ON THE DIOPHANTINE EQUATION $x^3 = dy^2 \pm q^6$

FADWA S. ABU MURIEFAH

(Received 21 December 2000)

ABSTRACT. Let $q > 3$ denote an odd prime and $d$ a positive integer without any prime factor $p \equiv 1 \pmod{3}$. In this paper, we have proved that if $(x,q) = 1$, then $x^3 = dy^2 \pm q^6$ has exactly two solutions provided $q \not\equiv \pm 1 \pmod{24}$.

2000 Mathematics Subject Classification. 11D41.

Cohn [1] and recently Zhang [2, 3] have solved the Diophantine equation

\[ x^3 = dy^2 \pm q^6 \]  

when $q = 1, 3, 4$, under some conditions on $d$. In this paper, we consider the general case of (1) where $q \neq 3$ is any odd prime by using arguments similar to those used by Cohn [1].

Let $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ be a solution of (1) with $x, y > 0$, then the solution is trivial if $x = 0, \pm q^2$ or $y = \pm 1$. We need the following lemma.

**Lemma 1.** The equation $p^2 = a^4 - 3b^2$, where $p$ denotes an odd prime and $(p, a) = 1$, may have a solution in positive integers $a$ and $b$ only if $p \equiv \pm 1 \pmod{24}$.

**Proof.** Suppose $3b^2 = a^4 - p^2$. Then clearly $a$ is odd and $b$ is even. Since $a^4 \equiv 3b^2 \pmod{p}$, and $(p, a) = 1$ therefore the Legendre symbol $(3/p) = 1$, and so $p \equiv \pm 1 \pmod{12}$. Now $(a^2 + p, a^2 - p) = 2$ implies that

\[ a^2 \pm p = 3.2c^2, \]  \hspace{1cm} (2)

\[ a^2 \mp p = 2d^2, \]  \hspace{1cm} (3)

where $2cd = b$ and $(c, d) = 1$. Whence

\[ a^2 = 3c^2 + d^2. \]  \hspace{1cm} (4)

Here $d$ is odd, otherwise we get a contradiction modulo 4. Then considering (3) modulo 8, we get $p \equiv \pm 1 \pmod{8}$. This completes the proof. \qed

Now we consider the upper sign in (1), our main result is laid down in the following.

**Theorem 2.** Let $d$ be a positive integer without prime factor $p \equiv 1 \pmod{3}$ and let $q \neq 3$ be an odd prime. If $q \not\equiv \pm 1 \pmod{24}$ and $(x, q) = 1$, then the Diophantine equation

\[ x^3 = dy^2 + q^6 \]  \hspace{1cm} (5)
has exactly two solutions given by

\[
\begin{align*}
x_1 &= \frac{3q^4 - 2q^2 - 1}{4}, \\
y &= ab, & \text{where } a &= \frac{3q^4 + 1}{4}, & db^2 &= \frac{3q^4 - 6q^2 - 1}{4}, \\
x_2 &= \frac{q^4 - 2q^2 - 3}{4}, \\
y &= 9ab, & \text{where } a &= \frac{q^4 + 3}{4}, & db^2 &= \frac{q^4 - 6q^2 - 3}{4}.
\end{align*}
\]

PROOF. If \(d\) has a square factor, then it can be absorbed into \(y\), so there is no loss of generality in supposing \(d\) a square free integer. Now

\[
dy^2 = x^3 - q^6 = (x - q^2)(x^2 + q^2x + q^4).
\]

If any prime \(r\) divides both \(d\) and \((x^2 + q^2x + q^4)\), then by hypothesis \(r \equiv 2 \pmod{3}\) or \(r = 3\). But \(r \mid (x^2 + q^2x + q^4)\) implies that \((2x + q^2)^2 + 3q^4 \equiv 0 \pmod{r}\) so the Legendre symbol \((-3/r) = 1\), which is a contradiction, whence \(r = 1\) or 3. Also since \((x, q) = 1\), therefore \((x - q^2, x^2 + q^2x + q^4) = 1\) or 3. So for (7) we have only two possibilities: either

\[
x^2 + q^2x + q^4 = a^2, \quad x - q^2 = db^2,
\]

or

\[
x^2 + q^2x + q^4 = 3a^2, \quad x - q^2 = 3db^2,
\]

where \((q, a) = 1\) and \((q, b) = 1\). Consider the first possibility when \((2x + q^2)^2 + 3q^4 = (2a)^2\) and \(y = ab\). This equation is known to have a finite number of solutions. It can be written as

\[
3q^4 = (2a + 2x + q^2)(2a - (2x + q^2)).
\]

