On nonsolvability of exponential Diophantine equations via transformation to elliptic curves

Renz Jimwel S. Mina
Department of Mathematics and Computer Science
College of Science
University of the Philippines Baguio
Baguio City 2600, Benguet
Philippines
rsmina1@up.edu.ph

Jerico B. Bacani*
Department of Mathematics and Computer Science
College of Science
University of the Philippines Baguio
Baguio City 2600, Benguet
Philippines
jbbacani@up.edu.ph

Abstract. Exponential Diophantine equations of the form $p^X + q^Y = Z^2$, with unknowns (X, Y, Z) in the set of positive integers, are of interest to many number theorists. Many of these equations are solved using congruence techniques and the quadratic reciprocity. The goal of this paper is to show unsolvability of some Diophantine equations of this type using the concept of elliptic curves. Similar types of exponential Diophantine equations are also considered in this study. To illustrate the results, examples are provided.
Keywords: exponential Diophantine equation, elliptic curve, congruences, factorization.

1. Introduction

Solving Diophantine equations is one of the oldest problems in Number Theory but is one of the hot topics of research in this field of mathematics in the past few years. Recently, several papers have been devoted in finding the non-negative integer solutions of Diophantine equations of the form

$$p^X + q^Y = Z^2 \tag{1}$$

with unknowns (X, Y, Z). Such equations are called exponential Diophantine equations as they require solutions in the exponents. In 2007, Acu [1] found the complete set of solutions of the Diophantine equation $2^X + 5^Y = Z^2$. In 2012 and 2013, Sroysang ([8],[9]) worked on the equations $3^X + 5^Y = Z^2$ and $8^X +$

∗. Corresponding author

$19^Y = Z^2$. On the other hand, Rabago [4] looked into Diophantine equations $3^X+19^Y = Z^2$ and $3^X+91^Y = Z^2$. Many other similar problems were considered in the references [11], [10], [5], [6], [7], [15] and [2].

Most of the tools used in the said studies were the congruence and factorization techniques. In 2019, Mina and Bacani [3] were able to provide some criteria for showing non-existence of solutions over the set of positive integers for such equations by using the values of the Legendre and Jacobi symbols.

In this paper, we will present several ways on determining whether equation (1) has no solutions in the set of positive integers. These are done by transforming such equations to another family of equations whose rational points form an abelian group structure. These equations are no other than equations that describe elliptic curves. The use of elliptic curves in solving Diophantine equations is not new and has already been done in the past. A classical example would be the Fermat equation

$$a^4 + b^4 = c^4, \; a \neq 0. \tag{2}$$

Using the transformation

$$x = 2\frac{b^2+c^2}{a^2} \quad \text{and} \quad y = 4\frac{b(b^2+c^2)}{a^3},$$

we get a corresponding elliptic curve

$$y^2 = x^3 - 4x$$

which has only the following rational solutions: $(x, y) = (0, 0), (2, 0), (-2, 0)$. These all correspond to $b = 0$, so there are no nontrivial solutions to (2).

We will also be dealing with equations of the form

$$p^X + q^Y = Z^n \tag{3}$$

where $n = 3$ or 6. This type of equation is generally not possible to study when using only congruence techniques. Most of the cases we will be dealing with require one of the exponents to be even. There are some theorems that guarantee non-existence of solutions to (1), such as those presented in [3] which deal with the case where one of the exponents is odd. Note that since computation of ranks of elliptic curves is generally a hard problem, most of the results will focus on the case where the bases p and q are fixed. We use a free mathematical software *SAGE* [13] for the computation of ranks and torsion subgroups of elliptic curves.

Throughout the paper, we will denote by $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Z}$ and $\mathbb{Q}$ the sets of positive integers, non-negative integers, integers and rational numbers, respectively.

