Indian J. pure appl. Math., **36**(8) : 431-439, August 2005

ON THE DIOPHANTINE EQUATION $x^2+3=py^n$

KH. HESSAMI PILEHROOD* AND T. HESSAMI PILEHROOD**

**Institute for Studies in Theoretical Physics and Mathematics (IPM), Tehran, Iran*
E-mail: hessamik@ipm.ir, hessamit@ipm.ir

(*Received* 13 *July* 2004; *after final revision* 30 *August* 2005; *accepted* 12 *November* 2005)

Let p be an odd prime such that $p-3$ is not a perfect square. In this paper we prove that the equation $x^2+3=py^{p-1}$ has no solutions in rational numbers x, y. The proof depends on the unique factorization in the ring of algebraic integers of $\mathbf{Q}(\sqrt{-3})$ and on certain congruence arguments. Furthermore, the equations $x^2+3=py^{\frac{p-1}{2}}$ and $x^2+3=py^6$ in rationals x, y are also considered.

Key Words: Diophantine Equation; Quadratic Field; Prime

1. INTRODUCTION

In the present paper we prove two results.

***Theorem* 1.1** — *Suppose p is an odd prime and $p-3$ is not a perfect square. Then a) the equation*

$$x^2+3=py^{p-1} \qquad \ldots (1.1)$$

has no solutions in rational numbers x, y.

b) In particular, if a prime $p \equiv 1 \pmod 4$, then the equation

$$x^2+3=py^{\frac{p-1}{2}} \qquad \ldots (1.2)$$

has no solutions in rational numbers x, y.

***Theorem* 1.2** — *Let $p > 3$ be a prime. If the equation*

$$x^2+3=py^6 \qquad \ldots (1.3)$$

***Present address*: Mathematics Department, Shahrekord University, Shahrekord, P. O. Box 115, Iran

This research was in part supported by a grant from IPM (No. 83110021 and 83110020).

is soluble in rational numbers x, y, then there exist positive integers A, B such that $p = A^2 + 3B^2$, *B is a cubic residue modulo p, and either* $B \equiv 0 \pmod 9$ *or* $B \equiv \pm 1 \pmod 9$.

Remark 1.3 : In Theorem 1.1, for primes p that can be written as the sum $p = a^2 + 3$, $a \in \mathbb{Z}$, one already has a trivial solution for equation (1.1) just taking $y = 1$.

When $p = 5$, eq. (1.2) reduces to $x^2 + 3 = 5y^2$, for which it is known that it has no rational solutions by Legendre's theorem (see. [2, p.269]).

Equations similar to (1.1), (1.2) were considered in [1], [5], where it was proved that the equation $x^2 + 3 = y^n$ is not solvable in positive integers $x, y, n \geq 3$, and the complete set of positive integer solutions (x, q, m, n) for the equation $x^2 = 4q^m - 4q^n + 1$ and in particular for the equation $x^2 + 3 = 4q^m$ was found.

Note that eqs. (1.1), (1.2), (1.3) are special cases of the equation $ax^2 + bx + c = dy^n$ with $b = 0$, $acd \neq 0$ and $n \geq 3$, which has only a finite number of integer solutions by Landau's, Ostrowski's [4] and Thue's [8] results (see [6]). Moreover it follows from ([7, Theorem 12.2]) that these solutions are effectively computable, in the usual sense, i.e., that it is possible to find all them by considering all values of say x, up to some bound $M(a, b, c, d)$ which can be explicitly calculated. In practice, the power of that method is limited by the huge size of the M that arises, but it does provide a theoretical method for solving such problems.

Note also that for $p \geq 11$, by Faltings' theorem [3, p. 269], eqs. (1.1), (1.2), considered as curves of genus at least two have finitely many rational solutions.

The following lemma is needed for the sequel.

Lemma 1.4 — Let $V, S \in \mathbb{Z}$. If 3 does not divide $V(S^2 - V^2)$, then $S \equiv 0 \pmod 3$.

