Bull. Aust. Math. Soc. **113** (2026), 26–39
doi:10.1017/S0004972725100324

A NOTE ON THE GENERALISED RAMANUJAN–NAGELL EQUATION $x^2 = 2^m + p^n$

YASUTSUGU FUJITA and MAOHUA LE

(Received 12 March 2025; accepted 7 June 2025; first published online 12 September 2025)

Abstract

Let p be a fixed odd prime. We prove the following results for positive integer solutions (x, m, n) of the equation $(*)$ $x^2 = 2^m + p^n$. (i) If $p \equiv 3 \pmod 8$, then $(*)$ has only the solution $(p, x, m, n) = (3, 5, 4, 2)$. (ii) If $p \equiv 5 \pmod 8$, then $(*)$ has only the solution $(p, x, m, n) = (5, 3, 2, 1)$. (iii) If $p \equiv 7 \pmod 8$, then $(*)$ has at most one solution (x, m, n), except for $p = 7$, $(x, m, n) = (3, 1, 1)$ and $(9, 5, 2)$. Moreover, if $p = 2^q - 1$ is a Mersenne prime with $p > 7$, where q is an odd prime with $q > 3$, then $(*)$ has exactly one solution $(x, m, n) = (2^q + 1, q + 2, 2)$. If $p \equiv 7 \pmod 8$, p is not a Mersenne prime and either $p < 1.5 \times 10^{12}$ or $p > C$, where C is an effectively computable absolute constant, then $(*)$ has only the solutions $p = a^2 - 2$, where a is an odd positive integer, $(x, m, n) = (a, 1, 1)$. (iv) If $p \equiv 1 \pmod 8$ with $p \neq 17$, then $(*)$ has at most two solutions (x, m, n).

2020 *Mathematics subject classification*: primary 11D45; secondary 11D61.

Keywords and phrases: polynomial-exponential Diophantine equation, generalised Ramanujan–Nagell equation, elementary approach.

1. Introduction

Let $\mathbb{Z}$ and $\mathbb{N}$ be the sets of all integers and positive integers, respectively. Let p be a fixed odd prime. We consider the generalised Ramanujan–Nagell equation of the form

$$x^2 = 2^m + p^n, \quad x, m, n \in \mathbb{N}. \tag{1.1}$$

In 2017, Wang and Jiang [11] proved that, for any fixed positive integer r, (1.1) has at most one solution (x, m, n) with $m = r$. Recently, Luca and Pink [6] determined all solutions (x, m, n) of (1.1) when $p = 2^{2^l} + 1$ is a Fermat prime, where l is a nonnegative integer. They proved that if p is a Fermat prime, then (1.1) has the solutions:

$$p = 3, \quad (x, m, n) = (5, 4, 2), \tag{1.2}$$

$$p = 5, \quad (x, m, n) = (3, 2, 1), \tag{1.3}$$

The first author is supported by JSPS KAKENHI Grant Number JP24K06654.

© The Author(s), 2025. Published by Cambridge University Press on behalf of Australian Mathematical Publishing Association Inc.

https://doi.org/10.1017/S0004972725100324 Published online by Cambridge University Press

$$p = 17, \quad (x, m, n) = (5, 3, 1), (7, 5, 1), (9, 6, 1), (23, 9, 1), (71, 7, 3),$$
$$p = 2^{2^l} + 1 \text{ with } l > 2, \quad (x, m, n) = (2^{2^{l-1}} + 1, 2^{l-1} + 1, 1), (2^{2^l} - 1, 2^{l+1} - 2, 1).$$

We discuss (1.1) for a general odd prime p. We will prove the following results.

THEOREM 1.1. *If $p \equiv 3 \pmod 8$, then (1.1) has only the solution (1.2). If $p \equiv 5 \pmod 8$, then (1.1) has only the solution (1.3).*

THEOREM 1.2. *If $p \equiv 7 \pmod 8$, then (1.1) has at most one solution (x, m, n), except for*

$$p = 7, \quad (x, m, n) = (3, 1, 1), (9, 5, 2). \tag{1.4}$$

Moreover, if

$$p = 2^q - 1 \quad \text{where } q \text{ is a prime}, \tag{1.5}$$

and p is a Mersenne prime with $p > 7$, then (1.1) has exactly one solution

$$(x, m, n) = (2^q + 1, q + 2, 2). \tag{1.6}$$

If $p \equiv 7 \pmod 8$, p is not a Mersenne prime and either $p < 1.5 \times 10^{12}$ or $p > C$, where C is an effectively computable absolute constant, then (1.1) has only the solutions

$$p = a^2 - 2 \quad \text{where } a \in \mathbb{N} \text{ with } 2 \nmid a, \ (x, m, n) = (a, 1, 1). \tag{1.7}$$

THEOREM 1.3. *If $p \equiv 1 \pmod 8$ with $p \neq 17$, then (1.1) has at most two solutions (x, m, n).*

Obviously, the synthesis of the above three theorems gives the best upper bound for the number of solutions (x, m, n) of (1.1). We further propose the following conjectures.

CONJECTURE 1.4. If $p \equiv 7 \pmod 8$, then (1.1) has only the solutions (1.4), (1.6) and (1.7).

CONJECTURE 1.5. There exist infinitely many odd primes p such that $p \equiv 1 \pmod 8$, p is not a Fermat prime and (1.1) has exactly two solutions (x, m, n).

2. Preliminaries

Let D be a nonsquare positive integer.

