On the diophantine equation $ax^2+b=cy^n$

Fadwa S. Abu Muriefah and Amal AL-Rashed

Princess Nora Bint Abdulrahman University, KSA
Email: fsabumuriefah@pnu.edu.sa, amal_dfr@hotmail.com
Received: 8 Feb. 2012; Revised 15 May. 2012; Accepted 23 Jul. 2012

Abstract: In this paper, we study the diophantine equation $ax^2+b=cy^n$ where $a, b, c, n, x, y$ are positive integers and we prove some results concerning this equation when $b=7, 11$. In Theorem 3, we are able to correct the result of Demirpolat and Cenberci appeared in [9].

Keywords: Diophantine equation, perfect square, quadratic field.

Introduction
Many special cases of the diophantine equation

$$ax^2+b=cy^n,$$ (1)

where $a, b, c, n$ are positive integers and $n \geq 3$, have been considered over the years. If we put $a=1, b=7, c=1$ and $y=2$ in (1) we obtain the equation

$$x^2+7=2^n,$$ (2)

which was studied by an Indian mathematician S. Ramanujan [1], and he conjectured that the equation (2) has only the following five solutions:

$$(n, x)=(3,1),(4,3),(5,5),(7,11),(15,181).$$

This conjecture was first proved by Nagell [2]. In 2003 Siksek and Cremona [4] solved equation (2) for $n=p$ where $p$ is odd prime and they proved that this equation has no solution for $11 \leq p \leq 18^8$.

Bugeaud and Shorey [3] were proved that equation (1) has no solution when $a=1, b=7$ and $c=4$.

In 2008, Abu Muriefah [5] studied the general case $px^2+q^{2m}=y^n$ where $p, q$ are primes under some conditions, and recently she proved with Luca and Togbé [6] that the equation $x^2+5^3=13^n$ where $a, b \geq 0$, has the following solution:

$$(x,y,a,b,n)=(70,17,0,1,3),(142,29,2,2,3), (4,3,1,1,4).$$

Now we study the equation (1) for $a=p, b=7^{m+1}, c=1$ and we prove the following theorem:

Theorem 1

If $p \neq 7$, $x$ is an even integer and $(h, p)=1$ where $h$ is the class number of the field $\mathbb{Q}((\sqrt{-7})p)$, then the diophantine equation

$$px^2+7^{2m+1}=y^p,$$ (3)

has no solution in integers $x$ and $y$.

Proof
I. \((x,y)=1,\)

If \(x\) is even then \(y\) is odd, we factorize equation (3) to obtain

\[
\sqrt{px} + 7^m \sqrt{-7} = \left(\sqrt{pa + b \sqrt{-7}}\right)^p,
\]

(4)

where \(a, b\) are integers and \(y = pa^2 + 7b^2\).

On equating the imaginary parts in (4) we get

\[
7^m = b \sum_{r=0}^{p-1} \left( \frac{p}{2r+1} \left( pa^2 \right)^{p-(2r+1)/2} (-7b^2)^r \right).
\]

(5)

Since \(y\) is odd, therefore \(b\) is odd, hence \(a\) is even and \((a,7)=1\).

If \(b=\pm 7^k\), \(0 \leq k < m\) then (5) is impossible modulo 7, so \(b=\pm 7^m\).

Let

\[
\alpha = a\sqrt{p} + b\sqrt{-7}, \quad \bar{\alpha} = a\sqrt{p} - b\sqrt{-7},
\]

(6)

hence from (4) we get

\[
\alpha^p = x\sqrt{p} + 7^m \sqrt{-7}, \quad \bar{\alpha}^p = x\sqrt{p} - 7^m \sqrt{-7}.
\]

(7)

From (6) and (7) we obtain

\[
U_p = \frac{\alpha^p - \bar{\alpha}^p}{\alpha - \bar{\alpha}} = \frac{2 \cdot 7^m \sqrt{-7}}{2b \sqrt{-7}} = \frac{7^m}{b} = \pm 1.
\]

Since \((\alpha\bar{\alpha}, (\alpha + \bar{\alpha})^2) = 1\) and \(\frac{\alpha}{\bar{\alpha}}\) is not a root of unity, therefore \(U_p(\alpha, \bar{\alpha})\) is a Lehmer pair with no primitive divisor. When \(p \in [5, 29]\), there are only finitely many possibilities for the pair \((\alpha, \bar{\alpha})\) and all such instances appear in Table 2 in [7]. A quick inspection of that table reveals that there exists no Lehmer number which has no primitive divisors whose roots \(\alpha\) and \(\bar{\alpha}\) are in \([i, i]\).

