

On the generalized Ramanujan-Nagell equation $x^2 + b^m = c^n$

Nobuhiro Terai (Oita University)

Abstract

In this paper, we consider the generalized Ramanujan-Nagell equations $x^2 + (2c - 1)^m = c^n$, $x^2 + (4c)^m = (c + 1)^n$, $x^2 + b^m = c^n$ with $a^2 + b^2 = c^2$, where a, b, c are positive integers. We propose conjectures concerning the above three equations, and verify that these conjectures are true for many cases.

1 Introduction

In 1913, Ramanujan [R] conjectured that the equation $x^2 + 7 = 2^n$ has only the positive integer solutions $(x, n) = (1, 3), (3, 4), (5, 5), (11, 7), (181, 15)$. In 1960, Nagell [N] resolved Ramanujan's conjecture. Let b and c be fixed relatively prime positive integers greater than one. Then the generalized Ramanujan-Nagell equation

$$x^2 + b^m = c^n$$

in positive integers x, m and n has been studied by a number of authors: (cf. [CD1], [CD2], [DGX], [Le1], [Le2], [Le3], [LS], [M], [To2] and [YW])

- (Tanahashi [Ta], Toyozumi [To1]) $x^2 + 7^m = 2^n$.
- (Alter-Kubota [AK], Tanahashi [Ta]) $x^2 + 11^m = 3^n$.
- (Bugeaud [Bu]) $x^2 + D^m = 2^n$.
- (Yaun-Hu [YH]) $x^2 + D^m = p^n$.
- (Terai [Te1], [Te3]) $x^2 + q^m = p^n$, $x^2 + q^m = c^n$.

In this paper, we consider the following generalized Ramanujan-Nagell equation:

$$\begin{aligned}x^2 + (2c - 1)^m &= c^n, \\x^2 + (4c)^m &= (c + 1)^n, \\x^2 + b^m &= c^n \text{ with } a^2 + b^2 = c^2,\end{aligned}$$

where a, b, c are positive integers. We propose conjectures concerning the above three equations. Using deep results of exponential Diophantine equations and Baker's method, we show that these conjectures are true for several cases. It is expected that for fixed coprime positive integers b, c , the equation $x^2 + b^m = c^n$ has at most three positive integer solutions (x, m, n) except for the equations $x^2 + 7^m = 2^n$ and $x^2 + 2^m = 3^n$ which have only the following solutions, respectively:

$$\begin{aligned}x^2 + 7^m = 2^n; (x, m, n) &= (1, 1, 3), (3, 1, 4), (5, 1, 5), (11, 1, 7), (181, 1, 15), (13, 3, 9), \\x^2 + 2^m = 3^n; (x, m, n) &= (1, 1, 1), (1, 3, 2), (5, 1, 3), (7, 5, 4).\end{aligned}$$

2 Preliminaries

In the proof of our Theorems, we need the following several Propositions concerning the generalized Fermat equations, the Nagell-Ljunggren equation, the generalized Ramanujan-Nagell equations and the Primitive Divisor Theorem.

Proposition 2.1 (Bennett-Skinner [BS]). *Let n be a positive integer with $n \geq 4$. Then the equation*

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

has no solutions in pairwise coprime positive integers (x, y, z) with $xyz > 1$.

Proposition 2.2 (Ellenberg [E]). *Let n be a positive integer with $n \geq 4$. Then the equation*

$$x^2 + y^4 = z^n$$

has no solutions in nonzero pairwise coprime integers x, y, z .

We will introduce here some notation. Let α_1 and α_2 be real algebraic numbers with $|\alpha_1| \geq 1$ and $|\alpha_2| \geq 1$. 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. As usual, the *logarithmic height* of an algebraic number α of degree d is defined as

$$h(\alpha) = \frac{1}{d} \left(\log |a_0| + \sum_{j=1}^d \log \max \left\{ 1, |\alpha^{(j)}| \right\} \right),$$

where a_0 is the leading coefficient of the minimal polynomial of α (over \mathbb{Z}) and $(\alpha^{(j)})_{1 \leq j \leq d}$ are the conjugates of α in the field of complex numbers. Let A_1 and A_2 be real numbers greater than 1 with

$$\log A_i \geq \max \left\{ h(\alpha_i), \frac{|\log \alpha_i|}{D}, \frac{1}{D} \right\}$$

for $i \in \{1, 2\}$, where D is the degree of the number field $\mathbb{Q}(\alpha_1, \alpha_2)$ over \mathbb{Q} . Define

$$b' = \frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1}.$$

We choose to use a result due to Laurent [La, Corollary 2] with $m = 10$ and $C_2 = 25.2$.

Proposition 2.3 ([La]). *Let Λ be given as above, with $\alpha_1 > 1$ and $\alpha_2 > 1$. Suppose that α_1 and α_2 are multiplicatively independent. Then*

$$\log |\Lambda| \geq -25.2 D^4 \left(\max \left\{ \log b' + 0.38, \frac{10}{D}, 1 \right\} \right)^2 \log A_1 \log A_2.$$

Proposition 2.4 (Ljunggren [Lj]). *The equation*

$$\frac{x^n - 1}{x - 1} = y^2$$

has no solutions in integers x, y, n with $|x| > 1$ and $n \geq 3$, except for $(n, x, y) = (4, 7, 20), (5, 3, 11)$.

Proposition 2.5 (Bugeaud [Bu]). *Let D be an odd positive integer. Then the equation*

$$x^2 + D^m = 2^n$$

in positive integers x, m, n has at most one solution (x, m, n) , except for the cases $D = 7, 23, 2^k - 1$ ($k \geq 4$), where the equation has only the following solutions, respectively.

(i) $c = 7$; $(x, m, n) = (1, 1, 3), (3, 1, 4), (5, 1, 5), (11, 1, 7), (181, 1, 15), (13, 3, 9)$.

(ii) $c = 23$; $(x, m, n) = (3, 1, 5), (45, 1, 11)$.

(iii) $c = 2^k - 1$ ($k \geq 4$); $(x, m, n) = (308, 1, 2), (5458, 1, 3)$.

Remark. In Theorem 3 of Bugeaud [Bu], it was stated that the exceptional cases are $D = 7, 15$. But we point out that the ones are $D = 7, 23, 2^k - 1$ ($k \geq 4$). (cf. Theorem 2 of Beukers [Be].)

