

第一页为封面页

参赛学生姓名： 冯凯晨

中学： 上海包玉刚实验学校

省份： 上海市

国家/地区： 中国

指导老师姓名： 李应凯

指导老师单位： 上海包玉刚实验学校

论文题目： A Complete Solution of a Lebesgue-Nagell Family:
From $x^2 - y^n = 4$ to $x^2 - y^n = 2^{2^m}$

A complete solution of a Lebesgue–Nagell family:

From $x^2 - y^n = 4$ to $x^2 - y^n = 2^{2m}$

Kaichen Feng

Abstract

We determine all positive integer solutions of $x^2 - y^n = 2^{2m}$ for $m \geq 1$ and $n \geq 2$. We factor $x^2 - 2^{2m}$ and compare the 2-adic valuations of its two factors. For odd n , this reduces the problem to binomial Thue-type equations whose coefficients are powers of 2. A consequence of results of Darmon–Merel and Ribet then gives the classification. For $n = 2$, there are exactly $m - 1$ positive integer solutions, given by an explicit parametrization. For $n \geq 3$, a solution exists if and only if $n \mid 2m + 3$, in which case n is necessarily odd and the unique solution for the fixed pair (m, n) is $(x, y) = (3 \cdot 2^m, 2^{(2m+3)/n})$. We first treat the case $m = 1$, for which the only solution is $(x, y, n) = (6, 2, 5)$, and then extend the argument to arbitrary m .

Keywords: exponential Diophantine equations; Lebesgue–Nagell equation; binomial Thue-type equations; 2-adic valuations.

Contents

1	Introduction	2
1.1	Exponential Diophantine equations and Catalan’s conjecture	2
1.2	The Lebesgue–Nagell equation and Mordell curves	2
1.3	Reduction to binomial Thue-type equations	2
2	Preliminaries	3
3	Small exponents for $x^2 - y^n = 4$	4
4	Reduction of the basic case to a binomial equation	5
5	The complete solution of $x^2 - y^n = 4$	6
6	The complete solution of $x^2 - y^n = 2^{2m}$	7
7	Conclusion and further directions	10

1 Introduction

1.1 Exponential Diophantine equations and Catalan's conjecture

In exponential Diophantine equations, one or more exponents are unknown integers; see Shorey and Tijdeman [1] for a general account. A classical example is Catalan's equation $x^p - y^q = 1$, whose only solution with $x, y, p, q \geq 2$ was conjectured to be $3^2 - 2^3 = 1$. In 1976, Tijdeman [3] used lower bounds for linear forms in logarithms to obtain effective bounds on the exponents and prove that there are only finitely many solutions. These bounds did not make an exhaustive computation practical. Mihăilescu proved the conjecture in 2002, and his paper appeared in 2004 [4]. His proof uses the arithmetic of cyclotomic fields and cyclotomic units. Bilu [5] and Metsänkylä [6] give accounts of the proof.

1.2 The Lebesgue–Nagell equation and Mordell curves

Fixing one exponent at 2 and replacing the constant by a nonzero integer gives the Lebesgue–Nagell equation

$$x^2 + D = y^n, \quad n \geq 3.$$

Lebesgue proved in 1850 that there are no positive integer solutions when $D = 1$, and Nagell proved the corresponding result for $D = 3$ in 1923; see the historical discussion in [9].

For $n = 3$, the change of coordinates $(X, Y) = (y, x)$ gives

$$Y^2 = X^3 - D,$$

a Mordell elliptic curve [7]. Positive integer solutions correspond exactly to its integral points with $X, Y > 0$. For $D > 0$, factorization in the imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$ is one classical approach. In the family considered in this paper, $D = -2^{2m}$, so the factorization already takes place in $\mathbb{Z}$.