Proof : If $(S, 3) = 1$, then $S^2 \equiv 1 \pmod 3$. Since for any integer V, either $V \equiv 0 \pmod 3$ or $V^2 \equiv 1 \pmod 3$, we conclude that $V(S^2 - V^2) \equiv 0 \pmod 3$. Hence, we obtain a contradiction, from which the lemma follows. □

2. Proof of Theorem 1.1

Proof : Assume that $x = X/Q, y = Y/T$ is a solution of (1.1) or (1.2) for some integers X, Y, Q, T

with $Q \geq 1, T \geq 1$ and

$$(X, Q) = (Y, T) = 1 \qquad \text{... (2.1)}$$

Put

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

Then eqs. (1.1) and (1.2) can be written in the form

$$X^2 T^{\frac{p-1}{2^n}} + 3Q^2 T^{\frac{p-1}{2^n}} = pQ^2 Y^{\frac{p-1}{2^n}} \qquad \text{... (2.2)}$$

or

$$X^2 T^{\frac{p-1}{2^n}} = Q^2 \left(pY^{\frac{p-1}{2^n}} - 3T^{\frac{p-1}{2^n}} \right),$$

whence taking into account (2.1), we get

$$T^{\frac{p-1}{2^n}} \equiv 0 \pmod{Q^2}. \qquad \text{... (2.3)}$$

In the same way, from (2.1) and the relation

$$pQ^2 Y^{\frac{p-1}{2^n}} = T^{\frac{p-1}{2^n}} (X^2 + 3Q^2)$$

we have

$$pQ^2 \equiv 0 \left(\bmod\ T^{\frac{p-1}{2^n}} \right) \qquad \text{... (2.4)}$$

Since $(p-1)/2^n$ is even, it follows from (2.3) and (2.4) that $Q^2 = T^{\frac{p-1}{2^n}}$. Then from (2.2) we deduce that

$$X^2 + 3T^{\frac{p-1}{2^n}} = pY^{\frac{p-1}{2^n}} \qquad \text{... (2.5)}$$

whence it follows that

$$(X, p) = (T, p) = (X, T) = (Y, T) = (X, Y) = (X, 3) = 1 \qquad \text{... (2.6)}$$

Rewrite equation (2.5) as

$$\left(X + i\sqrt{3}\,T^{\frac{p-1}{2^{n+1}}}\right)\left(X - i\sqrt{3}\,T^{\frac{p-1}{2^{n+1}}}\right) = pY^{\frac{p-1}{2^n}}. \qquad \dots (2.7)$$

It is easy to see from (2.6) that the two algebraic integers appearing in the left-hand side of eq. (2.7) are coprime in the ring of algebraic integers of $\mathbb{Q}[i\sqrt{3}]$.

Indeed, if we put $\delta = \left(X + i\sqrt{3}\,T^{\frac{p-1}{2^{n+1}}},\ X - i\sqrt{3}\,T^{\frac{p-1}{2^{n+1}}}\right)$, then $\delta \mid 2X, \delta \mid 2i\sqrt{3}\,T^{\frac{p-1}{2^{n+1}}}$. According to $(X, T) = 1$ we may take $\delta = 1, 2, i\sqrt{3}, 2i\sqrt{3}$. It is obvious that the case $2 \mid \delta$ is impossible by $(X, T) = 1$. We cannot also have $\delta = i\sqrt{3}$. For then $X \equiv 0 \pmod{i\sqrt{3}}$ $X \equiv 0 \pmod 3$ and we have a contradiction with $(X, 3) = 1$. So $\delta = 1$.

Since the ring of algebraic integers $\mathbb{Q}\left[\frac{1+i\sqrt{3}}{2}\right]$ of $\mathbb{Q}[i\sqrt{3}]$ is euclidean, it follows that there exist four integers a, b, S, V with $a \equiv b \pmod 2$, $S \equiv V \pmod 2$ and a unit ε in $\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]$ such that

$$X + i\sqrt{3}\,T^{\frac{p-1}{2^{n+1}}} = \varepsilon \cdot \frac{a + i\sqrt{3}\,b}{2} \cdot \left(\frac{S + i\sqrt{3}\,V}{2}\right)^{\frac{p-1}{2^n}}$$

