The Solution-free Diophantine Equation

\[ y^2 = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \]

R. Srikanth and S. Subburam

Mathematics Department
SASTRA University, Thanjavur-613 401, India
srikanth@maths.sastra.edu, ssubburam@maths.sastra.edu

Abstract

Let \( a_0, a_1, \ldots, a_n \) be integers. On \( a_0, a_1, \ldots, a_n \), we study some conditions under which the diophantine equation

\[ y^2 = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \]

has no integral solution \((x, y)\). Using this, we prove that some types of ternary exponential diophantine equations have no integral solution.

Mathematics Subject Classification: 11D25

Keywords: Diophantine equation, Legendre symbol, discriminant

1 Introduction

Consider the diophantine equation

\[ y^2 = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0, \tag{1} \]

where \( a_0, a_1, \ldots, a_n \) are integers. In 1969, Baker [2] proved that if \( n \geq 5 \) and \( a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \) is separable, then all integral solutions \((x, y)\) of equation (1) satisfy

\[ \max(|x|, |y|) \leq \exp \exp(n^{10n^3} H^{n^2}), \]

where \( H = \max\{|a_0|, |a_1|, \ldots, |a_n|\} \). In 1976, Sprindzuk [3] improved Baker’s bound showing that if \( a_n = 1 \) and \( f(x) \) has at least three simple zeros, then

\[ \max(|x|, |y|) \ll \exp(|D|^{(8+\epsilon)(6m^3+12m^2)}(\log H)^{1+\epsilon}), \epsilon > 0, \]

where \( D \) is the discriminant of \( a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \) and the positive constant implied by \( \ll \) only depends on \( \epsilon \) and \( m \) and is effectively computable.
In 2000, Szalay [5] produced an algorithm to find all integral solutions \((x, y)\) of equation (1) when \(n\) is multiple of 2, \(a_n = 1\) and \(a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0\) is not a perfect square over the rational field. In 2011, we simplified the algorithm of [5] in [4].

Our aim in this paper is to prove the following theorems.

**Theorem 1.1.** Consider equation (1). If \(a_0\) is prime \(\equiv 3(\text{mod} \ 4)\), \(a_1 = 0\) and if there exists an even positive integer \(k \leq n\) such that

\[
(i) \quad a_k = -1
\]

\[
(ii) \quad (a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0) + x^k \equiv 3(\text{mod} \ 4) \text{ for each integer } x.
\]

Then equation (1) has no integral solution \((x, y)\).

**Corollary 1.2.** The ternary exponential diophantine equation

\[
y^2 = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0
\]

with

\[
(1) \quad a_0 \text{ is prime } \equiv 3(\text{mod} \ 4)
\]

\[
(2) \quad a_1 = 0
\]

\[
(3) \quad a_2 = -1,
\]

\[
(4) \quad a_i \equiv 0(\text{mod} \ 4) \text{ for every positive integer } i \text{ with } 3 \leq i \leq n
\]

has no integral solution \((x, y, n)\) with \(n \geq 3\).

**Example 1.3.** The ternary exponential diophantine equation

\[
y^2 = 4x^n - x^2 + 43
\]

has no integral solution \((x, y, n)\) with \(n \geq 3\).

**Example 1.4.** The diophantine equation

\[
y^2 = 2^{978} x^{11} + 2^8 x^{10} + 2^{100} x^9 + 2^5 x^8 + 2^6 x^7 + 2^2 x^6 + 2^{1000} x^5 - x^4 + 2^{10} x^3 + 2^{11} x^2 + 3
\]

has no integral solution \((x, y)\).

**Theorem 1.5.** Let \(f(x)\) and \(g(x)\) be integer polynomials such that

\[
(i) \quad \gcd(f(x), g(x)) = 1 \text{ for each integer } x
\]
The solution-free Diophantine equation

$$(ii) \ g(x) \equiv 3 \pmod{4} \text{ for each integer } x$$

Then the ternary exponential diophantine equation

$$y^2 = -(f(x))^{2k} + g(x)$$

has no integral solution $(x, y, k)$ with $k \geq 1$.

**Corollary 1.6.** Let $b_0, b_1, \ldots, b_m$ be integers such that $b_0 \equiv 3 \pmod{4}$ and $b_i \equiv 0 \pmod{4}$ for $i = 1, 2, \ldots, m$. Then the ternary exponential diophantine equation

$$y^2 = -(b_m x^m + b_{m-1} x^{m-1} + \ldots + b_0 - 1)^{2k} + b_m x^m + b_{m-1} x^{m-1} + \ldots + b_0$$

has no integral solution $(x, y, k)$ with $k \geq 1$.

**Example 1.7.** The ternary exponential diophantine equation

$$y^2 = -(4x^{11} + 4x^4 + 2)^{2k} + 4x^{11} + 4x^4 + 3$$

has no integral solution $(x, y, k)$ with $k \geq 1$.

Let $p$ be a prime number and $n$ be an integer. Then $\left(\frac{n}{p}\right)$ is Legendre symbol (see [1]). We use this symbol in the following sections.