Proposition 2.6 (Bugeaud [Bu], Yaun-Hu [YH]). *Let $D > 2$ be an integer and let p be an odd prime not dividing D . If $(D, p) \neq (4, 5)$, then the equation*

$$x^2 + D^m = p^n$$

has at most two positive integer solutions (x, m, n) . If the two solutions are (x_1, m_1, n_1) and (x_2, m_2, n_2) , then $m_1 \not\equiv m_2 \pmod{2}$. The equation $x^2 + 4^m = 5^n$ has exactly three positive integer solutions (x, m, n) .

Proposition 2.7 (Le [Le4]). *The equation*

$$x^2 + 2^m = y^n, \gcd(x, y) = 1, n \geq 3$$

has only the positive integer solutions $(x, y, m, n) = (5, 3, 1, 3), (7, 3, 5, 4), (11, 5, 2, 3)$.

Proposition 2.8 (Ivorra [I]). *The equation*

$$x^2 - 2^m = y^n, \gcd(x, y) = 1, |y| > 1, m \geq 2, n \geq 3$$

has only the integer solutions $(x, y, m, n) = (\pm 13, -7, 9, 3), (\pm 71, 17, 7, 3)$.

Proposition 2.9 (Zsigmondy [Z]). *Let A and B be relatively prime integers with $A > B \geq 1$. Let $\{a_k\}_{k \geq 1}$ be the sequence defined as*

$$a_k = A^k + B^k.$$

If $k > 1$, then a_k has a prime factor not dividing $a_1 a_2 \cdots a_{k-1}$, whenever $(A, B, k) \neq (2, 1, 3)$.

3 The equation $x^2 + (2c - 1)^m = c^n$

In [Te3], the author showed that if $2c - 1$ is a prime and $2c - 1 \equiv 3, 5 \pmod{8}$, then the equation $x^2 + (2c - 1)^m = c^n$ has only the positive integer solution $(x, m, n) = (c - 1, 1, 2)$, and proposed the following:

Conjecture 3.1. *Let c be a positive integer with $c \geq 2$. Then the equation*

$$x^2 + (2c - 1)^m = c^n \tag{3.1}$$

has only the positive integer solution $(x, m, n) = (c - 1, 1, 2)$.

In this paper, we show that if $2c - 1 = 3p^l$ or $2c - 1 = 5p^l$, then Conjecture 3.1 is true without any congruence condition on a prime p :

Theorem 3.1. *Suppose that at least one of the following conditions holds:*

(C₁) $2c - 1 = 3p^l$ with p a prime and l a positive integer,

(C₂) $2c - 1 = 5p^l$ with p a prime and l a positive integer.

Then Conjecture 3.1 is true.

3.1 An important lemma

In this section, we show that if $\alpha t \geq 2$, then the equation $5^m + (2^t \cdot 3^\alpha - 5)^m = 2(5 \cdot 2^{t-1} \cdot 3^\alpha - 12)^N$ has no positive integer solutions m, N, α, t with $mN \equiv 1 \pmod{2}$, which will be needed in the proof of Theorem 1. (cf. Lemma 1 of Fujita-Terai [FT1])

Lemma 3.1. *The equation*

$$5^m + (2^t \cdot 3^\alpha - 5)^m = 2(5 \cdot 2^{t-1} \cdot 3^\alpha - 12)^N \quad (3.2)$$

has no solution (m, N, α, t) in positive integers with $mN \equiv 1 \pmod{2}$ and $\alpha t \geq 2$.

Remark. When $\alpha = t = 1$, equation (3.2) becomes

$$5^m + 1 = 2 \cdot 3^N.$$

It follows from Proposition 2.4 that the above equation has only the positive integer solution $(m, N) = (1, 1)$. (cf. Equation (2.2) in Terai [Te3] with $c = 3$.)

3.2 Proof of Theorem 3.1

(C₁) Let (x, m, n) be a solution of (3.1). By Proposition 3.3 of [Te3], we may suppose that $p \neq 3$.

Since $2c - 1 \equiv 0 \pmod{3}$, we have $c \equiv 2 \pmod{3}$. Taking (3.1) modulo 3 implies that n is even, say $n = 2N$. Then from (3.1), we have

$$(2c - 1)^m = (c^N + x)(c^N - x).$$

Since $2c - 1 = 3p$ and $\gcd(c^N + x, c^N - x) = 1$, we obtain the following two cases:

$$(2c - 1)^m + 1 = 2c^N \quad (3.3)$$

or

$$3^m + p^{lm} = 2c^N. \quad (3.4)$$

In the same way as in the proof of Theorem 1.2 of [Te3], It follows from Proposition 2.4 that equation (3.3) has only the solution $(m, N) = (1, 1)$.

Next we show that equation (3.4) has no solutions m, N . (It is not difficult to show that $m \geq 4$ in (3.4).) It follows from Proposition 2.1 that N is odd. The proof is divided into two cases (i) m is odd and (ii) m is even.

Case (i). m is odd. Then from (3.4), we show that $3 + p^l$ has an odd prime divisor r . On the contrary, suppose that $3 + p^l = 2^t$ with $t \geq 3$. If t is odd, then $\left(\frac{p^l}{3}\right) = \left(\frac{2}{3}\right) = -1$.

In view of $2c - 1 = 3p^l$, we have $\left(\frac{2c}{3}\right) = 1$. From (3.4), this is impossible, since N is odd. If t is even, then $p^l \equiv 13 \pmod{16}$ and so $c = (3p^l + 1)/2 \equiv 4 \pmod{8}$. Thus the left hand side of (3.4) is divisible by $p^l + 3 = 2^t$ (: exactly even power of 2), since $\frac{3^m + p^{lm}}{3 + p^l}$ is odd. On the other hand, the right hand side of (3.4) is divisible by exactly odd power of 2. This leads to a contradiction. Hence we see that $c = (3p^l + 1)/2$ is divisible by an odd prime divisor r of $3 + p^l$. Thus we have $c = (3p^l + 1)/2 \equiv 0 \pmod{r}$, i.e.,

$$-3^2 + 1 \equiv -2^3 \equiv 0 \pmod{r},$$

which is impossible.

