TAMKANG JOURNAL OF MATHEMATICS
Volume 31, Number 1, Spring 2000

ON THE DIOPHANTINE EQUATION $px^2 + 3^n = y^p$

FADWA S. ABU MURIEFAH

Abstract. Let p be a prime. In this paper we prove that: (1) the equation $px^2 + 3^{2m} = y^p$, $p \not\equiv 7(\bmod 8)$ has no solutions in positive integers (x, y, p) with $\gcd(3, y) = 1$. (2) if $3|y$ then the equation has at most one solution when $p = 3$ and for $p > 3$ it may have a solution only when $p \equiv 2(\bmod 3)$ and $\gcd(p, m) = 1$. (3) the equation $px^2 + 3^{2m+1} = y^p$, $p \not\equiv 5(\bmod 8)$, has a solution only when $p = 3$, and this solution exists only when $m = 3 + 3M$, and is given by $x = 46.3^{3M+1}$, $y = 13.3^{2M+1}$.

1. Introduction

Let Z, Q, N be the sets of integers, rational numbers and positive integers respective. Let p be an odd prime, in [5] Maohua proved two theorems concerning the equation $px^2+2^n = y^p$. In this paper we consider the same kind of diophantine equation $px^2+3^n = y^p$. In the begining we will consider n even, say $n = 2m$, where $m \in N$ and we prove the following two results:

Theorem 1. *The diophantine equation*

$$px^2 + 3^{2m} = y^p, \qquad p \not\equiv 7(\bmod 8) \tag{1}$$

has no solution with gcd$(3, y) = 1$.

Theorem 2. *Equation* (1) *has at most one solution when* $p = 3$ *and this solution exists only when* $2m = 8 + 6M$, *and then* $x = 10.3^{3M+1}$, $y = 7.3^{2M+1}$. *If* $p > 3$ *then equation* (1) *may have a solution only when* $3|y$, $p = 2(\bmod 3)$ *and gcd*$(p, m) = 1$.

For n odd we get the following result

Theorem 3. *The diophantine equation*

$$px^2 + 3^{2m+1} = y^p, \qquad p \not\equiv 5(\bmod 8), \quad m \in N \tag{2}$$

has a solution only when $p = 3$ *and* $m = 3 + 3M$, *and this solution is given by* $x = 46.3^{3M+1}$, $y = 13.3^{2M+1}$.

Received February 24, 1999; revised November 11, 1999.
1991 *Mathematics Subject Classification.* 11D41.
Key words and phrases. Diophantine equation, Legendre symbol.

2. Lemmas

Lemma 1 (Nagell [6]). *Let n be an odd integer ≥ 3, and let $A \in N$, be an odd square free. If the class number of the field $Q(\sqrt{-A})$ is not divisible by n, then the diophantine equation $Ax^2 + 1 = y^n$, has no solutions in positive integers x and y for y odd.*

Lemma 2 (Arif and Abu Muriefah [1]). *The diophantine equation $x^2 + 3^k = y^n$, where k is odd and $n \geq 3$, has only one solution given by $k = 5 + 6K$, $x = 10.3^{3K}$, $y = 7.3^{2K}$ and $n = 3$.*

Lemma 3 (Abu Muriefah and Arif [2]). *The diophantine equation $x^2 + 3^{2k} = y^n$, where $n \geq 3$, has only one solution give by $k = 2 + 3K$, $x = 46.3^{3K}$, $y = 13.3^{2K}$ and $n = 3$.*

3. Proofs

Proof of Theorem 1. By Lemma 1, it is sufficient to prove the case $m \in N$. Let (x, y, p) be a solution of (1) with $\gcd(y, 3) = 1$, then $p > 3$. If y is even then from (1) we get $p \equiv 7 (\bmod 8)$, so we conclude that y is odd. Since the class number of the field $Q(\sqrt{-p})$ is less than p, we factorize equation (1) to obtain

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

where $a, b \in Z$ and $y = a^2 + pb^2$ is odd, so a and b have opposite parity. On equating the real parts we get

$$3^m = a \sum_{r=0}^{\frac{p-1}{2}} \binom{p}{2r} a^{p-2r-1}(-pb^2)^r \tag{3}$$

From (3) we deduce that $a | 3^m$.

