

$$r^3 < m^2 \leq 2r^2 - 3r + z < 2r^2 - r$$

by Lemma 2.5.1. This is absurd. Therefore, $x = 2X = 2$, so $z = r$. This completes the proof of Theorem 2.1.2. □

By Theorem 4.2.2, it suffices to consider finite number of $m$'s in order to prove Conjecture 3.1.1 in the case $n = 1$ for a fixed $r \equiv 6 \pmod 8$.

Assume that $r \equiv 6 \pmod 8$ and $n = 1$. We know from Theorem 4.2.2 that Conjecture 3.1.1 is true for any $m \geq m_0$, where $m_0$ is the minimal integer satisfying (2.5.1). Hence we have to treat $m$'s with $m < m_0$. In the range $2r/\pi < m < m_0$, we may assume that solutions $x, y$ and $z$ are all even as seen in the proof of Lemma 2.5.3. From Lemma 2.5.5 we know that $y = 2\mathrm{ord}_2(u+v)/(\alpha+1)$ for

some integers $u, v$ satisfying $u > v > 0$, $\gcd(u, v) = 1$ and $uv = a$. By Lemmas 2.3.4 and 2.5.6, if $y > 2$, then the following conditions:

$$\frac{m^2}{r(2r-1)} < y = \frac{2\mathrm{ord}_2(u+v)}{\alpha+1} \in \mathbb{N},$$
$$2 \le x \le 4y-2, \quad \frac{r\max(x,y)}{4} < z < r\min(x,y)$$

and (2.5.6) must hold. If, for any $m$ with $2r/\pi < m < m_0$ and for any pair $(u, v)$, we verify that not all of the above conditions hold, then we can conclude that $y = 2$. As the proof of Theorem 4.2.2, it suffices to show that the case $x = 6$ does not hold. If we find a contradiction from $x = 6$, then Conjecture 3.1.1 is true for $m$'s with $2r/\pi < m$.

At the end of this section we will demonstrate the above procedure in the case $r = 6$.

**Example 2.5.1** Assume that $r = 6$ and $n = 1$. In this case, $m_0 = 50$ and $3 < 12/\pi < 4$. It is not difficult to show that $y = 2$ in the case $2 < m < 50$ by the above observations. Further, as seen in the proof of Theorem 4.2.2, we see that if $x \neq 2$, then $x = 6$, and so $z = 10$ since $9 < z < 12$ (by (ii) in Lemma 2.3.4) and $z \equiv 0 \pmod 2$. But these imply that $64 \equiv 0 \pmod{m^2}$ by (2.5.7). This forces $m = 4$ or 8, which is a contradiction since $a^6 + b^2 \neq c^{10}$ if $m = 4$ or 8. It remains to consider the case $m = 2$, so we consider the equation

$$117^x + 44^y = 5^z \quad \big(x, y, z \in \mathbb{N}\big). \tag{2.5.8}$$

Taking (2.5.8) modulo 3,5 and 8, we can observe that if $y > 1$, then $x, y$ and $z$ are all even, and that if $y = 1$, then $x$ is even and $z$ is odd. We claim that $y > 1$; suppose not. Then $x$ is even and $z$ is odd. We can write $x = 2X$, where $X \in \mathbb{N}$. Taking (2.5.8) modulo 9, we have $5^z \equiv -1 \pmod 9$. This implies that $z \equiv 0 \pmod 3$. We will observe that this leads to a contradiction. By a factorization in the ring of integers $\mathbb{Q}(\sqrt{-11})$, we have

$$(117^X + 2\sqrt{-11}\,)(117^X - 2\sqrt{-11}\,) = 5^z.$$

Since two factors on the left-hand side of this equality are relatively prime, the class number of $\mathbb{Q}(\sqrt{-11})$ equals to 1 and $z$ is divisible by 3, we can write

$$117^X + 2\sqrt{-11} = \pm\left(\frac{a_1 + b_1\sqrt{-11}}{2}\right)^3$$

for some integers $a_1$ and $b_1$. This leads to

$$\pm 8 \cdot 117^X = a_1(a_1^2 - 33b_1^2),$$
$$\pm 16 = b_1(3a_1^2 - 11b_1^2).$$

By the second equation above, we see that $(a_1, b_1) = (\pm 3, \pm 1)$. Then, by the first equation above, we see that $\pm 8 \cdot 117^X = \pm 72$, which is absurd.

Hence we may assume that $x, y$ and $z$ are all even. Then we can refer the equations (2.5.2)-(2.5.4). As similar arguments in the proof of Lemma 2.5.5,

we can show that $y = \mathrm{ord}_2(u - v)$ for some integers $u, v$ satisfying $u > v > 0$, $\gcd(u, v) = 1$ and $uv = 117$. We observe that $(u, v) = (13, 9)$ or $(117, 1)$. In both cases, we find that $u - v$ is exactly divisible by 4. Hence $y = 2$. It follows from (2.5.2)-(2.5.4) that $s = 11$ and $t = 2$, further, $117^X = 117$ and $5^Z = 125$. Therefore, $X = 1$ and $Z = 3$.

## 2.6 Proof of Theorem 2.1.3

In this section we prove Theorem 2.1.3. Let $p$ be a positive integer such that $p \geq 3$ and $p \equiv 1 \pmod 4$, and let $a, b, c$ be given by (ii). Since $p$ is odd, we see that

$$\begin{aligned} a &= m^2 - 1, \\ b &= \binom{p}{1} m^{p-1} + \binom{p}{3} m^{p-3} + \cdots + \binom{p}{p-2} m^2 + 1, \\ c &= m^p + \binom{p}{2} m^{p-2} + \cdots + \binom{p}{p-3} m^3 + \binom{p}{p-1} m, \end{aligned} \tag{2.6.1}$$

where $m$ is a positive even integer. Note that

$$(m+1)^p = c + b, \quad (m-1)^p = c - b, \quad c < b^2.$$

We consider the equation

$$(m^2 - 1)^x + \left( \frac{(m+1)^p - (m-1)^p}{2} \right)^y = \left( \frac{(m+1)^p + (m-1)^p}{2} \right)^z \tag{2.6.2}$$

where $x, y, z \in \mathbb{N}$.

Let $(x, y, z)$ be a solution of (2.6.2). We prepare some lemmas.

**Lemma 2.6.1** *$z \geq 2$.*

*Proof.* We know that $\gcd(m - 1, m + 1) = 1$ since $m$ is even. Suppose that $z = 1$. We will observe that this leads to a contradiction. Since $b^y < c < b^2$, we see that $y = 1$. Hence $(m^2 - 1)^x = c - b = (m - 1)^p$ by (2.6.2). This implies that $(m - 1)^p \equiv 0 \pmod{m + 1}$, which is absurd since $\gcd(m - 1, m + 1) = 1$. We conclude that $z \geq 2$. □

**Lemma 2.6.2** *$x$ is odd.*

*Proof.* By Lemma 2.6.1, we know that $z \geq 2$. Then taking (2.6.2) modulo $m^2$, we have $(-1)^x + 1 \equiv 0 \pmod{m^2}$. Hence $x$ is odd since $m^2 > 2$. □

**Lemma 2.6.3** *$z = 2$.*

*Proof.* Suppose that $z \geq 3$. We will observe that this leads to a contradiction. Then taking (2.6.2) modulo $m^3$, we see from Lemma 2.6.2 that

$$m^2 x - 1 + \binom{p}{p-2} m^2 y + 1 \equiv 0 \pmod{m^3},$$

so

$$x + \left(\frac{p-1}{2}\right) py \equiv 0 \pmod{m}.$$

Since $m$ and $(p-1)/2$ are even integers, it follows from the above congruence that $x$ is even. But this contradicts Lemma 2.6.2. Hence $z < 3$, so $z = 2$ by Lemma 2.6.1. □

Since $c < b^2$, we see from Lemma 2.6.3 that $b^y < c^2 < b^4$. Hence $y \leq 3$. Therefore, it suffices to observe that the case $y \in \{1, 3\}$ does not hold.

Suppose that $y = 1$. Then $a^x + b = a^p + b^2$, so $b(b-1) = a^p(a^{x-p} - 1)$. Hence $a^p$ divides $b - 1$ since $\gcd(a, b) = 1$. In particular, $a^p \leq b - 1$. On the other hand, we see that $a^p = c^2 - b^2 \geq c + b > b$. This is absurd.

Suppose that $y = 3$. Then $a^x + b^3 = a^p + b^2$, so $b^2(b-1) = a^x(a^{p-x} - 1)$. Hence $b^2$ divides $a^{p-x} - 1$ since $\gcd(a, b) = 1$. In particular, $b^2 \leq a^{p-x} - 1$. On the other hand, we see from (2.6.1) that

$$a^{p-x} \leq a^{p-1} < m^{2p-2} < p^2 m^{2p-2} < b^2,$$

which is absurd. This completes the proof of Theorem 2.1.3.

## 2.7 Proof of Theorem 2.1.4

In this section we prove Theorem 2.1.2. Let $p$ be a positive integer with $p \geq 3$, and let $a, b, c$ be given by (iii). Assume that $n = 1$. In this case, we have

$$a = 2m, \quad b = 2^{p-2}m^p - 1, \quad c = 2^{p-2}m^p + 1.$$

Note that $2m$ always divides $2^{p-2}m^p$.

We consider the equation

$$(2m)^x + (2^{p-2}m^p - 1)^y = (2^{p-2}m^p + 1)^z \tag{2.7.1}$$

where $x, y, z \in \mathbb{N}$.

We will consider the cases $m \geq 2$ and $m = 1$ separately.

### 2.7.1 The case $m \geq 2$

In this subsection we consider the case where $m \geq 2$. Let $(x, y, z)$ be a solution of (2.7.1). We prepare several lemmas.

**Lemma 2.7.1** *$y$ is even.*

*Proof.* Taking (2.7.1) modulo $2m$, we have $(-1)^y \equiv 1 \pmod{2m}$. Hence $y$ is even since $2m > 2$. □

By Lemma 2.7.1, we can write $y = 2Y$, where $Y \in \mathbb{N}$.

**Lemma 2.7.2** *$x \geq p$.*

*Proof.* Taking (2.7.1) modulo $2^{p-2}m^p$, we have $(2m)^x \equiv 0 \pmod{2^{p-2}m^p}$.

Suppose that $x \leq p-1$. We will observe that this leads to a contradiction. Since

$$2^{x-p+2}\, m^{x-p} = \frac{2}{m(2m)^{p-1-x}}$$

and $(2m)^{p-1-x}$ are integers, we see that $m(2m)^{p-1-x}$ is a divisor of 2. Hence $m(2m)^{p-1-x} = 2$ since $m \geq 2$. This implies that $m = 2$ and $x = p-1$. In particular, $2^{p-2}m^p = 2^{2p-2} = 4^{p-1} = 4^x$. Then we can rewrite (2.7.1) as

$$4^x + (4^x - 1)^{2Y} = (4^x + 1)^z.$$

Taking this modulo 3, we have $(-1)^z \equiv 1 \pmod 3$, so $z$ is even. Then, since $\{2^x, (4^x-1)^Y, (4^x+1)^{z/2}\}$ forms a primitive Pythagorean triple, we can write

$$(4^x - 1)^Y = s^2 - t^2, \quad 2^x = 2st,$$

where integers $s, t$ satisfy the condition $s > t > 0$, $\gcd(s,t) = 1$ and $s \not\equiv t \pmod 2$. It is easy to see from the second equation above that $t = 1$, so $s = 2^{x-1}$. Then $s^2 - t^2 < 4^x - 1 \leq (4^x-1)^Y$, which contradicts the first equation above. We conclude that $x \geq p$. □

**Lemma 2.7.3** *$z$ is even.*

*Proof.* We know from Lemma 2.7.2 that $x \geq p$. Since $(2m)^x \equiv 0 \pmod{(2m)^p}$ and

$$(2^{p-2}m^p - 1)^{2Y} \equiv -2^{p-2}m^p(2Y) + 1, \quad (2^{p-2}m^p + 1)^z \equiv 2^{p-2}m^p z + 1 \pmod{(2m)^p},$$

it follows from (2.7.1) that

$$-2^{p-1}m^p Y \equiv 2^{p-2}m^p z \pmod{(2m)^p},$$

so $z \equiv -2Y \pmod 4$. Hence $z$ is even. □

By Lemma 2.7.3, we can write $z = 2Z$, where $Z \in \mathbb{N}$. From (2.7.1) we can define even positive integers $D, E$ as follows:

$$(2m)^x = DE, \tag{2.7.2}$$

where

$$\begin{aligned} D &= (2^{p-2}m^p + 1)^Z + (2^{p-2}m^p - 1)^Y, \\ E &= (2^{p-2}m^p + 1)^Z - (2^{p-2}m^p - 1)^Y. \end{aligned} \tag{2.7.3}$$

Then $\gcd(D, E) = 2$, and

$$D \equiv 1 + (-1)^Y, \quad E \equiv 1 - (-1)^Y \pmod{2^{p-2}m^p}.$$

**Lemma 2.7.4** *$Y$ is odd.*

*Proof.* Suppose that $Y$ is even. Then $D \equiv 2 \pmod{2m}$. This gives that $D/2$ is prime to $m$, so $m^x$ divides $E$ and $D$ divides $2^x$. But this leads to

$$2^x \geq D > E \geq m^x,$$

which is absurd since $m \geq 2$. We conclude that $Y$ is odd. □

By Lemma 2.7.4, we see that $E \equiv 2 \pmod{2m}$. In particular, $E/2$ is prime to $m$. By (2.7.3), we see that $m^x$ divides $D$, and $E$ divides $2^x$. Further, $D \equiv 0 \pmod{2^{p-2}m^p}$.

**Lemma 2.7.5** *$D = 2^{x-1}m^x$ and $E = 2$.*

*Proof.* Suppose that $E > 2$. We will observe that this leads to a contradiction. Since $\gcd(D, E) = 2$ and $E$ is divisible by 4, we see that $D$ is exactly divisible by 2, hence $p = 3$ and $m$ is odd. Furthermore,

$$D = (2m^3 + 1)^Z + (2m^3 - 1)^Y = 2m^x,$$
$$E = (2m^3 + 1)^Z - (2m^3 - 1)^Y = 2^{x-1}.$$

Note that $x \geq 3$. Then

$$0 \equiv E \equiv (-1)^Z - 1 \equiv 0 \pmod{4},$$

so $Z$ is even. We can write $Z = 2Z'$, where $Z' \in \mathbb{N}$. Since $(2m^3 + 1)^{2Z'} = (D + E)/2 = m^x + 2^{x-2}$, and $2m^3 + 1$ is congruent to 3 modulo 4, we see that $x$ is odd. We can write $x = 2X + 1$, where $X \in \mathbb{N}$. It follows that

$$\begin{aligned}(2m^3 - 1)^Y &= (2m^3 + 1)^{2Z'} - 2^{2X} \\ &= \big((2m^3 + 1)^{Z'} + 2^X\big)\big((2m^3 + 1)^{Z'} - 2^X\big)\end{aligned}$$

It is clear that $Y > 1$. Since two factors on the right-hand side of the above equation are relatively prime, we can write

$$(2m^3 + 1)^{Z'} + 2^X = u^Y, \quad (2m^3 + 1)^{Z'} - 2^X = v^Y,$$

where integers $u, v$ satisfy $u > v > 0$ and $uv = 2m^3 - 1$. Subtracting the first equation from the second one, we have

$$(u - v)w = 2^{X+1},$$

where $w = u^{Y-1} + u^{Y-2}v + \cdots + v^{Y-1}$ is a positive integer. Since $w$ is a sum of $Y$ odd integers, we see from Lemma 2.7.4 that $w$ is odd. Hence $w = 1$, so $Y = 1$. This is a contradiction. We conclude that $E = 2$. □

By (2.7.2), (2.7.3) and Lemma 2.7.5, we see that

$$2^{x-2}m^x - 1 = (2^{p-2}m^p - 1)^Y. \tag{2.7.4}$$

If $x > p$, then $2^{p-2}m^pY \equiv 0 \pmod{2^{p-1}m^p}$ by Lemma 2.7.4 and (2.7.4), so $Y$ is even. This contradicts Lemma 2.7.4. It follows from Lemma 2.7.2 that $x = p$. Then $Y = 1$ by (2.7.4), so $z = 2$. This completes the proof of Theorem 4.2.2 in the case $m \geq 2$.