Since there are just six units, $\pm 1, \pm\omega, \pm\omega^2$, where $\omega = \exp(2\pi i/3) = (-1 + i\sqrt{3})/2$, it follows that these can be absorbed into the fraction $(a + i\sqrt{3}b)/2$. Thus for some rational integers A and B with the same parity

$$X + i\sqrt{3}\,T^{\frac{p-1}{2^{n+1}}} = \frac{A + i\sqrt{3}\,B}{2} \cdot \left(\frac{S + i\sqrt{3}\,V}{2}\right)^{\frac{p-1}{2^n}}, \qquad \dots (2.8)$$

where

$$p = \frac{A^2 + 3B^2}{4}. \qquad \dots (2.9)$$

Multiplying both parts of (2.8) by $2^{\frac{p-1}{2^n}+1} \cdot B^{\frac{p-1}{2^n}}$, we get

$$2^{\frac{p-1}{2^n}+1}\left(XB^{\frac{p-1}{2^n}} + i\sqrt{3}\,T^{\frac{p-1}{2^{n+1}}}B^{\frac{p-1}{2^n}}\right)$$

$$= (A + i\sqrt{3}B)\,(SB + AV - (A - i\sqrt{3}B)V)^{\frac{p-1}{2^n}}$$

$$= (A + i\sqrt{3}B)\left(U^{\frac{p-1}{2^n}} + (A - i\sqrt{3}B)(K + i\sqrt{3}R)\right)$$

for some U, K, R in $\mathbb{Z}$. Comparing imaginary parts and taking into account that $p \mid A^2 + 3B^2$, we obtain

$$2^{\frac{p-1}{2^n}+1} \cdot T^{\frac{p-1}{2^{n+1}}} \cdot B^{\frac{p-1}{2^n}} \equiv B \cdot U^{\frac{p-1}{2^n}} \pmod p.$$

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

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

This implies that

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

If $B^2 - 4 \equiv 0 \pmod p$, then $B^2 = 4 + pk \geq 0$ for some integer k. Now taking into account (2.9), we have $4p = A^2 + 3B^2 = A^2 + 12 + 3pk$ and hence, $0 \leq k \leq 1$.

For $k = 0$, we have $B^2 = 4$ and therefore,

$$p = \frac{A^2 + 3B^2}{4} = \left(\frac{A}{2}\right)^2 + 3,$$

i.e., $p - 3$ is a perfect square and we obtain a contradiction.

If $k = 1$, then $B^2 = 4 + p$ and from (2.9) we have $4p = A^2 + 12 + 3p$ or $p = A^2 + 12 = B^2 - 4 = (B - 2)(B + 2) > 12$ that is impossible since p is a prime.

If $B^2 + 4 \equiv 0 \pmod p$, then $B^2 = -4 + pk_1 \geq 0$ for some k_1 in $\mathbb{Z}$. Using (2.9), we get $4p = A^2 + 3B^2 = A^2 - 12 + 3pk_1$ or $4p - 3pk_1 + 12 \geq 0$ that implies $4 - 3k_1 \geq -12/p \geq -12/5$. Hence, $2 \geq k_1 \geq 1$.

If $k_1 = 2$, then $B^2 = -4 + 2p$ and $4p = A^2 + 3B^2 = A^2 - 12 + 6p$ or $0 = A^2 - 12 + 2p \geq A^2 - 2$. This implies that $A = 0$ or $A = 1$. For $A = 0$, we have $0 = -12 + 2p$ and this contradicts that p is a prime. For $A = 1$, we have $0 = -11 + 2p$ that is impossible. Hence, the unique case $k_1 = 1$ remains. Therefore, $B^2 = -4 + p$ and $4p = A^2 + 3B^2 = A^2 - 12 + 3p$ or $p = A^2 - 12 = B^2 + 4$. The last relation is equivalent to the following

$$A^2 - B^2 = (A - B)(A + B) = 16,$$

whence it follows $B = \pm 3, A = \pm 5, n = 1, p = 13$. For this case, from (2.8), we get

$$X + i\sqrt{3}\,T^3 = \frac{\pm 5 \pm 3i\sqrt{3}}{2}\left(\frac{S + i\sqrt{3}\,V}{2}\right)^6$$