Case (ii). m is even. Then it follows from Proposition 2.2 that if equation (3.1) has solutions (x, m, n) , then $m \equiv 2 \pmod{4}$. The left hand side of (3.4) is divisible by an odd prime divisor r of $(p^{2l} + 3^2)/2 \pmod{4}$. From (3.4), we see that r satisfies $c = (3p^l + 1)/2 \equiv 0 \pmod{r}$, i.e.,

$$3^2 p^{2l} - 1 \equiv 3^2 \cdot (-3^2) - 1 = -2 \cdot 41 \equiv 0 \pmod{r}.$$

This implies that $r = 41$ and so

$$p^{2l} + 3^2 = 2 \cdot 41^\alpha.$$

The above equation can be reduced to solving the following three elliptic equation according to $\alpha = 3u + v$ with $v = 0, 1, 2$:

$$Y^2 = X^3 - 36, \quad Y^2 = X^3 - 36 \cdot 41^2, \quad Y^2 = X^3 - 36 \cdot 41^4,$$

where

$$(X, Y) = (2 \cdot 41^u, 2p^l), \quad (2 \cdot 41^{u+1}, 2p^l \cdot 41), \quad (2 \cdot 41^{u+2}, 2p^l \cdot 41^2), \quad (3.5)$$

respectively. By Magma[BoCa], the above three elliptic curves have no integer points (X, Y) satisfying (3.5), respectively. Hence equation (3.1) has no positive integer solutions (x, m, n) .

(C_2) Let (x, m, n) be a solution of (3.1). By Proposition 3.3 of [Te3], we may suppose that $p \neq 5$.

Since $2c - 1 \equiv 0 \pmod{5}$, we have $c \equiv 3 \pmod{5}$. Taking (3.1) modulo 5 implies that n is even, say $n = 2N$. Then from (3.1), we have

$$(2c - 1)^m = (c^N + x)(c^N - x).$$

Since $2c - 1 = 5p^l$ and $\gcd(c^N + x, c^N - x) = 1$, we obtain the following two cases:

$$(2c - 1)^m + 1 = 2c^N \quad (3.6)$$

or

$$5^m + p^{lm} = 2c^N. \quad (3.7)$$

In the same way as in the proof of Theorem 1.2 of [Te3], it follows from Proposition 2.4 that equation (3.6) has only the solution $(m, N) = (1, 1)$.

Next we show that equation (3.7) has no solutions m, N . (It is not difficult to show that $m \geq 4$ in (3.4).) It follows from Proposition 2.1 that N is odd. The proof is divided into two cases (i) m is odd and (ii) m is even.

Case (i). m is odd. Then from (3.7), we show that $5 + p^l$ has an odd prime divisor r . On the contrary, suppose that $5 + p^l = 2^t$ with $t \geq 3$. If t is odd, then $\left(\frac{p^l}{5}\right) = \left(\frac{2}{5}\right) = -1$.

In view of $2c - 1 = 5p^l$, we have $\left(\frac{2c}{5}\right) = 1$. From (3.7), this is impossible, since N is odd. If t is even, then $p^l \equiv 11 \pmod{16}$ and so $c = (5p^l + 1)/2 \equiv 4 \pmod{8}$. Thus the left hand side of (3.7) is divisible by $p^l + 5 = 2^t$ (: exactly even power of 2), since $\frac{5^m + p^{lm}}{5 + p^l}$ is odd. On the other hand, the right hand side of (3.7) is divisible by exactly odd power of 2. This leads to a contradiction. Hence we see that $c = (5p^l + 1)/2$ is divisible by an odd prime divisor r of $5 + p^l$. Thus we have $c = (5p^l + 1)/2 \equiv 0 \pmod{r}$, i.e.,

$$-5^2 + 1 = -2^3 \cdot 3 \equiv 0 \pmod{r}.$$

This implies that $r = 3$ and so

$$p^l + 5 = 2^t \cdot 3^\alpha$$

for some positive integers α, t with $\alpha t \geq 2$. Hence, we have equation (3.2). Since both m and N are odd and $\alpha t \geq 2$, we see from Lemma 3.1 that equation (3.2) has no integer solutions.

Case (ii). m is even. Then it follows from Proposition 2.2 that if equation (3.1) has solutions (x, m, n) , then $m \equiv 2 \pmod{4}$. The left hand side of (3.7) is divisible by an odd prime divisor r of $(p^{2l} + 5^2)/2 \pmod{4}$. From (3.7), we see that r satisfies $c = (5p^l + 1)/2 \equiv 0 \pmod{r}$, i.e.,

$$5^2 p^{2l} - 1 \equiv 5^2 \cdot (-5^2) - 1 = -2 \cdot 313 \pmod{r}.$$

This implies that $r = 313$ and so

$$p^{2l} + 5^2 = 2 \cdot 313^\alpha.$$

The above equation can be reduced to solving the following three elliptic equation according to $\alpha = 3u + v$ with $v = 0, 1, 2$:

$$Y^2 = X^3 - 100, \quad Y^2 = X^3 - 100 \cdot 313^2, \quad Y^2 = X^3 - 100 \cdot 313^4,$$

where

$$(X, Y) = (2 \cdot 313^u, 2p^l), \quad (2 \cdot 313^{u+1}, 2p^l \cdot 313), \quad (2 \cdot 313^{u+2}, 2p^l \cdot 313^2), \quad (3.8)$$

respectively. By Magma[BoCa], the above three elliptic curves have no integer points (X, Y) satisfying (3.8), respectively. Hence equation (3.1) has no positive integer solutions (x, m, n) .

