A NOTE ON THE DIOPHANTINE EQUATION $qx + py = z^2$

LU LEI
Guangdong Country Garden School Foshan, Guangdong 528312, China.
leitonylu@hotmail.com

Abstract. In this paper, we investigate the non-negative integer solutions of the equation of the form $q^x + p^y = z^2$ for $x$, $y$, and $z$, with $p, q$ primes. In particular, we consider the equation $3^x + p^y = z^2$, with $p$ a prime congruent to 5 modulo 12. We prove that $(1, 0, 2)$ is the unique non-negative integer solution of this equation. Moreover, we prove that $(1, 0, 2)$ is also the unique non-negative integer solution for the equation $3^x + b^y = z^2$ where $b$ is a positive integer congruent to 1 modulo 4 and has a prime factor congruent to 5 modulo 12 or congruent to 7 modulo 12.

1. Introduction
The Diophantine equation problem is one of the major areas in number theory. Diophantine equations refer to the study of the solutions of polynomial equations in two or more variables in either integers or rational numbers, rather than in real or complex numbers. If a Diophantine equation has an additional variable or variables occurring as exponents, it is an exponential Diophantine equation, such as $am + bn = ck$. One of the most famous Diophantine equations is Fermat’s equation $an + bn = cn$ (in the year 1637), known as Fermat’s Last Theorem, which states that there are no integer solutions $(a, b, c)$ with $abc \neq 0$ and $n \geq 3$. However, Fermat did not give a proof except the case $n = 4$. Until the year 1994, Andrew Wiles gave a complete successful proof.

Theorem 1.1. (A.Wiles) [3]. There are no solutions in integers $x, y, z$ with $xyz \neq 0$ of $x^n + y^n = z^n$ when $n \geq 3$.

In the present paper, we investigate the non-negative integer solutions of the equation of the form $qx + py = z^2$ for $x$, $y$, and $z$, with $p, q$ primes. In particular, we consider the equation $3x + py = z^2$, with $p$ a prime. This equation has been solved in several cases. For example, Sroysang [1][2] proved that the equation has only one non-negative integer solutions $(1, 0, 2)$ when $p = 5, 17$. In this paper, we prove the following theorem (Theorem 3.1).

Theorem 1.2. When $p$ is a prime congruent to 5 modulo 12, the equation $3x + py = z^2$ has only one non-negative integer solution $(1, 0, 2)$.

2010 Mathematics Subject Classification. 11D61.
Keywords: Exponential Diophantine equation.
We remark here that in the above theorem the condition \( p \equiv 5 \mod 12 \) is equivalent to \( p \equiv 1 \mod 4 \) and \( p \equiv 2 \mod 3 \) by the Chinese Remainder Theorem. Here are a list of primes which are all congruent to 5 modulo 12:
\[
5, 17, 29, 41, 53, 89, 101, 113, 137, 149, 173, 197, 233, 257, 269, 281, 293, 317, 353, 389, ...
\]
We know that there are infinitely many primes which are congruent to 5 modulo 12 by Dirichlet’s theorem on arithmetic progressions, which asserts that there are infinitely many primes that are congruent to a modulo d, for any two positive coprime integers a and d.

Moreover, in the last section we will give a more general result for the equation \( 3x + by = z^2 \). In particular, we prove the following theorem (Theorem 4.1).

**Theorem 1.3.** The equation \( 3x + by = z^2 \) has only one non-negative integer solution \((1, 0, 2)\), when \( b \) is a positive integer congruent to \( 1 \mod 4 \) and has a prime factor congruent to \( 5 \mod 12 \) or a prime factor congruent to \( 7 \mod 12 \).

For example, in above theorem we can take \( b = 21, 25, 45, 49, 57, 65, 77, 85, ... \). Obviously, we can take infinitely many such integers \( b \), and \( b \) can be arbitrary large.