When n is also unknown, solving the integral-point problem for each fixed exponent does not by itself give a classification for all exponents. Bugeaud, Mignotte and Siksek combined classical methods with Frey curves and level lowering in their work on perfect powers in the Fibonacci and Lucas sequences [8]. Their subsequent paper on the Lebesgue–Nagell equation [9] determines all positive integer solutions for every $1 \leq D \leq 100$.

1.3 Reduction to binomial Thue-type equations

A standard approach to some Lebesgue–Nagell equations is to factor in a suitable number field and reduce the problem to finitely many Thue equations $F(X, Y) = c$, where F is an irreducible homogeneous polynomial over $\mathbb{Z}$ of degree at least 3 and $c \neq 0$ is fixed. The method of Tzanakis and de Weger [10] combines bounds from linear forms in logarithms with lattice reduction to solve such equations in practice.

For the family studied here, factorization and coprimality lead to equations of the simpler form

$$|aX^n - bY^n| = 1.$$

We call these binomial Thue-type equations, allowing the reducible cases as well. Bennett and de Weger [2] proved uniqueness results for positive integer solutions when $1 \leq a < b$ and $n \geq 3$, apart from a specified range of possible exceptions. Bennett, Győry, Mignotte and Pintér [11] later solved several families with variable exponent in which the prime divisors of the coefficients are restricted to a fixed small set S . The case relevant here is $S = \{2\}$. A consequence of work of Darmon–Merel [12] and Ribet [13] states that, if $n \geq 3$ and A, B are powers of 2 with nonnegative integer exponents, then $AX^n - BY^n = 1$ has no positive integer solution with $XY > 1$. The precise formulation is recorded in [11, p. 1103]. We use this result after an elementary analysis of the two factors $x - 2^m$ and $x + 2^m$.

The preliminary lemmas and the external result used in the proof are collected in Section 2. Section 3 deals with $n = 2, 3$ for $x^2 - y^n = 4$. For $n \geq 4$, Sections 4 and 5 reduce the problem to a binomial Thue-type equation, leaving only $n = 5$. Section 6 extends the argument to $x^2 - y^n = 2^{2m}$, and Section 7 gives some remarks on what happens when other primes occur on the right-hand side.

2 Preliminaries

Throughout, $\mathbb{N} = \{1, 2, 3, \dots\}$. For a nonzero integer a , let $v_2(a)$ be the largest integer $k \geq 0$ such that $2^k \mid a$. We use

$$v_2(ab) = v_2(a) + v_2(b), \quad v_2(a \pm b) \geq \min\{v_2(a), v_2(b)\},$$

whenever the displayed valuations are defined. If $v_2(a) \neq v_2(b)$, equality holds in the second relation. We will also use the following case of the lifting-the-exponent lemma (LTE).

Lemma 2.1. *Let u, v be distinct odd integers, and let $n \geq 3$ be odd. Then*

$$v_2(v^n - u^n) = v_2(v - u).$$

Proof. Factor

$$v^n - u^n = (v - u)(v^{n-1} + v^{n-2}u + \dots + u^{n-1}).$$

The second factor is a sum of n odd integers. Since n is odd, this factor is odd, so it contributes nothing to the 2-adic valuation. $\square$

Lemma 2.2. *Let $n \geq 2$. If $A, B, t \in \mathbb{N}$, $\gcd(A, B) = 1$ and $AB = t^n$, then there are positive integers u, v such that $A = u^n$ and $B = v^n$.*

Proof. Every prime divides at most one of A, B , so its exponent in that factor equals its exponent in AB and is divisible by n . $\square$

For a finite set of primes S , a positive integer is an integer S -unit if all its prime factors lie in S . In particular, the positive integer 2-units are $1, 2, 4, \dots$. The following theorem is the non-elementary input to the proof.