II. \((x,y)\neq1,\)

Let \(x = 7^u X, y = 7^v Y\) such that \(u, v > 0\) and \((7, X) = (7, Y) = 1\).

Equation (3) becomes

\[
p(7^u X)^2 + 7^{2m+1} = 7^{pv} Y^p.
\]

(8)

There are three cases:

1. If \(2u = \min(2u, pv, 2m+1)\) then equation (8) becomes

\[
pX^2 + 7^{2(m-u)+1} = 7^{pv-2u} Y^p.
\]

This equation is impossible modulo 7 unless \(pv-2u=0\), so

\[
pX^2 + 7^{2(m-u)+1} = Y^p,
\]
which has no solution from the first part of this proof, since \((X, Y)=1\).

(2) If \(2m+1=\min(2u, pv, 2m+1)\) then equation (8) becomes

\[ p7^{2u-2m-1}X^2 + 1 = 7^{pv-2m-1}Y^p, \]

This equation is impossible modulo 7 unless \(v-2m-1=0\), so

\[ 7p(7^{u-m-1}X)^2 + 1 = Y^p. \]

By [8] equation (9) has no solution.

(3) If \(pv=\min(2u, pv, 2m+1)\) then we get

\[ p7^{2u-pv}X^2 + 7^{2m+1-pv} = Y^p. \]

This equation is possible only if \(2u-pv=0\) or \(2m+1-pv=0\), and these two cases have been discussed before.◊

Now, we give a nice result in rational.

**Theorem 2**

Let \(p\) be an odd prime such that \(p-7\) has no perfect square.

I-The diophantine equation

\[ x^2 + 7 = py^{p/2}, \] (11)

has no solution in rational \(x\) and \(y\) such that \(y = \frac{Y}{t}\) where \(Y\) is an odd integer.

II- The diophantine equation

\[ x^2 + 7 = py^{(p-1)/2}, p \equiv 1 \pmod{4} \] (12)

has no solution in rational \(x\) and \(y\) such that \(y = \frac{Y}{t}\) where \(Y\) is an odd integer.

**Proof**

Assume that \(x = X/Q, \ y = Y/T\) is a solution of (11) or (12) for some integers \(X, Y, Q, T\) with \(Q \geq 1, T \geq 1\) and \((X, Q) = (Y, T) = 1\).

(13)

Put

\[ n = \begin{cases} 0, & \text{if } p \equiv 3 \pmod{4} \\ 1, & \text{if } p \equiv 1 \pmod{4}. \end{cases} \]

Then equation (11) and (12) can be written in the form

\[ X^{2T^{p-1/p^2}} + 7Q^{2T^{p-1/p^2}} = pQ^{2Y^{p-1/p^2}}. \]

(14)

Considering equation (14) modulo \(Q^2\), and from (13) we get

\[ T^{p-1/p^2} \equiv 0 \pmod{Q^2}. \]

(15)

In the same way, we get
\[ pQ^2 \equiv 0 \pmod{T^{\frac{p-1}{2^n}}}. \] (16)

Since \((p-1)/2^n\) is even, it follows from (15) and (16) that \( T^{\frac{p-1}{2^n}} = Q^2 \), hence from (14) we get

\[ X^2 + TT^{\frac{p-1}{2^n}} = pY^{\frac{p-1}{2^n}}. \] (17)

So it follows that

\[(X, p)= (T, p) = (Y, T) = (X, Y) = (X, 7) = 1.\]

Rewrite equation (17) as

\[
\begin{pmatrix}
X + T^{\frac{p-1}{2^n}} i\sqrt{7} \\
X - T^{\frac{p-1}{2^n}} i\sqrt{7}
\end{pmatrix} = pY^{\frac{p-1}{2^n}}. \] (18)