### 2.7.2 The case $m = 1$

In this subsection we consider the case where $m = 1$. Then we can rewrite (2.7.1) as

$$2^x + (2^{p-2} - 1)^y = (2^{p-2} + 1)^z \tag{2.7.5}$$

where $x, y, z \in \mathbb{N}$.

Let $(x, y, z)$ be a solution of (2.7.5). First, we consider the case $p = 3$. Then $2^x + 1^y = 3^z$. As is well-known, this implies that $(x, z) = (1, 1)$ or $(3, 2)$, and $y \geq 1$ arbitrary.

In what follows, we consider the case $p \geq 4$. It is easy to see that

$$y < 2z.$$

First, we want to obtain a sharp upper bound for $z$. We here use the following result due to Scott and Styer ([SS]), which is based on technical elementary arguments in quadratic fields (see [Sc]).

**Proposition 2.7.1 ([SS] Theorem 5)** *Let $C$ 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*

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

*we must have*

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

*for $P \geq 3$ and*

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

Using this result, we show the following.

**Lemma 2.7.6** *The following hold.*

(i) $z \leq 2^{p-2} - 1$.

(ii) *If $x$ is odd and $y$ is even, then $z < 2^{p-2} - 1$.*

*Proof.* To apply Proposition 2.7.1 to (2.7.5), we put

$$A = 2^x, \quad B = (2^{p-2} - 1)^y, \quad C = 2^{p-2} + 1, \quad Z = z.$$

Note that $B > 1$ since $p \geq 4$.

(i) By Proposition 2.7.1, we have

$$z \leq \frac{PQ}{2} \leq \frac{2(2^{p-2} - 1)}{2} = 2^{p-2} - 1.$$

(ii) Assume that $x$ is odd and $y$ is even. With the notation in Proposition 2.7.1, we see that $P = 2$, and $Q \leq 2^{p-2} - 1$. It follows from Proposition 2.7.1 that

$$z \leq \frac{Q+1}{2} \leq 2^{p-3} < 2^{p-2} - 1. \ \square$$

We consider the cases $x > 1$ and $x = 1$ separately.

**Lemma 2.7.7** *If $x > 1$, then $(x, y, z) = (p, 2, 2)$.*

*Proof.* Assume that $x > 1$. It is easy to see that if $z = 1$, then $x = y = 1$ by (2.7.5). Hence $z > 1$. Then we see that $y$ is even by taking (2.7.5) modulo 4. We can write $y = 2Y$, where $Y \in \mathbb{N}$. Taking (2.7.5) modulo $2^{p-2}$, we have $2^x \equiv 0 \pmod{2^{p-2}}$. This means that $x \geq p-2$.

To complete the proof, it suffices to show that $x \geq p-1$. In fact, if $x \geq p-1$, then we see that $z$ is even by taking (2.7.5) modulo $2^{p-1}$, further, by similar observations in the case $m \geq 2$, we can obtain $(x, y, z) = (p, 2, 2)$.

Suppose that $x = p-2$. We will observe that this leads to a contradiction. Then, by the above remark, we may assume that $z$ is odd. We can rewrite (2.7.5) as

$$2^{p-2} + (2^{p-2} - 1)^{2Y} = (2^{p-2} + 1)^z. \tag{2.7.6}$$

If $p$ is even, then $2^{p-2} \equiv 1 \pmod 3$, so $(-1)^z \equiv 1 \pmod 3$. This means that $z$ is even. So we may assume that $p$ is odd (hence $x$ is odd). Then, by a factorization in $\mathbb{Z}[\sqrt{-2}\,]$, we see from (2.7.6) that

$$\big((2^{p-2} - 1)^Y + 2^{\frac{p-3}{2}}\sqrt{-2}\big)\big((2^{p-2} - 1)^Y - 2^{\frac{p-3}{2}}\sqrt{-2}\big) = (2^{p-2} + 1)^z.$$

It is easy to see that two factors on the left-hand side of the above equality are relatively prime in a unique factorization domain $\mathbb{Z}[\sqrt{-2}\,]$. Hence we can write

$$(2^{p-2} - 1)^Y + 2^{\frac{p-3}{2}}\sqrt{-2} = (u + v\sqrt{-2}\,)^z, \tag{2.7.7}$$

where integers $u, v$ satisfy $u^2 + 2v^2 = 2^{p-2} + 1$. Note that $u$ is odd and $v$ is even (since $u^2 + 2v^2 \equiv 1 \pmod 4$). Comparing the coefficients of $\sqrt{-2}$ in (2.7.7), we have

$$2^{\frac{p-3}{2}} = zu^{z-1}v - 2\binom{z}{3}u^{z-3}v^3 + \cdots + (-1)^{\frac{z-1}{2}}2^{\frac{z-1}{2}}v^z. \tag{2.7.8}$$

Since $u, z$ are odd, we see that the right-hand side of the above equality is exactly divisible by the exact power of 2 in $v$. On the other hand, it is clear from (2.7.8) that $v$ divides $2^{\frac{p-3}{2}}$. Then $v = \pm 2^{\frac{p-3}{2}}$, so $u = \pm 1$. Dividing (2.7.8) by $v$, we have

$$\pm 1 = z - 2\binom{z}{3}v^2 + \cdots + (-1)^{\frac{z-1}{2}}2^{\frac{z-1}{2}}v^{z-1}.$$

This implies that $z \equiv \pm 1 \pmod{2^{p-2}}$ since $2v^2 = 2^{p-2}$. Hence $z \geq 2^{p-2} - 1$. But this contradicts (ii) in Lemma 2.7.6. □

**Lemma 2.7.8** *If $x = 1$, then $(x, y, z) = (1, 1, 1)$.*

*Proof.* Assume that $x = 1$. Then

$$2 + (2^{p-2} - 1)^y = (2^{p-2} + 1)^z. \tag{2.7.9}$$

Taking (2.7.9) modulo 4, we see that $y$ is odd. Since

$$(2^{p-2} - 1)^y \equiv 2^{p-2}y - 1, \quad (2^{p-2} + 1)^z \equiv 2^{p-2}z + 1 \pmod{2^{2p-4}},$$

it follows from (2.7.9) that

$$2 + 2^{p-2}y - 1 \equiv 2^{p-2}z + 1 \pmod{2^{2p-4}},$$

so

$$y \equiv z \pmod{2^{p-2}}.$$

Suppose that $y \neq z$. Since $|z - y| \geq 2^{p-2}$ and $y < 2z$, it follows that

$$2^{p-2} \leq |z - y| < z.$$

This contradicts (i) in Lemma 2.7.6. Hence $y = z$, so $y = z = 1$ by (2.7.9). □

Lemmas 2.7.7 and 2.7.8 complete the proof of Theorem 4.2.2 in the case $m = 1$, and so Theorem 2.1.4.

# Chapter 3

# Analogous problem of Jeśmanowicz' conjecture

## 3.1 Analogous problem of Jeśmanowicz' conjecture

In this section we propose a similar problem to Conjecture 3.1.1. As mentioned in Chapter 1, Sierpiński [Si] proved that the equation

$$3^x + 4^y = 5^z$$

has the unique solution $(x, y, z) = (2, 2, 2)$ in positive integers $x, y$ and $z$. Later, Jeśmanowicz [Je] further showed similar results for each of the following equations:

$$5^x + 12^y = 13^z, \quad 7^x + 24^y = 25^z, \quad 9^x + 40^y = 41^z, \quad 11^x + 60^y = 61^z,$$

and he proposed his conjecture (Conjecture 3.1.1). It is well-known that, for any primitive Pythagorean triple $(a, b, c)$ satisfying $a^2 + b^2 = c^2$ (we may assume that $b$ is even), we can write

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

where integers $m, n$ satisfy the condition

$$m > n > 0, \quad \gcd(m, n) = 1, \quad m \not\equiv n \pmod 2.$$

We will always consider the above expressions.

A number of special cases of Conjecture 1.1.1 have since been settled. As famous known results, Lu [Lu] proved that the conjecture is true if $n = 1$. This is the first result on the conjecture for an infinite number of triples. Extending some earlier works, Dem'janenko [De] proved that the conjecture is true if $c = b+1$. These results include those of Sierpiński and Jeśmanowicz and are crucially important since they are used in many earlier works. In Chapter 1 we generalized

these results by proving that the conjecture is true if $a \equiv \pm 1 \pmod{b}$ or $c \equiv 1 \pmod{b}$ (Theorems 1.2.1 and 1.2.2). For other known results, see for example [Ca, DC, Miy, Miy2].

On the other hand, for Pythagorean triples studied by Sierpiński and Jeśmanowicz (also, Dem'janenko and others): $(a, b, c) =$

$$(3, 4, 5), \quad (5, 12, 13), \quad (7, 24, 25), \quad (9, 40, 41), \quad (11, 60, 61),$$

we observe that

$$5^x + 12^y = 13^z, \quad 7^x + 24^y = 25^z, \quad 9^x + 40^y = 41^z, \quad 11^x + 60^y = 61^z,$$

that is, $c + b = a^2$. Note that $c = b + 1$ for each of the above cases. So it is worth studying a variant of (1):

$$c^x + b^y = a^z \tag{3}$$

where $x, y, z \in \mathbb{N}$. We propose an analogue of Conjecture 1.1.1 which we call the *shuffle* variant of Jeśmanowicz' problem.

**Conjecture 3.1.1** *Let $(a, b, c)$ be a primitive Pythagorean triple such that $a^2 + b^2 = c^2$ and $b$ is even. Then (3) has the unique solution $(x, y, z) = (1, 1, 2)$ if $c = b + 1$, and no solutions if $c > b + 1$.*

If $c = b + 1$, then, since $a^2 = c^2 - b^2 = (c + b)(c - b) = c + b$, we find that (3) always has the solution $(x, y, z) = (1, 1, 2)$. We remark that $c = b + 1$ if and only if $m = n + 1$.

We will prove that Conjecture 3.1.1 is true if $c \equiv 1 \pmod{b}$.

**Theorem 3.1.1** *If $c \equiv 1 \pmod{b}$, then Conjecture 3.1.1 is true.*

Clearly, this is an analogue of Theorem 1.2.2. In the proof of Theorem 3.1.1, we use similar techniques in the proof of Theorem 1.2.2, and further, a result on lower bounds for linear forms in the logarithms of algebraic numbers based on Baker's theory.

In the next section we prove that Conjecture 3.1.1 is true if $n = 1$ (which can be regarded as an analogue of the result in Proposition 1.2.1. This is an important step in the proof. In fact, if $n > 1$, then we can use the parameters $\alpha, \beta$ introduced in Section 1.3, which are useful to examine parities of exponential variables $x, y$ and $z$. It is crucially important to know parities of them for Conjecture 3.1.1. Using them, we prove that (3) has no solutions if $c \equiv 1 \pmod{b}$ and $c > b + 1$. In the final section we prove that (3) has the unique solution $(x, y, z) = (1, 1, 2)$ if $c = b + 1$ by using various elementary arguments and the known result on lower bounds for linear forms in two logarithms due to Mignotte [Mi].

In what follows, we consider the equation

$$(m^2 + n^2)^x + (2mn)^y = (m^2 - n^2)^z \tag{3.1.1}$$

where $x, y, z \in \mathbb{N}$.

## 3.2 Linear forms in two logarithms

In this section we quote a preliminary result on linear forms in two logarithms. We are interested in only rational integral cases.

The following is an immediate consequence of the corollary ([Mi, pp.110–111]).

**Lemma 3.2.1** *Let $\alpha_1$ and $\alpha_2$ be relatively prime positive integers greater than 1. We consider the linear form*

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

*where $b_1$ and $b_2$ are positive integers. Let $\rho, \lambda, a_1, a_2$ be real positive numbers such that $\rho \geq 4$, $\lambda = \log \rho$,*

$$a_i \geq (\rho + 1) \log \alpha_i$$

*for $1 \leq i \leq 2$, and*

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

*Further, let $h$ be a real number such that*

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

*We put $\chi = h/\lambda$ and $v = 4\chi + 4 + 1/\chi$. Then we have the lower bound*

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

*where*

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

Using this lemma, we prove the following.

**Lemma 3.2.2** *Let $(x, y, z)$ be a solution of (3.1.1). If $y = 1$, then $x < 4020 \log a$.*

*Proof.* Let $(x, y, z)$ be a solution of (3.1.1). Assume that $y = 1$, namely,

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

where $a = m^2 - n^2$, $b = 2mn$ and $c = m^2 + n^2$. Note that $a \geq 3$ and $c \geq 5$. Put

$$\Lambda = z \log a - x \log c.$$

Then $\Lambda > 0$. Since

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

we have

$$\log \Lambda < \log b - x \log c.$$

We will obtain a lower bound for $\log \Lambda$ by using Lemma 3.2.1. With the notation in Lemma 3.2.1, we put $(\alpha_1, \alpha_2, b_1, b_2) = (c, a, x, z)$. We may take $a_1 = (\rho+1)\log c$ and $a_2 = (\rho+1)\log a$. Let $\rho = 4.69$ and $\lambda = \log \rho$. Then we see that $a_1 a_2 \geq \max\{20, 4\lambda^2\}$. Since $c^{x+1} - a^z = (c-1)c^x - b \geq 4c - b > 0$, we have $z/\log c < (x+1)/\log a$, so

$$\frac{x}{\log a} + \frac{z}{\log c} < 2s + \frac{1}{\log a} \leq 2s + \frac{1}{\log 3},$$

where $s = x/\log a$. Then we may take

$$h = \max\left\{ 3.5,\ \log\left(2s + \frac{1}{\log 3}\right) + \log\lambda + 1.4 \right\}.$$

We will treat the two possible choices for $h$ in turn. If $h = 3.5$, then $\log(2s + 1/\log 3) < 1.7$, so $s < e^{1.7}/2 = 2.7$. Hence the lemma holds.

