#A64 INTEGERS 24 (2024)

ON THE EQUATION $(-1)^{\alpha}p^{x} + (-1)^{\beta}(2^{k}(2p-1))^{y} = z^{2}$ FOR PRIME PAIRS $(p, 2p-1)$

Jing Zhang
Department of Mathematics, Governors State University, University Park, Illinois
jzhang@govst.edu

Yuan Li
Department of Mathematics, Winston-Salem State University, Winston-Salem, North Carolina
liyu@wssu.edu

Received: 8/18/22, Revised: 6/22/23, Accepted: 6/17/24, Published: 7/8/24

Abstract

In this paper, for prime pairs p and $2p-1$, we consider the Diophantine equations $(-1)^{\alpha}p^{x} + (-1)^{\beta}(2^{k}(2p-1))^{y} = z^{2}$ with $\alpha, \beta \in \{0, 1\}$, $\alpha\beta = 0$ and a non-negative integer k. We first obtain all non-negative integer solutions for the following six types of equations with odd prime pairs p and $2p-1$:

(i) $p^{x} + (2p-1)^{y} = z^{2}$;
(ii) $p^{x} + (2^{2k+1}(2p-1))^{y} = z^{2}$ with $p \equiv 5, 7 \pmod 8$;
(iii) $p^{x} + (2^{2k}(2p-1))^{y} = z^{2}$ with $p \equiv 3 \pmod 4$ and $k \geq 1$;
(iv) $(2^{2k}(2p-1))^{x} - p^{y} = z^{2}$ with $p \equiv 3 \pmod 4$ and $k \geq 0$;
(v) $(2^{2k+1}(2p-1))^{x} - p^{y} = z^{2}$ with $p \equiv 5 \pmod 8$;
(vi) $p^{x} - (2^{2k+1}(2p-1))^{y} = z^{2}$ with $p \equiv 3 \pmod 8$.

In the literature, it has been conjectured that there are infinitely many prime pairs p and $2p-1$. Hence, it is reasonable to conjecture that there exist infinitely many prime pairs p and $2p-1$ such that $p \equiv i \pmod 8$ for $i = 1, 3, 5, 7$. Using the L-functions and Modular Forms database for the elliptic curve $y^{2} = x^{3} + ax + b$ over $\mathbb{Q}$, we solve six equations of the form $(-1)^{\alpha}2^{x} + (-1)^{\beta}(2^{k}(3))^{y} = z^{2}$, where $p = 2$, $\alpha, \beta, k \in \{0, 1\}$, and $\alpha\beta = 0$. Finally, with the same method, we give an affirmative answer for a question raised by Borah and Dutta.

1. Introduction

For various fixed pairs of integers (a, b), the Diophantine equations $a^{x} + b^{y} = z^{2}$ and $a^{x} - b^{y} = z^{2}$ have received a lot of attention in recent decades [1, 4, 6, 9, 13, 16, 19]. Borah and Dutta [1] showed that there is only one non-negative integer solution

DOI: 10.5281/zenodo.12685719

for the equation $7^x + 32^y = z^2$ and only two non-negative integer solutions for the equation $2^x + 7^y = z^2$ for $x \neq 1$. Gayo and Bacani [4] solved the equation $M_p^x + (M_q + 1)^y = z^2$ for Mersenne primes $M_p = 2^p - 1$ and $M_q = 2^q - 1$. Mina and Bacani [13] studied the equation $p^x + (p + 4k)^y = z^2$ for prime pairs p and $p + 4k$ and obtained many results. A summary of the most recent works on the equation $a^x + b^y = z^2$ can be found in their papers [4, 13].

In this paper, for prime pairs p and $2p - 1$, we solve six types of Diophantine equations of the form $(-1)^\alpha p^x + (-1)^\beta (2^k(2p-1))^y = z^2$ where $\alpha, \beta = 0, 1$, $\alpha\beta = 0$ and $k \in \{0\} \cup \mathbb{N}$. In Section 2, we list some results needed in the proof of our main theorems. In Section 3, we solve three equations of the form $p^x + (2^k(2p-1))^y = z^2$, when (1) k is zero; (2) $k > 0$ is odd; and (3) $k \geq 2$ is even and $p > 2$. In Section 4, we solve three other equations: $(2^{2k}(2p-1))^x - p^y = z^2$, $(2^{2k+1}(2p-1))^x - p^y = z^2$ and $p^x - (2^{2k+1}(2p-1))^y = z^2$, where p is an odd prime. In Section 5, for $p = 2$, using the database of elliptic curves in the L-functions and Modular Forms database (the LMFDB) [11], we solve six equations of the form $(-1)^\alpha 2^x + (-1)^\beta (2^k(3))^y = z^2$ with $\alpha, \beta, k = 0, 1$ and $\alpha\beta = 0$. In Section 6, we answer a question proposed by Borah and Dutta [1] by obtaining all non-negative integer solutions of the equation $2 + 7^y = z^2$.

2. Preliminaries

The following lemma was conjectured by Catalan in 1844 and proved in 2002 by Mihăilescu [12].

Lemma 1 (Catalan–Mihăilescu Theorem [12])**.** *If a, b, x, and y are integers and $\min\{a, b, x, y\} > 1$, then the Diophantine equation $a^x - b^y = 1$ has a unique integer solution $(a, b, x, y) = (3, 2, 2, 3)$.*

The following lemma is a direct consequence of a result of Ko [5] and a special case of the Catalan–Mihăilescu Theorem. One can also prove it directly.

Lemma 2. *If p is a prime number, then $p^x + 1 = y^2$ has only two non-negative integer solutions $(p, x, y) = (2, 3, 3)$ and $(p, x, y) = (3, 1, 2)$.*

We also need the following simple fact.