Then for the nontrivial solution of this equation we have only two cases:

CASE 1.

\[
3q^4 = 2a \pm (2x + q^2), \quad 1 = 2a \mp (2x + q^2),
\]

by subtracting and adding these two equations we get

\[
x = \frac{3q^4 - 2q^2 - 1}{4}, \quad a = \frac{3q^4 + 1}{4}.
\]

Here \(a > 1\), so \(y > 1\), and \(x - q^2 = db^2\) implies that

\[
db^2 = \frac{3q^4 - 6q^2 - 1}{4}.
\]

CASE 2.

\[
3 = 2a \pm (2x + q^2), \quad q^4 = 2a \mp (2x + q^2).
\]

As in Case 1 we get the nontrivial solution

\[
x = \frac{3q^4 - 2q^2 - 1}{4}, \quad a = \frac{3q^4 + 1}{4}, \quad db^2 = \frac{3q^4 - 6q^2 - 1}{4}.
\]
Now suppose the second possibility. Obviously \( a \) is odd and \( x^2 \equiv 3a^2 \pmod{q} \), and since \((q,a) = 1\), so the Legendre symbol \((3/q) = 1\), hence \( q \equiv \pm 1 \pmod{12} \). Eliminating \( x \) and dividing by 3, we get

\[
a^2 = q^4 + 3db^2(q^2 + db^2).
\]  
\[(16)\]

Considering \((16)\) modulo 8 we get either \( db^2 \equiv -1 \pmod{8} \) or \( db^2 \equiv 0 \pmod{8} \).

(1) \( db^2 \equiv -1 \pmod{8} \). Then from \((16)\) we get

\[
3d^2b^4 = (2a + 2q^2 + 3db^2)(2a - 2q^2 - 3db^2).
\]  
\[(17)\]

Let \( S \) be a common prime divisor of the two factors in the right-hand side of \((17)\), then \( S \) is odd, \( S \mid 4a \) and \( S \mid 2(2q^2 + 3db^2) \). But \( S^2 \) divides the left-hand side implies that \( S \mid 3db^2 \), so \( S \mid q^2 \). Here \( S = 1 \), otherwise \( x - q^2 = 3db^2 \) implies that \( q \mid x \) which is not true. Thus from \((17)\) we get

\[
2a \pm (2q^2 + 3db^2) = d_1^2b_1^4, \quad 2a \mp (2q^2 + 3db^2) = 3d_2^2b_2^4,
\]  
\[(18)\]

where \( d = d_1d_2 \) and \( b = b_1b_2 \). Whence

\[
\pm 2(2q^2 + 3db^2) = d_1^2b_1^4 - 3d_2^2b_2^4.
\]  
\[(19)\]

Considering this equation modulo 3, we get

\[
4q^2 = d_1^2b_1^4 - 3d_2^2b_2^4 - 6db^2.
\]  
\[(20)\]

Now we prove that \( d_1 = 1 \). Since \( d \) is odd, therefore \( d_1 \) must be odd. Let \( t \) be any odd prime dividing \( d_1 \) then by hypothesis \( t \equiv 2 \pmod{3} \) but then from \((20)\) we get

\[
4q^2 \equiv -3d_2^2b_2^4 \pmod{t},
\]  
\[(21)\]

so \((-3/t) = 1\), which is not true. Thus \( d_1 = 1 \) and \((20)\) becomes

\[
q^2 = b_1^4 - 3\left(\frac{b_1^2 + db_2^2}{2}\right)^2,
\]  
\[(22)\]

since \((q,b_1) = 1\), therefore by Lemma 1, \( q \equiv \pm 1 \pmod{24} \).