Theorem 2.3 (Darmon–Merel and Ribet; see [11, p. 1103]). *Let $n \geq 3$ be an integer and let*

$$A, B \in \{2^\alpha : \alpha \in \mathbb{Z}_{\geq 0}\}.$$

If X, Y are positive integers satisfying

$$AX^n - BY^n = 1,$$

then $X = Y = 1$. Consequently, the only possibility is $(A, B, X, Y) = (2, 1, 1, 1)$.

Remark 2.4. The exclusion of $XY > 1$ follows from results on generalized Fermat equations in [12, 13]. These results use modular methods, including Frey curves, Galois representations and level lowering. We take the theorem as given; the reductions below are elementary. The last assertion follows from $A - B = 1$: the only nonnegative integer powers of 2 differing by 1 are 2 and 1.

We first record the two cubic equations that will arise in Section 3.

Corollary 2.5. *Neither of the equations*

$$(1) \ a^3 - 4b^3 = 1, \quad (2) \ 4a^3 - b^3 = 1$$

has a positive integer solution.

Proof. The coefficient pairs are $(1, 4)$ and $(4, 1)$, so Theorem 2.3 forces $a = b = 1$ in either equation. Substitution gives -3 and 3 , respectively, neither of which is 1. $\square$

3 Small exponents for $x^2 - y^n = 4$

The substitution in Section 4 involves 2^{n-4} , so we first treat $n = 2$ and $n = 3$ separately.

Proposition 3.1. *The equation $x^2 - y^2 = 4$ has no positive integer solutions.*

Proof. We have $(x - y)(x + y) = 4$, where $0 < x - y < x + y$ and the two factors have the same parity. The only factor pair of 4 with the same parity is $(2, 2)$, which gives $y = 0$. $\square$

Theorem 3.2. *The equation $x^2 - y^3 = 4$ has no positive integer solutions.*

Proof. Suppose that $(x - 2)(x + 2) = y^3$. Since $y > 0$, we have $x > 2$, so both factors are positive. We have two cases according to the parity of y .

Case 1: y is odd. Both $x - 2$ and $x + 2$ are odd, and their gcd divides their difference 4. Thus they are coprime. By Lemma 2.2, write

$$x + 2 = a^3, \quad x - 2 = b^3$$

with $a > b \geq 1$. Then $a^3 - b^3 = 4$, whereas

$$a^3 - b^3 \geq (b+1)^3 - b^3 = 3b^2 + 3b + 1 \geq 7,$$

a contradiction.

Case 2: y is even. Then x is even, and $\gcd(x-2, x+2)$ is either 2 or 4.

Case 2.1: $\gcd(x-2, x+2) = 2$. Write $x+2 = 2u$ and $x-2 = 2v$. Then $u-v = 2$ and $\gcd(u, v) = 1$, so u, v are both odd. On the other hand, putting $y = 2k$ in $4uv = y^3$ gives $uv = 2k^3$, which is even. This is impossible.

Case 2.2: $\gcd(x-2, x+2) = 4$. Write $x+2 = 4u$ and $x-2 = 4v$. Then $u-v = 1$, $\gcd(u, v) = 1$ and $16uv = y^3$. Taking 2-adic valuations gives $3v_2(y) \geq 4$, so $4 \mid y$. Put $y = 4k$. We obtain

$$uv = 4k^3.$$

Since u, v are coprime, exactly one is even, and that factor is divisible by 4. If $4 \mid u$, write $u = 4u_1$. Then $u_1v = k^3$ with $\gcd(u_1, v) = 1$, so $u_1 = a^3$ and $v = b^3$. The relation $u-v = 1$ becomes $4a^3 - b^3 = 1$. If $4 \mid v$, the same argument gives $u = a^3$, $v = 4b^3$ and $a^3 - 4b^3 = 1$. Both equations are excluded by Corollary 2.5. $\square$

4 Reduction of the basic case to a binomial equation

We now assume $n \geq 4$ and determine the gcd of the two factors.