Lemma 3. *If $2^k + 1$ is a prime number, then $k = 0$ or $k = 2^s$ for $s \geq 0$.*

Proof. If $k \geq 1$ and $p \mid k$ for some odd prime number p, then $2^k + 1$ can be factored into a product of $2^{k/p} + 1$ and another integer greater than 1, using the identity

$$a^{2n+1} + 1 = (a + 1)(a^{2n} - a^{2n-1} + \cdots - a + 1),$$

and substitutions $a = 2^{k/p}$ and $2n + 1 = p$. So $2^k + 1$ is not a prime number if $k > 1$ has an odd factor greater than 1. Therefore, if $k \neq 0$, then $k = 2^s$ for $s \geq 0$. □

Lemma 4. *If p and $q = 2p-1$ are odd primes, and $k \geq 1$, then $1+(2^k(2p-1))^y = z^2$ has a unique non-negative integer solution $(k, p, y, z) = (4, 3, 1, 9)$.*

Proof. Rewriting the equation $1 + (2^k(2p-1))^y = z^2$ in the form

$$z^2 - (2^k q)^y = 1, \tag{2.1}$$

we have $z \geq 2$ and $y \geq 1$. If $y \geq 2$, then $\min\{z, 2^k q, 2, y\} > 1$, and Equation (2.1) has no integer solutions by Lemma 1. If $y = 1$, Equation (2.1) can be written as

$$(z-1)(z+1) = 2^k q. \tag{2.2}$$

Since $z + 1 > 0$, $z - 1 > 0$, and $k \geq 1$, it follows that $\gcd(z+1, z-1) = 2$. There are the following four possibilities.

(1) If $z - 1 = 2$ and $z + 1 = 2^{k-1}q$, then $4 = 2^{k-1}q$, which is impossible since $k \geq 1$ and $q \geq 5$.

(2) If $z - 1 = 2q$ and $z + 1 = 2^{k-1}$, then $2 = 2^{k-1} - 2q$. Hence $p = 2^{k-3}$, which is impossible.

(3) If $z - 1 = 2^{k-1}$ and $z + 1 = 2q$, then $2 = 2q - 2^{k-1}$, $q = 2^{k-2} + 1$ and $p = 2^{k-3} + 1$. Since p and q are odd prime numbers, we get $k - 2 = 2^r$ and $k - 3 = 2^s$ with $r > s \geq 0$ by Lemma 3. Hence, $2^r - 2^s = 1$, which implies $r = 1$ and $s = 0$. In this case, we obtain the solution $(k, p, y, z) = (4, 3, 1, 9)$.

(4) If $z - 1 = 2^{k-1}q$ and $z + 1 = 2$, then $q = 0$ which contradicts the fact that $q \geq 5$. □

Ljunggren and Nagell [3, 10] proved the following result.

Lemma 5 (Nagell–Ljunggren Theorem [3, 10])**.** *If $x, y > 1$, $n > 2$, and $q \geq 2$, then apart from the solutions $\frac{3^5-1}{3-1} = 11^2$, $\frac{7^4-1}{7-1} = 20^2$ and $\frac{18^3-1}{18-1} = 7^3$, the following equation*

$$\frac{x^n - 1}{x - 1} = y^q \tag{2.3}$$

has no other integer solution (x, y, n, q) if one of the following conditions is satisfied:

(i) $q = 2$;

(ii) 3 divides n;

(iii) 4 divides n;

(iv) $q = 3$ and $n \not\equiv 5 \pmod 6$.

More results related to the Nagell–Ljunggren equation can be found in [2, 3, 8, 18]. In 1993, Terai [16] proposed the following conjecture.

Conjecture 1. If $a^2 + b^2 = c^2$, where $\gcd(a, b, c) = 1$ and a is even, then the equation $x^2 + b^y = c^z$ has only the positive integer solution $(x, y, z) = (a, 2, 2)$.

Le [6] proved that Terai's conjecture holds if $b > 8 \times 10^6$, $b \equiv \pm 5 \pmod 8$, and c is a prime power. Later, Yuan and Wang proved the following result.

Lemma 6 ([19]). *If $a^2 + b^2 = c^2$, $\gcd(a, b, c) = 1$, $b \equiv \pm 5 \pmod 8$, and c is a prime number, then Terai's Conjecture holds.*

It has been conjectured that there exist infinitely many primes p such that $2p-1$ is also prime. Let $\mathbb{S}$ be the set of all prime pairs $(p, 2p-1)$. The set of such pairs when $p \leq 1000$ is as follows:

$$\begin{aligned}\mathbb{S}_{p\leq 1000} = \{&(2,3),(3,5),(7,13),(19,37),(31,61),(37,73),(79,157),(97,193),\\&(139,277),(157,313),(199,397),(211,421),(229,457),(271,541),\\&(307,613),(331,661),(337,673),(367,733),(379,757),(439,877),\\&(499,997),(547,1093),(577,1153),(601,1201),(607,1213),\\&(619,1237),(661,1321),(691,1381),(727,1453),(811,1261),\\&(829,1657),(877,1753),(937,1873),(967,1933),(997,1993)\}.\end{aligned}$$

For $k = 1, 3, 5, 7$, let $\mathbb{T}_k$ be the set of prime numbers p with $p \equiv k \pmod 8$ such that $2p - 1$ is also prime. Then, we have

$$\begin{aligned}&\mathbb{T}_1 = \{97, 337, 577, 601, 937, \dots\},\\&\mathbb{T}_3 = \{3, 19, 139, 211, 307, 331, 379, 499, 547, 619, 691, 811, \dots\},\\&\mathbb{T}_5 = \{37, 157, 229, 661, 829, 877, 997, \dots\},\\&\mathbb{T}_7 = \{7, 31, 79, 199, 271, 367, 439, 607, 727, 967, \dots\}.\end{aligned}$$

Generally, for $k = 1, 3, 5, \dots, 2^n - 1$, $n \in \mathbb{N}$, let $\mathbb{T}_k^n$ be the set of prime numbers p with $p \equiv k \pmod{2^n}$ such that $2p - 1$ is also prime. It is reasonable to conjecture that each set $\mathbb{T}_k^n$ is an infinite set.

Using the discriminant $\Delta = -16(4a^3 + 27b^2)$ of the elliptic curve $y^2 = x^3 + ax + b$ over $\mathbb{Q}$, the following lemma can be found in the LMFDB [11].

Lemma 7 ([11]). *Among the following three elliptic curves over $\mathbb{Q}$, we have that:*
(1) $y^2 = x^3 - 2$ has only the two integer solutions $(x, y) = (3, \pm 5)$.
(2) $y^2 = x^3 - 18$ has only the two integer solutions $(x, y) = (3, \pm 3)$.
(3) $y^2 = x^3 - 162$ has no integer solutions.