4 The equation $x^2 + (4c)^m = (c + 1)^n$

As an analogue of Conjecture 3.1, Terai-Nakashiki-Suenaga[TNS1] proposed the following:

Conjecture 4.1. *Let c be a positive integer with $c \geq 2$. Then the equation*

$$x^2 + (4c)^m = (c + 1)^n \quad (4.1)$$

has only the positive integer solution $(x, m, n) = (c - 1, 1, 2)$ except for the cases $c = 5, 7, 309$, where equation (4.1) has only the following positive integer solutions, respectively:

$$\begin{aligned} c = 5; & \quad (x, m, n) = (4, 1, 2), (14, 1, 3), \\ c = 7; & \quad (x, m, n) = (6, 1, 2), (22, 1, 3), (104, 3, 5), \\ c = 309; & \quad (x, m, n) = (308, 1, 2), (5458, 1, 3). \end{aligned}$$

In this section, we verify that this conjecture is true for several cases under some conditions on c . Our main result is the following:

Theorem 4.1. *Suppose that at least one of the following conditions is satisfied:*

- (i) $c = 2^k$, where k is a positive integer.
- (ii) $c = 2^k - 1$ ($k \geq 2$).
- (iii) $c = p^k - 1$, where p is a prime with $p \equiv 3 \pmod{4}$.
- (iv) $c = p^k$, where p is a prime with $p \equiv 3 \pmod{8}$ and k is odd.
- (v) $c = 2p^k$, where p is a prime with $p \equiv 1 \pmod{4}$.

Then Conjecture 4.1 is true.

4.1 The exponential Diophantine equations

We use the following Lemma 4.1 to show Theorem 4.1 (v).

Lemma 4.1. *Let q be an odd integer with $q \geq 3$.*

(1) *If $q \equiv 1 \pmod{4}$, then the equation*

$$2^{3m-2} + q^m = (2q+1)^n \quad (4.2)$$

has no positive integer solutions (m, n) .

(2) *If $q \equiv 1 \pmod{4}$, then the equation*

$$2^{3m-2}q^m + 1 = (2q+1)^n \quad (4.3)$$

has only the positive integer solution $(m, n) = (1, 1)$.

Proof. (1) It is clear that if $m = 1$, then equation (4.2) has no solutions. We may thus suppose that $m > 1$. Taking (4.2) modulo 4 implies that $q^m \equiv 3^n \pmod{4}$. In view of $q \equiv 1 \pmod{4}$, we see that n is even. Then it follows from Proposition 2.8 that equation (4.2) has no solutions.

(2) If $m = 1$, then equation (4.3) has only the solution $n = 1$. We may thus suppose that $m > 1$. Then taking (4.3) modulo 4 implies that $1 \equiv 3^n \pmod{4}$. Hence n is even, say $n = 2N$. Then

$$2^{3m-2}q^m = ((2q+1)^2 - 1) \frac{(2q+1)^{2N} - 1}{(2q+1)^2 - 1} = 2q \cdot (2q+2) \frac{(2q+1)^{2N} - 1}{(2q+1)^2 - 1}.$$

Since $\gcd(q+1, q) = 1$, the above implies that $(q+1) \mid 2^{3m-2}$, which is impossible, since $q \equiv 1 \pmod{4}$. \square

4.2 Proof of Theorem 4.1

(i) Our assertion follows from Proposition 2.7.

(ii) Let (x, m, n) be a solution of equation (4.1). Suppose that our assumptions are all satisfied.

We first note that that $n > m$ from (4.1). Indeed,

$$(c+1)^n = x^2 + (4c)^m > (4c)^m > (c+1)^m.$$

Since x is even, we put $x = 2^\alpha x_1$ with $\alpha \geq 1$ and x_1 odd. Then equation (4.1) leads to

$$2^{2\alpha} x_1^2 + 2^{2m} c^m = 2^{kn}. \quad (4.4)$$

We want to show that $\alpha = m$. If $\alpha > m$, then equation (4.4) implies that

$$2^{2m}(2^{2\alpha-2m} x_1^2 + c^m) = 2^{kn},$$

so $2m = kn > 2m$ from $k \geq 2$ and $n > m$, which is impossible. If $\alpha < m$, then equation (4.4), as above, implies that $2\alpha = kn$, so $2m > 2\alpha = kn > 2m$, which is impossible. Consequently we obtain $\alpha = m$. Dividing both sides of (4.4) by 2^{2m} yields

$$x_1^2 + (2^k - 1)^m = 2^{kn-2m}.$$

Then our assertion easily follows from Proposition 2.5.

(iii) In view of $p \equiv 3 \pmod{4}$, we see that m is odd. Then our assertion follows from Proposition 2.6.

(iv) Let (x, m, n) be a solution of equation (4.1). Suppose that our assumptions are all satisfied.

Put $c = p^k$ with $p \equiv 3 \pmod{8}$ and k odd. Since $c \equiv 3 \pmod{8}$, we can put $c + 1 = 2^2 d$ with d odd. From equation (4.1), x is even, say $x = 2^\alpha x_1$ with $\alpha \geq 1$ and x_1 odd. Then equation (4.1) leads to

$$2^{2\alpha} x_1^2 + 2^{2m} c^m = 2^{2n} d^n. \quad (4.5)$$

Note that $n > m$ as before. We want to show that $\alpha = m$. If $\alpha > m$, then equation (4.5) implies that $n = m$, which contradicts the fact that $n > m$. If $\alpha < m$, then equation (4.5) implies that $n = \alpha < m$, which contradicts the fact that $n > m$. Hence we obtain $\alpha = m$, so

$$x_1^2 + c^m = 2^{2(n-m)} d^n. \quad (4.6)$$

Then it follows that $n - m = 1$, since $x_1^2 + c^m \equiv 1 + 3^m \not\equiv 0 \pmod{8}$. From (4.6), we see that $1 + 3^m \equiv 4 \pmod{8}$, so m is odd. Therefore equation (4.6) can be written as

$$c^m = (2d^{\frac{m+1}{2}} + x_1)(2d^{\frac{m+1}{2}} - x_1).$$

Since two factors of the right hand side of the above are relatively prime and $c = p^k$, we obtain the following:

$$\begin{cases} 2d^{\frac{m+1}{2}} + x_1 = c^m, \\ 2d^{\frac{m+1}{2}} - x_1 = 1. \end{cases}$$

Adding these two equations yields

$$c^m + 1 = 4d^{\frac{m+1}{2}}. \quad (4.7)$$

From definition of d , we have

$$c + 1 = 4d.$$

If $m > 1$, then it follows from Proposition 2.9 that equation (4.7) has no solutions. Consequently we obtain $m = 1$, $n = 2$ and $x = c - 1$.

(v) Let (x, m, n) be a solution of equation (4.1). Suppose that our assumptions are all satisfied.