2. Basic concepts about elliptic curves

An elliptic curve defined over $\mathbb{Q}$ is a curve that is described by the following general Weierstrass equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}$. By completing the square, we get

$$\left(y + \frac{a_1 x}{2} + \frac{a_2}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right) x^2 + \left(a_4 + \frac{a_1 a_3}{2}\right) x + \left(\frac{a_3^2}{4} + a_6\right),$$

which can be written as

$$y_1^2 = x^3 + a_2' x^2 + a_4' x + a_6',$$

where $y_1 = y + a_1 x/2 + a_3/2$ and $a_2' = a_2 + a_1^2/4$. Furthermore, if we let $x_1 = x + a_2'/3$, then we get the simpler Weierstrass equation

$$y_1^2 = x_1^3 + Ax_1 + B, \quad \text{for some } A, B \in \mathbb{Q}.$$

In other words, an elliptic curve defined over the rationals is given by the following equation:

$$E : y^2 = x^3 + Ax + B,$$

where A and B are rational numbers. In addition, the discriminant $\Delta := 4A^3 + 27B^2$ must be nonzero. It is well-known that the rational points on the elliptic curve E over $\mathbb{Q}$ forms an abelian group called the Mordell-Weil group with the point at infinity $\mathcal{O}$ acting as the identity. The group is isomorphic to $E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$, where $E(\mathbb{Q})_{\text{tors}}$ is the group of elements of finite order, called the torsion subgroup, and $r \geq 0$ is called the rank of E. There are ways of solving the torsion subgroup, such as using the well-known Nagell-Lutz Theorem, but the computation of rank r is generally a hard problem.

One of the results in the theory of elliptic curves is the transformation of a quartic equation to the Weierstrass equation of elliptic curve, and vice-versa. The proof of this theorem can be seen in [12].

Theorem 2.1. *Consider the following equation*

$$v^2 = au^4 + bu^3 + cu^2 + du + q^2,$$

with coefficients $a, b, c, d, q \in \mathbb{Q}$. *Let*

$$x = \frac{2q(v+q) + du}{u^2}, \qquad y = \frac{4q^2(v+q) + 2q(du + cu^2) - (d^2u^2/2q)}{u^3}.$$

Define $a_1 = d/q,\ a_2 = c - (d^2/4q^2),\ a_3 = 2qb,\ a_4 = -4q^2 a,\ a_6 = a_2 a_4$. *Then,*

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

The inverse transformation is given by

$$u = \frac{2q(x+c) - (d^2/2q)}{y}, \quad v = -q + \frac{u(ux - d)}{2q}.$$

The point $(u, v) = (0, q)$ *corresponds to the point* $(x, y) = \mathcal{O}$, *and* $(u, v) = (0, -q)$ *corresponds to* $(x, y) = (-a_2, a_1 a_2 - a_3)$.

The next theorem is a well-known result regarding the torsion subgroup of the elliptic curve $y^2 = x^3 + B$.

Theorem 2.2. *Let $E : y^2 = x^3 + B$ be an elliptic curve for some sixth power-free integer B. Then, the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ of $E(\mathbb{Q})$ is isomorphic to one of the following groups:*

1. *$\mathbb{Z}/6\mathbb{Z}$ if $B = 1$,*
2. *$\mathbb{Z}/3\mathbb{Z}$ if $B \neq 1$ is a square or $B = -432$,*
3. *$\mathbb{Z}/2\mathbb{Z}$ if $B \neq 1$ is a cube,*
4. *$\{\mathcal{O}\}$, otherwise.*

3. Main results

For the first two theorems, we present some results about the transformation of the exponential Diophantine equation (1) into the Weierstrass equation of elliptic curve.

Theorem 3.1. *Let p be prime and q be an odd number such that $\gcd(p, q) = 1$. Then, the exponential Diophantine equation (1) has no solutions (X, Y, Z) in $\mathbb{N}$ if $X \equiv 0 \pmod 3$ and $Y \equiv 0 \pmod 4$.*

Proof. Suppose (X, Y, Z) is a solution of (1) such that $X \equiv 0 \pmod 3$ and $Y \equiv 0 \pmod 4$. This implies that $X = 3X_1$ and $Y = 4Y_1$, for some X_1, $Y_1 \in \mathbb{N}$. By factoring $p^X + q^Y = Z^2$, we get

$$(p^{X_1})^3 = (Z + (q^{Y_1})^2)(Z - (q^{Y_1})^2).$$

Since p is prime, there exist two non-negative integers α and β, $\alpha < \beta$ such that $\alpha + \beta = 3X_1$ and

$$p^\alpha(p^{\beta-\alpha} - 1) = p^\beta - p^\alpha = (Z + (q^{Y_1})^2) - (Z - (q^{Y_1})^2) = 2(q^{Y_1})^2.$$