Next we consider the case where

$$h = \log\left(2s + \frac{1}{\log 3}\right) + \log\lambda + 1.4 \geq 3.5.$$

We will find an upper bound for $C_0$. Since $\chi \geq (3.5)/\lambda$ and $v/4 > \chi + 1$ in Lemma 3.2.1, we see that

$$\frac{1}{2\chi(\chi+1)} \leq \frac{\lambda}{(24.5)/\lambda + 7},$$

$$\begin{aligned}\frac{4\lambda}{3v}\left(\frac{1}{a_1} + \frac{1}{a_2}\right) &< \frac{\lambda}{3(\chi+1)(\rho+1)}\left(\frac{1}{\log 3} + \frac{1}{\log 5}\right) \\ &\leq \frac{\lambda}{3((3.5)/\lambda+1)(\rho+1)}\left(\frac{1}{\log 3} + \frac{1}{\log 5}\right),\end{aligned}$$

and

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

Hence $C_0 < 0.7508$. By Lemma 3.2.1, we have

$$-26.25(h+\lambda)^2 \log a \log c < \log \Lambda < \log b - x \log c,$$

so

$$\begin{aligned} s &< \frac{\log b}{\log a \log c} + 26.25(h+\lambda)^2 \\ &\leq \frac{1}{\log 3} + 26.25\left(\log\left(2s + \frac{1}{\log 3}\right) + \lambda + \log\lambda + 1.4\right)^2. \end{aligned}$$

This implies that $s < 4020$. □

## 3.3 Proof of Theorem 3.1.1

In this section we prove Theorem 3.1.1.

### 3.3.1 The case $n = 1$

In this subsection we prove that Conjecture 3.1.1 is true if $n = 1$. When $n = 1$, $m$ may be any even positive integer.

The following can be regarded as an analogue of Proposition 1.2.1.

**Proposition 3.3.1** *If $n = 1$, then Conjecture 3.1.1 is true.*

*Proof.* When $n = 1$, we rewrite (3.1.1) as

$$(m^2+1)^x + (2m)^y = (m^2-1)^z \tag{3.3.1}$$

where $x, y, z \in \mathbb{N}$ and $m$ is an even positive integer.

Let $(x, y, z)$ be a solution of (3.3.1). Taking (3.3.1) modulo $2m$, we have $(-1)^z \equiv 1 \pmod{2m}$. Hence $z$ is even since $2m \geq 3$. We can write $z = 2Z$, where $Z \in \mathbb{N}$.

Suppose that $y > 1$. We will observe that this leads to a contradiction. Taking (3.3.1) modulo $2m^2$, we have $m^2x+1 \equiv 1 \pmod{2m^2}$, so $x \equiv 0 \pmod 2$. We can write $x = 2X$, where $X \in \mathbb{N}$. From (3.3.1) we define even positive integers $A$ and $B$ as follows:

$$(2m)^y = AB, \tag{3.3.2}$$

where

$$A = (m^2-1)^Z + (m^2+1)^X, \qquad B = (m^2-1)^Z - (m^2+1)^X.$$

It is easy to see that $\gcd(A, B) = 2$ and

$$A \equiv (-1)^Z + 1, \qquad B \equiv (-1)^Z - 1 \pmod{2m}.$$

We claim that $Z$ is odd. Indeed, if $Z$ is even, then $A \equiv 2 \pmod{2m}$, that is, $A/2 \equiv 1 \pmod m$. This means that $A/2$ is odd and prime to $m$. It follows from (3.3.2) that $A = 2$, which is clearly absurd. Hence $Z$ is odd. Then $B \equiv -2 \pmod{2m}$, that is, $B/2 \equiv -1 \pmod m$. This means that $B/2$ is odd and prime to $m$. It follows from (3.3.2) that $B = (m^2-1)^Z - (m^2+1)^X = 2$. Taking this modulo $m^2$, we have $4 \equiv 0 \pmod{m^2}$ since $Z$ is odd. Hence $m = 2$,

so $A = 3^Z + 5^X = 2^{2y-1}$ and $B = 3^Z - 5^X = 2$. But this implies that $3^Z = (A+B)/2 = 4^{y-1} + 1 \equiv 2 \pmod 3$, which is absurd. Therefore, $y = 1$.

Taking (3.3.1) modulo $m^2$, we have $1 + 2m \equiv 1 \pmod{m^2}$, so $2 \equiv 0 \pmod m$. Hence $m = 2$ and $5^x + 4 = 3^{2Z}$. From this we have $5^x = (3^Z + 2)(3^Z - 2)$. Since these two factors are relatively prime, we see that $3^Z - 2 = 1$, so $Z = 1$, hence $x = 1$. This completes the proof of Proposition 3.3.1. □

### 3.3.2 Preliminaries

In this subsection we prepare some lemmas for the proof of Theorem 3.1.1. First, we give lemmas to examine parities of exponential variables $x, y$ and $z$. It is crucially important to know parities of them for Conjecture 3.1.1.

We consider the case where $2\alpha \neq \beta + 1$. The following two lemmas will be used to determine parities of exponential variables. In particular, Lemma 3.3.1 will play an important role in the proof of the theorem.

**Lemma 3.3.1** *Let $(x, y, z)$ be a solution of* (3.1.1). *If $y > 1$, then $x \equiv z \pmod 2$.*

**Lemma 3.3.2** *Let $(x, y, z)$ be a solution of* (3.1.1). *If $x$ and $z$ are even, then $X \equiv Z \pmod 2$, where $X = x/2$ and $Z = z/2$.*

We can prove these lemmas just like as the proofs of Lemmas 1.3.1 and 1.3.2.

### 3.3.3 The case $c \equiv 1 \pmod b$ and $c > b + 1$

In this subsection we prove that (3.1.1) has no solutions if $c \equiv 1 \pmod b$ and $c > b + 1$.

Assume that $c \equiv 1 \pmod b$, or equivalently,

$$m^2 + n^2 = 1 + 2mnt, \tag{3.3.3}$$

where $t \in \mathbb{N}$. Then

$$m^2 \equiv 1 \pmod n, \tag{3.3.4}$$

$$n^2 \equiv 1 \pmod m. \tag{3.3.5}$$

By Proposition 3.3.1, we may assume that $n > 1$. We first prove an important lemma.

**Lemma 3.3.3** *With the notation in* (1.3.1), *we have*
(i) *$m$ or $n$ is divisible by $2t$.*
(ii) *$2\alpha \neq \beta + 1$.*

*Proof.* (i) Since $m > n$, we see from (3.3.3) that $2m^2 > m^2 + n^2 > 2mnt$, so $m > nt$. By (3.3.3), we see that $(U, V) = (m - nt, n)$ is a positive integer solution of the Pellian equation

$$U^2 - (t^2 - 1)V^2 = 1.$$

Since $t+\sqrt{t^2-1}$ is the fundamental solution of the above Pellian equation, all of the pairs $(m,n)$ satisfying (3.3.3) are given by

$$m = U_l + tV_l, \quad n = V_l,$$

where positive integers $U_l$ and $V_l$ are defined by

$$U_l + V_l\sqrt{t^2-1} = (t+\sqrt{t^2-1}\,)^l\,;\, l \geq 1.$$

We will prove (i) by induction on $l$. It is clear for $l=1$. Assume that (i) holds for some positive integer $l$, namely,

$$U_l + tV_l \equiv 0 \pmod{2t} \quad \text{or} \quad V_l \equiv 0 \pmod{2t}.$$

Then $U_{l+1} = tU_l + (t^2-1)V_l$ and $V_{l+1} = U_l + tV_l$. If $U_l + tV_l \equiv 0 \pmod{2t}$, then $V_{l+1} \equiv 0 \pmod{2t}$. If $V_l \equiv 0 \pmod{2t}$, then

$$U_{l+1} + tV_{l+1} = 2tU_l + (2t^2-1)V_l \equiv 0 \pmod{2t}.$$

Hence (i) is proved.

(ii) We consider the case where $m$ is even. As defined in (1.3.1), we put $m = 2^\alpha i$ and $n = 2^\beta j + e$. By (i), we know that $2^\alpha i$ is divisible by $2t$, in particular, $\mathrm{ord}_2(2t) \leq \alpha$ since $i$ is odd. It follows from (3.3.3) that

$$\beta + 1 = \mathrm{ord}_2\left((n-1)(n+1)\right) = \mathrm{ord}_2\left(m(m-2nt)\right) = \alpha + \mathrm{ord}_2(m-2nt).$$

Hence it suffices to check that $\mathrm{ord}_2(m-2nt) \neq \alpha$. If $\mathrm{ord}_2(2t) < \alpha$, then $\mathrm{ord}_2(2nt) < \alpha$, so $\mathrm{ord}_2(m-2nt) = \mathrm{ord}_2(2nt) < \alpha$. If $\mathrm{ord}_2(2t) = \alpha$, then $\mathrm{ord}_2(m-2nt) = \alpha + \mathrm{ord}_2(i - n(2t/2^\alpha)) > \alpha$. Therefore, $2\alpha \neq \beta + 1$. Similarly, we can prove (ii) for the case where $m$ is odd. □

**Lemma 3.3.4** *Let $(x,y,z)$ be a solution of* (3.1.1). *Then $z$ is even.*

*Proof.* Taking (3.1.1) modulo $m$, we have $(n^2)^x \equiv (-n^2)^z \pmod{m}$. Then $(-1)^z \equiv 1 \pmod{m}$ by (3.3.5). Hence $z$ is even since $m > n > 1$. □

The first purpose of this section is to prove the following.

**Proposition 3.3.2** *If $c \equiv 1 \pmod{b}$ with $c > b+1$, then* (3.1.1) *has no solutions with $y > 1$.*

For the proof of Proposition 3.3.2, we further assume that $c > b+1$, that is, $m > n+1$ or $t > 1$. Let $(x,y,z)$ be a solution of (3.1.1). Then $x < z$ since $c > a$. By Lemma 3.3.4, we can write $z = 2Z$, where $Z \in \mathbb{N}$.

Suppose that $y > 1$. We will observe that this leads to a contradiction. By Lemma 3.3.1 and (ii) in Lemma 3.3.3, we see that $x$ is even. We can write $x = 2X$, where $X \in \mathbb{N}$. From (3.1.1) we define even positive integers $D$ and $E$ as follows:

$$(2mn)^y = DE, \tag{3.3.6}$$

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 easy to see that $\gcd(D, E) = 2$. By (3.3.4) and (3.3.5), we have

$$D \equiv (-1)^Z + 1, \quad E \equiv (-1)^Z - 1 \pmod{m}$$

and

$$D \equiv 2, \quad E \equiv 0 \pmod{n}.$$

We prepare some lemmas.

**Lemma 3.3.5** *$X$ and $Z$ are odd.*

*Proof.* By Lemma 3.3.2 and (ii) in Lemma 3.3.3, we know that $X \equiv Z \pmod 2$. Suppose that $X$ and $Z$ are even. Then

$$D \equiv 2 \pmod 4, \quad D \equiv 2 \pmod m, \quad D \equiv 2 \pmod n.$$

This implies that $D/2$ is odd and prime to $mn$. It follows from (3.3.6) that $D = 2$, which is clearly absurd. Therefore, $X$ and $Z$ are odd. □

By Lemma 3.3.5, we have

$$D \equiv 0, \quad E \equiv -2 \pmod m.$$

It is easy to see that $E \equiv 2 \pmod 4$ if $m$ is even, and $D \equiv 2 \pmod 4$ if $m$ is odd.

**Lemma 3.3.6** *$y$ is even.*

*Proof.* First, we consider the case where $m$ is even. Then

$$E \equiv 2 \pmod 4, \quad E \equiv -2 \pmod m, \quad D \equiv 2 \pmod n.$$

This implies that $E/2$ is odd and prime to $m$, and $D$ is prime to $n$. It follows from (3.3.6) that $D = 2^{y-1}m^y$ and $E = 2n^y$. Hence $(m^2 - n^2)^Z = (D + E)/2 = 2^{y-2}m^y + n^y$. Since $Z$ is odd, we see from (3.3.5) that

$$n^y \equiv -1 \pmod m.$$

By (3.3.5), we see that if $y$ is even, then $2 \equiv 0 \pmod m$, so $m = 2$, hence $n = 1$, which is an excluded case. Further, if $y$ is odd, then $n + 1 \equiv 0 \pmod m$, so $m = n + 1$, which is an excluded case.

Next, we consider the case where $m$ is odd. Then

$$D \equiv 2 \pmod 4, \quad E \equiv -2 \pmod m, \quad D \equiv 2 \pmod n.$$

This implies that $D/2$ is odd and prime to $n$, and $E$ is prime to $m$. It follows from (3.3.6) that $D = 2m^y$ and $E = 2^{y-1}n^y$. Hence $(m^2 - n^2)^Z = (D+E)/2 = m^y + 2^{y-2}n^y$. We see from (3.3.4) that

$$m^y \equiv 1 \pmod{n}.$$

Suppose that $y$ is odd. We will observe that this leads to a contradiction. Then $m \equiv 1 \pmod{n}$ by (3.3.4). We can write $m = 1+hn$, where $h \in \mathbb{N}$. Substituting this into (3.3.3), we have

$$np = 2(t-h),$$

where $p = h(h-2t)+1$. By (i) in Lemma 3.3.3, we know that $n$ is divisible by $2t$, so $h$ is divisible by $t$. In particular, $h = t$ or $h \geq 2t$. If $h = t$, then $p = 0$, so $t^2 = 1$, hence $t = 1$, which is an excluded case. If $h \geq 2t$, then $p = h(h-2t)+1 > 0$, so $t - h = (np)/2 > 0$, which is clearly absurd. We conclude that $y$ is even. □

By Lemma 3.3.6 and its proof, we may assume that $m$ is odd and $y$ is even. We can write $y = 2Y$, where $Y \in \mathbb{N}$. Furthermore, we have

$$D = 2m^{2Y}, \quad E = 2^{2Y-1}n^{2Y}.$$

We will obtain sharp upper and lower bounds for solutions.