LEMMA 2.1 [8, Theorems 103 and 104]. *The equation*

$$u^2 - Dv^2 = 1, \quad u, v \in \mathbb{Z}, \tag{2.1}$$

has positive integer solutions (u, v) and it has a unique positive integer solution (u_1, v_1) such that $u_1 + v_1\sqrt{D} \leq u + v\sqrt{D}$, where (u, v) runs through all positive integer solutions of (2.1). The solution (u_1, v_1) is called the fundamental solution of (2.1). Every solution (u, v) of (2.1) can be expressed as

$$u + v\sqrt{D} = \lambda_1(u_1 + \lambda_2 v_1\sqrt{D})^t, \quad \lambda_1, \lambda_2 \in \{1, -1\}, \ t \in \mathbb{Z}, \ t \geq 0.$$

https://doi.org/10.1017/S0004972725100324 Published online by Cambridge University Press

LEMMA 2.2 ([9, Remark 5.5]; see also [10, descriptions after Conjectures 1.1 and 1.2]). *For any odd prime p with $p < 1.5 \times 10^{12}$, the fundamental solution (u_1, v_1) of the equation*

$$u^2 - pv^2 = 1, \quad u, v \in \mathbb{Z}, \tag{2.2}$$

satisfies $p \nmid v_1$.

LEMMA 2.3 [8, Theorem 107]. *For any odd prime p with $p \equiv 1 \pmod 4$, the equation*

$$u'^2 - pv'^2 = -1, \quad u', v' \in \mathbb{Z}, \tag{2.3}$$

has solutions (u', v').

With similar approaches to [8, proofs of Theorems 106 and 107], we can directly obtain the following two lemmas.

LEMMA 2.4. *If the equation*

$$U^2 - DV^2 = 2, \quad U, V \in \mathbb{Z}, \tag{2.4}$$

has solutions (U, V), then it has a unique positive integer solution (U_1, V_1) such that $U_1 + V_1\sqrt{D} \le U + V\sqrt{D}$, where (U, V) runs through all positive integer solutions of (2.4). The solution (U_1, V_1) is called the fundamental solution of (2.4).

(i) *Every solution (U, V) of (2.4) can be expressed as*

$$\frac{U + V\sqrt{D}}{\sqrt{2}} = \lambda_1\left(\frac{U_1 + \lambda_2 V_1\sqrt{D}}{\sqrt{2}}\right)^t, \quad \lambda_1, \lambda_2 \in \{1, -1\},\ t \in \mathbb{N},\ 2 \nmid t.$$

(ii) *The fundamental solution (u_1, v_1) of (2.1) satisfies $u_1 + v_1\sqrt{D} = (U_1 + V_1\sqrt{D})^2/2$.*

PROOF. Assume that (2.4) has solutions (U, V). Clearly, $2 \nmid U$, $2 \nmid V$, $D \equiv 7 \pmod 8$ and $(|U|, |V|)$ are positive integer solutions of (2.4). Since D is a nonsquare positive integer, $\sqrt{D}$ is irrational and (2.4) has a unique positive integer solution (U_1, V_1) such that $U_1 + V_1\sqrt{D} \le U + V\sqrt{D}$, where (U, V) runs through all positive integer solutions of (2.4). It follows that the fundamental solution (U_1, V_1) of (2.4) exists.

Since $D \equiv 7 \pmod 8$, for any positive integer solution (U, V) of (2.4), (2.1) has the positive integer solution

$$(u, v) = \left(\frac{U^2 + DV^2}{2}, UV\right) \tag{2.5}$$

with $2 \nmid v$. By (2.5), these solutions are related by

$$\left(\frac{U + V\sqrt{D}}{\sqrt{2}}\right)^2 = u + v\sqrt{D}, \quad 2 \nmid v. \tag{2.6}$$

https://doi.org/10.1017/S0004972725100324 Published online by Cambridge University Press

Let (u_1, v_1) be the fundamental solution of (2.1). Recall that (2.1) has solutions (u, v) with $2 \nmid v$. By Lemma 2.1, we have $2 \nmid v_1$. Hence, from (2.6),

$$\left(\frac{U_1 + V_1\sqrt{D}}{\sqrt{2}}\right)^2 = (u_1 + v_1\sqrt{D})^{2s+1}, \quad s \in \mathbb{Z}, s \geq 0. \tag{2.7}$$

If $s \geq 1$, let

$$U' + V'\sqrt{D} = (U_1 + V_1\sqrt{D})(u_1 - v_1\sqrt{D}). \tag{2.8}$$

From (2.7) and (2.8), U' and V' are positive integers satisfying $U'^2 - DV'^2 = 2$ and

$$\left(\frac{U' + V'\sqrt{D}}{\sqrt{2}}\right)^2 = (u_1 + v_1\sqrt{D})^{2s-1} \geq u_1 + v_1\sqrt{D}.$$

It follows that (U', V') with $U' + V'\sqrt{D} < U_1 + V_1\sqrt{D}$ is a positive integer solution of (2.4), which contradicts the definition of the fundamental solution (U_1, V_1) of (2.4). So we have $s = 0$ and, by (2.7), proposition (ii) is proved.