Since $\gcd(p, q) = 1$, we find that $\alpha = 0$ and we get the equation

$$(p^{X_1})^3 - 1 = 2(q^{Y_1})^2.$$

Multiplying both sides by 8 yields $(4q^{Y_1})^2 = (2p^{X_1})^3 - 8$. By substituting $x = 2p^{X_1}$ and $y = 4q^{y_1}$, we obtain the elliptic curve $E_1 : y^2 = x^3 - 8$. Using *SAGE*, we find that its rank is $r = 0$ and its torsion subgroup $E_1(\mathbb{Q})_{\text{tors}}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. We see that the rational points on $E_1(\mathbb{Q})$ are $(2, 0)$ and the point at infinity $\mathcal{O}$, all of which are of finite order. This yields $(p^{X_1}, q) = (1, 0)$, which is a contradiction to the assumption that q is positive. Therefore, (1) has no solutions in $\mathbb{N}$. $\square$

Theorem 3.2. *Let p be prime and q be an odd number such that* $\gcd(p, q) = 1$. *Then, the Diophantine equation* (1) *can be transformed to the elliptic curve* $E_2 : y^2 = x^3 - 8q^3$ *if* $X \equiv 0 \pmod 3$ *and* $Y \equiv 2 \pmod 4$. *Moreover, if the rank of* E_2 *is zero, then* (1) *has no solutions in* $\mathbb{N}$.

Proof. Let (X, Y, Z) be a solution such that $X = 3X_1$ and $Y = 4Y_1 + 2$, for some $X_1 \in \mathbb{N}$ and $Y_1 \in \mathbb{N}_0$. By factoring $p^X + q^Y = Z^2$, we have

$$(p^{X_1})^3 = (Z + q^{2Y_1+1})(Z - q^{2Y_1+1}).$$

Since p is prime, there exist two non-negative integers α and β, $\alpha < \beta$ such that $\alpha + \beta = 3X_1$, and

$$p^\alpha(p^{\beta-\alpha} - 1) = p^\beta - p^\alpha = (Z + q^{2Y_1+1}) - (Z - q^{2Y_1+1}) = 2q^{2Y_1+1}.$$

Since $\gcd(p, q) = 1$, we find that $\alpha = 0$ and we get the equation

$$(p^{X_1})^3 - 1 = 2q^{2Y_1+1}, \text{ or } (p^{X_1})^3 - 1 = 2q \cdot (q_1^Y)^2.$$

Multiplying both sides by $8q^3$ yields $(4q^{Y_1+2})^2 = (2q{\cdot}p^{X_1})^3 - 8q^3$. By substituting $x = 2q{\cdot}p^{X_1}$ and $y = 4q^{Y_1+2}$, we obtain the elliptic curve $E_2 : y^2 = x^3 - 8q^3$. Using Theorem 2.2, we find that $E_2(\mathbb{Q})_{\text{tors}}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. The torsion points on $E_2(\mathbb{Q})$ are $(2q, 0)$ and the point at infinity $\mathcal{O}$. This yields $(p^{X_1}, q) = (1, 0)$ which gives no solutions to the original equation since q is assumed to be positive. Moreover, since the rank of E_2 is assumed to be zero, this means that there are no other rational points on E_2, and consequently on (1). Hence, (1) has no solutions in $\mathbb{N}$. $\square$

Remark 3.1. In Theorems 3.1 and 3.2, the elliptic curves $y^2 = x^3 - 8$ and $y^2 = x^3 - 8q^3$ are also called Mordell curves [14]. The determination of values of q for which the second curve has rank zero is a difficult problem.

Let us now apply these two theorems to a specific exponential Diophantine equation of the form (1).

Example 3.1. The Diophantine equation $19^X + 27^Y = Z^2$ has no solutions (X, Y, Z) in $\mathbb{N}$.