Lemma 4.1. *Let $n \geq 4$. If $x^2 - y^n = 4$ has a positive integer solution, then*

$$\gcd(x-2, x+2) = 4.$$

Proof. Put $A = x-2$ and $B = x+2$. Then $A, B > 0$, $B-A = 4$ and $AB = y^n$, so $g = \gcd(A, B)$ belongs to $\{1, 2, 4\}$.

If $g = 1$, Lemma 2.2 gives $A = u^n$ and $B = v^n$ with $v > u \geq 1$. Hence $v^n - u^n = 4$. If $u \geq 2$, then

$$v^n - u^n \geq (u+1)^n - u^n \geq nu^{n-1} \geq 32 > 4.$$

If $u = 1$, then $v^n = 5$, which is also impossible.

If $g = 2$, the coprime integers $A/2$ and $B/2$ differ by 2, so both are odd. Thus $v_2(A) = v_2(B) = 1$. Taking valuations in $AB = y^n$ gives $nv_2(y) = 2$, contrary to $n \geq 4$.

Therefore $g = 4$. $\square$

This gives a reversible substitution into a binomial equation.

Lemma 4.2. *Let $n \geq 4$. The equation $x^2 - y^n = 4$ has a positive integer solution if and only if*

$$|2^{n-4}u^n - v^n| = 1 \tag{1}$$

has a positive integer solution. The recovery formulas are

$$y = 2uv, \quad x = 4 \min\{2^{n-4}u^n, v^n\} + 2.$$

Proof. Necessity. By Lemma 4.1, write $x - 2 = 4A_1$ and $x + 2 = 4B_1$. Then $B_1 - A_1 = 1$, $\gcd(A_1, B_1) = 1$ and

$$16A_1B_1 = y^n.$$

In particular, y is even. Write $y = 2Y$, giving

$$A_1B_1 = 2^{n-4}Y^n.$$

The coefficient is an integer since $n \geq 4$. The two factors A_1, B_1 are coprime and have opposite parity. Every odd prime has exponent divisible by n in whichever factor it divides. If the even factor is A_1 , its 2-adic valuation is $n - 4 + nv_2(Y)$, so

$$A_1 = 2^{n-4}u^n, \quad B_1 = v^n$$

for some coprime positive integers u, v . If the even factor is B_1 , the two expressions are interchanged. Substituting in $B_1 - A_1 = 1$ gives (1) in either case. This argument also applies when $n = 4$.

Sufficiency. Given a positive integer solution (u, v) of (1), set

$$A_1 = \min\{2^{n-4}u^n, v^n\}, \quad B_1 = \max\{2^{n-4}u^n, v^n\}.$$

Then $B_1 - A_1 = 1$. Taking $x = 4A_1 + 2$ and $y = 2uv$, we obtain

$$x^2 - 4 = 16A_1(A_1 + 1) = 16A_1B_1 = 2^n(uv)^n = y^n.$$

Both x and y are positive integers, as required. $\square$

5 The complete solution of $x^2 - y^n = 4$

It remains to solve (1) for $n \geq 4$.

Theorem 5.1. *For $n \geq 4$, the equation $x^2 - y^n = 4$ has a positive integer solution if and only if $n = 5$. In that case the unique solution is $(x, y) = (6, 2)$.*

Proof. By Lemma 4.2, we need only consider $|2^{n-4}u^n - v^n| = 1$.

Case 1: $n = 4$. The equation becomes $|u^4 - v^4| = 1$. Distinct positive fourth powers differ by at least $2^4 - 1^4 = 15$, so there is no solution.

Case 2: $n \geq 5$. Both coefficients are integer 2-units. Applying Theorem 2.3 to either sign of the difference forces $u = v = 1$. Thus

$$|2^{n-4} - 1| = 1.$$

Since $2^{n-4} \geq 2$, this holds exactly when $n = 5$. The recovery formulas give

$$y = 2, \quad x = 4 \min\{2, 1\} + 2 = 6.$$

Finally, $6^2 - 2^5 = 4$, so this pair is indeed a solution. $\square$

6 The complete solution of $x^2 - y^n = 2^{2m}$

We now allow any integer $m \geq 1$. We first handle the even exponents, then rule out equal valuations of $x - 2^m$ and $x + 2^m$ for odd exponents. The remaining case will again reduce to Theorem 2.3.