so that

$$128\,X + 128\,i\sqrt{3}\,T^3 = (\pm 5 \pm 3i\sqrt{3})\,(S_1 + i\sqrt{3}\,V_1)^3$$

$$= (\pm 5 \pm 3i\sqrt{3})\left(S_1^3 - 9S_1V_1^2 + i\left(3S_1^2V_1 - 3V_1^3\right)\sqrt{3}\right), \quad \ldots (2.10)$$

where $S_1 + i\sqrt{3}\,V_1 = (S + \sqrt{3}\,V)^2 = S^2 - 3V^2 + 2i\sqrt{3}\,SV$. Comparing imaginary parts of (2.10), we obtain

$$128\,T^3 = \pm 3\left(S_1^3 - 9S_1V_1^2\right) \pm 15\left(S_1^2V_1 - V_1^3\right).$$

This implies that $T = 3T_1$ for some T_1 in $\mathbb{Z}$ and therefore,

$$128 \cdot 9T_1^3 = \pm\left(S_1^3 - 9S_1V_1^2\right) \pm 5V_1\left(S_1^2 - V_1^2\right),$$

whence, by Lemma 1.4, we conclude that $S_1 \equiv 0 \pmod 3$ and hence, $V_1 \equiv 0 \pmod 3$. Comparing real parts of (2.10), we conclude that $X \equiv 0 \pmod 3$, so that $3 \mid (X, T)$, contradicting $(X, T) = 1$.

This completes the proof of Theorem 1.1. □

3. Proof of Theorem 1.2.

Proof : Let $(x, y) = (X/Q, Y/T)$ be a rational solution of (1.3), where X, Y, Q, T are integers, $Q > 0, T > 0$, and

$$(X, Q) = (Y, T) = 1 \quad \ldots (3.1)$$

Then from (1.3) we have

$$X^2 T^6 + 3Q^2 T^6 = pQ^2 Y^6, \qquad \text{... (3.2)}$$

whence it follows that

$$T^6 \equiv 0 \pmod{Q^2}, \quad pQ^2 \equiv 0 \pmod{T^6}.$$

Therefore,

$$T^6 = Q^2$$

and eq. (3.2) takes the form

$$X^2 + 3T^6 = pY^6. \qquad \text{... (3.3)}$$

Now it is readily seen from (3.1) and (3.3) that

$$(3, X) = (X, Y) = (T, X) = (X, p) = (T, p) = 1$$

and therefore the algebraic integers $X + i\sqrt{3}\,T^3, X - i\sqrt{3}\,T^3$ are coprime in the ring $\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]$

Arguing as above, we see that there exist rational integers A, B, S, U such that

$$X + i\sqrt{3}\,T^3 = \frac{A + i\sqrt{3}\,B}{2} \cdot \left(\frac{S + i\sqrt{3}\,U}{2}\right)^3, \qquad \text{... (3.4)}$$

$$p = \frac{A^2 + 3B^2}{4},$$

and

$$A \equiv B \pmod{2}, \qquad S \equiv U \pmod{2}. \qquad \text{... (3.5)}$$

Multiplying both sides of (3.4) by $16B^3$, we get

$$16XB^3 + 16\,i\sqrt{3}\,T^3B^3 = (A + i\sqrt{3}\,B)(SB + i\sqrt{3}\,UB)^3$$

$$= (A + i\sqrt{3}\,B)(SB + AU - (A - i\sqrt{3}\,B)\,U)^3.$$

Comparing imaginary parts and taking into account that $(p, T) = (p, B) = (p, 2) = 1$, we obtain

$$16\,T^3B^3 \equiv B \cdot (SB + AU)^3 \pmod{p},$$

whence it follows that $4B$ is a cubic residue modulo p.