Put $q = p^k$ with $p \equiv 1 \pmod{4}$ and $C = 2q + 1$. Then taking equation (4.1) modulo 4 implies that $1 \equiv 3^n \pmod{4}$, so n is even, say $n = 2N$. From (4.1), we have

$$(2^3 q)^m = (C^N + x)(C^N - x).$$

Since $\gcd(C^N + x, C^N - x) = 2$ and $q = p^k$, we obtain the following two cases:

$$\begin{cases} C^N \pm x = 2^{3m-1}, \\ C^N \mp x = 2q^m \end{cases} \quad (4.8)$$

or

$$\begin{cases} C^N \pm x = 2^{3m-1}q^m, \\ C^N \mp x = 2. \end{cases} \quad (4.9)$$

First consider case (4.8). Adding these two equations yields

$$2^{3m-2} + q^m = (2q + 1)^N,$$

which has no solutions by Lemma 4.1, (1).

Next consider case (4.9). Adding these two equations yields

$$2^{3m-2}q^m + 1 = (2q + 1)^N,$$

which has only the solution $(m, N) = (1, 1)$ by Lemma 4.1, (2). Hence equation (4.1) has only the solution $(x, m, n) = (c - 1, 1, 2)$.

5 The equation $x^2 + b^m = c^n$ with $a^2 + b^2 = c^2$

Let a, b, c be positive integers satisfying $a^2 + b^2 = c^2$. Such a triple (a, b, c) is called a *Pythagorean triple*. If a, b, c are relatively prime, this triple is called *primitive*. It is well-known that a primitive Pythagorean triple (a, b, c) with b even can be parameterized by

$$a = u^2 - v^2, \quad b = 2uv, \quad c = u^2 + v^2,$$

where u and v are positive integers with $u > v$, $\gcd(u, v) = 1$ and $u \not\equiv v \pmod{2}$. In 1956, Jeśmanowicz [J] proposed the following conjecture on the exponential Diophantine equation concerning primitive Pythagorean triples:

Conjecture J. *Fix u and v as above. The equation*

$$(u^2 - v^2)^x + (2uv)^y = (u^2 + v^2)^z$$

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

This is a famous unsolved problem in the field of exponential Diophantine equations. Conjecture J has been verified to be true in many special cases. (cf. [LSS], [M], [MT], [Te2], [YH])

Related to Conjecture J, the author [Te1] proposed the following:

Conjecture 5.1. *Fix u and v as above. The equation*

$$x^2 + (u^2 - v^2)^m = (u^2 + v^2)^n \quad (5.1)$$

has only the positive integer solution $(x, m, n) = (2uv, 2, 2)$.

The author [Te1] proved that if $b_1 = u^2 - v^2$ and $c_1 = u^2 + v^2$ are primes such that (i) $b_1^2 + 1 = 2c_1$ and (ii) $d_1 = 1$ or even if $b_1 \equiv 1 \pmod{4}$, then Conjecture 5.1 is true, where d_1 is the order of a prime divisor of (c_1) in the ideal class group of $\mathbb{Q}(\sqrt{-b_1})$. In [CD1], [CD2], [Le1], [Le3] and [YW], it was shown that if $b_1 \not\equiv 1 \pmod{8}$, and b_1 or c_1 is a prime power, then Conjecture 5.1 is true. However, other than under such special conditions, Conjecture 5.1 remains unsolved.

In this section, we propose the following conjecture on the Diophantine equation concerning Pythagorean triples:

Conjecture 5.2. Fix u and v as above.

(1) If $3u^2 - 8uv + 3v^2 \neq -1$, then the equation

$$x^2 + (2uv)^m = (u^2 + v^2)^n \quad (5.2)$$

has only the positive integer solutions $(x, m, n) = (u - v, 1, 1)$, $(u^2 - v^2, 2, 2)$, except for the case $(u, v) = (244, 231)$, where the equation

$$x^2 + 112728^m = 112897^n \quad (5.3)$$

has exactly the three positive integer solutions $(x, m, n) = (13, 1, 1)$, $(6175, 2, 2)$, $(2540161, 3, 3)$.

(2) If $3u^2 - 8uv + 3v^2 = -1$, then equation (5.2) has exactly the three positive integer solutions $(x, m, n) = (u - v, 1, 1)$, $(u^2 - v^2, 2, 2)$, $((u - v)(2u^2 + 2v^2 + 1), 1, 3)$.

A simple computer search shows that Conjecture 5.2 is valid for $1 \leq v < u \leq 10^5$ and $m \leq 11$, $n \leq 11$.

It is worth remarking that equation (5.1) has (at least) one trivial solution, whereas equation (5.2) has (at least) two trivial solutions except for the cases $(u, v) = (244, 231)$ and $3u^2 - 8uv + 3v^2 = -1$. As shown in [Bu] and [YH], the equation $x^2 + 4^m = 5^n$ is the only equation of the form $x^2 + D^m = p^n$ which has (exactly) three solutions x, m, n , where $D > 2$ is a positive integer and p is an odd prime not dividing D . In addition, Corollary 1.1 of [YH] implies that if $u^2 + v^2$ is a prime power, then Conjecture 5.2 holds. Our main result is the following:

Theorem 5.1. Suppose that at least one of the following conditions is satisfied:

- (i) $u^2 + v^2 = w^2 + 1$ for a positive integer w , and any of the following holds:
 - $uv = 2k^2$ for an odd integer k ;
 - $uv = 2p^t$ for an odd prime p with $p \not\equiv 5 \pmod{8}$ and a positive integer t ;
 - $uv \equiv 10 \pmod{12}$.
- (ii) $u \in \{p, p^2\}$ and $v = 2$ for an odd prime p .
- (iii) $u = 244$ and $v = 231$.

Then Conjecture 5.2 is true.

5.1 The equation $x^2 + 4u = (u^2 + 4)^n$

The goal of this section is to show the case $m = 1$ of (ii) in Theorem 5.1.

Lemma 5.1. Let p be an odd prime. If either $u = p$ or $u = p^2$, then the equation

$$x^2 + 4u = (u^2 + 4)^n \quad (5.4)$$

has only the positive solution $(x, n) = (u - 2, 1)$.