It is easy to see that the two algebraic integers appearing in the left-hand side of equation (18) are coprime in the ring of algebraic integers \((7)\). Since the ring \((7)\) is a unique factorization domain it follows that there exist four integers \(A, B, s, v\) with \( A \equiv B \pmod{2} \), \( s \equiv v \pmod{2} \) and two units \( \pm 1 \) such that

\[ X + T^{\frac{p-1}{2^n}} i\sqrt{7} = \pm \frac{A + B i \sqrt{7}}{2} \left( \frac{s + v i \sqrt{7}}{2} \right)^{\frac{p-1}{2^n}}, \] (19)

where \( p = \frac{A^2 + 7B^2}{4} \).

Multiplying both parts of (19) by \(2\frac{p-1}{2^n} B^{\frac{p-1}{2^n}}\) we get

\[ 2^{\frac{p-1}{2^n}+1} \left( XB^{\frac{p-1}{2^n}} + T^{\frac{p-1}{2^n}} B^{\frac{p-1}{2^n}} i\sqrt{7} \right) = \pm \left( A + B i \sqrt{7} \right) \left( sB + A v - (A - B i \sqrt{7} v) \right)^{\frac{p-1}{2^n}}, \]

for some \( U, K, R \) in \( \mathbb{Z} \). Comparing imaginary parts and taking into account that \( p \mid A^2 + 7B^2 \) we get

\[ 2^{\frac{p-1}{2^n}+1} T^{\frac{p-1}{2^n}} B^{\frac{p-1}{2^n}} \equiv BU^{\frac{p-1}{2^n}} \pmod{p}. \]

Raising both sides of the last congruence to the power \(\frac{p-1}{2^n+1}\), by Fermat’s little theorem we get

\[ 2^{\frac{p-1}{2^n+1}} \equiv B^{\frac{p-1}{2^n+1}} \pmod{p}, \]

for \( n \in \{0,1\} \).

For \( n=1 \), we get

\[(B^2 - 4)(B^2 + 4) \equiv 0 \pmod{p}. \]
• If $B^2 - 4 \equiv 0 \pmod{p}$, then $B^2 = 4 + kp \geq 0$ for some integer $k$, and we get $4p = A^2 + 28 + 7kp$, which implies that $k=0$, so $B^2 = 4$. Hence

$$p = \frac{A^2 + 7B^2}{4} = \left(\frac{A}{2}\right)^2 + 7,$$

this implies that $p-7$ is a perfect square and we get a contradiction.

• If $B^2 + 4 \equiv 0 \pmod{p}$, then $B^2 = -4 + kp \geq 0$ for some integer $k_1$, and we get $4p = A^2 - 28 + 7kp_1$, which implies that $4p + 28 - 7pk_1 \geq 0$, that is $k_1=0,1$.

If $k_1=0$, then $B^2 = -4$ which is not true, and if $k_1=1$, then $B^2 = -4 + p$.

If we get $p=5$. Hence from equation (3) and (4) we obtain $x^2 = 3 \pmod{5}$, which is impossible.

By using the same method we can prove that equation (3) has no solution when $n=0$. So our equations (11) and (12) has no solutions.

In the following theorem we study the equation $x^2 + 11^{2k+1} = y^n$ which was studied by the two mathematicians Demirpolat and Cenberci [9] but they failed to find all solutions of it.

**Theorem 3**

The diophantine equation

$$x^2 + 11^{2k+1} = y^n, \quad n \geq 3, \quad k \geq 0,$$

has only three families of solutions and these solutions are

$$\begin{align*}
(x, y, k, n) &= (4, 11^M, 3, 11^M, 3M, 3), \\
\end{align*}$$

Moreover when $n=3$, $(x, y)=1$ and $k \not\equiv 1 \pmod{3}$, the equation may have a solution given by

$$x = 8a^3 - 3a \quad \text{where } a \text{ is an integer satisfies } a = \sqrt[3]{\frac{11^{2k+1} + 1}{3}}.$$

**Proof**

If $k = 0$, then the equation (20) has only two solutions given by

$$(x, y, n) = (4, 3, 3), (58, 15, 3) \quad [10].$$

So we shall suppose $k > 0$.