Proof. Taking the equation in modulo 4 gives us $3^X + 3^Y \equiv Z^2 \pmod 4$. Since Z^2 is even, $Z^2 \equiv 0 \pmod 4$. Thus, $3^X + 3^Y \equiv 0 \pmod 4$. This implies that X and Y are of different parity. For the sake of our purpose, we will only deal with the case where X is odd and Y is even. The other cases yield no solution via congruence considerations. By letting $Y = 2Y_1$, for some $Y_1 \in \mathbb{N}$ and factoring, we get

$$19^X = (Z + 27^{Y_1})(Z - 27^{Y_1}).$$

Using the same reasoning as done in the proof of Theorem 3.1, we get the equation

$$19^X - 1 = 2 \cdot 27^{Y_1}.$$

Factoring this equation, we get $(19-1)(19^{X-1}+19^{X-2}+\cdots+1) = 18\cdot 3\cdot 27^{Y_1-1}$. This implies that $19^{X-1}+19^{X-2}+\cdots+1 = 3\cdot 27^{Y_1-1}$. Taking modulo 3 yields $X \equiv 0 \pmod 3$, i.e. $X = 3X_1$, for some $X_1 \in \mathbb{N}$.

Now, if Y_1 is odd, then our equation becomes $(19^{X_1})^3 + (27^{2Y_2+1})^2 = Z^2$, where $Y_1 = 2Y_2+1$. Now, we can transform the equation into the elliptic curve $y^2 = x^3 - 157464$. This has rank zero with torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Using Theorem 3.2, the equation has no solutions in $\mathbb{N}$.

For the second part of the proof, if Y_1 is even, i.e., $Y_1 = 2Y_2$, for some $Y_2 \in \mathbb{N}$, then the original equation becomes $(19^{X_1})^3 + (27^{Y_1})^4 = Z^2$. This resulting equation has no solutions in $\mathbb{N}$ using Theorem 3.1. $\square$

For the next results, we will consider another family of exponential Diophantine equations of the form (3).

Theorem 3.3. *Let p be prime and q be an odd number such that* $\gcd(p,q) = 1$. *Then, the Diophantine equation $p^X+q^Y = Z^6$ can be transformed into the elliptic curve $E_3 : y^2 = x^3 - 4p^3$ if $X \equiv 1 \pmod 2$ and $Y \equiv 0 \pmod 2$. Moreover, if the rank of E_3 is zero, then $p^X + q^Y = Z^6$ has no solutions in* $\mathbb{N}$.

Proof. Let $X = 2X_1+1$ and $Y = 2Y_1$, for some $X_1 \in \mathbb{N}_0$, $Y_1 \in \mathbb{N}$. By factoring, we have the following,

$$p^{2X_1+1} = (Z^3 + (q^{Y_1})^2)(Z^3 - (q^{Y_1})^2).$$

Since p is prime, there exist two non-negative integers α and β, $\alpha < \beta$ such that $\alpha + \beta = 2X_1 + 1$ and

$$p^{\alpha}(p^{\beta-\alpha} + 1) = p^{\beta} + p^{\alpha} = (Z^3 + (q^{Y_1})^2) + (Z^3 - (q^{Y_1})^2) = 2Z^3.$$

Note that $p \nmid Z$, otherwise $p \mid q$ which is not possible since $\gcd(p,q) = 1$. Hence, $\alpha = 0$ and we get the equation

$$p \cdot (p^{X_1})^2 - 1 = 2Z^3.$$

Multiplying both sides by $4p^3$ yields $(2p^{X_1+2})^2 = (2pZ)^3 - 4p^3$. By substituting $x = 2pZ$ and $y = 2p^{X_1+2}$, we obtain the elliptic curve $E_3 : y^2 = x^3 - 4p^3$. Using Theorem 2.2 the torsion subgroup $E_3(\mathbb{Q})_{\text{tors}}$ is isomorphic to $\{\mathcal{O}\}$. This implies that if the rank of E_3 is zero, then there are no solutions in $\mathbb{N}$ to the original equation. $\square$

Next, we are going to consider a larger family of equations of the form $p^X + q^Y = Z^3$, but this time both p and q are primes. In this case, we have the following two results.