Proof. It is easy to show that n must be odd. Consider the Pell equation

$$x^2 - (u^2 + 4)Y^2 = -4u. \quad (5.5)$$

For any solution (x, Y) to (5.5), there exist a non-negative integer ν and a solution (x_0, Y_0) to (5.5) such that

$$x + Y\sqrt{u^2 + 4} = (x_0 + Y_0\sqrt{u^2 + 4}) \left(\frac{u + \sqrt{u^2 + 4}}{2} \right)^{2\nu}$$

and

$$0 \leq |x_0| \leq u\sqrt{u}, \quad 0 < Y_0 \leq \sqrt{u} \quad (5.6)$$

in view of [St1, Theorem 2], together with the fact that the fundamental solution of the Pell equation $x^2 - (u^2 + 4)Y^2 = 4$ is $(u^2 + 2 + u\sqrt{u^2 + 4})/2$. In the case where $u = p$, since Theorem 6 in [St1] assures that (5.5) has at most one solution (x_0, Y_0) with x_0 non-negative satisfying (5.6), and $(x_0, Y_0) = (\pm(p-2), 1)$ satisfies (5.6), it follows that $x_0 = \pm(p-2)$ and $Y_0 = 1$. In the case where $u = p^2$, since the equation $x^2 - (p^4 + 4)Y^2 = -4$ has a solution $(x, Y) = (p^2, 1)$, we see from [St2, Theorem 3] that equation (5.5) has at most two solutions (x_0, Y_0) with x_0 non-negative satisfying (5.6), and thus $(x_0, Y_0) \in \{(\pm(p^2 - 2), 1), (p^3, p)\}$. Since one may consider only the solutions corresponding to the ones of equation (5.4), it follows from $\gcd(x, Y) = 1$ that $x_0 = \pm(p^2 - 2)$ and $Y_0 = 1$. In any case, therefore, one may write $x = \sigma_\nu$, where

$$\sigma_0 = \pm(u - 2), \quad \sigma_1 = \pm \frac{(u - 2)(u^2 + 2)}{2} + \frac{u(u^2 + 4)}{2}, \quad \sigma_{\nu+2} = (u^2 + 2)\sigma_{\nu+1} - \sigma_\nu,$$

which implies

$$x \equiv \pm(u - 2) \pmod{(u^2 + 4)}. \quad (5.7)$$

On the other hand, let $(x, n) = (x_1, n_1)$ be a solution of (5.4). Then, the Diophantine equation

$$x^2 + 4uy^2 = (u^2 + 4)^n$$

has a solution $(x, y, n) = (x_1, 1, n_1)$. After the same procedure as the proof of Proposition 3.1 of [FT2], we see from (5.7) and Theorem 2 in [Le2] that $(x, n) = (x_1, n_1)$ is a solution of the equation

$$x + 2\sqrt{-u} = \lambda_1 (u - 2 + 2\lambda_2\sqrt{-u})^n \quad (5.8)$$

with $\lambda_1, \lambda_2 \in \{\pm 1\}$. Let $\alpha = u - 2 + 2\sqrt{-u}$ and $\beta = u - 2 - 2\sqrt{-u}$. Then, $\alpha + \beta = 2(u - 2)$ and $\alpha\beta = u^2 + 4$ are coprime, and

$$\frac{\alpha}{\beta} = \frac{u^2 - 8u + 4 + 4(u - 2)\sqrt{-u}}{u^2 + 4}$$

is clearly not a root of unity in $\mathbb{Q}(\sqrt{-u})$. Thus, (α, β) is a Lucas pair. Moreover, since $U_{n_1}(\alpha, \beta) = \pm 1$, the Lucas number $U_{n_1}(\alpha, \beta)$ has no primitive divisor. Since n_1 is odd, it follows from Lemmas 2.5, 2.6 in [FT2] or [BHV] that $n_1 \in \{1, 3\}$. If $n_1 = 1$, then it is obvious that $x_1 = u - 2$. If $n_1 = 3$, then (5.8) implies that $3u^2 - 16u + 12 = \pm 1$, which yields $u = 1$, a contradiction. This completes the proof of Proposition 5.1. \square

5.2 An application of the theory of linear forms in logarithms

In this section, we first show that the equation $q^m + 2^{2m-2} = (q^2 + 4)^n$ has only one solution $(m, n) = (2, 1)$ with q an odd integer by the theory of linear forms in two logarithms, and that the equation $1 + 2^{2m-2}q^m = (q^2 + 4)^n$ has no solutions (m, n) by elementary methods. These results are used in proving the case $m > 1$ of Theorem 1.

Lemma 5.2. *Let q be an odd integer with $q \geq 3$.*

(1) *The equation*

$$q^m + 2^{2m-2} = (q^2 + 4)^n \quad (5.9)$$

has only the positive integer solution $(m, n) = (2, 1)$.

(2) *The equation*

$$1 + 2^{2m-2}q^m = (q^2 + 4)^n \quad (5.10)$$

has no positive integer solutions (m, n) .

Proof. (1) When $q = 3$, equation (5.9) has only the positive integer solution $(m, n) = (2, 1)$ from Hadano [Ha]. We may thus suppose that $q \geq 5$.

We easily see that if $m \leq 2$, then equation (5.9) has only the positive integer solution $(m, n) = (2, 1)$. From now on, we may suppose that $m \geq 3$.

We first want to obtain an upper bound for m . Now consider the following linear form in two logarithms:

$$\Lambda = n \log(q^2 + 4) - m \log q.$$

Using the inequality $\log(1 + t) < t$ for $t > 0$, we have

$$0 < \Lambda = \log \left(\frac{(q^2 + 4)^n}{q^m} \right) = \log \left(1 + \frac{2^{2m-2}}{q^m} \right) < \left(\frac{4}{q} \right)^m.$$

Hence we obtain

$$\log \Lambda < -m \log \frac{q}{4}. \quad (5.11)$$

On the other hand, we use Proposition 2.3 to obtain a lower bound for Λ . It follows from Proposition 2.3 that

$$\log \Lambda \geq -25.2 (\max \{ \log b' + 0.38, 10 \})^2 \log(q^2 + 4)(\log q), \quad (5.12)$$

where $b' = \frac{m}{\log(q^2 + 4)} + \frac{n}{\log q}$. We note that $q^{2m} > (4q)^m > q^m + 2^{2m-2} = (q^2 + 4)^n$. Hence $b' < \frac{3m}{\log(q^2 + 4)}$. Put $M = \frac{m}{\log(q^2 + 4)}$. Combining (5.11) and (5.12) leads to

$$m \log \frac{q}{4} < 25.2 (\max \{ \log(3M) + 0.38, 10 \})^2 \log(q^2 + 4)(\log q),$$

so

$$M < 25.2 (\max \{ \log(3M) + 0.38, 10 \})^2 \cdot 7.22,$$

since $\log q / \log(q/4) < 7.22$ for $q \geq 5$. We therefore obtain $M < 24403$, i.e.,

$$m < 24403 \log(q^2 + 4). \quad (5.13)$$

We next want to obtain a lower bound for m . From (5.9), we see that $m > 2n$, since $(q^2 + 4)^m > (q^m + 2^{2m-2})^2 = (q^2 + 4)^{2n}$ for $m \geq 3$.