3. Solutions of the Equation $p^x + (2^k(2p-1))^y = z^2$ with $k \geq 0$

In this section, we study the Diophantine equation of the form $p^x + (2^k(2p-1))^y = z^2$ when (a) $k = 0$; (b) $k > 0$ is odd; and (c) $k \geq 2$ is even.

Theorem 1. *If p and $2p-1$ are odd prime numbers, then the equation*

$$p^x + (2p-1)^y = z^2 \tag{3.1}$$

has a unique non-negative integer solution $(p, x, y, z) = (3, 1, 0, 2)$.

Proof. First, if $p \equiv 1 \pmod 8$, then by taking Equation (3.1) modulo 8, we get a contradiction $2 \equiv z^2 \pmod 8$. Next, if $p \equiv 5 \pmod 8$, then we have

$$p^x \equiv 5^x \equiv 1, 5 \pmod 8$$

and

$$(2p-1)^y \equiv 1 \pmod 8.$$

However, Equation (3.1) becomes

$$z^2 \equiv 2, 6 \pmod 8,$$

which cannot be true.

Now we only need to consider the case $p \equiv 3 \pmod 4$. If $x = 0$, then Equation (3.1) has no integer solutions by Lemma 2. If $y = 0$, then Equation (3.1) has a unique integer solution $(p, x, y, z) = (3, 1, 0, 2)$ by Lemma 2.

We may assume $x, y \geq 1$ from now on. By taking Equation (3.1) modulo p, we have $(-1)^y \equiv z^2 \pmod p$, which gives $\gcd(p, z) = 1$ and the Legendre symbol

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

So we have for some $m \in \mathbb{N}$, $y = 2m$. Letting $q = 2p - 1$, Equation (3.1) can be written as $p^x = (z - q^m)(z + q^m)$. Letting $d = \gcd(z - q^m, z + q^m)$, we have $d \mid 2q^m$ and $d \mid p^x$. Since p and q are distinct odd prime numbers, we get $d = 1$. Therefore we have $z - q^m = 1$ and $z + q^m = p^x$. Hence

$$2q^m = 2(2p-1)^m = p^x - 1. \tag{3.2}$$

Taking Equation (3.2) modulo p, we have

$$2(-1)^m + 1 \equiv 0 \pmod p.$$

If m is odd, then we get $-1 \equiv 0 \pmod p$, which is impossible. So m is even and $3 \equiv 0 \pmod p$, which implies $p = 3$. Letting $m = 2m_1$ and $P = 5^{m_1}$ for some non-negative integer m_1, Equation (3.2) can be written as

$$\frac{3^x - 1}{3 - 1} = P^2. \tag{3.3}$$

Since $x \neq 1, 2$ in Equation (3.3) and Condition (i) in Lemma 5 is satisfied, Equation (3.3) has no integer solutions. $\square$

Remark 1. In [14], Sroysang first proved that the equation $3^x + 5^y = z^2$ has a unique non-negative integer solution $(x, y, z) = (1, 0, 2)$. Mina and Bacani [13] solved the equation $p^x + (p+4k)^y = z^2$, where both p and $p+4k$ are prime numbers. If $q = 2p - 1 = p + 4k$, then $p = 4k + 1$ and $p \equiv 1 \pmod 4$. Hence, in Theorem 1, the cases $p \equiv 1, 5 \pmod 8$ were first solved in [13].

Theorem 2. *If p and $q = 2p - 1$ are prime numbers with $p \equiv 5, 7 \pmod 8$, then for any integer $k \geq 0$,*

$$p^x + (2^{2k+1}(2p-1))^y = z^2 \tag{3.4}$$

has no non-negative integer solutions.

Proof. Since $p \geq 5$, if $y = 0$, then Equation (3.4) has no integer solutions by Lemma 2. Since $2k + 1 \neq 4$ (or $p \neq 3$), by Lemma 4, if $x = 0$, then Equation (3.4) has no integer solutions.

Now we assume $x \geq 1$ and $y \geq 1$. Taking Equation (3.4) modulo p, we obtain

$$(2^{2k+1}(-1))^y \equiv z^2 \pmod p.$$

Hence, we have

$$1 = \left(\frac{z^2}{p}\right) = \left(\frac{(2^{2k+1}(-1))^y}{p}\right) = \left(\frac{2^{2k+1}}{p}\right)^y \left(\frac{-1}{p}\right)^y = \left(\frac{2}{p}\right)^{(2k+1)y} \left(\frac{-1}{p}\right)^y$$

$$= \begin{cases} (-1)^y(1)^y, & p \equiv 5 \pmod 8 \\ (1)^y(-1)^y, & p \equiv 7 \pmod 8 \end{cases} \equiv (-1)^y \pmod 8.$$

So we have $y = 2n$ for some $n \in \mathbb{N}$. We write Equation (3.4) in the form

$$p^x = (z - (2^{2k+1}q)^n)(z + (2^{2k+1}q)^n).$$

Let $d = \gcd(z - (2^{2k+1}q)^n, z + (2^{2k+1}q)^n)$. Since p and q are distinct odd prime numbers, $d \mid 2(2^{2k+1}q)^n = 2^{(2k+1)n+1}q^n$, and $d \mid p^x$, we have $d = 1$. So we have

$$\begin{cases} z - (2^{2k+1}q)^n = 1 \\ z + (2^{2k+1}q)^n = p^x. \end{cases}$$

Eliminating z, we get

$$2(2^{2k+1}q)^n = p^x - 1. \tag{3.5}$$

If $k = 0$ and $n = 1$, then $4q = 8p - 4 = p^x - 1$ or $p(8 - p^{x-1}) = 3$. This equation has no integer solutions. Therefore, we have either $k \geq 1$ or $n \geq 2$. Taking Equation (3.5) modulo 8, we obtain $p^x \equiv 1 \pmod 8$. So $x = 2m$ for some $m \in \mathbb{N}$ and Equation (3.5) can be written as

$$(p^m - 1)(p^m + 1) = 2^{(2k+1)n+1}q^n.$$

Obviously, $\gcd(p^m-1, p^m+1) = 2$, and we have the following three possibilities since $p^m - 1 < p^m + 1$.

