Solutions of some generalized Ramanujan–Nagell equations

by N. Saradha and Anitha Srinivasan

School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Mumbai-400005, India
Department of Mathematics, Indian Institute of Technology, Powai, Mumbai 400076, India

Communicated by Prof. R. Tijdeman at the meeting of June 20, 2005

1. INTRODUCTION

We consider the Diophantine equation

(1) \[ x^2 + D = y^n \]

in positive integers \(x, y, D\) and \(n > 2\) with \(\text{gcd}(x, y) = 1\). When \(D = 1\), the equation has no solution by an old result of Lebesgue [14]. We assume from now on that \(D > 1\). Eq. (1) has been extensively studied by many authors, in particular, by Cohn and Le. See [8,10-13] for several results. We also refer to [8] for a survey. The equation is referred as the generalized Ramanujan–Nagell equation who pioneered the study on (1). In his paper, Cohn solved (1) completely for 77 values of \(D \leq 100\). The values \(D = 74, 86\) were solved by Mignotte and de Weger [17] and \(D = 55, 95\) were solved by Bennett and Skinner [2]. Recently, Bugeaud, Mignotte and Siksek [6] covered the remaining 19 values \(\leq 100\). We write

(2) \[ D = p_1^{\alpha_1} \cdots p_r^{\alpha_r} = D_s D_t^2 \]

where \(p_1, \ldots, p_r\) are primes, \(\alpha_1, \ldots, \alpha_r\) are positive integers and \(D_s\) is the square free part of \(D\). We may also consider (1) with primes \(p_1, \ldots, p_r\) fixed and varying \(\alpha_1, \ldots, \alpha_r\). We mention a few results in this direction. Arif, Muriefah [1] and Luca...
[15] considered (1) without the condition \( \gcd(x, y) = 1 \) when \( r = 1 \) and \( p_1 = 3 \). They found two families of solutions viz.,

\[
(x, y, \alpha_1, n) = (10 \cdot 3^3, 7 \cdot 3^{2r}, 5 + 6t, 3) \quad \text{and} \quad (46 \cdot 3^3, 13 \cdot 3^{2r}, 4 + 6t, 3).
\]

Bugeaud [5] showed that

Eq. (1) with \( r = 1, p_1 = 7, n \geq 3 \) and \( y = 2 \) has exactly six solutions.

Bennett and Skinner [2] have also made some contributions on equation (1) with \( r = 1 \) and \( p_1 \in \{11, 13, 19, 29, 43, 53, 59, 61, 67\} \). The methods of [2] and [6] involve theory of linear forms in logarithms and the theory of Galois representation of modular forms. Earlier, Luca [16] completely solved (1) when \( r = 2 \) and \((p_1, p_2) = (2, 3)\) using the result on the existence of primitive divisors of Lucas numbers due to Bilu, Hanrot and Voutier [4]. Bugeaud and Shorey [7] applied [4] to determine the solutions of (1) when \( D \) is square free, \( D \equiv 7 \pmod{8} \) and \( h(-4D) \) equals 1 or a power of 2, where \( h(-4D) \) equals the class number of the unique quadratic order of discriminant \(-4D\). See also Bugeaud [5, Theorems 3, 4] for some results concerning equation (1) when \( D \) is not square free. We refer to Bilu [3] for a correction in the papers of [5] and [13]. For stating our results we denote by \( h_0 \), the class number of the quadratic field \( \mathbb{Q}(\sqrt{-D}) \). Suppose \( n = 2 \). Since \( D \) is odd, we find that

\[
(x, y) = \left( \frac{d_2 - d_1}{2}, \frac{d_2 + d_1}{2} \right)
\]

where \( d_1d_2 = D \) with \( d_1 < d_2 \) and \( \gcd(d_1, d_2) = 1 \) are solutions of (1). Thus there are exactly \( 2^{r-1} \) solutions. Henceforth we assume that \( n > 2 \).

**Theorem 1.** Suppose Eq. (1) holds with \( n > 2 \). Assume that \( D \) is given by (2) with \( D \equiv 3 \pmod{4} \) and such that \( y \) is odd when \( D \equiv 7 \pmod{8} \). Suppose

\[
\alpha_1 \equiv \cdots \equiv \alpha_r \equiv 1 \pmod{2}; \quad p_i \equiv 3 \pmod{4} \quad \text{for } 1 \leq i \leq r.
\]

Then \( n \) is odd and every prime divisor of \( n \) divides \( 3h_0 \). In particular, suppose \( h_0 \) is of the form \( 2^\alpha 3^\beta \) with \( \alpha, \beta \) non-negative integers, then (1) implies that \( n = 3^\gamma \) for some integer \( \gamma \geq 1 \).