For any positive integer r, let

$$u_r + v_r\sqrt{D} = (u_1 + v_1\sqrt{D})^r, \quad \frac{U_r + V_r\sqrt{D}}{\sqrt{2}} = \left(\frac{U_1 + V_1\sqrt{D}}{\sqrt{2}}\right)^{2r-1}. \tag{2.9}$$

Then,

$$u_r - v_r\sqrt{D} = (u_1 - v_1\sqrt{D})^r, \quad \frac{U_r - V_r\sqrt{D}}{\sqrt{2}} = \left(\frac{U_1 - V_1\sqrt{D}}{\sqrt{2}}\right)^{2r-1}. \tag{2.10}$$

By proposition (ii), from (2.9) and (2.10),

$$\begin{aligned}\frac{U_r + V_r\sqrt{D}}{\sqrt{2}} &= \left(\frac{U_{r-1} + V_{r-1}\sqrt{D}}{\sqrt{2}}\right)(u_1 + v_1\sqrt{D}) = \cdots \\ &= \left(\frac{U_1 + V_1\sqrt{D}}{\sqrt{2}}\right)(u_{r-1} + v_{r-1}\sqrt{D}).\end{aligned} \tag{2.11}$$

From (2.11), using the inductive method, $(U, V) = (U_r, V_r)$ $(r = 1, 2, \ldots)$ are positive integer solutions of (2.4) with

$$\left(\frac{U_r + V_r\sqrt{D}}{\sqrt{2}}\right)^2 = u_{2r-1} + v_{2r-1}\sqrt{D}, \quad r = 1, 2, \ldots. \tag{2.12}$$

Recall that $2 \nmid v_1$. By Lemma 2.1, $(u, v) = (u_{2r-1}, v_{2r-1})$ $(r = 1, 2, \ldots)$ are all positive integer solutions of (2.1) with $2 \nmid v$. Thus, we see from (2.6) and (2.12) that $(U, V) = (U_r, V_r)$ $(r = 1, 2, \ldots)$ are all positive integer solutions of (2.4). By (2.9), every positive integer solution (U, V) of (2.4) can be expressed as

$$\frac{U + V\sqrt{D}}{\sqrt{2}} = \left(\frac{U_1 + V_1\sqrt{D}}{\sqrt{2}}\right)^t, \quad t \in \mathbb{N},\ 2 \nmid t. \tag{2.13}$$

https://doi.org/10.1017/S0004972725100324 Published online by Cambridge University Press

Furthermore, every solution (U', V') of (2.4) can be expressed as

$$U' + V'\sqrt{D} = \lambda_1(U + \lambda_2 V\sqrt{D}), \quad \lambda_1, \lambda_2 \in \{1, -1\}, \tag{2.14}$$

where (U, V) is a positive integer solution of (2.4). The combination of (2.13) and (2.14) yields proposition (i). The lemma is proved. □

LEMMA 2.5. *For any odd prime p with $p \equiv 7 \pmod 8$, the equation*

$$U^2 - pV^2 = 2, \quad U, V \in \mathbb{Z}, \tag{2.15}$$

has solutions (U, V).

PROOF. By Lemma 2.1, (2.2) has positive integer solutions (u, v). Let (u_1, v_1) be the fundamental solution of (2.2). Then,

$$u_1^2 - pv_1^2 = 1, \quad u_1, v_1 \in \mathbb{N}. \tag{2.16}$$

If $2 \mid v_1$, then from (2.16),

$$u_1 + 1 = \begin{cases} 2a^2, \\ 2pb^2, \end{cases} \quad u_1 - 1 = \begin{cases} 2pb^2, \\ 2a^2, \end{cases} \quad v_1 = 2ab, \quad a, b \in \mathbb{N}, \tag{2.17}$$

whence we obtain either

$$a^2 - pb^2 = 1 \tag{2.18}$$

or

$$a^2 - pb^2 = -1. \tag{2.19}$$

When (2.18) holds, we see from (2.17) that $(u, v) = (a, b)$ is a positive integer solution of (2.2) with $a + b\sqrt{p} < u_1 + v_1\sqrt{p}$, which is a contradiction. When (2.19) holds, we have $p \mid a^2 + 1$ and $p \not\equiv 7 \pmod 8$, so we obtain $2 \nmid v_1$. Then, by (2.16),

$$u_1 + 1 = \begin{cases} a^2, \\ pb^2, \end{cases} \quad u_1 - 1 = \begin{cases} pb^2, \\ a^2, \end{cases} \quad v_1 = ab, \quad a, b, \in \mathbb{N}, \ 2 \nmid a, \ 2 \nmid b,$$

whence

$$a^2 - pb^2 = \pm 2. \tag{2.20}$$

Further, since $p \equiv 7 \pmod 8$, we see from (2.20) that $a^2 - pb^2 = 2$ and (2.15) has solutions (U, V). The lemma is proved. □

LEMMA 2.6 ([5, Lemmas 3 and 12 and Theorem 1]; [12, Theorem]). *Let p be an odd prime with $p \nmid D$.*

(i) *If $(\frac{D}{p}) = 1$, where $(\frac{D}{p})$ is the Legendre symbol, then the equation*

$$X^2 - DY^2 = p^Z, \quad X, Y \in \mathbb{Z}, \ \gcd(X, Y) = 1, \ Z \in \mathbb{N}, \tag{2.21}$$

https://doi.org/10.1017/S0004972725100324 Published online by Cambridge University Press

has solutions (X, Y, Z) *and it has a unique positive integer solution* (X_1, Y_1, Z_1) *such that* $Z_1 \le Z$,

$$1 < \frac{X_1 + Y_1\sqrt{D}}{X_1 - Y_1\sqrt{D}} < u_1 + v_1\sqrt{D},$$

where Z *runs through all solutions* (X, Y, Z) *of (2.21) and* (u_1, v_1) *is the fundamental solution of (2.1). The solution* (X_1, Y_1, Z_1) *is called the least solution of (2.21).*

(ii) *The least solution* (X_1, Y_1, Z_1) *of (2.21) satisfies* $Z_1 \mid h(4D)$, *where* $h(4D)$ *is the class number of binary quadratic primitive forms with discriminant* $4D$.