`Case 1.` If $p^m - 1 = 2$ and $p^m + 1 = 2^{(2k+1)n}q^n$, then we have $2 = 2^{(2k+1)n}q^n - 2$, which is not true since $q > 8$.

`Case 2.` If $p^m - 1 = 2q^n$ and $p^m + 1 = 2^{(2k+1)n}$, then $1 = 2^{(2k+1)n-1} - q^n$. If $n = 1$, then $p = 2^{2k-1}$ is not an odd prime number. If $n \geq 2$, by Lemma 1, the equation has no integer solutions.

`Case 3.` If $p^m - 1 = 2^{(2k+1)n}$ and $p^m + 1 = 2q^n$, then $1 = q^n - 2^{(2k+1)n-1}$. If $n \geq 2$, by Lemma 1, this equation has no integer solutions. If $n = 1$, then $q = 2^{2k} + 1$, and $p = 2^{2k-1} + 1$. By Lemma 3, $2k = 2^r$ and $2k - 1 = 2^s$, $r > s \geq 0$. From $2^r - 2^s = 1$, we get $r = 1$ and $s = 0$. Then $p = 3$, which is contrary to $p \equiv 5, 7 \pmod 8$. □

The following theorem can be similarly proved. We include a short proof here for the sake of completeness.

Theorem 3. *If p and $q = 2p - 1$ are prime numbers with $p \equiv 3 \pmod 4$, then for any integer $k \geq 1$, the equation*

$$p^x + (2^{2k}(2p-1))^y = z^2 \tag{3.6}$$

has only two non-negative integer solutions:
(1) $(p, x, y, z) = (3, 1, 0, 2)$*;*
(2) $(p, k, x, y, z) = (3, 2, 0, 1, 9)$.

Proof. If $y = 0$, then Equation (3.6) has a unique non-negative integer solution $(p, x, y, z) = (3, 1, 0, 2)$ by Lemma 2. If $x = 0$, then Equation (3.6) has a unique non-negative integer solution $(p, k, x, y, z) = (3, 2, 0, 1, 9)$ by Lemma 4. Now we assume $x \geq 1$ and $y \geq 1$. Taking Equation (3.6) modulo p, we obtain

$$(2^{2k}(-1))^y \equiv z^2 \pmod p.$$

Hence, $(\frac{-1}{p})^y = (-1)^y = 1$, which implies $y = 2n$ for some $n \geq 1$. Then Equation (3.6) is equivalent to the equation

$$p^x = (z - (2^{2k}q)^n)(z + (2^{2k}q)^n).$$

In this equation, since the two factors of p^x are relatively prime, we have

$$z - (2^{2k}q)^n = 1$$

and

$$z + (2^{2k}q)^n = p^x.$$

From $2(2^{2k}q)^n = p^x - 1$, we obtain $p^x \equiv 1 \pmod 8$. So we have $x = 2m$ for some $m \in \mathbb{N}$ and equation $2(2^{2k}q)^n = p^x - 1$ can be written in the form

$$(p^m - 1)(p^m + 1) = 2^{2kn+1}q^n.$$

Since the greatest common divisor of $p^m - 1$ and $p^m + 1$ is 2, and $p^m - 1 < p^m + 1$, we have the following three possibilities.

(1) If $p^m - 1 = 2$ and $p^m + 1 = 2^{2kn}q^n$, then $2 = 2^{2kn}q^n - 2 > 5$, which is absurd.

(2) If $p^m - 1 = 2q^n$ and $p^m + 1 = 2^{2kn}$, then $1 = 2^{2kn-1} - q^n$. This equation has no integer solutions when $n > 1$ by Lemma 1. When $n = 1$, taking $p^m - 1 = 2q$ modulo p, we get a contradiction $-1 \equiv -2 \pmod p$.

(3) If $p^m - 1 = 2^{2kn}$ and $p^m + 1 = 2q^n$, then $1 = q^n - 2^{2kn-1}$. This equation has no integer solutions when $n > 1$ by Lemma 1. When $n = 1$, taking $p^m + 1 = 2q$ modulo p, we have $p = 3$, $q = 5$, $m = 2$, and $1 = 5^1 - 2^{2k-1}$. The last equation cannot be true. □

4. Solutions of the Equations $(2^k(2p-1))^x - p^y = z^2$ and $p^x - (2^{2k+1}(2p-1))^y = z^2$ with $k \geq 0$

In this section, two equations $(2^k(2p-1))^x - p^y = z^2$ and $p^x - (2^{2k+1}(2p-1))^y = z^2$ with $k \geq 0$ are studied. We consider three cases for the first equation: (a) k is 0; (b) k is odd; and (c) $k \geq 2$ is even.

Theorem 4. *If p and $q = 2p - 1$ are prime numbers and $p \equiv 3 \pmod 4$, then the equation*

$$(2p - 1)^x - p^y = z^2 \tag{4.1}$$

has only the non-negative integer solutions $(x, y, z) = (0, 0, 0)$, $(p, x, y, z) = (3, 2, 2, 4)$ and $(p, x, y, z) = (2t^2 + 1, 1, 0, 2t)$, where for suitable $t \in \mathbb{N}$, both $2t^2 + 1$ and $4t^2 + 1$ are prime numbers with $2t^2 + 1 \equiv 3 \pmod 4$.

Proof. If $x = 0$, then $y = z = 0$, and $(x, y, z) = (0, 0, 0)$ is a solution. We may assume $x \geq 1$. If $y = 0$, then $(2p - 1)^x - z^2 = 1$. By Lemma 1, we obtain $x = 1$. Since $2p-1$ is odd and $(2p-1)-z^2 = 1$, we have $z = 2t$, $p = 2t^2+1$ and $q = 4t^2+1$ for some $t \in \mathbb{N}$. So $(p, x, y, z) = (2t^2 + 1, 1, 0, 2t)$, where both $2t^2 + 1$ and $4t^2 + 1$ are prime numbers with $2t^2 + 1 \equiv 3 \pmod 4$.