If $a = \pm 1$, then $y = 1 + pb^2$, but $\gcd(3, y) = 1$, so $pb^2 \equiv 0, 1 (\bmod 3)$. If $pb^2 \equiv 0 (\bmod 3)$ then equation (3) is impossible modulo 3. So $pb^2 \equiv 1 (\bmod 3)$ and since $a^2 \equiv 1 (\bmod 3)$ therefore the right hand side in (3) becomes

$$\sum_{r=0}^{\frac{p-1}{2}} \binom{p}{2r+1} (-1)^r = \frac{(1+i)^p - (1-i)^p}{2i} = 2^{p/2} \text{ Sin } \frac{p\pi}{4} \neq 0$$

where the left hand side is congruent to 0 modulo 3, which is a contradiction. So $a = \pm 3^j$, $0 < j \leq m$, and $\gcd(3, b) = 1$, where b is even. Then considering (3) modulo 3 we get $j = m$, hence equation (3) becomes

$$\pm 1 = \sum_{r=0}^{\frac{p-1}{2}} \binom{p}{2r} 3^{m(p-2r-1)}(-pb^2)^r.$$

Then $1 \equiv 3^{m(p-1)} (\bmod p)$ and so the lower sign is impossible. That is

$$1 = \sum_{r=0}^{\frac{p-1}{2}} \binom{p}{2r} 3^{m(p-2r-1)} (-pb^2)^r, \tag{4}$$

Now considering (4) modulo 3 we get $p \equiv 1 (\bmod 12)$, say $p = 1+3^k u$, where $\gcd(u, 3) = 1$, $4|u$ and $k \geq 1$. Then from (4) we obtain

$$\begin{aligned} 1 &\equiv \binom{p}{3} 3^{2m} (-pb^2)^{\frac{p-3}{2}} + pb^{p-1}(-p)^{\frac{p-1}{2}} (\bmod 3^{k+1}) \\ &\equiv \frac{p(p-2)}{2} \cdot 3^{k+2m-1} u (-pb^2)^{\frac{p-3}{2}} + pb^{p-1}(-p)^{\frac{p-1}{2}} (\bmod 3^{k+1}), \end{aligned}$$

since $m \geq 1$, therefore $k + 2m - 1 \geq k + 1$, so from the above we obtain

$$1 \equiv pb^{p-1}(-p)^{\frac{p-1}{2}} (\bmod 3^{k+1}).$$

Hence $p \equiv 1 (\bmod 3^{k+1})$ which is a contradiction.

Proof of Theorem 2. Let $p = 3$, then of course $m > 1$, and 3 divides both x and y, say $x = 3x'$ and $y = 3y'$ then dividing (1) by 27, we get

$$x'^2 + 3^{2m-3} = y'^3, \tag{5}$$

from Lemma 2, equation (5) has a unique solution given by $2m-3 = 5+6M$, $x' = 10.3^{3M}$ and $y' = 7.3^{2M}$.

So when $p = 3$, equation (1) has a solution only if $2m = 8 + 6M$ and the unique solution is given by $x = 10.3^{3M+1}$, $y = 7.3^{2M+1}$.

Now let $p > 3$, then from Theorem 1, it is sufficient to suppose $3|y$, so let $x = 3^u X$, $y = 3^\nu.Y$ where $u > 0$, $\nu > 0$ and $\gcd(3, X) = \gcd(3, Y) = 1$. Then (1) becomes

$$p(3^u X)^2 + 3^{2m} = 3^{\nu p} Y^p \tag{6}$$

We have three cases:-

1- $p\nu > 2u = 2m$. Then cancelling 3^{2m} in (6) we get

$$pX^2 + 1 = 3^{\nu p - 2m} Y^p \tag{7}$$

equation (7) implies that $p \equiv 2 (\bmod 3)$. Let $p|m$, then (7) becomes

$$pX^2 + 1 = (3^{\nu - 2m'} Y)^p$$

and this equation is known to have no solution (Lemma 1).