Lemma 6.1. *Let $m \geq 1$ and let $n \geq 2$ be even. The positive integer solutions of $x^2 - y^n = 2^{2m}$ are as follows. If $n = 2$, there are exactly $m - 1$ solutions, given by*

$$x = 2^{2m-a-1} + 2^{a-1}, \quad y = 2^{2m-a-1} - 2^{a-1}, \quad 1 \leq a \leq m - 1.$$

The parameter range is empty when $m = 1$. If $n \geq 4$, there are no positive integer solutions.

Proof. For $n = 2$, factor

$$(x - y)(x + y) = 2^{2m}.$$

Since $0 < x - y < x + y$, write $x - y = 2^a$ and $x + y = 2^b$, where $b > a \geq 0$ and $a + b = 2m$. If $a = 0$, adding gives $2x = 1 + 2^{2m}$, a parity contradiction. Thus $a \geq 1$, and

$$x = 2^{b-1} + 2^{a-1}, \quad y = 2^{b-1} - 2^{a-1}.$$

The conditions $b = 2m - a$ and $b > a$ give $1 \leq a \leq m - 1$. Each such value gives a positive integer solution, and different values give different solutions because $a = v_2(x - y)$.

Now suppose $n = 2k$ with $k \geq 2$. The same factorization gives

$$x - y^k = 2^a, \quad x + y^k = 2^b,$$

where $b > a \geq 1$ and $a + b = 2m$. Subtracting yields

$$y^k = 2^{a-1}(2^{b-a} - 1).$$

Write $y = 2^\alpha w$ with w odd. Comparing valuations and odd parts, we get

$$\alpha k = a - 1, \quad w^k + 1 = 2^{b-a}.$$

If $w = 1$, then $b - a = 1$, which is incompatible with $a + b = 2m$. We may therefore assume $w > 1$.

If k is even, then $w^k \equiv 1 \pmod{8}$. Hence $v_2(w^k + 1) = 1$, so again $b - a = 1$, a contradiction.

If k is odd, then $k \geq 3$ and

$$w^k + 1 = (w + 1)(w^{k-1} - w^{k-2} + \cdots - w + 1) = 2^{b-a}.$$

The second factor is odd. It is also greater than 1, since

$$\frac{w^k + 1}{w + 1} > 1$$

for $w > 1$ and $k \geq 3$. A power of 2 cannot have such a factor. □

For odd $n \geq 3$, put $A = x - 2^m$ and $B = x + 2^m$. A positive integer solution has $x > 2^m$, so $A, B > 0$, and

$$B - A = 2^{m+1}, \quad AB = y^n.$$

Let $a = v_2(A)$ and $b = v_2(B)$. If $a \neq b$, then $\min(a, b) = m + 1$. If $a = b = k$, write $A = 2^k A_0$ and $B = 2^k B_0$ with A_0, B_0 odd. Then

$$m + 1 = v_2(B - A) = k + v_2(B_0 - A_0) \geq k + 1,$$

so $k \leq m$. We next exclude this case.

Lemma 6.2. *Let $m \geq 1$ and let $n \geq 3$ be odd. A positive integer solution of $x^2 - y^n = 2^{2m}$ cannot satisfy*

$$v_2(x - 2^m) = v_2(x + 2^m) \leq m.$$

Proof. Suppose that $v_2(A) = v_2(B) = k \leq m$, and write $A = 2^k A_0$, $B = 2^k B_0$ with A_0, B_0 odd. Since $\gcd(A, B) \mid B - A = 2^{m+1}$, the odd parts A_0, B_0 are coprime.