Theorem 3.4. *Let p and q be distinct odd primes. Then, the Diophantine equation $p^X + q^Y = Z^3$ has no solutions (X,Y,Z) in $\mathbb{N}$ with $X \equiv 0 \pmod 2$ and $Y \equiv 0 \pmod 6$.*

Proof. Let $X = 2X_1$ and $Y = 6Y_1$, for some $X_1, Y_1 \in \mathbb{N}$. By factoring, we have the following:

$$p^{2X_1} = (Z - q^{2Y_1})(Z^2 + Zq^{2Y_1} + q^{4Y_1}).$$

Since p is prime, there exist two non-negative integers α and β, $\alpha < \beta$ such that $\alpha + \beta = 2X_1$ and

$$p^{\beta-\alpha} = \frac{p^\beta}{p^\alpha} = \frac{Z^2 + Zq^{2Y_1} + q^{4Y_1}}{Z - q^{2Y_1}} = Z^2 + 2q^{2Y_1} + \frac{3q^{4Y_1}}{Z - q^{2Y_1}}.$$

This means that $Z - q^{2Y_1}$ divides $3q^{4Y_1}$. Since q is prime, $Z - q^{2Y_1} = 3q^j$ or $Z - q^{2Y_1} = q^j$, for some $0 \le j \le 4Y_1$. If $j > 0$, then $q \mid Z$ which is a contradiction. Hence $j = 0$ and we have either $Z - q^{2Y_1} = 3$ or $Z - q^{2Y_1} = 1$. For the first case, we have

$$p^X + q^{6Y_1} = (q^{2Y_1} + 3)^3 = q^{6Y_1} + 9q^{4Y_1} + 27q^{2Y_1} + 27,$$

which implies that $p^X = 9q^{4Y_1} + 27q^{2Y_1} + 27$. This means that $9 \mid p^X$ or $p = 3$. This gives us $3^{X-2} = q^{4Y_1} + 3q^{2Y_1} + 3$. Since $\gcd(p, q) = \gcd(3, q) = 1$, we have $X = 2$ and consequently, $1 = q^{4Y_1} + 3q^{2Y_1} + 3$, a contradiction.

For the second case, we have

$$p^X + q^{6Y_1} = (q^{2Y_1} + 1)^3 = q^{6Y_1} + 3q^{4Y_1} + 3q^{2Y_1} + 1.$$

This implies that $p^{2X_1} = 3q^{4Y_1} + 3q^{2Y_1} + 1$. Let $u = q^{Y_1}$ and $v = p^{X_1}$ so that $v^2 = 3u^4 + 3u^2 + 1$. Using Theorem 2.1, if we let $\widehat{x} = \frac{2v+2}{u^2}$ and $\widehat{y} = \frac{4v+4+6u^2}{u^3}$ and define $a_1 = 0$, $a_2 = 3$, $a_3 = 0$, $a_4 = -12$ and $a_6 = -36$, then we get the elliptic curve

$$\widehat{y}^2 = \widehat{x}^3 + 3\widehat{x}^2 - 12\widehat{x} - 36.$$

By letting $x = \widehat{x} + 1$ and $y = \widehat{y}$, we obtain the elliptic curve

$$E_4 : y^2 = x^3 - 15x - 22.$$

We have computed its rank to be $r = 0$ and the torsion subgroup $E_4(\mathbb{Q})_{\text{tors}}$ of E_4 to be $\{\mathcal{O}, (-2, 0)\} \cong \mathbb{Z}/2\mathbb{Z}$. This means that $(x, y) = (-2, 0)$ is the only $\mathbb{Q}$-rational point on E_4. We retrieve $(\widehat{x}, \widehat{y}) = (-3, -1)$, which corresponds to no integer point in the original equation. $\square$

Theorem 3.5. *Let $\widehat{p}$ and q be distinct odd primes, and $p = \widehat{p}^k$, for some $k \in \mathbb{N}$. Then, the Diophantine equation $p^X + q^Y = Z^3$ can be transformed into the elliptic curve $E_4 : y^2 = x^3 - 15p^2x - 22p^3$ if $X \equiv 1 \pmod 2$, $Y \equiv 0 \pmod 6$ and k is even. Moreover, if the Mordell-Weil group of E_4 is trivial, then $p^X + q^Y = Z^3$ has no solutions in $\mathbb{N}$.*