2- $2u > 2m = \nu p$. Then cancelling 3^{2m} in (6) we get $p(3^{u-m}X)^2 + 1 = Y^p$. This equation from lemma 1 has no solution.

3- $3m > 2u = p\nu$. Then

$$pX^2 = 3^{2(m-u)} = Y^p,$$

and this equation has no solution from Theorem 1.

Summarizing the above two theorems we get

Conclusion

The diophantine equation $px^2 + 3^{2m} = y^p$, $p > 3$ may have a solution only when $p \equiv 23(\bmod 24)$, $\gcd(p, m) = 1$ and $3|y$.

Proof of Theorem 3. Let (x, y, p) be a solution of (2) with $\gcd(y, 3) = 1$, then $p > 3$. If y even then $p \equiv 5(\bmod 8)$, so we conclude that y is odd. Since the class number of the field $Q(\sqrt{-3p})$ is less than p. Then, according to the analysis in [4], we have

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

where $a, b \in Z$ and $y = 3a^2 + pb^2$ is odd, so a and b have opposite parity. On equating the coefficient of $\sqrt{3}$ in both sides, we get

$$3^m = a\sum_{r=0}^{\frac{p-1}{2}} \binom{p}{2r} (3a^2)^{\frac{p-2r-1}{2}}(-pb^2)^r \tag{8}$$

From (8) we deduce that $a = \pm 3^m$, hence $\gcd(3, b) = 1$, and b even. So dividing (8) by 3^m we get

$$\pm 1 = \sum_{r=0}^{\frac{p-1}{2}} \binom{p}{2r} (3^{2m+1})^{\frac{p-2r-1}{2}}(-pb^2)^r \tag{9}$$

If the negative sign holds in (9), then

$$-1 = \sum_{r=0}^{\frac{p-1}{2}} \binom{p}{2r} (3^{2m+1})^{\frac{p-2r-1}{2}}(-pb^2)^r \tag{10}$$

Now considering (10) modulo 4, we get $-1 \equiv (3^{2m+1})^{\frac{p-1}{2}}(\bmod 4)$, so $p \equiv 3(\bmod 4)$. Also modulo p we get $-1 \equiv (3^{2m+1})^{\frac{p-1}{2}}(\bmod p)$, that is $-1 \equiv (3)^{\frac{p-1}{2}}(\bmod p)$. But Legendre symbol $(3/p) = -1$ if and only if $p \equiv 5, 7(\bmod 12)$, and since $p \equiv 3(\bmod 4)$, we get $p \equiv 7(\bmod 12)$. Now let $p = 1 + 2.3^k u$, where $\gcd(u, 6) = 1$ and $k \geq 1$, then from (10) we get

$$-1 \equiv pb^{p-1}(-p)^{\frac{p-1}{2}}(\bmod 3^{k+1}).$$

But $\gcd(3, b) = 1$, so $-1 \equiv p(-p)^{\frac{p-1}{2}}(\bmod 3^{k+1})$ hence $1 \equiv (p)^{\frac{p+1}{2}}(\bmod 3^{k+1})$, squaring this equation we get $1 \equiv (p)^{2+2.3^k u}(\bmod 3^{k+1})$ and this is implies that $1 \equiv p^2(\bmod 3^{k+1})$, which is a contradiction.