**I.** Let $11 \mid x$, then from [11] the equation has no solution when $n \geq 5$.

(1) $n=3$, we factorize equation (20) to obtain

$$x + 11^k \sqrt{-11} = (a + b \sqrt{-11})^3,$$

where $y = a^2 + 11b^2$ is odd, so $a$ and $b$ have the opposite parity.

Or

$$x + 11^k \sqrt{-11} = \left(\frac{a + b \sqrt{-11}}{2}\right)^3,$$

(22)
where \( y = \frac{a^2 + 11b^2}{4} \) and \( a \equiv b \equiv 1(\text{mod} \ 2) \).

On equating the imaginary parts in equation (21) we get
\[ \pm 11^k = b(3a^2 - 11b^2). \]  
(23)

From (23) we deduce that \( b = 11^l \), \( 0 \leq l \leq k \), so (23) becomes
\[ \pm 11^{k-l} = 3a^2 - 11^{2l+1}. \]  
(24)

Equation (24) is impossible modulo 11, unless \( l = k \), that is
\[ \pm 1 = 3a^2 - 11^{2k+1}. \]  
(25)

The negative sign is impossible, and for the positive sign equation (25) has no solution if \( 3 \mid 2k + 1 \), [11].

So, the equation (20) may have solution when \( n = 3 \) and \( k \not\equiv 1(\text{mod} \ 3) \)

and this solution if it exists is given by \( x = 8a^3 - 3a \) where \( a \) is an integer satisfies \( a = \sqrt{\frac{11^{2k+1} + 1}{3}} \).

Now we equating the imaginary parts in (23) and we get
\[ 8 \cdot 11^k = b(3a^2 - 11b^2). \]  
(26)

We have two cases:
i. If \( b = \pm 11^l \) where \( 0 \leq l < k \), then the equation (26) is impossible modulo 11.

ii. If \( b = \pm 11^k \), then the equation (26) becomes \( 8 = 3a^2 - 11^{2k+1} \). This equation has one solution \((a, k) = (21, 1) \) [12], which implies \( x = 9324 \) and \( y = 443 \).

(2) \( n = 4 \), here we can write equation (20) as
\[ \begin{cases} y^2 + x = 11^{2k+1}, \\ y^2 - x = 1. \end{cases} \]

We get
\[ 2y^2 = 11^{2k+1} + 1, \]
this equation is impossible modulo 11.

Summarizing the above, equation (20) has the following solution when \((11, x) = 1\) we
\((x, y, k, n) = (4, 3, 0, 3), (58, 15, 0, 3), (9324, 443, 1, 3)\).

II. Let, \( 11 \mid x \), then \( x = 11^s X \) and \( y = 11^t Y \) such that \( s, t > 0 \) and \((X, 11) = (Y, 11) = 1\). Equation (20) becomes
\[ 11^{2s} X^2 + 11^{2k+1} = 11^w Y^n, \]  
(27)

We have two cases:
(1) If \( 2s = nt \), then from (27) we get
\[ X^2 + 11^{2(k-x)+1} = Y^n, \]
this equation has solution when \( n = 3 \) and either \( k-s = 0 \) or \( k-s = 1 \), since \( 2x = 3t \) then \( 3 \mid x \). Let \( s = 3M \) then \( t = 2M \), hence either \( k = 3M \) or \( k = 3M + 1 \).

So equation (20) has three families of solution
2. If $2k+1=nt$ then equation (27) become
\[ 11(11^{-k}X)^2 + 1 = Y^n, \]
which has no solution [8].◊

By using the same argument used in Theorem 2 we get the following:

**Theorem 4**

If $p$ an odd prime such that $p \not\equiv 5 (\text{mod } 8)$ and $(h,p)=1$ where $h$ is the class number of the field $\mathbb{Q}(\sqrt{-11p})$, then the diophantine equation
\[ px^2 + 11^{2k+1} = y^n, \quad p > 11, \]
has no solution in integers $x$ and $y$.◊

**References**