(iii) *Every solution* (X, Y, Z) *of (2.21) can be expressed as*

$$Z = Z_1 t, \quad t \in \mathbb{N},$$
$$X + Y\sqrt{D} = (X_1 + \lambda Y_1\sqrt{D})^t (u + v\sqrt{D}), \quad \lambda \in \{1, -1\},$$

where (X_1, Y_1, Z_1) *is the least solution of (2.21) and* (u, v) *is a solution of (2.1).*

Notice that $(\frac{2}{p}) = 1$ if and only if $p \equiv \pm 1 \pmod 8$, $h(8) = 1$ and the fundamental solution of the equation

$$u^2 - 2v^2 = 1, \quad u, v \in \mathbb{Z}, \tag{2.22}$$

is $(u_1, v_1) = (3, 2)$. By Lemma 2.5, we can directly obtain the following lemma.

LEMMA 2.7. *For any odd prime* p *with* $p \equiv \pm 1 \pmod 8$, *the equation*

$$X^2 - 2Y^2 = p^Z, \quad X, Y \in \mathbb{Z},\ \gcd(X, Y) = 1,\ Z \in \mathbb{N}, \tag{2.23}$$

has solutions (X, Y, Z) *and its least solution* (X_1, Y_1, Z_1) *satisfies*

$$1 < \frac{X_1 + Y_1\sqrt{2}}{X_1 - Y_1\sqrt{2}} < 3 + 2\sqrt{2} \tag{2.24}$$

and $Z_1 = 1$. *Moreover, every solution* (X, Y, Z) *of (2.23) can be expressed as*

$$X + Y\sqrt{2} = (X_1 + \lambda Y_1\sqrt{2})^Z (u + v\sqrt{2}), \quad \lambda \in \{1, -1\},$$

where (u, v) *is a solution of (2.22).*

LEMMA 2.8. *If* p *is a Mersenne prime with* $p \ge 7$, *then (2.23) has solutions* (X, Y, Z) *and its least solution is*

$$(X_1, Y_1, Z_1) = (2^{(q+1)/2} - 1, 2^{(q-1)/2} - 1, 1), \tag{2.25}$$

where q *is an odd prime defined as in (1.5).*

https://doi.org/10.1017/S0004972725100324 Published online by Cambridge University Press

PROOF. From (1.5), $(2^{(q+1)/2}-1)^2-2(2^{(q-1)/2}-1)^2=2^q-1=p$. Since $2^{(q+1)/2}-1$ and $2^{(q-1)/2}-1$ are coprime positive integers, (2.23) has a positive integer solution $(X,Y,Z)=(2^{(q+1)/2}-1,2^{(q-1)/2}-1,1)$. Further, since

$$1<\frac{(2^{(q+1)/2}-1)+(2^{(q-1)/2}-1)\sqrt{2}}{(2^{(q+1)/2}-1)-(2^{(q-1)/2}-1)\sqrt{2}}=\left(\frac{2^{q/2}-1}{2^{q/2}+1}\right)\left(\frac{\sqrt{2}+1}{\sqrt{2}-1}\right)$$
$$<\frac{\sqrt{2}+1}{\sqrt{2}-1}=3+2\sqrt{2}, \tag{2.26}$$

by Lemma 2.7, we find from (2.24) and (2.26) that (2.25) is the least solution of (2.23) for $p=2^q-1$ with $p\geq 7$. The lemma is proved. □

LEMMA 2.9 [7]. *The equation*

$$X^r-Y^s=1,\quad X,Y,r,s\in\mathbb{N},\ \min\{X,Y,r,s\}>1,$$

has only the solution $(X,Y,r,s)=(3,2,2,3)$.

LEMMA 2.10 [2]. *All solutions* (X,Y,m,n) *of the equation*

$$X^2-2^m=Y^n,\quad X,Y,m,n\in\mathbb{N},\ \gcd(X,Y)=1,Y>1,\ m>1,\ 2\nmid n,$$

satisfy $n=1$, *except for* $(X,Y,m,n)=(71,17,7,3)$.

LEMMA 2.11. *All solutions* (x,m,n) *of (1.1) with* $2\mid m$ *are (1.2) and*

$$p=2^{2^l}+1,\quad \text{where } l\in\mathbb{N},(x,m,n)=(2^{2^l-1}+1,2(2^l-1),1). \tag{2.27}$$

PROOF. Assume that (x,m,n) is a solution of (1.1) with $2\mid m$. Since p is an odd prime, we see from (1.1) that $2\nmid x$, $\gcd(x+2^{m/2},x-2^{m/2})=1$ and

$$x+2^{m/2}=p^n,\quad x-2^{m/2}=1.$$

It follows that

$$2x=p^n+1 \tag{2.28}$$

and

$$2^{m/2+1}=p^n-1. \tag{2.29}$$

When $n>1$, by Lemma 2.9, we can only obtain $p=3$, $m/2+1=3$ and $n=2$ from (2.29). Hence, by (2.28), we get (1.2).