## 2 Proof of Theorem 1.1

Suppose that there is an integral solution $(x, y) = (a, b)$ for the given equation. Then we have

$$b^2 = a_n a^n + a_{n-1} a^{n-1} + \ldots + a_0. \quad (2)$$

By our hypothesis, $a_0$ is prime $\equiv 3 \pmod{4}$, $a_1 = 0$ and there is an even positive integer $k \leq n$ such that

(i) $a_k = -1$

(ii) $a_n a^n + a_{n-1} a^{n-1} + \ldots + a_{k-1} a^{k-1} + a_{k+1} a^{k+1} + \ldots + a_0 \equiv 3 \pmod{4}.$

So (ii) implies that $a_n a^n + a_{n-1} a^{n-1} + \ldots + a_{k-1} a^{k-1} + a_{k+1} a^{k+1} + \ldots + a_0$ has a prime divisor $p \equiv 3 \pmod{4}$. We shall prove that $p$ does not divide $a$. Assume that $p$ divides $a$. Then $p$ divides $a_0$. So $p = a_0$, since $a_0$ is prime. Therefore $b^2$ is multiple of $p^2$, but $a_n a^n + a_{n-1} a^{n-1} + \ldots + a_0$ is not multiple of $p^2$, because $a_1 = 0$. This is a contradiction to equation (2). This proves that $p$ does not
divide a. So p does not divide \( a_n a^n + a_{n-1} a^{n-1} + \ldots + a_0 \). Therefore by the definition of Legendre symbol, from (2), we can write

\[
\left( \frac{a_n a^n + a_{n-1} a^{n-1} + \ldots + a_0}{p} \right) = 1.
\]

That is,

\[
\left( \frac{-a^k}{p} \right) = 1.
\]

Since \( k \) is even,

\[
\left( \frac{-1}{p} \right) = 1.
\]

Since \( \left( \frac{-1}{p} \right) = (-1)^{(p-1)/2} \),

\[
(-1)^{\frac{p-1}{2}} = 1.
\]

This implies that \( p \equiv 1 \pmod{4} \). This is a contradiction to \( p \equiv 3 \pmod{4} \). This proves the theorem.

3 Proof of Corollary 1.2

Fix any positive integer \( n \geq 3 \). Since \( a_i \equiv 0 \pmod{4} \) for every positive integer \( i \) with \( 3 \leq i \leq n \) and \( a_0 \equiv 3 \pmod{4} \),

\[
a_n x^n + a_{n-1} x^{n-1} + \ldots + a_3 x^3 + a_0 \equiv 3 \pmod{4}
\]

for every integer \( x \). So by our hypothesis and Theorem 1.1, we have that the diophantine equation

\[
y^2 = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0
\]

has no integral solution \((x, y)\). This proves the corollary.

4 Proof of Theorem 1.5

Suppose that there is an integral solution \((x, y, k) = (a, b, k)\) for the given equation with \( k \geq 1 \). Then we have

\[
b^2 = -f(a)^{2k} + g(a) \tag{3}
\]

with

(i) \( \gcd(f(a), g(a)) = 1 \)
(ii) \( g(a) \equiv 3 \pmod{4} \).

So (ii) implies that there is a prime divisor \( p \) for \( g(a) \) such that \( p \equiv 3 \pmod{4} \). Since \( \gcd(f(a), g(a)) = 1 \), \( p \) does not divide \( f(a) \). This implies that \( p \) does not divide \(-f(a)^{2k} + g(a)\). By the definition of Legendre’s symbol, from (3), we can write

\[
\left( \frac{-f(a)^{2k} + g(a)}{p} \right) = 1.
\]

Since \( p \mid g(a) \),

\[
\left( \frac{-f(a)^{2k}}{p} \right) = 1.
\]

From this, we observe that

\[
\left( \frac{-1}{p} \right) = 1.
\]

Since \( \left( \frac{-1}{p} \right) = (-1)^{(p-1)/2} \),

\[
(-1)^{\frac{p-1}{2}} = 1.
\]

This means that \( p \equiv 1 \pmod{4} \) which is a contradiction to \( p \equiv 3 \pmod{4} \). This proves the theorem.

5 Proof of Corollary 1.6

Since \( b_0 \equiv 3 \pmod{4} \)

and \( b_i \equiv 0 \pmod{4} \)

for \( i = 1, 2, \ldots, m \),

\[
b_m x^n + b_{m-1} x^{m-1} + \ldots + b_0 \equiv 3 \pmod{4}
\]

for each integer \( x \). Also it is clear that for any integer \( x \),

\[
\gcd(b_m x^n + b_{m-1} x^{m-1} + \ldots + b_0, b_m x^n + b_{m-1} x^{m-1} + \ldots + b_0 - 1) = 1.
\]

Therefore by Theorem 1.5, we have the result.

Acknowledgement. Authors thank Prof. D. Surya Ramana (Harish-Chandra Research Institute) for appreciating the results of this paper when he visited SASTRA University.
References


Received: June, 2012