Now, we consider the case $x \geq 1$ and $y \geq 1$. From Equation (4.1), we have

$$(-1)^x \equiv z^2 \pmod p.$$

Since $(\frac{-1}{p}) = -1$, we get $(-1)^x = 1$. Therefore $x = 2m$ for some $m \in \mathbb{N}$ and Equation (4.1) can be changed to an equivalent form

$$(q^m - z)(q^m + z) = p^y.$$

Since p and q are odd prime numbers, $q^m - z$ and $q^m + z$ are relatively prime. So we have $q^m - z = 1$, $q^m + z = p^y$, and $2q^m = p^y + 1$. Taking the equation modulo p, we get $2(-1)^m \equiv 1 \pmod{p}$. If m is even, then $2 \equiv 1 \pmod{p}$, which is impossible. So m is odd and $p \mid 3$. Hence $p = 3$, $q = 5$ and Equation (4.1) is reduced to the form $5^x - 3^y = z^2$. Since $x, y \geq 1$, we have $z \geq 1$. Now we only need to find the positive integer solutions of the equation $z^2 + 3^y = 5^x$.

Letting $a = 4$, $b = 3$, and $c = 5$, we have $a^2 + b^2 = c^2$, $\gcd(a, b, c) = 1$, $b = 3 \equiv -5 \pmod{8}$, and a prime number $c = 5$. By Lemma 6, Conjecture 1 (Terai's Conjecture) is true and the equation $z^2 + 3^y = 5^x$ has a unique positive integer solution $(z, y, x) = (4, 2, 2)$, which gives the solution $(p, x, y, z) = (3, 2, 2, 4)$. □

Remark 2. The first four values of t such that $p = 2t^2 + 1$ and $q = 4t^2 + 1$ are prime, and $p \equiv 3 \pmod{4}$, are $t = 1, 3, 27, 45$. The corresponding prime pairs are $(p, q) = (3, 5), (19, 37), (1459, 2917), (4051, 8101)$.

Example 5. By Theorem 4, the equation $5^x - 3^y = z^2$ only has three non-negative integer solutions $(x, y, z) = (0, 0, 0), (1, 0, 2), (2, 2, 4)$. For the pairs in Remark 2, each of the corresponding equations has exactly two non-negative integer solutions listed below:

1. $37^x - 19^y = z^2$: $(x, y, z) = (0, 0, 0), (1, 0, 6)$;
2. $2917^x - 1459^y = z^2$: $(x, y, z) = (0, 0, 0), (1, 0, 54)$;
3. $8101^x - 4051^y = z^2$: $(x, y, z) = (0, 0, 0), (1, 0, 90)$.

Theorem 6. *If p and $q = 2p - 1$ are prime numbers with $p \equiv 3 \pmod{4}$, then for any integer $k \geq 1$, the equation*

$$(2^{2k}(2p-1))^x - p^y = z^2 \tag{4.2}$$

has a unique non-negative integer solution $(x, y, z) = (0, 0, 0)$.

Proof. If $x = 0$, then $y = z = 0$ and $(x, y, z) = (0, 0, 0)$ is a solution. Assuming $x \geq 1$ and taking Equation (4.2) modulo q, we have

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

From $\left(\frac{-p^y}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{p}{q}\right)^y = \left(\frac{q}{p}\right)^y = \left(\frac{-1}{p}\right)^y = (-1)^y = 1$, we have $2 \mid y$. On the other hand, taking Equation (4.2) modulo 4, we get $-(-1)^y \equiv z^2 \pmod{4}$, which implies $2 \nmid y$. Hence, assuming $x \geq 1$, we obtain a contradiction and conclude that $(x, y, z) = (0, 0, 0)$ is the unique solution. □

Theorem 7. *If p and $q = 2p - 1$ are prime numbers with $p \equiv 5 \pmod{8}$, then for any integer $k \geq 0$, the equation*

$$(2^{2k+1}(2p-1))^x - p^y = z^2 \tag{4.3}$$

only has the following non-negative integer solutions:

(1) $(x, y, z) = (0, 0, 0)$*;*

(2) $(p, k, x, y, z) = (\frac{t^2+3}{4}, 0, 1, 0, t)$*, where for suitable* $t \in \mathbb{N}$*, both* $\frac{t^2+3}{4}$ *and* $\frac{t^2+1}{2}$ *are prime and* $\frac{t^2+3}{4} \equiv 5 \pmod 8$*.*

Proof. If $x = 0$, then $y = z = 0$ and $(x, y, z) = (0, 0, 0)$ is a trivial solution. We assume $x \geq 1$. If $y = 0$, then $(2^{2k+1}(2p-1))^x - z^2 = 1$. By Lemma 1, $x \geq 2$ is impossible. So $x = 1$, and $2^{2k+1}q = z^2 + 1$. Taking this equation modulo 8, if $k \geq 1$, then $z^2 + 1 \equiv 0 \pmod 8$, which is impossible. Hence, $k = 0$ and $2q = z^2 + 1$. We know that z is odd and $q = \frac{z^2+1}{2}$ is prime. Let $z = t$ such that both $\frac{t^2+3}{4} (= p)$ and $\frac{t^2+1}{2}$ are prime and $\frac{t^2+3}{4} \equiv 5 \pmod 8$. Then $(p, k, x, y, z) = (\frac{t^2+3}{4}, 0, 1, 0, t)$ is a solution.

The last case is $x \geq 1$ and $y \geq 1$. From Equation (4.3) , we have

$$(2^{2k+1}(-1))^x \equiv z^2 \pmod p.$$

Since $\left(\frac{-1}{p}\right) = 1$ and $\left(\frac{2}{p}\right) = -1$, we obtain $(-1)^x = 1$, which gives $x = 2m$ for some $m \geq 1$. If we rewrite Equation (4.3) in the form

$$((2^{2k+1}q)^m - z)((2^{2k+1}q)^m + z) = p^y,$$

then $(2^{2k+1}q)^m - z = 1$ and $(2^{2k+1}q)^m + z = p^y$. So we have $2(2^{2k+1}q)^m = p^y + 1$. Hence, $p^y + 1 \equiv 0 \pmod 4$. However, $p \equiv 5 \pmod 8$ implies $p^y + 1 \equiv 2 \pmod 4$. We obtain a contradiction. □

Remark 3. The first two values of t such that $\frac{t^2+3}{4}$ and $\frac{t^2+1}{2}$ are prime, and $\frac{t^2+3}{4} \equiv 5 \pmod 8$, are $t = 25$ and $t = 199$. The corresponding prime numbers p and q are $(p, q) = (157, 313)$ and $(p, q) = (9901, 19801)$, respectively.