When $n=1$, by (2.29),

$$p=2^{m/2+1}+1. \tag{2.30}$$

It follows that p is a Fermat prime. Therefore, since $p=2^{2^l}+1$, where $l\in\mathbb{N}$, by (2.28) and (2.30), we get (2.27). The lemma is proved. □

LEMMA 2.12. *All solutions* (x,m,n) *of (1.1) with* $2\mid n$ *are (1.6) with (1.5).*

https://doi.org/10.1017/S0004972725100324 Published online by Cambridge University Press

PROOF. Assume that (x, m, n) is a solution of (1.1) with $2 \mid n$. Since $2 \nmid x$, by (1.1), we have $\gcd(x + p^{n/2}, x - p^{n/2}) = 2$ and

$$x + p^{n/2} = 2^{m-1}, \quad x - p^{n/2} = 2,$$

giving

$$x = 2^{m-2} + 1 \tag{2.31}$$

and

$$p^{n/2} = 2^{m-2} - 1. \tag{2.32}$$

Applying Lemma 2.9 to (2.32), we obtain $n/2 = 1$ and

$$p = 2^{m-2} - 1. \tag{2.33}$$

From (2.33), p is a Mersenne prime, so p can be expressed as (1.5). By (1.5), (2.31) and (2.33), we obtain the solutions (1.6). The lemma is proved. □

3. Proof of Theorem 1.1

Let (x, m, n) be a solution of (1.1). Since $2 \nmid p$, by (1.1), $2 \nmid x$, $x^2 \equiv 1 \pmod 8$ and

$$p^n \equiv x^2 - 2^m \equiv 1 - 2^m \equiv \begin{cases} 7 \pmod 8 & \text{if } m = 1, \\ 5 \pmod 8 & \text{if } m = 2, \\ 1 \pmod 8 & \text{if } m \geq 3. \end{cases} \tag{3.1}$$

When $p \equiv 3 \pmod 8$, since

$$p^n \equiv \begin{cases} 1 \pmod 8 & \text{if } 2 \mid n, \\ 3 \pmod 8 & \text{if } 2 \nmid n, \end{cases} \tag{3.2}$$

we see from (3.1) and (3.2) that $2 \mid n$. Therefore, by Lemma 2.12, (1.1) has only the solution (1.2) for $p \equiv 3 \pmod 8$.

When $p \equiv 5 \pmod 8$,

$$p^n \equiv \begin{cases} 1 \pmod 8 & \text{if } 2 \mid n, \\ 5 \pmod 8 & \text{if } 2 \nmid n. \end{cases} \tag{3.3}$$

By (3.1) and (3.3), either $2 \mid n$ or $m = 2$ and $2 \nmid n$. Hence, by Lemma 2.12, (1.1) has no solutions (x, m, n) with $2 \mid n$ for $p \equiv 5 \pmod 8$. However, by Lemma 2.11, (1.1) has only the solution (1.3) with $m = 2$ and $2 \nmid n$. The theorem is proved.

4. Proof of Theorem 1.2

LEMMA 4.1 [3]. *All solutions (X, Y, n) of the equation*

$$X^2 - 2 = Y^n, \quad X, Y, n \in \mathbb{N}, \tag{4.1}$$

satisfy $n < 550\,000$.

https://doi.org/10.1017/S0004972725100324 Published online by Cambridge University Press

LEMMA 4.2 [1]. *Let $f(t) \in \mathbb{Z}[t]$ be a polynomial of degree n with at least three distinct zeros and coefficients with absolute values at most H. Then, all solutions (X, Y) of the equation*

$$X^2 = f(Y), \quad X, Y \in \mathbb{Z},$$

satisfy $\max\{|X|, |Y|\} < \exp\exp\exp((n^{10n}H)^{n^2})$.

The following lemma can be obtained directly from Lemmas 4.1 and 4.2.

LEMMA 4.3. *All solutions (X, Y, n) of (4.1) with $n \geq 3$ satisfy $Y < C$, where C is an effectively computable absolute constant.*

LEMMA 4.4. *If (x, n) is a solution of the equation*

$$x^2 - 2 = p^n, \quad x, n \in \mathbb{N}, \tag{4.2}$$

then $2 \nmid n$ and

$$(U_1, V_1) = (x, p^{(n-1)/2}) \tag{4.3}$$

is the fundamental solution of (2.15).

PROOF. Assume that (x, n) is a solution of (4.2). Then, $2 \nmid x$ and $p^n \equiv x^2 - 2 \equiv 1 - 2 \equiv 7 \pmod 8$. It follows that $2 \nmid n$ and $p \equiv 7 \pmod 8$. Hence, we see from (4.2) that (2.15) has a positive integer solution

$$(U, V) = (x, p^{(n-1)/2}). \tag{4.4}$$

Applying Lemma 2.4(i) to (4.4),

$$\frac{x + p^{(n-1)/2}\sqrt{p}}{\sqrt{2}} = \left(\frac{U_1 + V_1\sqrt{p}}{\sqrt{2}}\right)^t, \quad t \in \mathbb{N},\ 2 \nmid t, \tag{4.5}$$

where (U_1, V_1) is the fundamental solution of (2.15). By (4.5),

$$2^{(t-1)/2}p^{(n-1)/2} = V_1 \sum_{i=0}^{(t-1)/2} \binom{t}{2i+1} U_1^{t-2i-1}(pV_1^2)^i. \tag{4.6}$$

If $t > 1$, since $t \geq 3$, $U_1 \geq 3$ and

$$\sum_{i=0}^{(t-1)/2} \binom{t}{2i+1} U_1^{t-2i-1}(pV_1^2)^i > tU_1^{t-1} > 2^{(t-1)/2},$$

it follows from (4.6) that $n > 1$ and $p \mid tV_1$. Let

$$p^\alpha \parallel tV_1, \quad p^{\beta_i} \parallel 2i + 1, \quad i \in \mathbb{N}. \tag{4.7}$$

https://doi.org/10.1017/S0004972725100324 Published online by Cambridge University Press