**Lemma 3.3.7** *$2m \leq Z - X$.*

*Proof.* Taking (3.1.1) modulo $m^2$, we have $(n^2)^{2X} \equiv (n^2)^{2Z} \pmod{m^2}$. We see from (3.3.3) that $n^2 \equiv 1 + 2mnt \pmod{m^2}$. Hence $(1+2mnt)^{2X} \equiv (1+2mnt)^{2Z} \pmod{m^2}$, so $4mntX \equiv 4mntZ \pmod{m^2}$. Similarly, we can prove that $4mntX \equiv 4mntZ \pmod{n^2}$ by taking (3.1.1) modulo $n^2$. Hence $4mntX \equiv 4mntZ \pmod{m^2n^2}$ as $\gcd(m,n) = 1$, so $4tX \equiv 4tZ \pmod{mn}$. By (i) in Lemma 3.3.3, we know that $n$ is divisible by $2t$. Therefore, $2X \equiv 2Z \pmod{m}$, so $X \equiv Z \pmod{m}$ since $m$ is odd. Furthermore, $X \equiv Z \pmod{2m}$ by Lemma 3.3.5. Since $Z > X$, we conclude that $2m \leq Z - X$. □

**Lemma 3.3.8** *We have*

$$Z < 4Y, \quad Y \leq \frac{\log(c-1)}{8\log 2}.$$

*Proof.* Since $\{c^X, b^Y, a^Z\}$ forms a primitive Pythagorean triple, we can write

$$c^X = k^2 - l^2, \quad b^Y = 2kl, \quad a^Z = k^2 + l^2,$$

where integers $k, l$ satisfy the condition $k > l > 0$, $\gcd(k,l) = 1$ and $k \not\equiv l \pmod{2}$. Since $b < a^2$, we see that $a^Z < 4k^2l^2 = b^{2Y} < a^{4Y}$, so

$$Z < 4Y.$$

Since $E = a^Z - c^X = 2l^2$, we have

$$l = 2^{Y-1}n^Y.$$

Further, since $(k+l)(k-l) = c^X$ and $\gcd(k+l, k-l) = 1$, we can write

$$k + l = u^X, \quad k - l = v^X,$$

where odd integers $u, v$ satisfying $u > v > 0$ and $uv = c$. Hence

$$(2n)^Y = 2l = u^X - v^X = (u - v)w,$$

where

$$w = \frac{u^X - v^X}{u - v} = u^{X-1} + u^{X-2}v + \cdots + v^{X-1}$$

is an integer. Since $w$ is a sum of $X$ odd integers, we see from Lemma 3.3.5 that $w$ is odd. Therefore, we obtain

$$(\alpha + 1)Y = \mathrm{ord}_2(u - v).$$

Since $u - v \le u - 1 \le c - 1$, it follows that

$$Y = \frac{\mathrm{ord}_2(u-v)}{\alpha+1} \le \frac{\log(u-v)}{(\alpha+1)\log 2} \le \frac{\log(c-1)}{2\log 2}. \ \square$$

Since $c = m^2 + n^2 \le m^2 + (m-1)^2 = 2m^2 - 2m + 1$, it follows from Lemmas 3.3.7 and 3.3.8 that

$$2m + 2 \le \frac{2\log(2m^2 - 2m)}{\log 2},$$

which is a contradiction. This completes the proof of Proposition 3.3.2.

At the end of this section, we prove the following.

**Proposition 3.3.3** *If* $c \equiv 1 \pmod b$ *and* $c > b+1$*, then* (3.1.1) *has no solutions with* $y = 1$*.*

*Proof.* Assume that $c \equiv 1 \pmod b$ with $c > b + 1$. By Proposition 3.3.1, it suffices to consider the case where $n > 1$. Let $(x, y, z)$ be a solution of (3.1.1). By the same observations in the proof of Lemma 3.3.4, we see that $z$ is even. We can write $z = 2Z$, where $Z \in \mathbb{N}$. Suppose that $y = 1$. We will observe that this leads to a contradiction. By similar observations in the proof of Lemma 3.3.7, we see that $(1 + 2mnt)^x + 2mn \equiv (1 + 2mnt)^z \pmod{m^2n^2}$, so $2tx + 2 \equiv 2tz \pmod{mn}$. It follows from (i) in Lemma 3.3.3 that $2 \equiv 0 \pmod{2t}$, so $t = 1$, that is, $c = b + 1$. This is a contradiction. This completes the proof of Proposition 3.3.3. $\square$

### 3.3.4 The case $c = b + 1$

In this subsection we will complete the proof of Theorem 3.1.1. By Propositions 3.3.2 and 3.3.3, it suffices to prove that if $c = b + 1$, that is, $m = n + 1$, then (3.1.1) has the unique solution $(x, y, z) = (1, 1, 2)$.

When $m = n + 1$, we rewrite (3.1.1) as

$$(2m^2 - 2m + 1)^x + \big(2m(m-1)\big)^y = (2m-1)^z \tag{3.3.7}$$

where $x, y, z \in \mathbb{N}$, and $m$ is a positive integer such that $m \geq 2$. By Proposition 3.3.1, it suffices to consider the case where $m \geq 3$.

Let $(x, y, z)$ be a solution of (3.3.7). Then $z$ is even by Lemma 3.3.4. We can write $z = 2Z$, where $Z \in \mathbb{N}$. First we will show that $y = 1$. For this we consider the case where $m$ is even and the case where $m$ is odd separately.

**Lemma 3.3.9** *If $m$ is even, then $y = 1$.*

*Proof.* Assume that $m$ is even. Suppose that $y > 1$. We will observe that this leads to a contradiction. By Lemma 1.3.1 and (ii) in Lemma 3.3.3, we see that $x$ is even. We can write $x = 2X$, where $X \in \mathbb{N}$. Similarly to the proof of Lemma 3.3.6, we observe that

$$D = (2m-1)^Z + (2m^2-2m+1)^X = 2^{y-1}m^y,$$
$$E = (2m-1)^Z - (2m^2-2m+1)^X = 2(m-1)^y.$$

Then $(2m^2-2m+1)^X = (D-E)/2 = 2^{y-2}m^y - (m-1)^y$. Since $2^{y-2}m^y$ is divisible by $2m$ and $(m-1)^y \equiv (-1)^{y-1}my + (-1)^y \pmod{2m}$, we see that $1 \equiv (-1)^y my + (-1)^{y+1} \pmod{2m}$, that is,

$$(-1)^y + 1 \equiv my \pmod{2m}.$$

From this we have $(-1)^y \equiv -1 \pmod{m}$, so $y$ is odd since $m \geq 3$. Then, however, the above congruence implies that $my \equiv 0 \pmod{2m}$, so $y \equiv 0 \pmod{2}$, which is a contradiction. We conclude that $y = 1$. □

**Lemma 3.3.10** *If $m$ is odd, then $y = 1$.*

*Proof.* Assume that $m$ is odd. Suppose that $y > 1$. We will observe that this leads to a contradiction. By Lemma 1.3.1 and (ii) in Lemma 3.3.3, we see that $x$ is even. We can write $x = 2X$, where $X \in \mathbb{N}$. Similarly to the proof of Lemma 3.3.6, we observe that

$$D = (2m-1)^Z + (2m^2-2m+1)^X = 2m^y,$$
$$E = (2m-1)^Z - (2m^2-2m+1)^X = 2^{y-1}(m-1)^y.$$

If $m = 3$, then $5^Z = (D+E)/2 = 3^y + 4^{y-1}$, which contradicts the result in [Si]. If $y = 2$, then $X = Z = 1$ by the first equation above, which is absurd since $x < z$. Hence $m \geq 5$ and $y \geq 3$. Since $D > E$, it follows that

$$1 < \frac{D}{E} = 4\left(\frac{m}{2(m-1)}\right)^y = 4\left(\frac{5}{8}\right)^y \leq 4\left(\frac{5}{8}\right)^3 = \frac{125}{128},$$

which is a contradiction. We conclude that $y = 1$. □

By Lemmas 3.3.9 and 3.3.10, we rewrite (3.3.7) as

$$(M+1)^x + M = (2M+1)^Z \tag{3.3.8}$$

for $x, Z \in N$ where $M = 2m(m-1)$. Note that $M$ is divisible by 4 (since the product of two consecutive integers $m(m-1)$ is even). It suffices to prove that (3.3.8) has the unique solution $(x, Z) = (1, 1)$.

Let $(x, Z)$ be a solution of (3.3.8). Taking (3.3.8) modulo $M+1$, we have $(-1)^Z \equiv -1 \pmod{M+1}$. Hence $Z$ is odd.

We claim that $x = 1$ if $x \le Z$ or $x + 1 \ge 2Z$. If $x \le Z$, then

$$M \le (2M+1)^x - (M+1)^x \le (2M+1)^Z - (M+1)^x = M.$$

This implies that $x = Z = 1$. If $x + 1 \ge 2Z$, then

$$\begin{aligned}(M+1)^{2Z} &< (M+1)^{2Z} + M(M+1) \\ &\le (M+1)^{x+1} + M(M+1) \\ &= (M+1)(2M+1)^Z \\ &< (M+1)^{Z+1}\, 2^Z,\end{aligned}$$

so

$$\left(\frac{M+1}{2}\right)^{Z-1} < 2.$$

Since $M \ge 4$, it follows that $Z = 1$, so $x = 1$.

To obtain a sharp lower bound for $x$ and some necessary conditions on the existence of solutions of (3.3.8), we prove the following lemma.

**Lemma 3.3.11** *If $x > 1$, then the following hold.*

(i) $2Z \equiv 1 \pmod{M+1}$ *and* $x+1 \equiv 2Z \pmod{2M}$. *In particular, $x$ is odd.*

(ii) $x \ge 2M + 5$.

*Proof.* We know that $Z$ is odd. Suppose that $x > 1$. Then $Z < x$ and $x+1 < 2Z$.

(i) Taking (3.3.8) modulo $(M+1)^2$, we have $M \equiv -M^{2Z} \pmod{(M+1)^2}$, so $M^{2Z-1} + 1 \equiv 0 \pmod{(M+1)^2}$. Hence

$$1 - M + M^2 - \cdots + M^{2Z-2} = \frac{M^{2Z-1}+1}{M+1} \equiv 0 \pmod{M+1},$$

so $2Z \equiv 1 \pmod{M+1}$.

Since $M$ is divisible by 4, we observe that

$$(M+1)^x \equiv \binom{x}{2} M^2 + Mx + 1, \qquad (2M+1)^Z \equiv 2MZ + 1 \pmod{2M^2}.$$

By (3.3.8), we have

$$\binom{x}{2} M^2 + Mx + 1 + M \equiv 2MZ + 1 \pmod{2M^2},$$

so

$$x + 1 + \binom{x}{2} M \equiv 2Z \pmod{2M}.$$

Reducing this modulo 4, we have $x \equiv 1 \pmod 4$ since $Z$ is odd. It follows from the above congruence that $x + 1 \equiv 2Z \pmod{2M}$.

(ii) Since $Z \leq x - 2$ and $x + 1 < 2Z$, it follows from (i) that

$$x + 1 + 2M \leq 2Z \leq 2x - 4,$$

so $2M + 5 \leq x$. □

Now we are ready to prove Theorem 3.1.1.

*Proof of Theorem 3.1.1.* Let $(x, Z)$ be a solution of (3.3.8). By Lemma 3.2.2, we see that $x < 2010 \log(2M + 1)$. Suppose that $x > 1$. We will observe that this leads to a contradiction. By (ii) in Lemma 3.3.11, we have

$$2M + 5 \leq x < 2010 \log(2M + 1).$$

This implies that $M \leq 9940$. It remains to consider $M$'s such that $M \leq 9940$ and $M \equiv 0 \pmod 4$. Fix such a $M$. Then, for each $x$ in the above range, we can determine the corresponding $Z$ by using the inequalities $(2M + 1)^Z < (M + 1)^{x+1} < (2M + 1)^{Z+1}$ (which easily follows from (3.3.8)). Additionally, we can check that such a pair $(x, Z)$ does not satisfy all of the conditions of (i) in Lemma 3.3.11. This is a contradiction. We conclude that $x = 1$, so $Z = 1$. This completes the proof of Theorem 3.1.1. □

# Chapter 4

# Upper bounds for solutions

## 4.1 Results on upper bounds for solutions

In this section we give several sharp upper bounds for solutions $x, y, z$ of (1) in terms of $a, b, c$ for the following cases:

(1) $x, y$ and $z$ are even.

(2) $x, y$ are even and $z$ is odd.

(3) $x$ and $z$ are divisible by 4.

(4) $x, z$ are even and $y$ is odd.

For Cases (1) and (2), we should consider the case where $c$ is odd. Indeed, if $c$ is even and (1) has a solution with even $x$ and $y$, then $c^z$ is a sum of two squares of odd integers, so it is exactly divisible by 2, which implies that $z = 1$.

For a prime number $p$ and a non-zero integer $m$, we denote $\mathrm{ord}_p(m)$ by the exact power of $p$ in $m$.

For Cases (1) and (4), we will use the following elementary fact on 2-adic calculations (cf. [Ri, p.11; P1.2]).

**Lemma 4.1.1** *Let $U$ and $V$ be odd positive integers with $U > V$, and $e$ be a positive integer. Then*

$$\mathrm{ord}_2\big(U^{2e} - V^{2e}\big) = \mathrm{ord}_2(U \pm V) + \mathrm{ord}_2(e) + 1$$

*for the proper sign for which* $\mathrm{ord}_2(U \pm V) \geq 2$.

**Theorem 4.1.1** *We consider the case where $b$ is even. Let $(x, y, z)$ be a solution of* (1)*. Assume that $x, y$ and $z$ are even. We write $x = 2X$, $y = 2Y$ and $z = 2Z$. Then the following* (i) *and* (ii) *hold.*

(i) *If*

$$(a, c, X, Y, Z) \neq \left(\frac{b^{2q}}{4} - 1,\ \frac{b^{2q}}{4} + 1,\ 1,\ q,\ 1\right); q \geq 1,$$

*then*

$$X < \frac{2Y\log(b/2)}{\log a}, \quad Z < \frac{2Y\log(b/2)+\log 2}{\log c}.$$

(ii) *Suppose that* $Y > 1$. *If*

$$(Y,Z) \neq \left(\frac{\log(c-1)}{\log b},\, 1\right),$$

*then*

$$Y \leq \frac{\log\min\bigl(a/p(a)+p(a),\, 2\sqrt{c-1}\,\bigr)}{\mathrm{ord}_2(b)\log 2},$$

*where* $p(a)$ *is the least prime factor of* $a$.

*Proof.* Assume that $x, y$ and $z$ are even. We can write $x = 2X$, $y = 2Y$ and $z = 2Z$, where $X, Y, Z \in \mathbb{N}$. As is well-known (cf. [Ri, p.32; P3.1]), we can write

$$a^X = k^2 - l^2, \quad b^Y = 2kl, \quad c^Z = k^2 + l^2,$$

where integers $k, l$ satisfy the condition $k > l > 0$, $\gcd(k,l) = 1$ and $k \not\equiv l \pmod 2$. Since $(k+l)(k-l) = a^X$ and $\gcd(k+l, k-l) = 1$, we can write

$$k + l = u^X, \quad k - l = v^X,$$

where odd integers $u, v$ satisfy the condition $u > v > 0, \gcd(u,v) = 1$ and $uv = a$.

We consider the cases $l = 1$ and $l > 1$ separately.

First, we consider the case $l = 1$. Then $k^2 - a^X = 1$ and $c^Z - k^2 = 1$. We know that these are Catalan's equations. Since $a$ is odd, it follows from [Ko, Le] that $X = Z = 1$. Hence $k = b^Y/2$, so $a = b^{2Y}/4 - 1$ and $c = b^{2Y}/4 + 1$.

In what follows, we consider the case $l > 1$. We claim that $l \geq 2^{Y-1}$. If $l$ is even, then $2l$ is a $Y$-th power of an even positive integer since $2kl = b^Y$ and $\gcd(k, 2l) = 1$, in particular, $l \geq 2^{Y-1}$. If $l$ is odd, then $l$ is a $Y$-th power of an odd positive integer since $2kl = b^Y$ and $\gcd(2k, l) = 1$, in particular, $l \geq 3^Y$.

Since $a^X < k^2 = b^{2Y}/(4l^2)$ and $c^Z < 2k^2 = b^{2Y}/(2l^2)$, we can obtain the desired upper bounds for $X$ and $Z$.