Taking valuations in $2^{2k} A_0 B_0 = y^n$ gives $n \mid 2k$. As n is odd, $n \mid k$. Write $k = \lambda n$ with $\lambda \geq 0$. Then $v_2(y) = 2\lambda$ and

$$A_0 B_0 = \left(\frac{y}{2^{2\lambda}} \right)^n.$$

By Lemma 2.2, there are odd integers $v > u \geq 1$ such that $A_0 = u^n$ and $B_0 = v^n$. Subtracting gives

$$v^n - u^n = 2^r, \quad r = m + 1 - \lambda n \geq 1.$$

By Lemma 2.1, $v_2(v - u) = r$, so $v - u \geq 2^r$. But $v^n - u^n > v - u$ for $v > u \geq 1$ and $n \geq 3$, giving

$$2^r = v^n - u^n > v - u \geq 2^r,$$

a contradiction. □

We can now state the full classification.

Theorem 6.3. *Let $m \geq 1$ and $n \geq 2$ be integers. The positive integer solutions of*

$$x^2 - y^n = 2^{2m}$$

are classified as follows.

1. *If $n = 2$:*

(a) *If $m = 1$, there are no positive integer solutions.*

(b) *If $m \geq 2$, there are exactly $m - 1$ distinct positive integer solutions, given by*

$$x = 2^{2m-a-1} + 2^{a-1}, \quad y = 2^{2m-a-1} - 2^{a-1}, \quad a \in \{1, \dots, m-1\}.$$

2. *If $n \geq 3$, a positive integer solution exists if and only if $n \mid 2m + 3$. In this case n is necessarily odd, and for the fixed pair (m, n) the unique solution is*

$$x = 3 \cdot 2^m, \quad y = 2^{\frac{2m+3}{n}}.$$

Proof. Lemma 6.1 gives the stated classification for even n . It remains to consider odd $n \geq 3$.

Put $A = x - 2^m$ and $B = x + 2^m$. Then $A, B > 0$, $B - A = 2^{m+1}$ and $AB = y^n$. As shown above, equal valuations would have to be at most m , and Lemma 6.2 excludes that possibility. Hence

$$\min\{v_2(A), v_2(B)\} = v_2(B - A) = m + 1.$$

Write $A = 2^{m+1}A_1$ and $B = 2^{m+1}B_1$. We have

$$B_1 - A_1 = 1, \quad 2^{2m+2}A_1B_1 = y^n.$$

In particular, A_1, B_1 are coprime and have opposite parity.

Let $\alpha = v_2(A_1B_1) \geq 1$. All factors of 2 lie in the even member of $\{A_1, B_1\}$. For every odd prime, its exponent in whichever member it divides is a multiple of n , because $2^{2m+2}A_1B_1 = y^n$ and the two members are coprime. Thus

$$\{A_1, B_1\} = \{2^\alpha u^n, v^n\}$$

for some coprime positive odd integers u, v . Since $B_1 - A_1 = 1$, either

$$2^\alpha u^n - v^n = 1 \quad \text{or} \quad v^n - 2^\alpha u^n = 1.$$

Theorem 2.3 applies to both equations and forces $u = v = 1$.

The second equation would give $1 - 2^\alpha = 1$, which is impossible. The first gives $2^\alpha - 1 = 1$, so $\alpha = 1$. Therefore $A_1 = 1$ and $B_1 = 2$. It follows that

$$x - 2^m = 2^{m+1}, \quad y^n = 2^{2m+2}A_1B_1 = 2^{2m+3}.$$

Hence $x = 3 \cdot 2^m$, and an integer y exists exactly when $n \mid 2m + 3$, in which case $y = 2^{(2m+3)/n}$.