Since $p^{\beta_i} \le 2i+1$ and

$$\beta_i \le \frac{\log(2i+1)}{\log p} < i, \quad i \in \mathbb{N}, \tag{4.8}$$

by (4.7) and (4.8),

$$V_1\binom{t}{2i+1}U_1^{t-2i-1}(pV_1^2)^i \equiv tV_1\binom{t-1}{2i}U_1^{t-2i-1}\frac{(pV_1^2)^i}{2i+1} \equiv 0 \pmod{p^{\alpha+1}}, \quad i \in \mathbb{N}. \tag{4.9}$$

Hence, from (4.6), (4.7) and (4.9), $\alpha = (n-1)/2$ and $tV_1 \ge p^{(n-1)/2}$. So $2^{(t-1)/2}p^{(n-1)/2} > tU_1^{t-1}V_1 \ge U_1^{t-1}p^{(n-1)/2}$ and $2^{(t-1)/2} > U_1^{t-1} \ge 3^{t-1}$, which is a contradiction. It follows that $t = 1$ and by (4.5), we get (4.3). The lemma is proved. □

LEMMA 4.5. *For any Mersenne prime p with $p \ge 7$, (4.2) has no solutions (x, n) with $n > 1$.*

PROOF. Assume that (x, n) is a solution of (4.2) with $n > 1$. By Lemma 4.4, $p \mid V_1$, where (U_1, V_1) is the fundamental solution of (2.15). Further, by Lemma 2.4(ii), $v_1 = U_1V_1$, where (u_1, v_1) is the fundamental solution of (2.2). So $p \mid v_1$. Therefore, by Lemma 2.2, $p > 1.5 \times 10^{12}$ and by (1.5),

$$q > 40. \tag{4.10}$$

According to well-known properties of Mersenne primes, by (4.10), we just need to consider the case

$$q \ge 61, \quad p \ge 2^{61} - 1 > 2 \times 10^{18}. \tag{4.11}$$

We see from (4.2) that (2.23) has a solution

$$(X, Y, Z) = (x, 1, n). \tag{4.12}$$

Applying Lemmas 2.7 and 2.8 to (4.12),

$$x + \sqrt{2} = (X_1 + \lambda Y_1\sqrt{2})^n(u - \lambda v\sqrt{2}), \quad \lambda \in \{1, -1\}, \tag{4.13}$$

where X_1, Y_1 satisfy (2.25) and (u, v) is a positive integer solution of (2.22). Since the fundamental solution of (2.22) is $(u_1, v_1) = (3, 2)$, by Lemma 2.1,

$$u + v\sqrt{2} = (3 + 2\sqrt{2})^t, \quad t \in \mathbb{N}. \tag{4.14}$$

Hence, by (4.13) and (4.14), $x - \sqrt{2} = (X_1 - \lambda Y_1\sqrt{2})^n(u + \lambda v\sqrt{2})$ and

$$\frac{x+\sqrt{2}}{x-\sqrt{2}} = \begin{cases} \left(\dfrac{X_1 + Y_1\sqrt{2}}{X_1 - Y_1\sqrt{2}}\right)^n (3 + 2\sqrt{2})^{-2t} & \text{if } \lambda = 1, \\ \left(\dfrac{X_1 - Y_1\sqrt{2}}{X_1 + Y_1\sqrt{2}}\right)^n (3 + 2\sqrt{2})^{2t} & \text{if } \lambda = -1. \end{cases} \tag{4.15}$$

https://doi.org/10.1017/S0004972725100324 Published online by Cambridge University Press

Here, $n > 1$, $2 \nmid n$, $x > p^{n/2} \geq p^{3/2} > 10^{27}$, $1.01 > (x+\sqrt{2})/(x-\sqrt{2}) > 1$ and X_1, Y_1 satisfy (2.24) by Lemmas 2.7 and 2.8. If $\lambda = 1$, then from (2.24) and (4.15),

$$(3+2\sqrt{2})^{2t} < \left(\frac{x+\sqrt{2}}{x-\sqrt{2}}\right)(3+2\sqrt{2})^{2t} = \left(\frac{X_1+Y_1\sqrt{2}}{X_1-Y_1\sqrt{2}}\right)^n < (3+2\sqrt{2})^n,$$

whence we obtain $2t < n$ and

$$n \geq 2t+1. \tag{4.16}$$

Similarly, if $\lambda = -1$, then

$$(3+2\sqrt{2})^{2t} = \left(\frac{x+\sqrt{2}}{x-\sqrt{2}}\right)\left(\frac{X_1+Y_1\sqrt{2}}{X_1-Y_1\sqrt{2}}\right)^n < 1.01(3+2\sqrt{2})^n < (3+2\sqrt{2})^{n+1},$$

whence $n+1 > 2t$ and (4.16) is still true, since $2 \nmid n$.

Further, by (2.26) and (4.15),

$$\frac{x+\sqrt{2}}{x-\sqrt{2}} = \begin{cases} (3+2\sqrt{2})^{n-2t}\theta^{-n} & \text{if } \lambda = 1, \\ (3+2\sqrt{2})^{-(n-2t)}\theta^n & \text{if } \lambda = -1, \end{cases} \tag{4.17}$$

where

$$\theta = \frac{2^{q/2}+1}{2^{q/2}-1}. \tag{4.18}$$

If $\lambda = 1$, then from (4.16) and (4.17),

$$1.01\theta^n > \left(\frac{x+\sqrt{2}}{x-\sqrt{2}}\right)\theta^n = (3+2\sqrt{2})^{n-2t} \geq 3+2\sqrt{2}. \tag{4.19}$$

Similarly, if $\lambda = -1$, then

$$\theta^n = \left(\frac{x+\sqrt{2}}{x-\sqrt{2}}\right)(3+2\sqrt{2})^{n-2t} > (3+2\sqrt{2})^{n-2t} \geq 3+2\sqrt{2}.$$

This implies that (4.19) is still true for $\lambda = -1$.