Proof. Let $k = 2k_1$, $X = 2X_1 + 1$ and $Y = 6Y_1$, for some $X_1, \in \mathbb{N}_0, k_1, Y_1 \in \mathbb{N}$. By factoring, we have the following:

$$p^{2X_1+1} = (Z - q^{2Y_1})(Z^2 + Zq^{2Y_1} + q^{4Y_1}).$$

Since $p = \widehat{p}^k$, where $\widehat{p}$ is prime, there exist two non-negative integers α and β, $\alpha < \beta$ such that $\alpha + \beta = k(2X_1 + 1)$ and

$$\widehat{p}^{\beta-\alpha} = \frac{\widehat{p}^{\beta}}{\widehat{p}^{\alpha}} = \frac{Z^2 + Zq^{2Y_1} + q^{4Y_1}}{Z - q^{2Y_1}} = Z^2 + 2q^{2Y_1} + \frac{3q^{4Y_1}}{Z - q^{2Y_1}}.$$

This means that $Z - q^{2Y_1}$ divides $3q^{4Y_1}$. Since q is prime, $Z - q^{2Y_1} = 3q^j$ or $Z-q^{2Y_1} = q^j$, for some $0 \leq j \leq 4Y_1$. If $j > 0$, then $q \mid Z$ which is a contradiction. Hence, $j = 0$ and we have either $Z - q^{2Y_1} = 3$ or $Z - q^{2Y_1} = 1$. For the first case, we have

$$p^X + q^{6Y_1} = (q^{2Y_1} + 3)^3 = q^{6Y_1} + 9q^{4Y_1} + 27q^{2Y_1} + 27,$$

which implies that $p^X = 9q^{4Y_1} + 27q^{2Y_1} + 27$. This means that $9 \mid p^X$ or that is, $\widehat{p} = 3$. This gives us $3^{k(X-2)} = q^{4Y_1} + 3q^{2y_1} + 3$. Since $\gcd(p, q) = \gcd(3^k, q) = 1$, we have $X = 2$ which gives $1 = q^{4Y_1} + 3q^{2Y_1} + 3$, a contradiction. For the second case, we have

$$p^X + q^{6Y_1} = (q^{2Y_1} + 1)^3 = q^{6Y_1} + 3q^{4Y_1} + 3q^{2Y_1} + 1.$$

This implies that $p \cdot p^{2X_1+1} = 3pq^{4Y_1} + 3pq^{2Y_1} + p$. Let $u = q^{Y_1}$ and $v = p^{X_1+1}$ so that $v^2 = 3pu^4 + 3pu^2 + 1$. Using Theorem 2.1, if we let $\widehat{x} = \frac{2\widehat{p}^{k_1}v+2p}{u^2}$ and $\widehat{y} = \frac{4p^2v+4p\widehat{p}^{k_1}+6p\widehat{p}^{k_1}u^2}{u^3}$ and define $a_1 = 0$, $a_2 = 3p$, $a_3 = 0$, $a_4 = -12p^2$ and $a_6 = -36p^3$, then we get the elliptic curve

$$\widehat{y}^2 = \widehat{x}^3 + 3p\widehat{x}^2 - 12p^2\widehat{x} - 36p^3.$$

By letting $x = \widehat{x} + 1$ and $y = \widehat{y}$, we obtain the elliptic curve

$$E_5 : y^2 = x^3 - 15p^2x - 22p^3.$$

One can use the SAGE to determine the torsion and the rank of this elliptic curve for a specific value of p. Moreover, if the Mordell-Weil group of E_4 is trivial, then $p^X + q^Y = Z^3$ has no solutions in $\mathbb{N}$. $\square$

We have the following example demonstrating the use of Theorem 3.4 and Theorem 3.5.