Example 8. For the two pairs (p, q) in Remark 3, each of the corresponding equations has exactly two non-negative integer solutions as follows:

1. $626^x - 157^y = z^2$: $(x, y, z) = (0, 0, 0), (1, 0, 25)$;
2. $39602^x - 9901^y = z^2$: $(x, y, z) = (0, 0, 0), (1, 0, 199)$.

Theorem 9. *If* p *and* $q = 2p - 1$ *are prime numbers with* $p \equiv 3 \pmod 8$*, then for any integer* $k \geq 0$*, the equation*

$$p^x - (2^{2k+1}(2p-1))^y = z^2 \tag{4.4}$$

has a unique non-negative integer solution $(x, y, z) = (0, 0, 0)$*.*

Proof. Obviously, $(x, y, z) = (0, 0, 0)$ is a solution. So we may assume $x \geq 1$. Taking Equation (4.4) modulo p, we have

$$-(2^{2k+1}(-1))^y \equiv z^2 \pmod p.$$

Then we have a contradiction:

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

□

5. Solutions of the Equation $(-1)^\alpha 2^x + (-1)^\beta (2^k 3)^y = z^2$

In this section, for $\alpha, \beta, k = 0, 1$ and $\alpha\beta = 0$, we solve six Diophantine equations of the form $(-1)^\alpha 2^x + (-1)^\beta (2^k 3)^y = z^2$. We first prove the following lemma using Tomita's method [17].

Lemma 8 ([17])**.** *The Diophantine equation $3^x = y^2 + 2$ has only two non-negative integer solutions: $(x, y) = (1, 1)$ and $(x, y) = (3, 5)$.*

Proof. Let $x = 3k + a$, $k \in \mathbb{Z}$ and $a = 0, 1, 2$.

If $x = 3k$, letting $X = 3^k$ and $Y = y$, then

$$Y^2 = X^3 - 2.$$

By Lemma 7, we obtain $(X, Y) = (3, \pm 5)$. Hence, $(x, y) = (3, 5)$ is a non-negative integer solution.

If $x = 3k + 1$, letting $X = 3^{k+1}$ and $Y = 3y$, then

$$Y^2 = X^3 - 18.$$

By Lemma 7, $(X, Y) = (3, \pm 3)$. So $(x, y) = (1, 1)$ is another non-negative integer solution.

If $x = 3k + 2$, letting $X = 3^{k+2}$ and $Y = 9y$, then

$$Y^2 = X^3 - 162.$$

By Lemma 7, there are no integer points on this elliptic curve. □

We need the following lemma proved by Leu and Li [7].

Lemma 9 ([7])**.** *The Diophantine equation $2x^2 + 1 = 3^y$ has only four non-negative integer solutions: $(x, y) = (0, 0), (1, 1), (2, 2), (11, 5)$.*

Remark 4. Lemma 9 can be obtained from Lemma 5 if we write $2x^2 + 1 = 3^y$ in the form $\frac{3^y - 1}{3 - 1} = x^2$. Using the substitution method in Lemma 8, together with the LMFDB, we can give a direct proof. In fact, generally, for any given (fixed) integers c, A, B, and C, one can use the database of the elliptic curves $Y^2 = X^3 + aX + b$ over $\mathbb{Q}$ in the LMFDB to solve the equation $Ac^x = By^2 + C$ by considering three cases $x = 3k, 3k + 1$, and $3k + 2$ for some non-negative integer k.

Theorem 10. *Six equations of the form*

$$(-1)^{\alpha}2^x + (-1)^{\beta}(2^k3)^y = z^2$$

for $\alpha, \beta, k = 0, 1$ *and* $\alpha\beta = 0$ *only has the following non-negative integer solutions:*
(*i*) $2^x + 3^y = z^2$: $(x, y, z) = (0, 1, 2), (3, 0, 3), (4, 2, 5)$.
(*ii*) $2^x - 3^y = z^2$: $(x, y, z) = (0, 0, 0), (1, 0, 1), (2, 1, 1)$.
(*iii*) $-2^x + 3^y = z^2$: $(x, y, z) = (0, 0, 0), (1, 1, 1), (1, 3, 5), (3, 2, 1), (5, 4, 7)$.
(*iv*) $2^x + 6^y = z^2$: $(x, y, z) = (3, 0, 3), (6, 2, 10)$.
(*v*) $2^x - 6^y = z^2$: $(x, y, z) = (0, 0, 0), (1, 0, 1)$.
(*vi*) $-2^x + 6^y = z^2$: $(x, y, z) = (0, 0, 0), (1, 1, 2), (5, 2, 2), (9, 4, 28), (5, 5, 88)$.

Proof. (*i*) The equation $2^x + 3^y = z^2$ was solved by Banyat Sroysang in 2013 [15].

(*ii*) For $2^x - 3^y = z^2$, letting $x = 0, 1, 2$, we get three solutions:

$$(x, y, z) = (0, 0, 0), (1, 0, 1), (2, 1, 1).$$

If $x \geq 3$, then $-3^y \equiv z^2 \pmod 8$, which is absurd.

(*iii*) For $-2^x + 3^y = z^2$, if $x = y = 0$, then $(x, y, z) = (0, 0, 0)$. If $x = 0$ and $y \geq 1$, then we have an equation

$$3^y = z^2 + 1,$$

which has no integer solutions since $z^2 \equiv -1 \pmod 3$ is not true. If $x = 1$, then $3^y = z^2 + 2$. By Lemma 8, $(y, z) = (1, 1), (3, 5)$. Hence, we obtain the solutions

$$(x, y, z) = (1, 1, 1), (1, 3, 5).$$

If $x \geq 2$, then

$$3^y \equiv z^2 \pmod 4.$$

Hence, $y = 2m$ for some $m \in \{0\} \cup \mathbb{N}$. Since $x \geq 2$, we have $m \geq 1$ and an equation

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

which implies that $3^m - z = 2$ and $3^m + z = 2^{x-1}$. Eliminating z, we have

$$3^m - 2^{x-2} = 1.$$

By Lemma 1, we obtain $(m, x) = (1, 3), (2, 5)$. So we get the solutions

$$(x, y, z) = (3, 2, 1), (5, 4, 7).$$

(*iv*) For the equation $2^x + 6^y = z^2$, if $y = 0$, then $(x, y, z) = (3, 0, 3)$ by Lemma 2. If $y \geq 1$, then

$$2^x \equiv z^2 \pmod 3,$$

which gives $x = 2m$ for some non-negative integer m. If $m = 0$, then $z^2 - 6^y = 1$ has no integer solutions by Lemma 1. We may assume $m \geq 1$ from now on.