Taking logarithms on both sides of (4.19),

$$n\log\theta > \log\left(\frac{3+2\sqrt{2}}{1.01}\right) > 1.75. \tag{4.20}$$

Further, since $\log(1+\alpha) < \alpha$ for any $\alpha > 0$, by (4.18),

$$\log\theta = \log\left(1+\frac{2}{2^{q/2}-1}\right) < \frac{2}{2^{q/2}-1}. \tag{4.21}$$

Therefore, by (4.11), (4.20) and (4.21),

$$n > \tfrac{1}{2}(1.75(2^{q/2}-1)) > 0.87(2^{61/2}-1) > 10^9. \tag{4.22}$$

However, by Lemma 4.1, (4.22) is impossible. The lemma is proved. □

https://doi.org/10.1017/S0004972725100324 Published online by Cambridge University Press

PROOF OF THEOREM 1.2. Assume that (x, m, n) is a solution of (1.1) for $p \equiv 7 \pmod 8$. Since

$$p^n \equiv \begin{cases} 1 \pmod 8 & \text{if } 2 \mid n, \\ 7 \pmod 8 & \text{if } 2 \nmid n, \end{cases} \tag{4.23}$$

by (3.1) and (4.23), the solution (x, m, n) satisfies either $2 \mid n$ or $m = 1$ and $2 \nmid n$.

We first consider the case that p is a Mersenne prime. Then, p can be expressed as (1.5), where q is an odd prime. By Lemma 2.12, (1.1) has only one solution (1.6) with $2 \mid n$. However, by Lemma 4.5, if the solution (x, m, n) satisfies $m = 1$ and $2 \nmid n$, then $n = 1$. Hence, by (1.1) and (1.5),

$$x^2 - 2^q = 1. \tag{4.24}$$

Applying Lemma 2.9 to (4.24), we can only obtain $x = 3$, $q = 3$ and

$$p = 7, \quad (x, m, n) = (3, 1, 1). \tag{4.25}$$

From the combination of (1.6) and (4.25), if $p = 7$, then (1.1) has exactly two solutions (1.4); otherwise, (1.1) has only one solution (1.6). It follows that the theorem holds when p is a Mersenne prime.

Next, we consider the case where p is not a Mersenne prime. Then, by Lemma 2.12, (1.1) has no solutions (x, m, n) with $2 \mid n$. Hence, the solution (x, m, n) must satisfy $2 \nmid n$. Further, by Lemma 2.10, we have $m = 1$. Therefore, from the uniqueness of the fundamental solution (U_1, V_1) of (2.15), by Lemma 2.4(i), we find from Lemma 4.4 that (1.1) has at most one solution (x, m, n) for any fixed p in this case. Further, by Lemmas 2.2, 2.4, 4.4 and 4.3, $p > 1.5 \times 10^{12}$ and $p < C$ if $n > 1$. However, if $n = 1$, then from (4.2), we obtain only the solution (1.7). From this analysis, the theorem is proved. □

5. Proof of Theorem 1.3

In this section, we assume that $D \equiv 1 \pmod 8$ and $p \equiv 1 \pmod 8$ with $p \nmid 17$. Then, (1.1) is related to the equation

$$y^2 - D = 2^{z+2}, \quad y, z \in \mathbb{N}. \tag{5.1}$$

If D satisfies one of the following three types, then D is called an exceptional case of (5.1); otherwise, it is called nonexceptional:

(I) $D = 2^{2r} - 3 \cdot 2^{r+1} + 1$, where $r \in \mathbb{N}$ with $r \geq 3$;
(II) $D = ((2^{2r+1} - 17)/3)^2 - 32$, where $r \in \mathbb{N}$ with $r \geq 3$;
(III) $D = 2^{2r_1} + 2^{2r_2} - 2^{r_1+r_2+1} - 2^{r_1+1} - 2^{r_2+1} + 1$, where $r_1, r_2 \in \mathbb{N}$ are such that $r_2 > r_1 + 1 > 2$.

LEMMA 5.1 [4]. *If D is nonexceptional and the equation*

$$u'^2 - Dv'^2 = -1, \quad u', v' \in \mathbb{Z}$$

has solutions (u', v'), then (5.1) has at most two solutions (y, z).

https://doi.org/10.1017/S0004972725100324 Published online by Cambridge University Press

LEMMA 5.2. *If D is an exceptional case of (5.1) with $D \neq 17$, then D is not an odd prime.*

PROOF. When D is an exceptional case of type (I) with $D \neq 17$,

$$D = (2^r - 1)^2 - 2^{r+2} = (2^r + 1)^2 - 2^{r+3} \quad \text{with } r \in \mathbb{N},\ r \geq 4,$$

whence we get the following factorisations of D in positive integers:

$$D = \begin{cases} (2^r + 2^{r/2+1} - 1)(2^r - 2^{r/2+1} - 1) & \text{if } 2 \mid r, \\ (2^r + 2^{(r+3)/2} + 1)(2^r - 2^{(r+3)/2} + 1) & \text{if } 2 \nmid r. \end{cases} \tag{5.2}$$

Since $r \geq 4$, we have $2^r + 2^{r/2+1} - 1 > 2^r - 2^{r/2+1} - 1 > 1$ and also $2^r + 2^{(r+3)/2} + 1 > 2^r - 2^{(r+3)/2} + 1 > 1$. Hence, we see from (5.2) that D is not an odd prime.