### 2. Preliminaries

In this section, we will quickly first recall the basic knowledge of quadratic residue and quadratic reciprocity law, and then prove two useful results for the main theorem. Let \( p \) be an odd prime and \( a \) be an integer coprime to \( p \). We say that \( a \) is a quadratic residue modulo \( p \) if \( a \) is a square modulo \( p \). Otherwise, it is a quadratic non-residue. Recall that the Legendre symbol is defined to be

\[
\left( \frac{a}{p} \right) = \begin{cases} 
1 & \text{if } a \text{ is quadratic residue modulo } p \\
-1 & \text{if } a \text{ is quadratic non-residue modulo } p 
\end{cases}
\]

for odd prime \( p \), when \((a, p) = 1\). Moreover, it is known to all that we have the following quadratic reciprocity law

\[
\left( \frac{q}{p} \right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot \left( \frac{p}{q} \right) = \begin{cases} 
1 & \text{if } p \equiv 1 \mod 4 \text{ or } q \equiv 1 \mod 4 \\
-1 & \text{otherwise}
\end{cases}
\]

where \( p \) and \( q \) are both odd primes.

The following proposition is crucial in the proof of our main theorem. Although the following result has been proved in [1] for \( q = 3 \), but here we will give a more general and simpler proof.

**Proposition 2.1.** For the Diophantine equation \( qx + 1 = z^2 \) with \( q \) a prime, we have the following results.

1. It has only one non-negative integer solution \((3, 3)\) for \( q = 2 \).
2. It has only one non-negative integer solution \((1, 2)\) for \( q = 3 \).
3. It has no non-negative integer solution for \( q \geq 5 \).

**Proof.** For the equation \( qx + 1 = z^2 \), we have that \( qx = z^2 - 1 \), therefore \( qx = (z+1)(z-1) \). So we have that \( q(z+1)(z-1) \). As \((z+1)-(z-1) = 2\), so \((z+1)\) and \((z-1)\) can not be both divided by \( q \geq 3 \).

1. For \( q = 2 \), we must have \( z + 1 = 2x1 \) and \( z - 1 = 2x2 \) with \( x1 + x2 = x \). Then we get \((z + 1) - (z - 1) = 2x1 - 2x2 = 2\), i.e. \( 2x1 - 2x2 = 1 \). Hence \( x1 = 1 \) and \( x2 = 1 \). So \( x = 3 \) and \( z = 3 \).
2. For \( q = 3 \), we have \( 3(z + 1) \), but \( 3 - (z - 1) \). So we must have \( 3x = z + 1 \) and \( 1 = z - 1 \). So \( x = 1 \) and \( z = 2 \).
(3) For $q \geq 5$, we have $q(z+1)$, but $q - (z - 1)$. So we must have $qx = z + 1$ and $1 = z - 1$. Hence $z = 2$ and $qx = 3$, which is obviously not soluble for $x$. So there is no non-negative integer solution in this case.

**Lemma 2.2.** For the equation $3x + ny = z^2$, if $n \equiv 1 \pmod{4}$, then $x$ must be odd.

**Proof.** As $3x \equiv 3, 1 \pmod{4}$, and $ny \equiv 1 \pmod{4}$, and $z^2 \equiv 0, 1 \pmod{4}$, we must have $3x \equiv 3 \pmod{4}$, and $z^2 \equiv 0 \pmod{4}$, so $z$ must be even and $x$ must be odd.

### 3. Proof of the theorem

In this section, we are going to prove the following main theorem.

**Theorem 3.1.** When $p$ is a prime congruent to 5 modulo 12, the equation $3x + py = z^2$ has only one non-negative integer solution $(1,0,2)$.

**Proof.** When $y = 0$, $(1,0,2)$ is the only solution of the equation by Proposition 2.1. When $y \neq 0$, we consider the equation $3x + py = z^2$ modulo $p$, we have that $3x \equiv z^2 \pmod{p}$.

The above congruence has a solution if and only if $3x$ is a quadratic residue of modulo $p$, that is, the Legendre symbol $\left(\frac{3x}{p}\right) = 1$. We first have that

$$\left(\frac{3x}{p}\right) = \left(\frac{3^{x-1}}{p}\right) \left(\frac{3}{p}\right).$$

Since $x$ is an odd number by Lemma 2.2, we have that $x - 1$ is even, so $\left(\frac{3^{x-1}}{p}\right) = 1$.

Hence

$$\left(\frac{3x}{p}\right) = \left(\frac{3}{p}\right).$$

Note that $p \equiv 1 \pmod{4}$, we now have

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) \left(-1\right)^{\frac{p-1}{2}} = \left(\frac{p}{3}\right),$$

by the quadratic reciprocity law. Since when $p \equiv 2 \pmod{3}$, we get

$$\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Therefore it is a contradiction, so the equation has no solution when $y \neq 0$. This completes the proof of the theorem.

