J. Anal. Num. Theo. 1, No. 1, 15-21 (2013)

Journal of Analysis & Number Theory
An International Journal

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

$$ax^2+b=cy^n, \tag{1}$$

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

$$x^2+7=2^n, \tag{2}$$

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 $x^2+5^a.13^b=y^n$ 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 $a=p$, $b=7^{2m+1}$, 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 $\mathbb{Q}(\sqrt{-7p})$, then the diophantine equation

$$px^2+7^{2m+1}=y^p, \tag{3}$$

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

$$\sqrt{p}x+7^m\sqrt{-7}=\left(\sqrt{p}a+b\sqrt{-7}\right)^p, \tag{4}$$

where a, b are integers and $y=pa^2+7b^2$.

On equating the imaginary parts in (4) we get

$$7^m=b\sum_{r=0}^{\frac{p-1}{2}}\binom{p}{2r+1}(pa^2)^{\frac{p-(2r+1)}{2}}(-7b^2)^r. \tag{5}$$

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

If $b=\pm7^k$, $0\le k<m$ then (5) is impossible modulo 7, so $b=\pm7^m$.

Let

$$\alpha=a\sqrt{p}+b\sqrt{-7}\ ,\ \bar{\alpha}=a\sqrt{p}-b\sqrt{-7}\ , \tag{6}$$

hence from (4) we get

$$\alpha^p=x\sqrt{p}+7^m\sqrt{-7}\ \ ,\ \ \bar{\alpha}^p=x\sqrt{p}-7^m\sqrt{-7}. \tag{7}$$

From (6) and (7) we obtain

$$U_p=\frac{\alpha^p-\bar{\alpha}^p}{\alpha-\bar{\alpha}}=\frac{2\cdot7^m\sqrt{-7}}{2b\sqrt{-7}}=\frac{7^m}{b}=\pm1.$$

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 has 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 α and $\bar{\alpha}$ are in $\mathbb{Q}[i]$.

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

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

Equation (3) becomes

$$p(7^uX)^2+7^{2m+1}=7^{pv}Y^p. \tag{8}$$

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

$$7p(7^{u-m-1}X)^2+1=Y^p. \tag{9}$$

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

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

$$p7^{2u-pv}X^2+7^{2m+1-pv}=Y^p. \tag{10}$$

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

$$x^2+7=py^{p-1}, \tag{11}$$

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

II- The diophantine equation

$$x^2+7=py^{(p-1)/2},\ p\equiv 1(\bmod 4) \tag{12}$$

has no solution in rational x and y such that $y=\dfrac{Y}{t}$ 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

$$(X, Q)=(Y,T)=1. \tag{13}$$

Put

$$n=\begin{cases}0, & if\quad p\equiv 3(\bmod 4)\\ 1, & if\quad p\equiv 1(\bmod 4).\end{cases}$$

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

$$X^2T^{\frac{p-1}{2^n}}+7Q^2T^{\frac{p-1}{2^n}}=pQ^2Y^{\frac{p-1}{2^n}}. \tag{14}$$

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

$$T^{\frac{p-1}{2^n}}\equiv 0(\bmod Q^2). \tag{15}$$

In the same way, we get

$$pQ^2 \equiv 0 (\bmod T^{\frac{p-1}{2^n}}). \quad (16)$$

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

$$X^2 + 7T^{\frac{p-1}{2^n}} = pY^{\frac{p-1}{2^n}}. \quad (17)$$

So it follows that

$$(X, p)=(T,p)=(X,T)=(Y,T)=(X, Y)=(X, 7)=1.$$

Rewrite equation (17) as

$$\left(X + T^{\frac{p-1}{2^{n+1}}} i\sqrt{7}\right)\left(X - T^{\frac{p-1}{2^{n+1}}} i\sqrt{7}\right) = pY^{\frac{p-1}{2^{n+1}}}. \quad (18)$$

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 $\mathbb{Q}(i\sqrt{7})$. Since the ring $\mathbb{Q}(i\sqrt{7})$ is a unique factorization domain it follows that there exist four integers *A*, *B*, *s*, *v* with $A \equiv B (\bmod 2), s \equiv v (\bmod 2)$ and two units ±1 such that

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

where $p = \dfrac{A^2 + 7B^2}{4}$.

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

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

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

$$2^{\frac{p-1}{2^n}+1} T^{\frac{p-1}{2^{n+1}}} B^{\frac{p-1}{2^n}} \equiv BU^{\frac{p-1}{2^n}} (\bmod p).$$

Raising both sides of the last congruence to the power 2^{n+1}, by Fermat's little theorem we get

$$2^{2^{n+1}} \equiv B^{2^{n+1}} (\bmod p), \quad n \in \{0,1\}.$$

For *n*=1, we get

$$(B^2 - 4)(B^2 + 4) \equiv 0 (\bmod p).$$

• If $B^2 - 4 \equiv 0 (\mathrm{mod}\, p)$, 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 $B^2 + 4 \equiv 0 (\mathrm{mod}\, p)$, then $B^2 = -4 + k_1 p \geq 0$ for some integer k_1, and we get $4p=A^2-28+7pk_1$, 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 $B^2 = -4+p$,

and we get p=5. Hence from equation (3) and (4) we obtain $x^2 = 3 (\mathrm{mod}\, 5)$, 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

$$x^2+11^{2k+1}=y^n, \quad n \geq 3,\ k \geq 0, \tag{20}$$

has only three families of solutions and these solutions are

$$(x, y, k, n) = (4.\ 11^{3M},\ 3.\ 11^{2M},\ 3M, 3),$$

$$(58.\ 11^{3M}, 15.\ 11^{2M},\ 3M, 3),\ (9324.\ 11^{3M}, 443.\ 11^{2M}, 3M, 3).$$

Moreover when n=3, (x, y)=1 and $k \not\equiv 1 (\mathrm{mod}\, 3)$, the equation may have a solution given by $x = 8a^3 - 3a$ where a is an integer satisfies $a = \sqrt{\dfrac{11^{2k+1}+1}{3}}$.