Conversely, if $n \mid 2m + 3$, these values satisfy

$$(3 \cdot 2^m)^2 - \left(2^{\frac{2m+3}{n}}\right)^n = 9 \cdot 2^{2m} - 8 \cdot 2^{2m} = 2^{2m}.$$

This proves both existence and uniqueness. $\square$

For fixed m , the exponents $n \geq 3$ giving solutions are precisely the divisors of $2m + 3$ other than 1. Thus, if τ denotes the number of positive divisors, there are $\tau(2m + 3) - 1$ solution triples (x, y, n) with $n \geq 3$, and

$$m + \tau(2m + 3) - 2$$

with $n \geq 2$. The largest possible exponent is $2m + 3$, attained by $(x, y) = (3 \cdot 2^m, 2)$.

For fixed odd $n \geq 3$, the condition is equivalently $m \equiv (n - 3)/2 \pmod{n}$. The solutions can therefore be written as

$$m = nt + \frac{n - 3}{2}, \quad x = 3 \cdot 2^m, \quad y = 2^{2t+1},$$

where $t \geq 0$ and $m \geq 1$; for $n = 3$, this means $t \geq 1$.

The boundary case $m = 0$ can also be included. The odd-exponent argument above still applies and gives $x = 3$, $y^n = 8$, hence $(x, y, n) = (3, 2, 3)$. For even n , the factorization $(x - y^{n/2})(x + y^{n/2}) = 1$ rules out positive solutions.

7 Conclusion and further directions

For the equation $x^2 - y^n = 2^{2m}$, the factorization in $\mathbb{Z}$ is enough to reduce the problem to a known result. The gcd of $x - 2^m$ and $x + 2^m$ is a power of 2. For odd n , equal valuations are impossible while unequal valuations leave two consecutive coprime factors. Their odd parts are n th powers, so Theorem 2.3 determines both factors and gives the classification.

Once the results of Darmon–Merel and Ribet [12, 13] are available, the argument requires no separate Thue or newform computations for each (m, n) .

The same initial factorization applies more generally, but other prime factors change the reduced equations.

- **Odd prime bases.** Consider $x^2 - y^n = p^{2m}$ with p an odd prime. If $A = x - p^m$, $B = x + p^m$ and $d = \gcd(A, B)$, then

$$B - A = 2p^m, \quad d \mid 2p^m, \quad \frac{B}{d} - \frac{A}{d} = \frac{2p^m}{d}.$$

Thus the relevant prime set is generally $S = \{2, p\}$, and the reduced right-hand side need not be 1. For example, $6^2 - 3^3 = 3^2$ gives factors 3, 9; after division by their gcd, the difference is $3 - 1 = 2$.

Even for binomial equations supported on a single odd prime, a general exclusion of non-trivial solutions is false: $9 \cdot 1^3 - 2^3 = 1$. An extension would therefore require classifying the remaining solutions for specified primes and coefficient patterns. The results of [11] already solve the right-hand-side ± 1 families for several small prime sets.

- **Several prime factors.** More generally, put $N = p_1^{m_1} \cdots p_k^{m_k}$ and consider $x^2 - y^n = N^2$. Writing $d = \gcd(x - N, x + N)$ gives $d \mid 2N$. The coprime factors $(x - N)/d$ and $(x + N)/d$ differ by $2N/d$. After extracting n th powers, one obtains equations of the form

$$aU^n - bV^n = C,$$

where a, b, C are positive integer S -units for $S = \{p : p \text{ is prime and } p \mid 2N\}$. In particular, $C = 1$ cannot be assumed. For fixed N and n , the choices of d and the valuations of the coefficients give finitely many cases. Local congruences and existing results on binomial equations can then be used to eliminate cases before any further computation.

References

- [1] T.N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Tracts in Mathematics, vol. 87, Cambridge University Press, 1986.
- [2] M. A. Bennett and B. M. M. de Weger, *On the diophantine equation $|ax^n - by^n| = 1$* , Math. Comp. **67** (1998), no. 221, 413–438.
- [3] R. Tijdeman, *On the equation of Catalan*, Acta Arith. **29** (1976), 197–209.