So in eq. (9) only the positive sign holds, that is

$$1 = \sum_{r=0}^{\frac{p-1}{2}} \binom{p}{2r} (3^{2m+1})^{\frac{p-2r-1}{2}} (-pb^2)^r \tag{11}$$

considering eq. (11) modulo 4, we obtain $p \equiv 1 (\mathrm{mod}\, 4)$. Also modulo p, eq (11) implies $1 \equiv (3)^{\frac{p-1}{2}} (\mathrm{mod}\, p)$. But Legendre symbol $(3/p) = 1$ if and only if $p \equiv 1, 11 (\mathrm{mod}\, 12)$. Since $p \equiv 1 (\mathrm{mod}\, 4)$ we conclude that $p \equiv 1 (\mathrm{mod}\, 12)$, and by much the same argument as the proof of Theorem 1, eq. (11) is impossible. So eq. (2) has no solution when $\gcd(3, y) = 1$.

Let $p = 3$, then of course 3 divides both x and y, say $x = 3x'$ and $y = 3y'$ then dividing (2) by 27, we get

$$x'^2 + 3^{2(m-1)} = y'^3, \tag{12}$$

If $m = 1$, eq. (12) has no solution [3]. So $m > 1$, and from Lemma 3, equation (12) has a unique solution given by $m - 1 = 2 + 3M$, $x' = 46.3^{3M}$ and $y' = 13.3^{2M}$. So when $p = 3$, equation (2) has a solution only if $m = 3 + 3M$ and the unique solution is given by $x = 46.3^{3M+1}$, $y = 13.3^{2M+1}$.

Now let $p > 3$, and suppose $3|y$, so $x = 3^u X$, $y = 3^\nu .Y$ where $u > 0$, $\nu > 0$ and $\gcd(3, X) = \gcd(3, Y) = 1$. Then (2) becomes

$$p(3^u X)^2 + 3^{2m+1} = 3^{\nu p} Y^p \tag{13}$$

We have three cases:-

1- $2m + 1 = \min(p\nu, 2u, 2m + 1)$. Then cancelling 3^{2m+1} in (13) we get

$$3p(3^{u-m-1} X)^2 + 1 = 3^{\nu p - 2m - 1} Y^p \tag{14}$$

equation (14) modulo 3, implies $p\nu - 2m - 1 = 0$, so $3p(3^{u-m-1}X)^2 + 1 = Y^p$, and this equation is known to have no solution (Lemma 1).

2- $2u = \min(p\nu, 2u, 2m + 1)$. Then cancelling 3^{2u} in equation (13) we get $pX^2 + 3^{2(m-u)+1} = 3^{p\nu - 2uY^p}$. Considering this equation modulo 3, we get $p\nu - 2u = 0$, then $pX^2 + 3^{2(m-u)+1} = Y^p$, with $\gcd(3, Y) = 1$ and this equation has no solution from the first part of this proof.

3- $p\nu = \min(p\nu, 2u, 2m + 1)$. Then

$$p3^{2u - p\nu} X^2 + 3^{2m+1-p\nu} = Y^p,$$

and this equation is possible only if $2u - p\nu = 0$ or $2m + 1 - p\nu = 0$, and these two cases have been discussed before.

References

[1] S. A. Arif and Fadwa S. Abu Muriefah, *The diophantine equation* $x^2 + 3^m = y^n$, Inter. J. Math. and Math. Sci. Vol., **21**(1998), 619-620.

[2] Fadwa S. Abu Muriefah and S. A. Arif, *On a diophantine equation*, Bull. Austral. Math. Soc., **57**(1998), 189-198.

[3] V. A. Lebesgue, *Sur I'impossibilities en nombres entieers de I'equation* $x^m = 1 + y^2$, Von. Ann. Des. Math., **9**(1850), 178-181.

[4] W. Ljunggren, *On a diophantine equation*, Norske. Vid. Selsk. Forh. Trondheim, **18**(1945), 125-128.

[5] L. Maohua, *On the diophantine equation* $px^2 + 2^n = y^p$, Proc. of the Amer. Math. Soc., **123**(1995), 321-326.

[6] T. Nagell, *Contributions to the theory of a category of diophantine equations of the second degree with two unknowns*, Nova. Acta Soc. Sci. Upsal. Ser 4, **16**(1955), 1-38.

Mathematics Department, Girls College of Education, P. O. Box 60561, Riyadh-11555, Saudi Arabia.