From the results [CD, Theorem 5] and [CD2, Lemma 10], we see that $Y = 1$ or $X, Z$ are odd. From now on, we assume that $Y > 1$. Then both $X$ and $Z$ are odd.

We consider the cases $v = 1$ and $v > 1$ separately.

If $v = 1$, then $k - l = 1$, so $c^Z - b^Y = (k-l)^2 = 1$. Since $Y > 1$ and $Z$ is odd, it follows from [Mi] that $Z = 1$.

In what follows, we assume that $v > 1$. Since $4kl = (k+l)^2 - (k-l)^2 = u^{2X} - v^{2X}$, we see from Lemma 4.1.1 that

$$\begin{aligned} Y\mathrm{ord}_2(b) &= \mathrm{ord}_2(b^Y) \\ &= \mathrm{ord}_2(2kl) \\ &= \mathrm{ord}_2\left(\frac{u^{2X}-v^{2X}}{2}\right) \\ &= \mathrm{ord}_2\bigl(u^{2X}-v^{2X}\bigr) - 1 = \mathrm{ord}_2(u \pm v) \end{aligned}$$

for the proper sign. Since $v > 1$, we see that $u \pm v \leq u + v \leq a/p(a) + p(a)$, hence

$$Y = \frac{\mathrm{ord}_2(u \pm v)}{\mathrm{ord}_2(b)} \leq \frac{\log\bigl(a/p(a) + p(a)\bigr)}{\mathrm{ord}_2(b)\log 2}.$$

On the other hand, we rewrite $k^2 + l^2 = c^Z$ as

$$(k + l\sqrt{-1}\,)(k - l\sqrt{-1}\,) = c^Z.$$

Since $c$ is odd, we see that two factors on the left-hand side in the above equality are relatively prime in $\mathbb{Z}[\sqrt{-1}\,]$. Hence there exist integers $a_1, b_1$ with $a_1^2 + b_1^2 = c$ such that

$$k + l\sqrt{-1} = (a_1 + b_1\sqrt{-1}\,)^Z.$$

Note that $a_1 \not\equiv b_1 \pmod 2$. Since $Z$ is odd, we have

$$k = a_1\left(a_1^{Z-1} - \binom{Z}{Z-2}a_1^{Z-3}b_1^2 + \cdots \pm \binom{Z}{3}a_1^2\,b_1^{Z-3} \pm Zb_1^{Z-1}\right),$$
$$l = b_1\left(Za_1^{Z-1} - \binom{Z}{Z-3}a_1^{Z-3}b_1^2 + \cdots \pm \binom{Z}{2}a_1^2\,b_1^{Z-3} \pm b_1^{Z-1}\right).$$

It is easy to see that $k/\,a_1$ and $l/\,b_1$ are odd integers. Since

$$Y\,\mathrm{ord}_2(b) = \mathrm{ord}_2(b^Y) = \mathrm{ord}_2(2kl) = \mathrm{ord}_2(2a_1b_1),$$

it follows that

$$Y = \frac{\mathrm{ord}_2(2a_1b_1)}{\mathrm{ord}_2(b)}.$$

Since $a_1 \not\equiv b_1 \pmod 2$ and $|a_1|, |b_1| \leq \sqrt{c-1}$, we obtain

$$Y \leq \frac{\log\bigl(2\sqrt{c-1}\,\bigr)}{\mathrm{ord}_2(b)\log 2}.$$

□

**Remark 4.1.1** Under the assumption of Theorem 4.1.1, we can not generally deduce upper bounds for $Y$ such as $Y \leq \mathcal{C}\log b$, where $\mathcal{C}$ is an absolute constant. Indeed, we know the following identity:

$$(2^{2p-2} - 1)^2 + 2^{2p} = (2^{2p-2} + 1)^2 \ (p \geq 2).$$

**Theorem 4.1.2** *We consider the case where $b$ is even. Put*

$$\mathcal{C}_2 = \frac{2\log\max(a,b)}{\log 3}.$$

*Let $(x, y, z)$ be a solution of (1). Assume that $x, y$ are even and $z$ is odd. We write $x = 2X$ and $y = 2Y$. Then*

$$Y \leq \frac{\log(c-1)}{2\,\mathrm{ord}_2(b)\log 2}.$$

*Further, we suppose that $c-1$ is not a square, or*

$$\frac{\operatorname{ord}_2(c-1)}{2\operatorname{ord}_2(b)} < \frac{\log(c-1)}{2\log b},$$

*or*

$$Y \neq \frac{\operatorname{ord}_2(c-1)}{2\operatorname{ord}_2(b)}.$$

*Then*

$$\text{(i)} \quad X \le \frac{\log(c-1)}{\log 3}, \qquad z < \mathcal{C}_2 + \frac{\log 2}{\log c} \qquad \text{if } z \le \sqrt{c-1},$$

$$\text{(ii)} \quad X \le \frac{2\log z}{\log 3}, \qquad \frac{z}{\log z} < \frac{2\,\mathcal{C}_2}{\log c} + \frac{2\log 2}{\log^2 c} \qquad \text{if } \sqrt{c-1} < z.$$

*If $\mathcal{C}_2 \le \sqrt{c} - (\log 2)/\log c$, then* (i) *holds.*

*Proof.* Assume that $x, y$ are even and $z$ is odd. We can write $x = 2X$ and $y = 2Y$, where $X, Y \in \mathbb{N}$. It suffices to consider the case where $c = 5$ or $c \ge 13$. Indeed, $c$ is odd, and $c$ can not have any prime factors congruent to 3 modulo 4 since $c^z$ is a sum of two squares of relatively prime integers.

We rewrite (1) as

$$(a^X + b^Y\sqrt{-1}\,)(a^X - b^Y\sqrt{-1}\,) = c^z.$$

Since $c$ is odd, we see that two factors on the left-hand side in the above equality are relatively prime in $\mathbb{Z}[\sqrt{-1}\,]$. Hence there exist integers $a_2, b_2$ with $a_2^2 + b_2^2 = c$ such that

$$a^X + b^Y\sqrt{-1} = (a_2 + b_2\sqrt{-1}\,)^z.$$

Note that $a_2 \not\equiv b_2 \pmod 2$. Since $z$ is odd, we have

$$a^X = a_2\left(a_2^{z-1} - \binom{z}{z-2}a_2^{z-3}\,b_2^2 + \cdots \pm \binom{z}{3}a_2^2\,b_2^{z-3} \pm z b_2^{z-1}\right),$$

$$b^Y = b_2\left(z a_2^{z-1} - \binom{z}{z-3}a_2^{z-3}\,b_2^2 + \cdots \pm \binom{z}{2}a_2^2\,b_2^{z-3} \pm b_2^{z-1}\right).$$

It is clear that $a_2$ divides $a^X$ and $b_2$ divides $b^Y$. In particular, $a_2$ and $b_2$ are relatively prime non-zero integers. Then $a_2$ is odd since $a$ is odd, so $b_2$ is even. Since $a_2, z$ are odd, we see that $b^Y/\,b_2$ is an odd integer, in particular,

$$Y = \frac{\operatorname{ord}_2(b_2)}{\operatorname{ord}_2(b)}.$$

Since $|b_2| \le \sqrt{c-1}$, we have

$$Y \le \frac{\log(c-1)}{2\operatorname{ord}_2(b)\log 2} \le \frac{\log\sqrt{c-1}}{\log 2}.$$

We consider the cases $|a_2| = 1$ and $|a_2| > 1$ separately.

First, we consider the case $|a_2| = 1$. Then, since $b_2^2 = c - 1$, we see that $b^{2Y}/(c-1) = \left(b^Y / b_2\right)^2$ is an odd positive integer, in particular,

$$\frac{\log(c-1)}{2\log b} \le Y = \frac{\operatorname{ord}_2(c-1)}{2\operatorname{ord}_2(b)}.$$

Next, we consider the case $|a_2| > 1$. Then $a_2$ has an odd prime factor $p$. Hence $p$ divides $a$, and $p$ does not divide $b$ since $\gcd(a,b) = 1$. It is easy to see that $c \neq 5$, so $c \ge 13$. The argument below is based on an observation in [HY].

We claim that

$$X \operatorname{ord}_p(a) = \operatorname{ord}_p(a_2) + \operatorname{ord}_p(z).$$

For this, it suffices to show that if $z$ is divisible by $p$, then

$$\operatorname{ord}_p\left(\binom{z}{i} a_2^{i-1}\right) > \operatorname{ord}_p(z)$$

for $i = 3, 5, ..., z$. Then, since $p \ge 3$, $i \ge 3$ and

$$\operatorname{ord}_p(i!) = \sum_{j=1}^{\infty} \left\lfloor \frac{i}{p^j} \right\rfloor < \sum_{j=1}^{\infty} \frac{i}{p^j} = \frac{i}{p-1},$$

where $\lfloor \cdot \rfloor$ is the floor function, we see that

$$\begin{aligned}
\operatorname{ord}_p\left(\binom{z}{i} a_2^{i-1}\right) &= \operatorname{ord}_p\left(\frac{z(z-1)\cdots(z-i+1)}{i!}\right) + \operatorname{ord}_p\left(a_2^{i-1}\right) \\
&= \operatorname{ord}_p\left(z(z-1)\cdots(z-i+1)\right) - \operatorname{ord}_p(i!) + (i-1)\operatorname{ord}_p(a_2) \\
&> \operatorname{ord}_p(z) - \frac{i}{p-1} + i - 1 \\
&= \operatorname{ord}_p(z) + \left(\frac{p-2}{p-1}\right) i - 1 \\
&> \operatorname{ord}_p(z).
\end{aligned}$$

Hence the claim holds. Then, since $|a_2| \le \sqrt{c-1}$, we have

$$X \le \operatorname{ord}_p(a_2) + \operatorname{ord}_p(z) \le \frac{\log|a_2| + \log z}{\log p} \le \frac{2\log\max\left(\sqrt{c-1},\, z\right)}{\log 3},$$

so

$$M := \max(X, Y) \le \frac{2\log\max\left(\sqrt{c-1},\, z\right)}{\log 3}.$$

Since $c^z = a^{2X} + b^{2Y} \le a^{2M} + b^{2M} < 2\max(a,b)^{2M}$, we have

$$z < \frac{2M\log\max(a,b)}{\log c} + \frac{\log 2}{\log c}.$$

If $z \le \sqrt{c-1}$, then $M \le (\log c)/\log 3$ and $z < \mathcal{C}_2 + (\log 2)/\log c$, so Case (i) holds.

If $\sqrt{c-1} < z$, then $\sqrt{c} \le z$ and $M \le (2\log z)/\log 3$, so

$$\frac{z}{\log z} < \frac{2M \log \max(a,b)}{(\log c)\log z} + \frac{\log 2}{(\log c)\log z} < \frac{2\,\mathcal{C}_2}{\log c} + \frac{2\log 2}{\log^2 c},$$

hence Case (ii) holds. Further, since $c \ge 13$ and

$$\frac{z \log c}{\log z} < 2\,\mathcal{C}_2 + \frac{2\log 2}{\log c},$$

we have

$$2\sqrt{c} = \frac{\sqrt{c}\,\log c}{\log \sqrt{c}} < 2\,\mathcal{C}_2 + \frac{2\log 2}{\log c},$$

so $\mathcal{C}_2 > \sqrt{c} - (\log 2)/\log c$. From this we see that if $\mathcal{C}_2 \le \sqrt{c} - (\log 2)/\log c$, then $z \le \sqrt{c-1}$, so Case (i) holds. □

**Remark 4.1.2** In the statement of Theorem 4.1.2, the condition $\mathcal{C}_2 \le \sqrt{c} - (\log 2)/\log c$ holds if $a^2 + b^2 = c$. Indeed, if $a^2 + b^2 = c$, then

$$\sqrt{c} - \frac{\log 2}{\log c} > \sqrt{a^2+b^2} - 1 > \max(a,b) - 1$$

and

$$\frac{\max(a,b)-1}{\log \max(a,b)} \ge \frac{2}{\log 3}.$$

This is valid since $\max(a,b) \ge 3$.

**Theorem 4.1.3** *We consider the case where $b$ is even. Let $(x,y,z)$ be a solution of (1). Assume that $x$ and $z$ are divisible by 4. We write $x = 4X$ and $z = 4Z$. Then*

$$y < \frac{\log b}{\mathrm{ord}_2(b)\log 2}, \quad X < \frac{\log\left(b/2^{\mathrm{ord}_2(b)}\right)}{2\log a}\,y, \quad Z < \frac{\log\left(b/2^{\mathrm{ord}_2(b)-1}\right)}{2\log c}\,y.$$

*Proof.* Assume that $x$ and $z$ are divisible by 4. We can write $x = 4X$ and $z = 4Z$, where $X, Z \in \mathbb{N}$. As is well-known (cf. [Ri, p.34; P3.2]), there are no positive integers $A, B$ and $C$ such that $A^4 + B^2 = C^4$. Hence it suffices to consider the case where $y$ is odd.

From (1) we define positive integers $D, E$ as follows:

$$b^y = DE,$$

where

$$D = c^{2Z} + a^{2X}, \quad E = c^{2Z} - a^{2X}.$$

It is easy to see that $\gcd(D,E) = 2$, and that $D$ is exactly divisible by 2 since it is a sum of two squares of odd integers. Hence there exist relatively prime odd positive integers $s, t$ with $b = 2^{\beta} st$ such that

$$D = 2s^y, \quad E = 2^{\beta y - 1} t^y,$$

where $\beta = \mathrm{ord}_2(b) \geq 1$.

Since $D \leq b^y/2^{\beta y-1}$, $a^{2X} < D/2$ and $c^{2Z} < D$, we can obtain the desired upper bounds for $X$ and $Z$.

Then $\beta \geq 2$ or $t \geq 3$. Indeed, if $\beta = 1$ and $t = 1$, then $2^{y-1} = (c^Z + a^X)(c^Z - a^X)$, so $c^Z + a^X = 2^{y-2}$. This implies that $2s^y = D < (c^Z + a^X)^2 = 2^{2y-4}$, so $s < 4$. This is absurd since we see from the first equality above that $s > 1$ and $s$ can not be divisible by 3.