The equation $2^x + 6^y = z^2$ can be written as

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

Let $d = \gcd(z - 2^m, z + 2^m)$, then $d \mid 2^{m+1}$ and $d^2 \mid 2^y 3^y$. Hence, $d = 2^k$, $1 \leq k \leq \min\{m+1, \lfloor \frac{y}{2} \rfloor\}$. There are two cases: either $z - 2^m = 2^k$ and $z + 2^m = 2^{y-k} 3^y$, or $z - 2^m = 2^{y-k}$ and $z + 2^m = 2^k 3^y$.

`Case 1.` If $z - 2^m = 2^k$ and $z + 2^m = 2^{y-k} 3^y$, then

$$2^{m+1} = 2^{y-k} 3^y - 2^k.$$

Since 2^k divides 2^{m+1}, 2^k divides 2^{y-k}. So $y \geq 2k$ and $2^{m+1-k} = 2^{y-2k} 3^y - 1$. This equation holds only if $m + 1 - k \geq 1$ and $2^{y-2k} 3^y - 1$ is even. So $y = 2k$. Now we have $2^{m+1-k} = 3^y - 1$, or $3^y - 2^{m+1-k} = 1$. By Lemma 1, $y = 2$ and $m + 1 - k = 3$. Hence, $(x, y, z) = (6, 2, 10)$ is a solution.

`Case 2.` If $z - 2^m = 2^{y-k}$ and $z + 2^m = 2^k 3^y$, then

$$2^{m+1} = 2^k 3^y - 2^{y-k},$$

or

$$2^{m+1-k} = 3^y - 2^{y-2k}.$$

The equation holds only if $m + 1 - k \geq 1$ by Lemma 1, and $y = 2k$ since 2^{m+1-k} is even. Therefore $2^{m+1-k} = 3^y - 1$, or $3^y - 2^{m+1-k} = 1$. By Lemma 1, $y = 2$, $m + 1 - k = 3$. Hence, $k = 1$, $m = 3$ and $(x, y, z) = (6, 2, 10)$.

(v) If $2^x - 6^y = z^2$ and $y = 0$, then

$$2^x - z^2 = 1.$$

By Lemma 1, we obtain $(x, y, z) = (0, 0, 0), (1, 0, 1)$. If $y \geq 1$, then

$$2^x \equiv z^2 \pmod{3}.$$

So we have $x = 2m$ for some integer $m \geq 1$ and the equation $2^x - 6^y = z^2$ can be written as

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

Let $d = \gcd(2^m - z, 2^m + z)$, then $d \mid 2^{m+1}$ and $d^2 \mid 2^y 3^y$. Hence, $d = 2^k$, $1 \leq k \leq \min\{m+1, \lfloor \frac{y}{2} \rfloor\}$. There are two cases.

`Case 1.` If $2^m - z = 2^k$ and $2^m + z = 2^{y-k} 3^y$, then we have

$$2^{m+1} = 2^{y-k} 3^y + 2^k,$$

or

$$2^{m+1-k} = 2^{y-2k}3^y + 1.$$

Obviously $m + 1 - k \geq 1$ and 2^{m+1-k} is even. Hence, $2^{y-2k}3^y + 1$ is also even and $y = 2k$. Now we have $2^{m+1-k} = 3^y + 1$, or $2^{m+1-k} - 3^y = 1$, which has no integer solutions by Lemma 1 since $y = 2k \geq 2$.

Case 2. If $2^m - z = 2^{y-k}$ and $2^m + z = 2^k 3^y$, then

$$2^{m+1} = 2^k 3^y + 2^{y-k},$$

or

$$2^{m+1-k} = 3^y + 2^{y-2k}.$$

Obviously $m + 1 - k \geq 1$ and $y = 2k$. So we have

$$2^{m+1-k} = 3^y + 1$$

or

$$2^{m+1-k} - 3^y = 1,$$

which has no integer solutions by Lemma 1.

(vi) If $-2^x + 6^y = z^2$ and $y = 0$, then $(x, y, z) = (0, 0, 0)$. If $y \geq 1$, then taking the equation modulo 3, we have

$$(-1)^{x+1} \equiv z^2 \pmod{3},$$

and this equation holds only if $2 \nmid x$. There are two cases: $2 \mid y$ and $2 \nmid y$.

Case 1. If $2 \nmid x$ and $2 \mid y$, (assuming $x, y \geq 1$), letting $y = 2m$, $m \geq 1$, we have

$$(6^m - z)(6^m + z) = 2^x,$$

which implies $6^m - z = 2^k$ and $6^m + z = 2^{x-k}$ with $1 \leq k < x - k$. So we have

$$2^{m+1-k}3^m = 2^{x-2k} + 1.$$

If $m + 1 - k = 0$, then $3^m - 2^{x-2k} = 1$. By Lemma 1, we obtain

$$(m, x - 2k) = (1, 1), (2, 3).$$

Hence, $(x, y, z) = (5, 2, 2), (9, 4, 28)$ are two solutions in this case. If $m + 1 - k \geq 1$, then $2^{m+1-k}3^m$ is even, so $x = 2k$, which is contrary to our assumption.