Now consider another linear form in two logarithms:

$$\Lambda_0 = \log(q^2 + 4) - 2 \log q (> 0).$$

Then

$$\begin{aligned} m\Lambda_0 - 2\Lambda &= m(\log(q^2 + 4) - 2 \log q) - 2(n \log(q^2 + 4) - m \log q) \\ &= (m - 2n) \log(q^2 + 4) \geq \log(q^2 + 4), \end{aligned}$$

since $m > 2n$. Note that

$$\Lambda_0 = \log\left(\frac{q^2 + 4}{q^2}\right) = \log\left(1 + \frac{4}{q^2}\right) < \frac{4}{q^2}.$$

Hence we obtain

$$m \geq \frac{\log(q^2 + 4)}{\Lambda_0} + \frac{2\Lambda}{\Lambda_0} > \frac{\log(q^2 + 4)}{\Lambda_0} > \frac{q^2}{4} \log(q^2 + 4). \quad (5.14)$$

Combining (5.13) and (5.14) yields

$$q^2 < 24402 \cdot 4.$$

Consequently we conclude that $q \leq 311$. Finally, following the strategy described in Section 3 of [B], based on the fact that n/m gives a good approximation to the irrational $\log q / \log(q^2 + 4)$, we checked by MAGMA that in the range $5 \leq q \leq 311$, equation (5.9) has no solution (m, n) with $2n < m < 24403 \log(q^2 + 4)$.

(2) It is easy to see that if $m \leq 2$, then equation (5.10) has no solutions. We may thus suppose that $m > 2$. Then taking (5.10) modulo 8 implies that $1 \equiv 5^n \pmod{8}$. Hence n is even, say $n = 2N$. Then

$$2^{2m-2}q^m = ((q^2 + 4)^2 - 1) \frac{(q^2 + 4)^{2N} - 1}{(q^2 + 4)^2 - 1} = (q^2 + 3)(q^2 + 5) \frac{(q^2 + 4)^{2N} - 1}{(q^2 + 4)^2 - 1}. \quad (5.15)$$

We now distinguish the cases (a) $q \not\equiv 0 \pmod{3}$ and (b) $q \equiv 0 \pmod{3}$.

(a) $q \not\equiv 0 \pmod{3}$. Then $\gcd(q^2 + 3, q) = 1$. From (5.15), we have

$$(q^2 + 3) \mid 2^{2m-2},$$

which is impossible, since $(q^2 + 3)/4$ is odd (> 1).

(b) $q \equiv 0 \pmod{3}$. Then $\gcd(q^2 + 3, q) = 3$. If $q = 3$, then the right hand side of (5.15) is divisible by 7, which is impossible. We may thus suppose that $q > 3$. There is an odd prime factor $r > 3$ of odd $(q^2 + 3)/4$. Indeed, if $q^2 + 3 = 4 \cdot 3^k$ with $k \geq 2$, then $3(q/3)^2 + 1 = 4 \cdot 3^{k-1}$, which is impossible. From (5.15), we have $q \equiv 0 \pmod{r}$, which contradicts the fact that $\gcd(q^2 + 3, q) = 3$. \square

5.3 Proof of Theorem 5.1, (ii)

We here give a proof of Theorem 5.1, (ii).

(ii) When $m = 1$, our assertion follows from Lemma 5.1. When $m > 1$, taking (5.2) modulo 8 implies that n is even, say $n = 2N$. In view of $u \in \{p, p^2\}$ and $v = 2$, equation (5.2) implies that either

$$q^m + 2^{2m-2} = (q^2 + 4)^N \text{ or } 1 + 2^{2m-2}q^m = (q^2 + 4)^N$$

with $q := u$. Now our assertion follows from Lemma 5.2.

References

- [AK] R. Alter and K. K. Kubota, The Diophantine Equation $x^2 + 11 = 3^n$ and a Related Sequence, *J. Number Theory* **7** (1975), 5–10.
- [B] M. A. Bennett, On some exponential equations of S. S. Pillai, *Canad. J. Math.* **53** (2001), no. 5, 897–922.
- [BoCa] W. Bosma and J. Cannon, Handbook of magma functions, Department of Math., University of Sydney, available at <http://magma.maths.usyd.edu.au/magma/>.
- [BS] M. A. Bennett and C. Skinner, Ternary Diophantine equations via Galois representations and modular forms, *Canad. J. Math.* **56** (2004), no. 1, 23–54.
- [Be] F. Beukers, On the generalized Ramanujan-Nagell equation. I, *Acta Arith.* **38** (1980/81), no. 4, 389–410.
- [BHV] Y. Bilu, G. Hanrot and P. M. Voutier, Existences of primitive divisors of Lucas and Lehmer numbers (with an appendix by M. Mignotte), *J. Reine Angew. Math.* **539** (2001), 75–122.
- [Bu] Y. Bugeaud, On some exponential Diophantine equations, *Monatsh. Math.* **132** (2001), no. 2, 93–97.
- [CD1] Z. Cao and X. Dong, On Terai’s conjecture, *Proc. Japan Acad. Ser. A Math. Sci.* **74** (1998), no. 8, 127–129.
- [CD2] Z. Cao and X. Dong, The Diophantine equation $x^2 + b^y = c^z$, *Proc. Japan Acad. Ser. A Math. Sci.* **77** (2001), no. 1, 1–4.
- [CDL] Z. Cao, X. Dong, Z. Li, A new conjecture concerning the Diophantine equation $x^2 + b^y = c^z$, *Proc. Japan Acad. Ser. A Math. Sci.* **78** (2002), no. 10, 199–202.
- [D] M. Deng, A note on the Diophantine equation $x^2 + q^m = c^{2n}$, *Proc. Japan Acad. Ser. A Math. Sci.* **91** (2015), no. 2, 15–18.
- [DGX] M. Deng, J. Guo, A. Xu, A note on the Diophantine equation $x^2 + (2c - 1)^m = c^n$, *Bull. Aust. Math. Soc.* **98** (2018), no. 2, 188–195.
- [E] J. S. Ellenberg, Galois representations attached to \mathbb{Q} -curves and the generalized Fermat equation $A^4 + B^2 = C^p$, *Amer. J. Math.* **126** (2004), no. 4, 763–787.
- [FT1] Y. Fujita and N. Terai, On the generalized Ramanujan-Nagell equation $x^2 + (2c - 1)^m = c^n$, *Acta Math. Hungar.* **162** (2020), no. 2, 518–526.
- [FT2] Y. Fujita and N. Terai, On exponential Diophantine equations concerning Pythagorean triples, *Publ. Math. Debrecen* **101** (2022), no. 1-2, 147–168.
- [Ha] T. Hadano, On the Diophantine equation $a^x = b^y + c^z$, *Math. J. Okayama Univ.* **19** (1976/77), no. 1, 25–29.
- [HL] J. Hu, X. Li, On the generalized Ramanujan-Nagell equation $x^2 + q^m = c^n$ with $q^r + 1 = 2c^2$, *Bull. Math. Soc. Sci. Math. Roumanie (N.S.)* **60(108)** (2017), no. 3, 257–265.