We rewrite $c^{2Z} + a^{2X} = 2s^y$ as

$$(c^Z + a^X\sqrt{-1}\,)(c^Z - a^X\sqrt{-1}\,) = (1 + \sqrt{-1}\,)(1 - \sqrt{-1}\,)s^y.$$

It is easy to see that two factors on the left-hand side in the above equality are relatively prime in $\mathbb{Z}[\sqrt{-1}\,]$. Hence there exist integers $d_1, e_1$ with $d_1^2 + e_1^2 = s$ such that

$$c^Z + a^X\sqrt{-1} = (1 + \varepsilon\sqrt{-1}\,)(d_1 + e_1\sqrt{-1}\,)^y,$$

where $\varepsilon = \pm 1$. Note that $d_1 \not\equiv e_1 \pmod 2$. Let $I$ and $J$ be the real part and the imaginary part of $(d_1 + e_1\sqrt{-1}\,)^y$, respectively. Then

$$I = d_1\left(d_1^{y-1} - \binom{y}{2}d_1^{y-3}e_1^2 + \cdots \pm y e_1^{y-1}\right),$$
$$J = e_1\left(y d_1^{y-1} - \binom{y}{3}d_1^{y-3}e_1^2 + \cdots \pm e_1^{y-1}\right),$$

further, $c^Z + \varepsilon a^X = 2I$ and $c^Z - \varepsilon a^X = -2\varepsilon J$. Hence

$$2^{\beta y-1}t^y = E = (c^Z + \varepsilon a^X)(c^Z - \varepsilon a^X) = -4\varepsilon IJ.$$

Since $y$ is odd and $d_1 \not\equiv e_1 \pmod 2$, we see that $I/d_1$ and $J/e_1$ are odd integers, so

$$\beta y - 1 = \mathrm{ord}_2(4\varepsilon IJ) = \mathrm{ord}_2(4d_1e_1) = \mathrm{ord}_2(d_1e_1) + 2.$$

Since $2|d_1e_1| < d_1^2 + e_1^2 = s = b/(2^\beta t)$, and $\beta \geq 2$ or $t \geq 3$, it follows that

$$\begin{aligned}
\beta y &= \mathrm{ord}_2(d_1e_1) + 3 \\
&\leq \frac{\log|d_1e_1|}{\log 2} + 3 \\
&< \frac{\log\left(b/(\,2^{\beta+1}\,t)\,\right)}{\log 2} + 3 \\
&= \frac{\log b}{\log 2} - \left(\beta + \frac{\log t}{\log 2}\right) + 2 \leq \frac{\log b}{\log 2},
\end{aligned}$$

so the conclusion holds. □

**Remark 4.1.3** In Theorem 4.1.3, we can further conclude that $y = 1$ by the result in [Da].

**Theorem 4.1.4** *We consider the case where $b$ is odd and $b \geq 5$. Let $(x, y, z)$ be a solution of* (1)*. Assume that $x, z$ are even and $y$ is odd. We write $x = 2X$ and $z = 2Z$.*

*If*

$$(a, b, c, X, y, Z) \neq (2, 17, 3, 3, 1, 2),$$

*or*

$$(X, Z) \neq \left(1, \frac{\log(a+1)}{\log c}\right), \left(\frac{\log(c-1)}{\log a}, 1\right),$$

*then*

$$X < \frac{y \log\left(b/p(b)\right) - \log 2}{\log a}, \quad Z < \frac{\log\left(b/p(b)\right)}{\log c}\, y,$$

*where $p(b)$ is the least prime factor of $b$. Furthermore, the following* (i) *and* (ii) *hold.*

(i) *If $a$ is even, then*

$$y \leq \mathcal{C}_4 \log a + 1,$$

*where*

$$\mathcal{C}_4 = \frac{\log\bigl(b/(2p(b)) + p(b)/2\bigr)}{\mathrm{ord}_2(a)(\log 2)\log\bigl(\sqrt{b+1} - 1\bigr)} \quad (< 3).$$

(ii) *If $c$ is even, then*

$$Z \leq \frac{\log\bigl(b/(2p(b)) + p(b)/2\bigr)}{\mathrm{ord}_2(c)\log 2}.$$

*Proof.* Assume that $x, z$ are even and $y$ is odd. We can write $x = 2X$ and $z = 2Z$, where $X, Z \in \mathbb{N}$. From (1) we define positive integers $D, E$ as follows:

$$b^y = DE,$$

where

$$D = c^Z + a^X, \quad E = c^Z - a^X.$$

It is easy to see that $\gcd(D, E) = 1$. Hence we can write

$$D = s^y, \quad E = t^y,$$

where integers $s, t$ satisfy the condition $s > t > 0$, $\gcd(s, t) = 1$ and $st = b$. Then

$$s^y + t^y = 2c^Z, \quad s^y - t^y = 2a^X.$$

We consider the cases $t = 1$ and $t > 1$ separately.

If $t = 1$, then $E = 1$, so $c^Z - a^X = 1$. It follows from [Mi] that $X = 1$ or $Z = 1$ or $(a, b, c, X, y, Z) = (2, 17, 3, 3, 1, 2)$.

In what follows, we assume that $t > 1$. Then $t \geq p(b)$. Since $D \leq b^y/E$, $E \geq p(b)^y$, $a^X < D/2$ and $c^Z < D$, we can obtain the desired upper bounds for $X$ and $Z$.

Note that $s \geq \sqrt{b+1}+1$. Indeed, since $s \geq t+2$ and $st = b$, we have $s^2 \geq b+2s$, so $(s-1)^2 \geq b+1$. Hence

$$\begin{aligned} 2a^X &= s^y - t^y \\ &= s^y - \left(\frac{b}{s}\right)^y \\ &\geq \left(\sqrt{b+1}+1\right)^y - \left(\sqrt{b+1}-1\right)^y \geq 2y\left(\sqrt{b+1}-1\right)^{y-1}, \end{aligned}$$

so $\left(\sqrt{b+1}-1\right)^{y-1} \leq a^X$. Since $b \geq 5$, we have

$$y - 1 \leq \frac{\log a}{\log\left(\sqrt{b+1}-1\right)} X.$$

Since $4a^X c^Z = s^{2y} - t^{2y}$, we see from Lemma 4.1.1 that

$$\operatorname{ord}_2(a^X c^Z) = \operatorname{ord}_2(s^{2y} - t^{2y}) - 2 = \operatorname{ord}_2(s \pm t) - 1$$

for the proper sign. Since $s \pm t \leq s + t \leq b/p(b) + p(b)$, we have

$$\begin{aligned} X \operatorname{ord}_2(a) + Z \operatorname{ord}_2(c) &= \operatorname{ord}_2(a^X c^Z) \\ &\leq \frac{\log(s \pm t)}{\log 2} - 1 \\ &\leq \frac{\log\left(b/p(b) + p(b)\right)}{\log 2} - 1 = \frac{\log\left(b/(2p(b)) + p(b)/2\right)}{\log 2}. \end{aligned}$$

The desired conclusions follow from this. □

## 4.2 Applications

Let $\{F_n\}_{n\geq 0}$ be Fibonacci numbers, the numbers $\{F_n\}_{n\geq 0}$ defined by

$$F_0 = 0, \quad F_1 = 1, \quad F_{n+2} = F_{n+1} + F_n.$$

For instance, the first several Fibonacci numbers are given in the following table:

| $n$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $F_n$ | 0 | 1 | 1 | 2 | 3 | 5 | 8 | 13 | 21 | 34 | 55 | 89 | 144 |

We can find many works related to Fibonacci numbers in various Diophantine problems (cf. [BLMS], [BMS], [Coh], [Coh2], [Du], [Fi]). There are a number of fascinating formulas on those numbers (cf. [Ko]). One of the most important formulas on Fibonacci numbers is *Cassini's identity* (cf. [Ko, p.74; Theorem 5.3]):

$$F_n^2 = (-1)^{n+1} + F_{n-1}F_{n+1} \quad (n \geq 1).$$

Cassini's identity can be generalized for the generalized Fibonacci numbers (cf. [Ko, Ch.7]). In the study of Fibonacci numbers, we often observe that Lucas numbers $\{L_n\}_{n\geq 0}$ work well. They are defined by

$$L_0 = 2, \quad L_1 = 1, \quad L_{n+2} = L_{n+1} + L_n.$$

For instance, the first several Lucas numbers are given in the following table:

| $n$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $L_n$ | 2 | 1 | 3 | 4 | 7 | 11 | 18 | 29 | 47 | 76 | 123 | 199 | 322 |

Fibonacci numbers and Lucas numbers are companionable in a number of ways. There are many relations among those numbers (cf. [Ko]).

In 1876 Lucas proved the following elegant formulas (cf. [Ko, p.79; Corollary 5.4]):

$$F_n^2 + F_{n+1}^2 = F_{2n+1},$$

$$F_n^2 + F_{2n+2} = F_{n+2}^2$$

for $n \geq 0$. It is worth stating that the formulas of these types do not seem to be seen in other Lucas sequences (cf. [Ko]). From these formulas we consider the exponential Diophantine equations:

$$F_n^x + F_{n+1}^y = F_{2n+1}^z \quad \big(x, y, z \in \mathbb{N}\big), \tag{4.2.1}$$

$$F_n^x + F_{2n+2}^y = F_{n+2}^z \quad \big(x, y, z \in \mathbb{N}\big). \tag{4.2.2}$$

It is clear that (4.2.1) has the solution $(x, y, z) = (2, 2, 1)$, and (4.2.2) has the solution $(x, y, z) = (2, 1, 2)$. In 2002 at ICM, Terai [Te3] proposed to study (4.2.1) and he proved, under strict assumptions on $n \geq 3$, that (4.2.1) has the unique solution $(x, y, z) = (2, 2, 1)$ by using the theory of linear forms in two logarithms.

Applying Theorems 4.1.1-4.1.4 to (4.2.1) and (4.2.2), we prove the following results.

**Theorem 4.2.1** *For each $n \geq 3$, (4.2.1) has the unique solution $(x, y, z) = (2, 2, 1)$.*

**Theorem 4.2.2** *For each $n \geq 3$, (4.2.2) has the unique solution $(x, y, z) = (2, 1, 2)$.*

### 4.2.1 Proof of Theorem 4.2.1

In this subsection we prove Theorem 4.2.1. Let $n \geq 3$. We first note that $F_n, F_{n+1}$ and $F_{2n+1}$ are pair-wise relatively prime positive integers greater than 1.

Let $(x, y, z)$ be a solution of (4.2.1). We prepare some lemmas. First we determine the parities of $x, y$ by using congruence reductions. Further we obtain congruence relations among $x, y, z$.

**Lemma 4.2.1**

(i) *$x$ and $y$ are even.*

(ii) *$X \equiv z \pmod{F_{n+1}}$ and $Y \equiv z \pmod{F_n}$, where $X = x/2$ and $Y = y/2$.*

*Proof.* We first consider the case $n = 3$. In this case, we rewrite (4.2.1) as

$$2^x + 3^y = 13^z. \tag{4.2.3}$$

Taking (4.2.3) modulo 3, we have $(-1)^x \equiv 1 \pmod 3$, so $x$ is even. Then taking (4.2.3) modulo 4, we have $(-1)^y \equiv 1 \pmod 4$, so $y$ is even. Hence we can write $x = 2X$ and $y = 2Y$, where $X, Y \in \mathbb{N}$. Taking (4.2.3) modulo 5, we have $3^z \equiv \pm 2 \pmod 5$, which implies that $z$ is odd. By Theorem 4.1.2, we see that $z < 2 + (\log 2)/\log 13 < 3$, so $z = 1$. This yields $X = Y = 1$. Hence the lemma holds for the case $n = 3$. Similarly, we can prove the lemma for the case $n = 4$. Hence it suffices to consider the case $n \geq 5$. Then $F_{n+1} > F_n + 1$ and $F_n > F_{n-1} + 1$. Indeed, $F_{n+1} - F_n = F_{n-1} > 1$ and $F_n - F_{n-1} = F_{n-2} > 1$ since $n \geq 5$. In particular,

$$F_n \not\equiv \pm 1 \pmod{F_{n+1}}, \quad F_{n+1} \not\equiv \pm 1 \pmod{F_n}.$$

We write $x = 2X + x_1$, where $X$ is a non-negative integer and $x_1 \in \{0, 1\}$. Then taking (4.2.1) modulo $F_{n+1}^2$, we have

$$F_n^{2X} F_n^{x_1} + F_{n+1}^y \equiv F_n^{2z} \pmod{F_{n+1}^2}.$$

By Cassini's identity, we see that

$$F_n^2 = \delta + F_{n-1}F_{n+1} \equiv \delta - F_n F_{n+1} \pmod{F_{n+1}^2},$$

where $\delta = (-1)^{n+1}$. Hence

$$\left(\delta^X - \delta^{X-1} F_n F_{n+1} X\right) F_n^{x_1} + F_{n+1}^y \equiv \delta^z - \delta^{z-1} F_n F_{n+1} z \pmod{F_{n+1}^2}.$$

Reducing this modulo $F_{n+1}$, we have

$$\delta^X F_n^{x_1} \equiv \delta^z \pmod{F_{n+1}}.$$

If $x_1 = 1$, then $F_n \equiv \pm 1 \pmod{F_{n+1}}$, which is absurd. Hence $x_1 = 0$, that is, $x = 2X$. Then $\delta^X \equiv \delta^z \pmod{F_{n+1}}$. This implies that $\delta^X = \delta^z$ since $\delta = \pm 1$ and $F_{n+1} \geq 3$. Hence

$$-\delta^{X-1} F_n X + F_{n+1}^{y-1} \equiv -\delta^{X-1} F_n z \pmod{F_{n+1}}.$$

Similarly, we can prove that $y$ is even by taking (4.2.1) modulo $F_n^2$ (for this, we use the congruences $F_{n+1}^2 \equiv -\delta + F_n F_{n+1} \pmod{F_n^2}$ and $F_{n+1} \not\equiv \pm 1 \pmod{F_n}$), and further,

$$F_n^{x-1} + (-\delta)^{Y-1} F_{n+1} Y \equiv (-\delta)^{Y-1} F_{n+1} z \pmod{F_n},$$

where $Y = y/2$. Since $x \geq 2$ and $y \geq 2$, it follows from two congruences above that $X \equiv z \pmod{F_{n+1}}$ and $Y \equiv z \pmod{F_n}$. □

By (i) in Lemma 4.2.1, we can write $x = 2X$ and $y = 2Y$, where $X, Y \in \mathbb{N}$.

It suffices to consider the case where $F_{2n+1}$ is odd. Indeed, if $F_{2n+1}$ is even, then $F_n$ and $F_{n+1}$ are odd, so $F_{2n+1}^z = F_n^{2X} + F_{n+1}^{2Y} \equiv 2 \pmod 4$. This gives that $z = 1$, so $X = Y = 1$ since $F_{2n+1} = F_n^2 + F_{n+1}^2$.

In what follows, we consider the case where $F_{2n+1}$ is odd. Then $F_n$ or $F_{n+1}$ is even, and $n \geq 5$.

We remark that if $\max(X, Y) \leq z$, then $X = Y = z = 1$. Indeed, if $\max(X, Y) \leq z$, then

$$(F_n^2 + F_{n+1}^2)^z = F_{2n+1}^z = F_n^{2X} + F_{n+1}^{2Y} \leq (F_n^2)^z + (F_{n+1}^2)^z,$$

so $z = 1$, hence $X = Y = 1$.

We will obtain sharp upper bounds for $X$ and $Y$ by using Theorems 4.1.1 and 4.1.2. For this we consider the case where $z$ is even and the case where $z$ is odd separately.

**Lemma 4.2.2** *Suppose that $z$ is even. Then the following hold.*

(i) *If $F_n$ is even, then we have the upper estimates*

$$X \leq \frac{\log(F_{n+1} + 1)}{\mathrm{ord}_2(F_n) \log 2}, \quad Y \leq 2X - 1.$$

(ii) *If $F_{n+1}$ is even, then we have the upper estimates*

$$Y \leq \frac{\log(F_n + 1)}{\mathrm{ord}_2(F_{n+1}) \log 2}, \quad X \leq 2Y - 1.$$

*Proof.* Suppose that $z$ is even. We can write $z = 2Z$, where $Z \in \mathbb{N}$. Note that $\max(X, Y) > z \geq 2$.