When D is an exceptional case of type (II),

$$D = \tfrac{1}{9}(2^{2r+1} + 2^{r+3} - 1)(2^{2r+1} - 2^{r+3} - 1). \tag{5.3}$$

Since $r \geq 3$, we have $2^{2r+1} + 2^{r+3} - 1 > 2^{2r+1} - 2^{r+2} - 1 \geq 95$ and

$$0 \equiv \begin{cases} 2^{2r+1} + 2^{r+3} - 1 \pmod 9 & \text{if } r \equiv 0, 2, 4 \pmod 6, \\ 2^{2r+1} - 2^{r+3} - 1 \pmod 9 & \text{if } r \equiv 1, 3, 5 \pmod 6. \end{cases} \tag{5.4}$$

We see from (5.3) and (5.4) that D is not an odd prime.

When D is an exceptional case of type (III),

$$D = \begin{cases} (2^{r_2} - 2^{r_1} + 2^{r_1/2} - 1)(2^{r_2} - 2^{r_1} - 2^{r_1/2+1} - 1) & \text{if } 2 \mid r_1, \\ (2^{r_2} + 2^{r_2/2+1} - 2^{r_1} - 1)(2^{r_2} - 2^{r_2/2+1} - 2^{r_1} - 1) & \text{if } 2 \mid r_2, \\ (2^{r_2} + 2^{r_1} + 2^{(r_2+r_1)/2+1} - 1)(2^{r_2} + 2^{r_1} - 2^{(r_2+r_1)/2+1} - 1) & \text{if } 2 \nmid r_1 r_2. \end{cases} \tag{5.5}$$

Since $r_2 > r_1 + 1 > 2$, we see from (5.5) that D is not an odd prime. The lemma is proved. □

PROOF OF THEOREM 1.3. Since $p \equiv 1 \pmod 8$, by Lemma 2.12, (1.1) has no solutions (x, m, n) with $2 \mid n$. So we have $2 \nmid n$. Further, since $p \equiv 1 \pmod 8$, we see from (1.1) that $m \geq 3$. Therefore, since $p \neq 17$, by Lemma 2.10, the solutions (x, m, n) of (1.1) must satisfy $n = 1$. This implies that there is a one-to-one correspondence $(x, m, n) = (y, z + 2, 1)$ between the solutions (x, m, n) of (1.1) and the solutions (y, z) of the equation

$$y^2 - p = 2^{z+2}, \quad y, z \in \mathbb{N}. \tag{5.6}$$

In particular, if $p \equiv 1 \pmod 8$ and $p \neq 17$, then the numbers of solutions to these two equations are the same.

Since $p \equiv 1 \pmod 8$, by Lemma 2.3, (2.3) has solutions (u', v'). Since p is an odd prime with $p \neq 17$, by Lemma 5.2, p is nonexceptional for (5.6). Therefore, by Lemma 5.1, (5.6) has at most two solutions (y, z). The theorem is proved. □

https://doi.org/10.1017/S0004972725100324 Published online by Cambridge University Press

Acknowledgement

The authors thank the referee for careful reading and pertinent suggestions.

References

[1] A. Baker, 'Bounds for the solutions of the hyperelliptic equation', *Math. Proc. Cambridge Philos. Soc.* **65** (1969), 439–444.
[2] M. A. Bennett and C. M. Skinner, 'Ternary Diophantine equations via Galois representations and modular forms', *Canad. J. Math.* **56** (2004), 23–54.
[3] Y. Bugeaud, 'On the Diophantine equation $x^2 - 2^m = \pm y^n$', *Proc. Amer. Math. Soc.* **125** (1997), 3203–3208.
[4] M.-H. Le, 'On the number of solutions of the generalized Ramanujan–Nagell equation $x^2 - D = 2^{n+2}$', *Acta Arith.* **60** (1991), 149–167.
[5] M.-H. Le, 'Some exponential Diophantine equations I: The equation $D_1x^2 - D_2y^2 = \lambda k^z$', *J. Number Theory* **55** (1995), 209–221.
[6] F. Luca and I. Pink, 'On the Diophantine equation $2^s + p^k = m^2$ with a Fermat prime p', *J. Number Theory* **268** (2025), 49–71.
[7] P. Mihăilescu, 'Primary cyclotomic units and a proof of Catalan's conjecture', *J. reine angew. Math.* **572** (2004), 167–195.
[8] T. Nagell, *Introduction to Number Theory* (Wiley, New York, 1951).
[9] A. Reinhart, 'On orders in quadratic number fields with unusual sets of distances', *Acta Arith.* **211** (2023), 61–92.
[10] A. Reinhart, 'A counterexample to the Pellian equation conjecture of Mordell', *Acta Arith.* **215** (2024), 85–95.
[11] T.-T. Wang and Y.-Z. Jiang, 'On the number of positive integer solutions (x, n) of the generalized Ramanujan–Nagell equation $x^2 - 2^r = p^n$', *Period. Math. Hungar.* **75** (2017), 150–154.
[12] H. Yang and R.-Q. Fu, 'An upper bound for least solutions of the exponential Diophantine equation $D_1x^2 - D_2y^2 = \lambda k^z$', *Int. J. Number Theory* **11** (2015), 1107–1114.

YASUTSUGU FUJITA, Department of Mathematics,
College of Industrial Technology,
Nihon University, 2-11-1 Shin-ei, Narashino, Chiba, Japan
e-mail: fujita.yasutsugu@nihon-u.ac.jp

MAOHUA LE, Institute of Mathematics,
Lingnan Normal College, Zhanjiang, Guangdong 524048, PR China
e-mail: lemaohua2008@163.com

https://doi.org/10.1017/S0004972725100324 Published online by Cambridge University Press