Example 3.2. Consider the Diophantine equation $7^X + 11^Y = Z^3$ over the set of positive integers. Taking modulo 7, we get $Z^3 \equiv 4^Y \pmod 7$. Now, since $Z^3 \equiv 0, 1, 6 \pmod 7$, we get $4^Y \equiv 1 \pmod 7$ or that is $Y \equiv 0 \pmod 3$. Using Theorem 3.4, the equation has no solutions in $\mathbb{N}$ if X and Y are even. On the other hand, consider the Diophantine equation $49^X + 11^Y = Z^3$ where X is odd and Y is even. Using Theorem 3.5, this can be transformed into the elliptic curve $E : y^2 = x^3 - 36015x - 2588278$ which has rank 0. Furthermore, its torsion subgroup is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. We can easily see that $(-98, 0)$ is the only non-trivial torsion point of E which does not correspond to an integer solution in the original equation.

4. Summary

In this paper, we presented a way of determining nonsolvability of exponential Diophantine equations of type $p^X + q^Y = Z^n$, where n is either $2, 3$ or 6, via transformation to a Weierstrass equation of elliptic curves. We did this because the rational points on an elliptic curve form an abelian group, and so are easier to determine. Theorems 3.1 and 3.2 are dedicated for the case when $n = 2$, and Theorems 3.3, 3.4 and 3.5 for the case when $n = 3$ and 6. These theorems do not cover all possible scenarios when solving a certain Diophantine equation but are effective in reducing the number of cases to be considered when solving for its solutions. For future works, some of the results can be extended to a more general family of exponential Diophantine equations or to any similar types of equation.

Acknowledgment

The authors would like to thank the University of the Philippines Baguio for the support. They are also very grateful to the referees who read carefully the manuscript and gave constructive comments that made the paper of better quality.

References

[1] D. Acu, *On a Diophantine equation* $2^x + 5^y = z^2$, Gen. Math., 15 (2007), 145-148.

[2] J.B. Bacani, J.F.T. Rabago, *The complete set of solutions of the Diophantine equation* $p^x + q^y = z^2$ *for twin primes* p *and* q, Int. J. Pure Appl. Math., 104 (2015), 517-521.

[3] R.J.S. Mina, J.B. Bacani, *Non-existence of solutions of Diophantine equations of the form* $p^x + q^y = z^{2n}$, Math. Stat., 7 (2019), 78-81.

[4] J.F.T. Rabago, *On two Diophantine equations* $3^x + 19^y = z^2$ *and* $3^x + 91^y = z^2$, Int. J. Math. Sci. Comp., 3 (2012), 28-29.

[5] J.F.T. Rabago, *More on Diophantine equations of type* $p^x + q^y = z^2$, Int. J. Math. Sci. Comp., 3 (2013), 15-16.

[6] J.F.T. Rabago, *On an open problem by B. Sroysang,* Konuralp J. Math., 1 (2013), 30-32.

[7] J.F.T. Rabago, *A note on two Diophantine equations* $17^x + 19^y = z^2$ *and* $71^x + 73^y = z^2$, Math. J. Interdisciplinary Sci., 2 (2013), 19-24.

[8] B. Sroysang, *On the Diophantine equation* $3^x + 5^y = z^2$, Int. J. Pure Appl. Math., 81 (2012), 605-608.

[9] B. Sroysang, *More on the Diophantine equation* $8^x + 19^y = z^2$, Int. J. Pure Appl. Math., 91 (2014), 139-142.

[10] B. Sroysang, *On the Diophantine equation* $3^x + 45^y = z^2$, Int. J. Pure Appl. Math., 81 (2014), 269-272.

[11] A. Suvarnamani, A. Singta, S. Chotchaisthit, *On two Diophantine equations* $4^x + 7^y = z^2$ *and* $4^x + 11^y = z^2$, Sci. Technol. RMUTT J., 1 (2011), 25-28.

[12] L.C. Washington, *Elliptic curves: number theory and cryptography*, CRC Press, 2003.

[13] W.A. Stein et al., *Sage Mathematics Software* (Version 9.2), The Sage Development Team, 2020, http://www.sagemath.org

[14] E.W. Weisstein, *Mordell curve*, From MathWorld–A Wolfram Web Resource. https://mathworld.wolfram.com/MordellCurve.html

[15] W. Jr. Gayo, J. Bacani, *On the Diophantine equation* $M_p^x + (M_q + 1)^y = z^2$, Eur. J. Pure Appl. Math., 14 (2021), 396-403.

Accepted: October 29, 2021