- [I] 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), no. 4, 327–338.
- [J] L. Jeśmanowicz, Some remarks on Pythagorean numbers (in Polish), *Wiadom. Mat.* **1** (1955/1956), 196–202.
- [La] M. Laurent, Linear forms in two logarithms and interpolation determinants. II, *Acta Arith.* **133** (2008), no. 4, 325–348.
- [Le1] M. Le, A Note on the Diophantine Equation $x^2 + b^y = c^z$, *Acta Arith.* **71** (1995), no. 3, 253–257.
- [Le2] M. Le, On Terai’s conjecture concerning Pythagorean numbers, *Acta Arith.* **100** (2001), no. 1, 41–45.
- [Le3] M. Le, A Note on the Diophantine Equation $x^2 + b^y = c^z$, *Czechoslovak Math. J.* **56(131)** (2006), no. 4, 1109–1116.
- [Le4] M. Le, On Cohn’s conjecture concerning the Diophantine equation $x^2 + 2^m = y^n$, *Arch. Math.* **78** (2002), no. 1, 26–35.
- [LS] M. Le and G. Soydan, A brief survey on the generalized Lebesgue-Ramanujan-Nagell equation, *Surv. Math. Appl.* **15** (2020), 473–523.
- [LSS] M. Le, R. Scott and R. Styer, A survey on the ternary purely exponential Diophantine equation $a^x + b^y = c^z$, *Surv. Math. Appl.* **14** (2019), 109–140.
- [Lj] W. Ljunggren, Some theorems on indeterminate equations of the form $\frac{x^n - 1}{x - 1} = y^q$ (Norwegian), *Norsk Mat. Tidsskr.* **25** (1943), 17–20.
- [M] T. Miyazaki, A polynomial-exponential equation related to the Ramanujan-Nagell equation, *Ramanujan J.* **45** (2018), no. 3, 601–613.
- [MT] T. Miyazaki and N. Terai, On Jeśmanowicz’ conjecture concerning primitive Pythagorean triples. II, *Acta Math. Hungar.* **147** (2015), no. 2, 286–293.
- [R] S. Ramanujan, Question 446, *J. Indian Math. Soc.* **5** (1913), 120.
- [N] T. Nagell, The Diophantine equation $x^2 + 7 = 2^n$, *Ark. Mat.* **4** (1961), 185–187.
- [St1] B. Stolt, On the Diophantine equation $u^2 - Dv^2 = \pm 4N$, *Ark. Mat.* **2** (1952), 1–23.
- [St2] B. Stolt, On the Diophantine equation $u^2 - Dv^2 = \pm 4N$. III, *Ark. Mat.* **3** (1955), 117–132.
- [Ta] K. Tanahashi, On the Diophantine equations $x^2 + 7^m = 2^n$ and $x^2 + 11^m = 3^n$, *J. Prezent. Fac. Gifu College Dent.* **3** (1977), 77–79.
- [Te1] N. Terai, The Diophantine Equation $x^2 + q^m = p^n$, *Acta Arith.* **63** (1993), no. 4, 351–358.
- [Te2] N. Terai, On Jeśmanowicz’ conjecture concerning primitive Pythagorean triples, *J. Number Theory* **141** (2014), 316–323.
- [Te3] N. Terai, A note on the Diophantine equation $x^2 + q^m = c^n$, *Bull. Aust. Math. Soc.* **90** (2014), no. 1, 20–27.

- [TNS1] N. Terai, S. Nakashiki and Y. Suenaga, On the generalized Ramanujan-Nagell equation $x^2 + (4c)^m = (c + 1)^n$, *Int. Math. Forum* **17** (2022), no. 1, 1–10.
- [TNS2] N. Terai, S. Nakashiki and Y. Suenaga, On the generalized Ramanujan-Nagell equation $x^2 + b^m = c^n$ with $a^2 + b^r = c^2$, *SUT J. Math.* **58** (2022), no. 1, 77–89.
- [To1] M. Toyozumi, On the Diophantine equation $y^2 + D^m = 2^n$, *Comment. Math. Univ. St. Paul.* **27** (1978/79), no. 2, 105–111.
- [To2] M. Toyozumi, On the Diophantine equation $x^2 + D^m = p^n$, *Acta Arith.* **42** (1983), no. 3, 303–309.
- [YH] P. Yuan and Y. Hu, On the Diophantine equation $x^2 + D^m = p^n$, *J. Number Theory* **111** (2005), no. 1, 144–153.
- [YW] P. Yuan and J. B. Wang, On the Diophantine equation $x^2 + b^y = c^z$, *Acta Arith.* **84** (1998), no. 2, 145–147.
- [Z] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math. Phys.* **3** (1892), no. 1, 265–284.