We use Theorem 4.1.1. First, we consider the case where $F_n$ is even. We apply Theorem 4.1.1 to the case where $(a, b, c) = (F_{n+1}, F_n, F_{2n+1})$. Since $F_{n+1} + 1 \leq 2\sqrt{F_{2n+1} - 1}$, it follows that

$$Y < \frac{2 \log(F_n/2)}{\log F_{n+1}} X < 2X, \qquad X \leq \frac{\log(F_{n+1} + 1)}{\mathrm{ord}_2(F_n) \log 2}.$$

Next, we consider the case where $F_{n+1}$ is even. We apply Theorem 4.1.1 to the case where $(a, b, c) = (F_n, F_{n+1}, F_{2n+1})$. Since $F_n + 1 \leq 2\sqrt{F_{2n+1} - 1}$, it follows that

$$X < \frac{2 \log(F_{n+1}/2)}{\log F_n} Y < 2Y, \qquad Y \leq \frac{\log(F_n + 1)}{\mathrm{ord}_2(F_{n+1}) \log 2}.$$

□

Next we consider the case where $z$ is odd. To use Theorem 4.1.2 we give an easy observation on values of $\mathrm{ord}_2(L_m)$.

For all $m \geq 0$, we see from two tables in Section 1 that $L_m \equiv 2 \pmod 4$ when $F_m \equiv 0 \pmod 4$, and $L_m \equiv 4 \pmod 8$ when $F_m \equiv 2 \pmod 4$, further, $L_m$ is odd when $F_m$ is odd. In particular, $\mathrm{ord}_2(L_m) \leq 2$ for all $m \geq 0$.

**Lemma 4.2.3** *Assume that $z$ is odd. Then the following hold.*

(i) *If $F_n$ is even, then we have the upper estimates*

$$X \leq \frac{\log(F_{2n+1} - 1)}{2 \,\mathrm{ord}_2(F_n) \log 2}, \quad Y \leq \frac{\log(F_{2n+1} - 1)}{\log 3}.$$

(ii) *If $F_{n+1}$ is even, then we have the upper estimates*

$$X \le \frac{\log(F_{2n+1}-1)}{\log 3}, \quad Y \le \frac{\log(F_{2n+1}-1)}{2\,\mathrm{ord}_2(F_{n+1})\log 2}.$$

*Proof.* Assume that $z$ is odd. It suffices to show that Case (i) in Theorem 4.1.2 holds.

Since $F_{2n+1} = F_n^2 + F_{n+1}^2$ and $L_m = F_{m+1} + F_{m-1}$ for all $m \ge 1$, we see from Cassini's identity that if $n$ is even, then

$$F_{2n+1} - 1 = F_n^2 + (F_{n+1}^2 - 1) = F_n^2 + F_n F_{n+2} = F_n L_{n+1},$$

and that if $n$ is odd, then

$$F_{2n+1} - 1 = (F_n^2 - 1) + F_{n+1}^2 = F_{n-1}F_{n+1} + F_{n+1}^2 = L_n F_{n+1}.$$

Hence

$$\mathrm{ord}_2(F_{2n+1}-1) = \begin{cases} \mathrm{ord}_2(F_n) + \mathrm{ord}_2(L_{n+1}) & \text{if } n \text{ is even,} \\ \mathrm{ord}_2(L_n) + \mathrm{ord}_2(F_{n+1}) & \text{if } n \text{ is odd.} \end{cases}$$

We only consider the case where $F_n$ is even (the case where $F_{n+1}$ is even is similar). We apply Theorem 4.1.2 to the case where $(a,b,c) = (F_{n+1}, F_n, F_{2n+1})$. Since $F_{2n+1} - 1 > F_n^2$,

$$\mathrm{ord}_2(F_{2n+1}-1) = \begin{cases} \mathrm{ord}_2(F_n) & \text{if } n \text{ is even,} \\ \mathrm{ord}_2(L_n) & \text{if } n \text{ is odd,} \end{cases}$$

and $\mathrm{ord}_2(L_n) \le 2$, we see that

$$\frac{\mathrm{ord}_2(F_{2n+1}-1)}{2\,\mathrm{ord}_2(F_n)} \le \frac{\mathrm{ord}_2(F_n)+1}{2\,\mathrm{ord}_2(F_n)} \le 1 < \frac{\log(F_{2n+1}-1)}{2\log F_n}.$$

Therefore, Case (i) in Theorem 4.1.2 holds. □

**Remark 4.2.1** Lemma 4.2.3 can be also shown by the result in [Fi], which states that the only Fibonacci numbers being a square increased by 1 are $F_1 = F_2 = 1$, $F_3 = 2$ and $F_5 = 5$. Another proof of this result is given in [BLMS]. Further, if the condition

$$Y = \frac{\mathrm{ord}_2(c-1)}{2\,\mathrm{ord}_2(b)}$$

holds, then $Y = 1$ by an observation in the proof of Lemma 4.2.3. Then we may apply results on lower bounds for liner forms in two logarithms (for example, [La]) to the equation. As a result, we can estimate the value of $X$ as follows: $X \ll \log F_{2n+1}$. But the implied constant is very larger than one obtained in Lemma 4.2.3.

We are ready to prove Theorem 4.2.1.

*Proof of Theorem 4.2.1.* We only consider the case where $F_{n+1}$ is even (the case where $F_n$ is even is similar). Let $(x, y, z)$ be a solution of (4.2.1). By (i) in Lemma 4.2.1, we can write $x = 2X$ and $y = 2Y$, where $X, Y \in \mathbb{N}$. It suffices to show that $M := \max(X, Y) \leq z$.

Suppose that $M > z$. We will observe that this leads to a contradiction. Then $z \geq 2$. We use (ii) in Lemma 4.2.1, (ii) in Lemma 4.2.2 and (ii) in Lemma 4.2.3. If $M = X$, then

$$F_{n+1} + z \leq X \leq \max\left( \frac{2\log(F_n + 1)}{\mathrm{ord}_2(F_{n+1})\log 2} - 1,\ \frac{\log(F_{2n+1} - 1)}{\log 3} \right),$$

which does not hold. If $M = Y$, then

$$F_n + z \leq Y \leq \max\left( \frac{\log(F_n + 1)}{\mathrm{ord}_2(F_{n+1})\log 2},\ \frac{\log(F_{2n+1} - 1)}{2\,\mathrm{ord}_2(F_{n+1})\log 2} \right) = \frac{\log(F_{2n+1} - 1)}{2\,\mathrm{ord}_2(F_{n+1})\log 2},$$

which does not hold. Therefore, $M \leq z$. This completes the proof of Theorem 4.2.1. □

### 4.2.2 Proof of Theorem 4.2.2

In this subsection we prove Theorem 4.2.2. Let $n \geq 3$. We first note that $F_n, F_{n+2}$ and $F_{2n+2}$ are pair-wise relatively prime positive integers greater than 1.

Let $(x, y, z)$ be a solution of (4.2.2). We prepare several lemmas. First we determine the parities of $x, z$ by using congruence reductions.

**Lemma 4.2.4** *$x$ and $z$ are even.*

*Proof.* Similarly to the proof of Lemma 4.2.1, we can prove the lemma for the case $n \leq 4$. Hence it suffices to consider the case $n \geq 5$. Then $F_n \not\equiv \pm 1 \pmod{F_{n+2}}$ and $F_{n+2} \not\equiv \pm 1 \pmod{F_n}$.

We write $x = 2X + x_2$, where $X$ is a non-negative integer and $x_2 \in \{0, 1\}$. Then taking (4.2.2) modulo $F_{n+2}$, we have

$$F_n^{2X} F_n^{x_2} \equiv (-1)^{y+1} F_n^{2y} \pmod{F_{n+2}}.$$

By Cassini's identity, we see that

$$F_n^2 \equiv F_{n+1}^2 = -\delta + F_n F_{n+2} \equiv -\delta \pmod{F_{n+2}},$$

where $\delta = (-1)^{n+1}$. Hence

$$(-\delta)^X F_n^{x_2} \equiv (-1)^{y+1} (-\delta)^y \pmod{F_{n+2}}.$$

If $x_2 = 1$, then $F_n \equiv \pm 1 \pmod{F_{n+2}}$, which is absurd. Hence $x_2 = 0$, that is, $x = 2X$. Similarly, we can prove that $z$ is even by taking (4.2.2) modulo $F_n$ (for this, we use the congruences $F_{n+2}^2 \equiv -\delta \pmod{F_n}$ and $F_{n+2} \not\equiv \pm 1 \pmod{F_n}$). □

By Lemma 4.2.4, we can write $x = 2X$ and $z = 2Z$, where $X, Z \in \mathbb{N}$.

**Lemma 4.2.5** *If $y > 1$, then $X + Z \equiv 0 \pmod{F_{n+1}}$. In particular, $F_{n+1} \leq X + Z$.*

*Proof.* Suppose that $y > 1$. Note that $F_{n+1}$ divides $F_{2n+2}$. Taking (4.2.2) modulo $F_{n+1}^2$, we have

$$F_n^{2X} \equiv F_{n+2}^{2Z} \pmod{F_{n+1}^2}.$$

By Cassini's identity, we see that

$$\begin{aligned} F_n^2 &= \delta + F_{n-1}F_{n+1} \equiv \delta - F_nF_{n+1} \pmod{F_{n+1}^2}, \\ F_{n+2}^2 &= \delta + F_{n+1}F_{n+3} \equiv \delta + F_nF_{n+1} \pmod{F_{n+1}^2}, \end{aligned}$$

where $\delta = (-1)^{n+1}$. Hence

$$\delta^X - \delta^{X-1}F_nF_{n+1}X \equiv \delta^Z + \delta^{Z-1}F_nF_{n+1}Z \pmod{F_{n+1}^2}.$$

Reducing this modulo $F_{n+1}$, we have $\delta^X \equiv \delta^Z \pmod{F_{n+1}}$. This implies that $\delta^X = \delta^Z$ since $\delta = \pm 1$ and $F_{n+1} \geq 3$. It follows from the above congruence that $X + Z \equiv 0 \pmod{F_{n+1}}$. □

From (4.2.2) we define positive integers $D, E$ as follows:

$$F_{2n+2}^{\,y} = DE, \tag{4.2.4}$$

where

$$D = F_{n+2}^Z + F_n^X, \quad E = F_{n+2}^Z - F_n^X. \tag{4.2.5}$$

If $y = 1$, then $F_{n+2}^Z < F_{2n+2}$, which gives that $Z < (\log F_{2n+2})/\log F_{n+2} < 2$, so $Z = 1$, hence $X = 1$.

In what follows, we put

$$\alpha = \mathrm{ord}_2(F_{n+1}), \quad \beta = \mathrm{ord}_2(F_{2n+2}).$$

Since $F_{2n+2} = F_{n+1}L_{n+1}$, we have $\beta = \alpha + \mathrm{ord}_2(L_{n+1})$. It is easy to see from two tables in Section 1 that $\beta \geq 3$ when $\alpha \geq 1$, and $\beta = 3$ when $\alpha = 1$, further, $\beta = 0$ when $\alpha = 0$.

It is easy to see from the first table in Section 1 that

$$F_m \not\equiv 6 \pmod{8}$$

for all $m \geq 0$.

**Lemma 4.2.6** *$y$ is odd.*

*Proof.* Suppose that $y$ is even. We will observe that this leads to a contradiction. We can write $y = 2Y$, where $Y \in \mathbb{N}$. By Lemma 4.2.5, we have

$$F_{n+1} \leq X + Z.$$

We use Theorem 4.1.1. Similarly to the proof of Lemma 4.2.2, we can prove that $X + Z \ll F_n$. As a result, $n, X, Y$ and $Z$ are bounded above. It is easy to see that any of them does not satisfy (4.2.2). This is a contradiction. We conclude that $y$ is odd. □

We consider the cases $\alpha = 0$ and $\alpha \geq 1$ separately. It is easy to see that $\gcd(D, E) = 2$ when $\alpha \geq 1$.

**Lemma 4.2.7** *If $F_{n+1}$ is even, then $X$ and $Z$ are odd.*

*Proof.* We consider the case where $F_{n+1}$ is even, that is, $\alpha \geq 1$. Then $\beta \geq 3$. Suppose that $X$ or $Z$ is even. We will observe that this leads to a contradiction. Since $y > 1$, we see from Lemma 4.2.5 that both $X$ and $Z$ are even, and

$$F_{n+1} \leq X + Z.$$

We can write $X = 2X'$ and $Z = 2Z'$, where $X', Z' \in \mathbb{N}$. Applying Theorem 4.1.3 to the case where $(a, b, c) = (F_n, F_{2n+2}, F_{n+2})$, we have

$$y < \frac{\log F_{2n+2}}{3 \log 2},$$

$$X' < \frac{\log (F_{2n+2}/8)}{2 \log F_n}\, y < y, \quad Z' < \frac{\log (F_{2n+2}/4)}{2 \log F_{n+2}}\, y < y.$$

Hence

$$\frac{F_{n+1}}{2} \leq X' + Z' \leq 2y - 2 < \frac{2 \log F_{2n+2}}{3 \log 2} - 2,$$

which does not hold. This is absurd. We conclude that $X$ and $Z$ are odd. □

**Lemma 4.2.8** *If $F_{n+1} \equiv 2 \pmod 4$, then $(X, y, Z) = (1, 1, 1)$.*

*Proof.* We consider the case where $F_{n+1} \equiv 2 \pmod 4$, that is, $\alpha = 1$. Then $\beta = 3$. It is easy to see that $F_n \equiv 1 \pmod 4$ and $F_{n+2} \equiv -1 \pmod 4$. By Lemma 4.2.7, we know that $X$ and $Z$ are odd. Hence $D = F_{n+2}^Z + F_n^X \equiv (-1)^Z + 1 \equiv 0 \pmod 4$. Since $\gcd(D, E) = 2$, we see from (4.2.4) and (4.2.5) that there exist relatively prime odd positive integers $S, T$ such that

$$D = F_{n+2}^Z + F_n^X = 2^{3y-1} S,$$
$$E = F_{n+2}^Z - F_n^X = 2T.$$

Then $F_{n+2}^Z = (D + E)/2 = 2^{3y-2} S + T$, so $2^{3y-2} S \equiv 3 - T \pmod 4$. Note that the square of an odd integer is congruent to 1 modulo 8. Since $F_m \not\equiv 6 \pmod 8$ for all $m \geq 0$, and

$$2T = F_{n+2}^Z - F_n^X \equiv F_{n+2} - F_n = F_{n+1} \pmod 8,$$

it follows that $2T \equiv 2 \pmod 8$, that is, $T \equiv 1 \pmod 4$. Hence $2^{3y-2} S \equiv 2 \pmod 4$. This gives that $y = 1$, so $X = Z = 1$. □

**Lemma 4.2.9** *If $F_{n+1} \equiv 0 \pmod 4$, then $(X, y, Z) = (1, 1, 1)$.*

*Proof.* We consider the case where $F_{n+1} \equiv 0 \pmod 4$, namely, $\alpha \geq 2$. Then $\beta \geq 3$, and $L_{n+1}$ is even. Note that $n \geq 5$. It is easy to see that $F_n \equiv F_{n+2} \equiv 1 \pmod 4$, so $D = F_{n+2}^Z + F_n^X \equiv 2 \pmod 4$. Since $\gcd(D, E) = 2$, we see from (4.2.4) that $E$ is divisible by $2^{\beta y - 1}$. In particular, $E$ is divisible by 4 since $\beta y - 1 \geq 3y - 1 \geq 2$.