(2) \( db^2 \equiv 0 \pmod{8} \). Now we prove that if \((16)\) has a solution, then \( q \equiv \pm 1 \pmod{24} \). Since \( d \) is a square free, \( b \) should be even. Suppose \( b = 2m \), then \((16)\) can be written as

\[
12d^2m^4 = (a + q^2 + 6dm^2)(a - q^2 - 6dm^2).
\]  
\[(23)\]

As before we can prove that the common divisor of the two factors in the right-hand side of \((23)\) is 2, so

\[
a \pm (q^2 + 6dm^2) = 2d_1^2m_1^4, \quad a \mp (q^2 + 6dm^2) = 6d_2^2m_2^4,
\]  
\[(24)\]

where \( d = d_1d_2 \) and \( m = m_1m_2 \). It is clear that \((a,q) = 1\) implies that \((m_1,q) = 1\).
Subtracting the two equations in (24) we get
\[ \pm (q^2 + 6dm^2) = d_1^2 m_1^4 - 3d_2^2 m_2^4, \]
(25)
again considering this equation modulo 3, we get \( q^2 = d_1^2 m_1^4 - 3d_2^2 m_2^4 - 6dm^2 \). As before \( d_1 \) cannot have any odd prime divisor, so \( d_1 = 1 \) or \( 2 \).

If \( d_1 = 1 \), then
\[ q^2 = 4m_1^4 - 3(m_1^2 + dm_2^2). \]
(26)
Here \( m_1 \) is odd, otherwise we get a contradiction modulo 8. Since \((m_1, q) = 1\), then from (26) we get
\[ 2m_1^2 \equiv q \equiv 3s^2, \quad 2m_1^2 \equiv q \equiv n^2, \]
(27)
where \( sn = m_1^2 + dm_2^2 \), so \( s \) and \( n \) are both odd. Hence \( q \equiv \pm 1 \pmod{8} \), combining this result with \( q \equiv \pm 1 \pmod{12} \), we get \( q \equiv \pm 1 \pmod{24} \).

If \( d_1 = 2 \), then
\[ q^2 = 16b_1^4 - 3(b_1^2 + db_2^2)^2 \]
(28)
which is impossible modulo 8.

Using the same argument as in Theorem 2 we can prove the following theorem.

**Theorem 3.** Let \( d \) be a positive integer without prime factor \( p \equiv 1 \pmod{3} \) and \( q \not\equiv 3 \pmod{5} \) an odd prime. If \( q \not\equiv \pm 1 \pmod{24} \) and \((x, q) = 1\), then the Diophantine equation \( x^3 = dy^2 - q^6 \) has exactly two solutions given by
\[
\begin{align*}
x_1 &= \frac{3q^4 + 2q^2 - 1}{4}, \quad y = ab, \quad \text{where} \quad a = \frac{3q^4 + 1}{4}, \quad db^2 = \frac{3q^4 + 6q^2 - 1}{4}, \\
x_2 &= \frac{q^4 + 2q^2 - 3}{4}, \quad y = 9ab, \quad \text{where} \quad a = \frac{q^4 + 3}{4}, \quad db^2 = \frac{q^4 + 6q^2 - 3}{4}.
\end{align*}
\]
(29)

Sometimes, combining our results with Cohn’s result [1] we can solve the title equation completely when \( d \) has no prime factor \( \equiv 1 \pmod{3} \), as we show in the following example.

**Example 4.** Consider the Diophantine equation \( x^3 = 5y^2 + 5^6 \) where \( d \) has no prime factor \( \equiv 1 \pmod{3} \) and \((5, d) = 1\).

Here \( q = 5 \), when \((x, 5) = 1\), using Theorem 2 for the positive sign this equation has only two solutions given by \( x_1 = 456, \quad db^2 = 431, \quad x_2 = 143, \quad db^2 = 118 \). So \( d = 431, 118 \). Now let \( 5 \mid x \), then because \((5, d) = 1\), the equation reduces to the form \( x^3 = 5dy^2 + 1 \), which by [1, Theorem 1] has no solution in positive integers.

So the equation \( x^3 = dy^2 + 5^6 \) has a solution only if \( d = 431, 118 \).

For the negative sign this equation has two solutions when \((x, 5) = 1\) given by
\[
\begin{align*}
x_1 &= 481, \quad db^2 = 506, \quad x_2 = 168, \quad db^2 = 193,
\end{align*}
\]
(30)
that is, when \( d = 506, 193 \). If \( 5 \mid x \), then the equation reduces to the form \( x^3 = 5dy^2 - 1 \), which by [1, Theorem 2] has no solution in positive integers.
ON THE DIOPHANTINE EQUATION $x^3 = dy^2 \pm q^6$

REFERENCES


FADWA S. ABU MURIEFAH: MATHEMATICS DEPARTMENT, GIRLS COLLEGE OF EDUCATION, RIYADH, SAUDI ARABIA