Case 2. Now we consider the case $2 \nmid x$ and $2 \nmid y$, where $x, y \geq 1$. Let $z = 2^r z_1$, where $z_1 \in \mathbb{N}$ and $2 \nmid z_1$. If $x > y$, then

$$2^y(3^y - 2^{x-y}) = 2^{2r}z_1^2.$$

Since both $3^y - 2^{x-y}$ and z_1^2 are odd, we have $2|y$, which is contrary to our assumption. If $x < y$, then

$$2^x(2^{y-x}3^y - 1) = 2^{2r}z_1^2.$$

Hence $2|x$, contradicting our assumption. If $x = y$, then $2^x(3^x - 1) = 2^{2r}z_1^2$, or $3^x - 1 = 2^{2r-x}z_1^2$. If $2r - x \geq 2$, we obtain $3^x - 1 \equiv 0 \pmod 4$, which is contrary to our assumption. Since x is odd, $2r - x \neq 0$. So the only possibility is $2r - x = 1$ and

$$3^x = 2z_1^2 + 1.$$

By Lemma 9, we have $(z_1, x) = (0,0), (1,1), (2,2), (11,5)$. Since x is odd, we have $(z_1, x) = (1,1), (11,5)$. Hence, we obtain the solutions $(x, y, z) = (1,1,2), (5,5,88)$ in this case. □

6. Solution of the Diophantine Equation $2 + 7^y = z^2$

In [1], Borah and Dutta asked if $(y, z) = (1,3)$ is the only non-negative integer solution of the Diophantine equation $2 + 7^y = z^2$. Using the method of Tomita, we give an affirmative answer to their question.

Theorem 11. *The Diophantine equation $2 + 7^y = z^2$ has a unique non-negative integer solution $(y, z) = (1,3)$.*

Proof. We write $y = 3k + a$, where $k \in \mathbb{Z}$ and $a = 0,1,2$.

`Case 1.` If $y = 3k$, $k \geq 0$, letting $X = 7^k$ and $Y = z$, the original equation can be written as an elliptic curve $Y^2 = X^3 + 2$ with the discriminant -1728. Using the LMFDB, its integer points are $(X, Y) = (-1, \pm 1)$. So the equation has no non-negative integer solutions in this case.

`Case 2.` If $y = 3k + 1$, $k \geq 0$, letting $X = 7^{k+1}$ and $Y = 7z$, the original equation can be written as $Y^2 = X^3 + 98$. The discriminant of this elliptic curve is -4148928. Using the LMFDB, there are only two integer points $(X, Y) = (7, \pm 21)$. Hence, $(y, z) = (1,3)$ is the solution in this case.

`Case 3.` If $y = 3k + 2$, $k \geq 0$, letting $X = 7^{k+2}$ and $Y = 49z$, we have $Y^2 = X^3 + 4802$. Its discriminant is -9961576128. Using the LMFDB, it has no integer points. Hence, the equation has no non-negative integer solutions in this case. □

Acknowledgment. The authors thank the referees and editor for the valuable comments.

References

[1] P. B. Borah and M. Dutta, On the Diophantine equation $7^x + 32^y = z^2$ and its generalization, *Integers* **22** (2022), #A29.

[2] Y. Bugeaud, M. Mignotte, and Y. Roy, On the Diophantine equation $\frac{x^n-1}{x-1} = y^q$, *Pacific J. Math.* **193** (2000), 257-268.

[3] Y. Bugeaud and P. Mihăilescu, On the Nagell-Ljunggren equation $\frac{x^n-1}{x-1} = y^q$, *Math. Scand.* **101** (2007), 177-183.

[4] W. S. Gayo and J. B. Bacani, On the Diophantine equation $(M_p)^x + (M_q + 1)^y = z^2$, *Eur. J. Pure Appl. Math.* **14**, no. 2, (2021), 396-403.

[5] C. Ko, On the Diophantine equation $x^2 = y^n + 1$, $xy \neq 0$, *Sci. Sin.* **14** (1965), 457-460.

[6] M. H. Le, A note on the Diophantine equation $x^2 + b^y = c^z$, *Acta Arith.* **71** (1995), 253-257.

[7] M. G. Leu and G. W. Li, On the Diophantine equation $2x^2 + 1 = 3^n$, *Proc. Amer. Math. Soc.* **131** (2003), 3643-3645.

[8] Y. Li and M. H. Le, On the Diophantine equation $\frac{x^m-1}{x-1} = y^n$, *Acta Arith.* **73**, no. 4, (1995), 363-366.

[9] Y. Li, J. Zhang, and B. Liu, On equations $(-1)^\alpha p^x + (-1)^\beta (2^k(2p+1))^y = z^2$ with Sophie Germain prime p, *Involve*, to appear.

[10] W. Ljunggren, Noen Setninger om ubestemte likninger av formen $\frac{x^n-1}{x-1} = y^q$, *Norsk Mat. Tidsskr.* **25** (1943), 17-20.

[11] The L-functions and Modular Forms database, https://www.lmfdb.org/ EllipticCurve/Q/.

[12] P. Mihăilescu, Primary cycolotomic units and a proof of Catalan's conjecture, *J. Reine Angew Math.* **572** (2004), 167-195.

[13] R. J. S. Mina and J. B. Bacani, On the solutions of the Diophantine equation $p^x + (p+4k)^y = z^2$ for prime pairs p and $p + 4k$, *Eur. J. Pure Appl. Math.* **14**, no. 2, (2021), 471-479.

[14] B. Sroysang, On the Diophantine equation $3^x + 5^y = z^2$, *Int. J. Pure Appl. Math.* **81**, no. 4, (2012), 605-608.

[15] B. Sroysang, More on the Diophantine equation $2^x + 3^y = z^2$, *Int. J. Pure Appl. Math.* **84**, no. 2, (2013), 133-137.

[16] N. Terai, The Diophantine equation $x^2 + q^m = p^n$, *Acta Arith.* **63** (1993), 351-358.

[17] S. Tomita, $5^x - y^2 = 4$ Diophantine Equation, https://math.stackexchange.com/questions/4184457/$5^x - y^2 = 4$-diophantine-equation.

[18] P. Z. Yuan, A note on the Diophantine equation $\frac{x^m-1}{x-1} = y^n$ (Chinese), *Acta Math. Sin. (Chinese Ser.)* **39**, no. 2, (1996), 184-189.

[19] P. Z. Yuan and J. B. Wang, On the Diophantine equation $x^2 + b^y = c^z$, *Acta Arith.* **84**, no. 2, (1998), 145-147.