By the above theorem, we can immediately get the following result.

**Corollary 3.2.** When $p$ is a prime congruent to 5 modulo 12, the equation $3x + py = z^2k$ has no non-negative integer solution for $x, y, z$, where $k \geq 2$ is an integer.

**Proof.** According to Theorem 3.1, when $p \equiv 5 \pmod{12}$, the equation $3x + py = z^2k$ has a solution if and only if $x = 1, y = 0, zk = 2$, which is not soluble since $z$ is an integer and $k \geq 2$, so there is no non-negative integer solution for $x, y, z$.

### 4. Generalisation

In this section, we will generalise the main theorem to a more general equation $3^x + b^y = z^2$, where $b$ is a positive integer congruent to 1 modulo 4. In particular, we prove the following theorem.
Theorem 4.1. The equation $3x + by = z^2$ has only one non-negative integer solution $(1, 0, 2)$, when $b$ is an positive integer congruent to $1$ modulo $4$ and has a prime factor congruent to $5$ modulo $12$ or a prime factor congruent to $7$ modulo $12$.

Proof. When $y = 0$, $(1, 0, 2)$ is the only solution of the equation by Proposition 2.1. When $y \neq 0$, we consider the equation $3x + by = z^2$ modulo $p$, where $p|b$ and $p$ is a prime congruent to $5$ modulo $12$ or congruent to $7$ modulo $12$, so we have that $3x \equiv z^2 \mod p$.

According to Lemma 2.2, we know that $x$ is odd. By the same arguments of Theorem 3.1, we know that there is no non-negative integer solution in the case that $p$ is congruent to $5$ modulo $12$. While if $p \equiv 7 \mod 12$, i.e. $p \equiv 3 \mod 4$ and $p \equiv 1 \mod 3$, we still have that

$$
\left( \frac{3^x}{p} \right) = \left( \frac{3^{x-1}}{p} \right) \left( \frac{3}{p} \right) = \left( \frac{3}{p} \right).
$$

Note that $p \equiv 3 \mod 4$, we now have

$$
\left( \frac{3}{p} \right) = \left( \frac{p}{3} \right) \left( -1 \right)^{\frac{p-1}{2} \frac{3-1}{2}} = -\left( \frac{p}{3} \right),
$$

by the quadratic reciprocity law. Since when $p \equiv 1 \mod 3$, we get

$$
\left( \frac{3}{p} \right) = -\left( \frac{p}{3} \right) = -\left( \frac{1}{3} \right) = -1.
$$

So we have that there is no non-negative integer solution in the case that $p$ is congruent to $7$ modulo $12$. Hence $(1, 0, 2)$ is the only non-negative integer solution for the equation $3^x + p^y = z^2$ where $b$ is a positive integer congruent to $1$ modulo $4$ and has a prime factor congruent to $5$ modulo $12$ or congruent to $7$ modulo $12$.

Corollary 4.2. When $b$ is an positive integer congruent to $1$ modulo $4$ and has a prime factor congruent to $5$ modulo $12$ or a prime factor congruent to $7$ modulo $12$, the equation $3x + py = z^{2k}$ has no non-negative integer solution for $x, y, z$, where $k$ is an integer greater than $1$.

Proof. According to Theorem 4.1, under the above assumptions, the equation $3x + by = z^{2k}$ has a solution if and only if $x = 1, y = 0, zk = 2$, which is not soluble since $z$ is an integer, so there is no non-negative integer solution for $x, y, z$.

In conclusion, we remark that for the exponential equation of the type $q^x + p^y = z^2$ with $p, q$ primes, we can try to find all non-negative integer solutions for $x, y, z$ by similar methods.

References

[1] B. Sroysang, On the Diophantine equation $3x + 5y = z^2$, International Journal of Pure and Applied Mathematics, Volume 81, No.4, 2012, 605–608.

[2] B. Sroysang, On the Diophantine equation $3x + 17y = z^2$, International Journal of Pure and Applied Mathematics, Volume 89, No.1, 2013, 111–114.

[3] A. Wiles, Modular elliptic curves and Fermat’s last theorem, Ann. of Math. 141 (1995), 443–551.