- [4] P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math. **572** (2004), 167–195.
- [5] Y.F. Bilu, *Catalan's conjecture [after Mihăilescu]*, Séminaire Bourbaki (2002/2003), Exp. 909, Astérisque **294** (2004), 1–26.
- [6] T. Metsänkylä, *Catalan's conjecture: another old Diophantine problem solved*, Bull. Amer. Math. Soc. (N.S.) **41** (2004), 43–57.
- [7] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 106, Springer, 1986.
- [8] Y. Bugeaud, M. Mignotte and S. Siksek, *Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers*, Ann. of Math. **163** (2006), 969–1018.
- [9] Y. Bugeaud, M. Mignotte and S. Siksek, *Classical and modular approaches to exponential Diophantine equations II. The Lebesgue–Nagell equation*, Compos. Math. **142** (2006), 31–62.
- [10] N. Tzanakis and B.M.M. de Weger, *On the practical solution of the Thue equation*, J. Number Theory **31** (1989), 99–132.
- [11] M.A. Bennett, K. Györy, M. Mignotte and Á. Pintér, *Binomial Thue equations and polynomial powers*, Compos. Math. **142** (2006), 1103–1121.
- [12] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's last theorem*, J. Reine Angew. Math. **490** (1997), 81–100.
- [13] K.A. Ribet, *On the equation $a^p + 2^\alpha b^p + c^p = 0$* , Acta Arith. **79** (1997), 7–16.

研究背景

这项研究源于我学习数论时对指数丢番图方程的兴趣，尤其是带未知指数的方程。我最初关注的只是 $x^2 - y^n = 4$ 的正整数解，后来觉得把4换成 2^{2m} 后，原来的方法可能仍然适用，于是就沿着这个想法继续做了下去。

指导老师与参赛学生的关系

本项目只有一名参赛学生，即本人冯凯晨，目前就读于上海民办包玉刚实验学校。李应凯是指导老师，他是我在校内的数学老师，我们为校内师生关系。李老师是无偿指导，主要帮我看论文写作规范、结构和表达，也协助了报名和学校盖章。在论证检查方面，李老师提供了有限的帮助（他对个别已完成的论证步骤进行了简要核查）。剩余的所有部分（选题、文献阅读、分类讨论、证明和写作）由我负责。

研究过程、困难与解决

由于这是我第一次写数学研究论文，开始时我不太清楚该怎么找文献。后来我主要利用互联网，“指数丢番图方程”“二项方程”等关键词逐步缩小范围，慢慢找到并确认了本文需要引用的结果。

研究中没有任何数据采集或实验，主要为文献阅读和数学推导。最初研究 $x^2 - y^n = 4$ 时，我进行因式分解，讨论两个因子的最大公因数和其中各素因子的指数，再把问题归到文献中已有的二项方程结果。推广到 2^{2m} 后，我又重新分了偶数指数和奇数指数的情况，整理出对应的解。

中间比较麻烦的一点，是怎样把自己能的初等推导与文献中较深的结果连接起来。引用某个定理之前，需要先看清楚它对变量的要求，确认用法没问题。另外，不同的奇偶性和赋值情况需要分开讨论，写的时候很容易漏。为了处理这些问题，我主要靠逐步核对（把每一步都重新验一遍，检查用法是否正确以及有没有哪种情况被漏掉）。

具体分工与贡献

论文的初稿与终稿都是由我撰写的，包括研究背景、理论推导以及结论。老师就文章结构、格式和表达提出了意见，未承担具体的数论证明工作。文献中使用的结果及其来源已在正文和参考文献中注明。

AI 使用说明

本论文的全部研究过程与论文撰写均由人类完成，未使用任何生成式人工智能。

2026 S.-T. Yau High School Science Award
仅用于2026丘成桐中学科学奖论文公示