By Lemma 4.2.7, we can write $X = 2X' + 1$ and $Z = 2Z' + 1$, where $X', Z'$ are non-negative integers. Then

$$E = F_{n+2}^Z - F_n^X \equiv F_n^Z - F_n^X = F_n\big(F_n^{2Z'} - F_n^{2X'}\big) \pmod{F_{n+1}}.$$

By Cassini's identity, we see that

$$F_n^2 = \delta + F_{n-1}F_{n+1} \equiv \delta \pmod{F_{n+1}},$$

where $\delta = (-1)^{n+1}$. Hence

$$E \equiv F_n\big(\delta^{Z'} - \delta^{X'}\big) \pmod{F_{n+1}}.$$

Reducing this modulo 4, we have $\delta^{Z'} - \delta^{X'} \equiv 0 \pmod 4$. This implies that $\delta^{Z'} - \delta^{X'} = 0$ since $\delta = \pm 1$. Hence $E \equiv 0 \pmod{F_{n+1}}$. It follows that $D/2$ is odd and prime to $F_{n+1}$. Since $F_{2n+2} = F_{n+1}L_{n+1}$, we can rewrite (4.2.4) as

$$\left(\frac{D}{2}\right) E = 2^{y-1} F_{n+1}^y \left(\frac{L_{n+1}}{2}\right)^y.$$

This implies that $D/2$ divides $(L_{n+1}/2)^y$ and $E$ is divisible by $2^{y-1}F_{n+1}^y$.

Since $L_{n+1} = F_{n+1} + 2F_n$ and $F_n/F_{n+1} \leq 5/8$, we see that

$$1 < \frac{D}{E} \leq \frac{2\left(L_{n+1}/2\right)^y}{2^{y-1}F_{n+1}^y} = 4\left(\frac{L_{n+1}}{4F_{n+1}}\right)^y = 4\left(\frac{1}{4} + \frac{F_n}{2F_{n+1}}\right)^y \leq 4\left(\frac{9}{16}\right)^y.$$

This gives that $y < 3$. By Lemma 4.2.6, we conclude that $y = 1$, so $X = Z = 1$. □

We are ready to prove Theorem 4.2.2.

*Proof of Theorem 4.2.2.* By Lemmas 4.2.8 and 4.2.9, it suffices to consider the case where $F_{n+1}$ is odd, that is, $\alpha = 0$. Then $\beta = 0$. Let $(x, y, z)$ be a solution of (4.2.2). By Lemma 4.2.4, we can write $x = 2X$ and $z = 2Z$, where $X, Z \in \mathbb{N}$. By Lemma 4.2.6, we know that $y$ is odd.

If $n = 3$, then $4^X + 21^y = 25^Z$. Taking this modulo 8, we have $4^X \equiv 4 \pmod 8$, hence $X = 1$.

We apply Theorem 4.1.4 to the case where $(a, b, c) = (F_n, F_{2n+2}, F_{n+2})$. Then

$$X < \frac{y \log\big(F_{2n+2}/p(F_{2n+2})\big) - \log 2}{\log F_n} < 3y,$$

$$Z < \frac{\log\big(F_{2n+2}/p(F_{2n+2})\big)}{\log F_{n+2}}\, y < 2y.$$

Suppose that $y > 1$. We will observe that this leads to a contradiction.

If $F_n$ is even, then

$$y \le \mathcal{C}_4 \log F_{n+2} + 1,$$

where

$$\mathcal{C}_4 = \frac{\log\bigl(F_{2n+2}/(2p(F_{2n+2})) + p(F_{2n+2})/2\bigr)}{\mathrm{ord}_2(F_n)(\log 2)\log\bigl(\sqrt{F_{2n+2}+1}-1\bigr)}.$$

Hence Lemma 4.2.5 yields

$$F_{n+1} \le X + Z \le 5y - 2 \le 5\,\mathcal{C}_4 \log F_{n+2} + 3,$$

which implies that $n = 3$ and $y = 3$. This is absurd since $4 + 21^3 \ne 25^Z$.

If $F_{n+2}$ is even, then

$$Z \le \frac{\log\bigl(F_{2n+2}/(2p(F_{2n+2})) + p(F_{2n+2})/2\bigr)}{\mathrm{ord}_2(F_{n+2})\log 2}.$$

Hence Lemma 4.2.5 yields

$$\begin{aligned} F_{n+1} \le X + Z &< \left(\frac{\log F_{n+2}}{\log F_n} + 1\right) Z \\ &\le \left(\frac{\log F_{n+2}}{\log F_n} + 1\right) \frac{\log\bigl(F_{2n+2}/(2p(F_{2n+2})) + p(F_{2n+2})/2\bigr)}{\mathrm{ord}_2(F_{n+2})\log 2}, \end{aligned}$$

which does not hold. This is a contradiction. We conclude that $y = 1$, so $X = Z = 1$. This completes the proof of Theorem 4.2.2. □

# List of papers by Takafumi Miyazaki

**(1)** Takafumi Miyazaki, On the conjecture of Jeśmanowicz concerning Pythagor ean triples, *Bull. Austral. Math. Soc.* **80** (2009), 413–422.

**(2)** Takafumi Miyazaki, Exceptional cases of Terai's conjecture on Diophantine equations, *Arch. Math. (Basel)* **95** (2010), 519–527.

**(3)** Takafumi Miyazaki, Terai's conjecture on exponential Diophantine equations, *Int. J. Number Theory* **4** (2011), 981–999.

**(4)** Takafumi Miyazaki, The shuffle variant of Jeśmanowicz' conjecture concerning Pythagorean triples, *J. Austral. Math. Soc.* **90** (2011), 355–370.

**(5)** Takafumi Miyazaki, Jeśmanowicz' conjecture on exponential Diophantine equations, *Funct. Approx. Comment. Math.* **45** (2011), 207–229.

**(6)** Takafumi Miyazaki, Generalizations of classical results on Jeśmanowicz' conjecture concerning Pythagorean triples, submitted.

**(7)** Takafumi Miyazaki, Upper bounds for solutions of exponential Diophantine equations with applications to Fibonacci numbers, submitted.

**(8)** Takafumi Miyazaki (with Alain Togbé), The Diophantine equation $(2am-1)^x+(2m)^y=(2am+1)^z$, submitted.

**(9)** Takafumi Miyazaki, The shuffle variant of Terai's conjecture on exponential Diophantine equations, submitted.

# Bibliography


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

[BS] F. Beukers and H. P. Schlickewei, 'The equation $x + y = l$ in finitely generated groups', *Acta Arith.* **78** (1996), 189–199.

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

[Br] N. Bruin, 'The Diophantine equations $x^2 \pm y^4 = \pm z^6$ and $x^2 + y^8 = z^3$', *Compositio Math.* **118** (1999), 305–321.

[Br2] ——, 'On powers as sums of two cubes', ANTS IV, Leiden 2000, 169–184, *Lecture Notes in Comput. Sci.* **1838** (Springer, 2000).

[Br3] ——, 'Chabauty methods using elliptic curves', *J. Reine Angew. Math.* **562** (2003), 27–49.

[BLMS] Y. Bugeaud, F. Luca, M. Mignotte and S. Siksek, 'Fibonacci Numbers at most one away from a perfect power', *Elem. Math.* **63** (2008), 65–75.

[BMS] Y. Bugeaud, M. Mignotte and S. Siksek, 'Classical and modular approaches to exponential Diophantine equations. I. Fibonacci and Lucas perfect powers', *Annals of Math.* **163** (2006), 969–1018.

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

[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.

[CM] M. Cipu and M. Mignotte, 'On a conjecture on exponential Diophantine equations', *Acta Arith.* **140** (2009), 251–270.

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

[Coh] J. H. E. Cohn, 'On square Fibonacci numbers', *J. London Math. Soc.* **39** (1964), 537–540.

[Coh2] ——, 'Lucas and Fibonacci numbers and some Diophantine equations', *Proc. Glasgow Math. Assoc.* **7** (1965), 24–28.

[Coh3] ——, 'The Diophantine equation $x^2 + 2^k = y^n$', *Arch. Math. (Basel)* **59** (1992), 341–344.

[Cr] J. Cremona, *Algorithms for Modular Elliptic Curves* (Cambridge University Press, 1992).

[Da] H. Darmon, 'The equation $x^4 - y^4 = z^p$', *C. R. Math. Rep. Acad. Sci. Canada.* **15** (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. Vyssh. Ucebn. Zaved. Mat.* **48** (1965), 52–56 (in Russian).

[DC] M. -J. Deng and G. L. Cohen, 'A note on a conjecture of Jeśmanowicz', *Colloq. Math.* **86** (2000), 25–30.

[Di] L. E. Dicson, *History of the Theory of Numbers*, Vol. 2 (Chelsea, New York, 1966).

[Du] A. Dujella, 'A proof of the Hoggatt-Bergum conjecture', *Proc. Amer. Math. Soc.* **127** (1999), 1999–2005.

[Eu] L. Euler, 'Auflösung solcher Fragen, worzu Cubi erfordert werden', Opera Omnia, (1), I, Capital **15**, 484–498.

[Fi] R. Finkelstein, 'On Fibonacci numbers which are more than a square', *J. Reine Angew. Math.* **262/263** (1973), 171–178.

[Ha] T. Hadano, 'On the Diophantine equation $a^x + b^y = c^z$', *Math. J. Okayama Univ.* **19**, No.1 (1976/77), 25–29.

[Hi] N. Hirata-Kohno, '$S$-unit equations and integer solutions to exponential Diophantine equations', *Analytic Number Theory and Surrounding Areas. RIMS Kokyuroku* **1511** (2006), 92–97.

[HY] Z. -Y. Hu and P. -Z. Yuan, 'On the exponential Diophantine equation $a^x + b^y = c^z$', *Acta Mathematica Sinica, Chinese Series* **48** (2005), 1175–1178 (in Chinese).

[Iv] W. Ivorra, 'Sur les équations $x^p + 2^\beta y^p = z^2$ et $x^p + 2^\beta y^p = 2z^2$', *Acta Arith.* **108** (2003), 327–338.

[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 Jeśmanowicz conjecture', ibid. **2** (1958), 81–90 (in Chinese).

[Ko3] ——, 'On the Diophantine equation $x^2 = y^n + 1, xy \neq 0$', *Sci. Sinica*, **14** (1965), 457–460.

[Kos] T. Koshy, *Fibonacci Numbers and Lucas Numbers with Applications* (Pure and Applied Mathematics, Wiley, 2001).

[La] M. Laurent, 'Linear forms in two logarithms and interpolation determinants II', *Acta Arith.* **133.4** (2008), 325–348.

[Le] V.A. Lebesgue, 'Sur l'impossibilité, en nombres entiers, de l'équation $x^m = y^2 + 1$', *Nouvelles annales de mathématiques* **9** (1850), 178–181.

[Lem] M. -H. Le, 'A conjecture concerning the exponential Diophantine equation $a^x + b^y = c^z$', *Acta Arith.* **106** (2003), 345–353.

[Lem2] ——, 'An open problem concerning the Diophantine equation $a^x + b^y = c^z$', *Publ. Math. Debrecen* **68** (2006), 283–295.

[Lem3] ——, 'A note on the Diophantine system $a^2 + b^2 = c^r$ and $a^x + b^y = c^z$', *Acta Mathematica Sinica, Chinese Series* **51** (2008), 677–684 (in Chinese).

[Lem4] ——, 'A note on Jeśmanowicz' conjecture concerning primitive Pythagorean triplets', *Acta Arith.* **138** (2009), 137–144.

[Lem5] ——, 'The pure exponential Diophantine equation $a^x + b^y = c^z$ for generalized Pythagorean triples', *Acta Mathematica Sinica, Chinese Series* **53** (2010), 1239–1248 (in Chinese).

[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).

[Ma] K. Mahler, 'Zur Approximation algebraischer Zahlen I: Über den grössten Primteiler binärer Formen', *Math. Ann.* **107** (1933), 691–730.

[Mak] A. Makowski, 'On the Diophantine equation $2^x + 11^y = 5^z$', *Noridisk Mat. Tidskr.* **7** (1959), 81.

[Mi] P. Mihăilescu, 'Primary cyclotomic units and a proof of Catalan's conjecture', *J. reine angew. Math.* **572** (2004), 167–195.

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

[Miy] T. Miyazaki, 'On the conjecture of Jeśmanowicz concerning Pythagorean triples', *Bull. Austral. Math. Soc.* **80** (2009), 413–422.

[Miy2] ——, 'Exceptional cases of Terai's conjecture on Diophantine equations', *Arch. Math. (Basel)* **95** (2010), 519–527.

[Miy3] ——, 'Terai's conjecture on exponential Diophantine equations', *Int. J. Number Theory* **4** (2011), 981–999.

[Miy4] ——, 'The shuffle variant of Jeśmanowicz' conjecture concerning Pythagorean triples', *J. Austral. Math. Soc.* **90** (2011), 355–370.

[Miy5] ——, 'Jeśmanowicz' conjecture on exponential Diophantine equations', *Funct. Approx. Comment. Math.* **45** (2011), 207–229.

[Miy6] ——, 'Generalizations of classical results on Jeśmanowicz' conjecture concerning Pythagorean triples', submitted.

[Miy7] ——, 'Upper bounds for solutions of exponential Diophantine equations with applications to Fibonacci numbers', submitted.

[Na] T. Nagell, 'Sur une classe d'equations exponentielles', *Ark. Mat.* **3** (1958), 569–582.

[Na] ——, *Introduction to number theory* (Chelsea, New York, 1981).

[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 ?* (Academic Press, Boston, MA, 1994).

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

[Si2] ——, *Pythagorean Triangles*, The Scripta Mathematica Studies, vol. 9, (Graduate School of Science, Yeshiva University, New York, 1962); Translated from the Polish by Dr. Ambikeshwar Sharma.

[Sik] S. Siksek, 'On the Diophantine equation $x^2 = y^p + 2^k z^p$', *J. Théor. Nombres Bordeaux* **15** (2003), 839–846.

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

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

[Te3] ——, 'On an exponential Diophantine equation concerning Fibonacci numbers', *Abstracts of short communications and poster sessions: Beijing 2002 August 20 - 28*, International Congress of Mathematicians (Higher Education Press, 2002).

[Uc] S. Uchiyama, 'On the Diophantine equation $2^x = 3^y + 13^z$', *Math. J. Okayama Univ.* **19** (1976), 31–38.

[Wa] A. Wakulicz, 'On the equation $x^3 + y^3 = 2z^3$', *Colloq. Math.* **5** (1957), 11–15.