Proof

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

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

So we shall suppose $k > 0$.

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

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

$$x + 11^k \sqrt{-11} = (a + b\sqrt{-11})^3. \tag{21}$$

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

Or

$$x + 11^k \sqrt{-11} = \left(\frac{a + b\sqrt{-11}}{2}\right)^3, \tag{22}$$

where $y=\dfrac{a^2+11b^2}{4}$ and $a\equiv b\equiv 1 \pmod 2$.

On equating the imaginary parts in equation (21) we get

$$\pm 11^k = b(3a^2-11b^2). \tag{23}$$

From (23) we deduce that $b=11^l,\ 0\le l\le k$, so (23) becomes

$$\pm 11^{k-l} = 3a^2-11^{2l+1}. \tag{24}$$

Equation (24) is impossible modulo 11, unless $l = k$, that is

$$\pm 1 = 3a^2-11^{2k+1}. \tag{25}$$

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

So, the equation (20) may have solution when n=3 and $k\not\equiv 1 \pmod 3$

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

Now we equating the imaginary parts in (23) and we get

$$8.11^k=b(3a^2\text{-}11b^2). \tag{26}$$

We have two cases:

i. If $b=\pm 11^l$ where $0\le l<k$, then the equation (26) is impossible modulo 11.

ii. If $b=\pm 11^k$, then the equation (26) becomes $8=3a^2\text{-}11^{2k+1}$.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

$$\left.\begin{aligned} y^2+x&=11^{2k+1},\\ y^2-x&=1.\end{aligned}\right\}$$

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, $11|x$ then $x=11^sX$ and $y=11^tY$ such that $s, t>0$ and $(X, 11)=(Y, 11)=1$. Equation (20) becomes

$$11^{2s}X^2+11^{2k+1}=11^{nt}Y^n, \tag{27}$$

We have two cases:

(1) If $2s=nt$, then from (27) we get

$$X^2+11^{2(k-s)+1}=Y^n,$$

this equation has solution when n=3 and either k-s=0 or k-s=1, since $2s=3t$ then $3|s$. Let $s=3M$ then $t=2M$, hence either $k=3M$ or $k=3M+1$.

So equation (20) has three families of solution

$(x,y,k,n)=(4.11^{3M},3.11^{2M},3M,3)$, $(58.\ 11^{3M},15.\ 11^{2M},3M,3)$,

$$(9324.\ 11^{3M}, 443.\ 11^{2M}, 3M+1, 3).$$

(2) If $2k+1=nt$ then equation (27) become

$$11(11^{s-k-1}X)^2+1=Y^n,$$

which has no solution [8].◊

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

Theorem4

If p an odd prime such that $p\not\equiv 5(mod\,8)$ and $(h,p)=1$ where h is the class number of the field $\mathbb{Q}(\sqrt{-11p})$, then the diophantine equation

$$px^2+11^{2k+1}=y^p,\ p>11,$$

has no solution in integers x and y.◊

References

[1] S. Ramanujan, "Collected papers of Ramanujan", Cambridge univ. press, Cambridge, (1927).

[2] T. Nagell, "The diophantine equation $x^2+7=2^n$ ", Nordisk. Mat. Tidsker, 30, 62-64, *Ark. Mat*., 4(1960), 185-187.

[3] Y. Bugeaud and T. Shorey, "On the number of solutions of the generalized Ramanujan-Nagell equation", *J. Reine Angew. Math.,* 539(2001), 55-74.

[4] S. Siksek and J. Cremona, "On the diophantine equation $x^2+7=y^m$", Acta Arith.109 (2003), 143-149.

[5] F. S. Abu Muriefah, " On the diophantine equation $px^2+q^{2k}=y^p$" , J. Number Theory, 90 (2008), 1-6.

[6] F. S. Abu Muriefah, F. Luca and A. A. Togbé, "On the diophantine equation $x^2+5^a.13^b=y^n$", Glasg. Math. J., 50(2008), 175-181.

[7] Y. Bilu, G. Hanrot and P. M. Voutier, "Existence of primitive divisor of Lucas and Lehmer numbers", J. *Reine Angew. Math*., 539 (2001), 75-122.

[8] W. Ljunggren, "Einige bemerkungen uber die darstellung ganzer zahlen durch binary kubische formen mite positive diskriminante", Acta Math., 75 (1942),1-21.

[9] E. Demirpolat and S. Cenberci, "On the diophantine equation $x^2+11^{2k+1}=y^n$", *Internat. Math. Forum*, 4(2009), 277-280.

[10] J. H. E. Cohn, "The diophantine equation $x^2+C=y^n$", Acta Arith., 65 (1993), 367-381.

[11] S. A. Arif and F. S. Abu Muriefah," On the diophantine equation $x^2+q^{2k+1}= y^n$ ", J. Number Theory, 95 (2002), 95-100.

[12] O. Korhonen,"On the diophantine equation $Cx^2+D=y^n$", Acta Univ. Oulu. Ser. Asci. Rerum. Natur. Math., 25 (1981), 9-17.

[13] L. J. Mordell, "Diophantine equations", *Academic press, London*, (1969).