In addition, from (3.4) we find

$$16\,T^3 = A\,(3S^2U - 3U^3) + B\,(S^3 - 9\,SU^2) \qquad \text{... (3.6)}$$

$$16\,X = A\,(S^3 - 9\,SU^2) + 9B\,(U^3 - S^2U). \qquad \text{... (3.7)}$$

Note that $(S, 3) = 1$. Otherwise, if $S \equiv 0 \pmod 3$, then, by (3.6), (3.7), we obtain $T \equiv 0 \pmod 3$ and $X \equiv 0 \pmod 3$. This gives a contradiction as $(T, X) = 1$. Since $(S, 3) = 1$, by Lemma 1.4, we conclude that 3 divides $U(S^2 - U^2)$. Then it follows from (3.6) that

$$-2T^3 \equiv BS^3 \pmod 9.$$

Since $(S, 3) = 1$, the last congruence implies that

$$\text{either } B \equiv 0 \pmod 9 \quad \text{or} \quad B \equiv \pm 2 \pmod 9. \qquad \text{... (3.8)}$$

To conclude the proof, it remains to note that A and B are even, i.e., $A = 2A_1$, $B = 2B_1$, where $A_1, B_1 \in \mathbb{Z}$, and therefore, $p = A_1^2 + 3B_1^2$; since $4B$ is a cubic residue modulo p, so is B_1, and congruences (3.8) take the form

$$\text{either } B_1 \equiv 0 \pmod 9 \quad \text{or} \quad B_1 \equiv \pm 1 \pmod 9.$$

Indeed, if by (3.5), S and U are both even, i. e., $S = 2S_1$, $U = 2U_1$ then from (3.6), (3.7) we have

$$2T^3 = 3AU_1\left(S_1^2 - U_1^2\right) + BS_1\left(S_1^2 - 9U_1^2\right) \qquad \text{... (3.9)}$$

$$2X = AS_1\left(S_1^2 - 9U_1^2\right) + 9BU_1\left(U_1^2 - S_1^2\right). \qquad \text{... (3.10)}$$

If $U_1 + S_1$ is odd, then (3.9), (3.10) imply that $2 \mid B$ and $2 \mid A$.

If $U_1 + S_1$ is even, then from (3.9), (3.10) we conclude that $2 \mid T$ and $2 \mid X$, contradicting $(X, T) = 1$.

If S and U are both odd, rewrite (3.6) in the form

$$16T^3 = B(S + AU/B)^3 - 3AU^3 - 9BSU^2 - 3SA^2U^2/B - A^3U^3/B^2,$$

or

$$16B^2T^3 = (BS + AU)^3 - 3AB^2U^3 - 9B^3SU^2 - 3BA^2SU^2 - A^3U^3.$$

If we replace $BS + AU$ by Z in the last relation, we obtain

$$Z^3 - 3(A^2 + 3B^2)ZU^2 + 2A(A^2 + 3B^2)U^3 = 16B^2T^3. \qquad \text{... (3.11)}$$

Taking into account that $A^2 + 3B^2 = 4p$, we conclude that Z is even, i.e., $Z = 2Z_1$, $Z_1 \in \mathbb{Z}$, and then (3.11) takes the form

$$Z_1^3 - 3pZ_1 U^2 + ApU^3 = 2B^2 T^2.$$

Since p and U are odd, it follows easily that A is even and therefore, by (3.5), B is even. This completes the proof of Theorem 1.2. □

REFERENCES

1. J. H. E. Cohn, The diophantine equation $x^2 + 3 = y^n$, *Glasgow Math. J.*, **35** (1993), 203-06.
2. E. Grosswald, *Topics from the theory of numbers*, 2. ed., Birkhäuser Boston, 1984.
3. M. Hindry and J. H. Silverman, *Diophantine geometry: an introduction*, Springer-Verlag New York, 2000.
4. E. Landau and A. Ostrowski, On the diophantine equation $ay^2 + by + c = dx^n$, *Proc. London Math. Soc.*, **19**(2) (1920), 276-80.
5. F. Luca, On the diophantine equation $x^2 = 4q^m - 4q^n + 1$, *Proc. American Math. Soc.*, **131**(5) (2002), 1339-45.
6. L. J. Mordell, *Diophantine equations*, Academic Press, London, 1969.
7. T. N. Shorey and Tijdeman, *Exponential Diophantine equations*, Cambridge University Press, 1986.
8. A. Thue, Über die Unlösbarkeit der Gleichung $ax^2 + bx + c = dy^n$ in grossen ganzen Zahlen x und y, *Arch. Math. Naturv. Kristiania*, Nr. 16, 34 (1917).