Let \( D \equiv 3 \pmod{8} \). The assumptions on \( D \) in Theorem 1 imply that the number of primes \( \equiv 3 \pmod{8} \) dividing \( D \) is odd and the number of primes \( \equiv 7 \pmod{8} \) dividing \( D \) is even. Likewise, when \( D \equiv 7 \pmod{8} \), we see that the number of primes \( \equiv 3 \pmod{8} \) dividing \( D \) is even and the number of primes \( \equiv 7 \pmod{8} \) dividing \( D \) is odd. We give two corollaries.

**Corollary 1.** Let \( n \geq 3 \) and \( h_0 > 1 \). Assume that \( D \) satisfies conditions of Theorem 1 with \( \gcd(n, h_0) = 1 \) and \( 3 \nmid h_0 \). Further we suppose that one of the following holds:
(i) $3 \mid D$.
(ii) $\text{ord}_3(D) > 1$ and none of $D/27 \pm 8$ is a square.
(iii) $3 \nmid D$ and none of $(D + 1)/3, (D \pm 8)/3$ is a square.

Then Eq. (1) does not hold.

As an example we see that, the equation

$$x^2 + 3 \cdot 11^{\alpha_2} 19^{\alpha_3} = y^n$$

with $\alpha_2$ and $\alpha_3$ odd

has no solution. Note that $h_0 = 4$ in this case. In section 4, we give all the values of $D$ with $D_s < 10000$, $h_0 > 1$ a power of 2 and for which conditions (ii) or (iii) of Corollary 1 are satisfied. For these values of $D$, we conclude by Corollary 1 that Eq. (1) has no solution. For instance, the equations

$$x^2 + 3^{\alpha_1} 7^{\alpha_2} 31^{\alpha_3} = y^n$$

with $\alpha_1, \alpha_2, \alpha_3$ odd,

$$x^2 + 7^{\alpha_1} 11^{\alpha_2} 23^{\alpha_3} = y^n$$

with $\alpha_1, \alpha_2, \alpha_3$ and $y$ odd

have no solution.

Next we consider the case of those $D$ satisfying conditions of Theorem 1 with $h_0 = 1$. As is well known, there are 9 values of $D_s$ for which $h_0 = 1$. Since $D > 1$ is odd, we see that $D = p^\ell$ where $p \in \{3, 7, 11, 19, 43, 67, 163\}$ with $\ell$ odd. By the results quoted in the beginning, we see that Eq. (1) is completely solved when $D = 3^\ell$ or when $\ell = 1$ and $p \neq 163$. In the latter case, the only solutions are given by

$$\begin{align*}
(x, y, D, n) &\in \{(4, 3, 11, 3), (58, 15, 11, 3), (18, 7, 19, 3), (22434, 55, 19, 5), (110, 23, 67, 3)\}.
\end{align*}$$

See [8]. By a result of Darmon and Granville [9, Theorem 2], it is clear that (1) has only finitely many solutions whenever $D = t^\ell$ with $\ell > 6$ and any integer $t > 1$. In the following corollary we show that (1) has no solution with $D = p^\ell$ whenever $\ell$ is divisible by a prime $> 5$ and $p \in \{11, 19, 43, 67, 163\}$.

**Corollary 2.** Let $n \geq 3$. Suppose (1) holds with $D = p^\ell$ with $p \in \{11, 19, 43, 67, 163\}$ and $\ell$ odd. Then $\ell = 3^{\beta 5^\gamma}$ for some non-negative integers $\beta$ and $\gamma$. In particular, if $\ell = 1$, then the solutions are given by (4). If $\ell$ is an odd prime then the only solution is $(x, y, D, n) = (9324, 443, 11^3, 3)$. Further suppose $D = 7^\ell$ with $\ell$ and $y$ odd. Then Eq. (1) has no solution.

2. PRELIMINARIES

We assume throughout that (1) holds with $D_s \equiv 3 \pmod{4}$. Let $n \geq 3$. Suppose $y$ is even. Then $x$ is odd and $D + 1 \equiv 0 \pmod{8}$ which contradicts our assumption on $y$. Thus we may assume that

$y$ is odd and hence $x$ is even
while proving Theorem 1 and Corollaries 1 and 2. Suppose \( n \) is even. Reducing (1) modulo 4, we get \( D_s \equiv 1 \pmod{4} \), a contradiction. Thus there is no loss of generality in assuming that

\[ n \] is an odd prime.

We begin with a lemma which is [2, Theorem 1.2].

**Lemma 1.** Let \( \ell \geq 7 \) be prime, \( \alpha \geq 2 \) be an integer. Then the Diophantine equation

\[ x^\ell + 2^\alpha y^\ell = 3z^2 \]

has no solution in non-zero co-prime integers \((x, y, z)\) with \( xy \neq \pm 1 \).

The following lemma is part of [7, Lemma 1]. See also [12].

**Lemma 2.** The solutions of the equation

\[ X^2 + DZ^2 = Y^N \]

(5)

\[ X^2 + DZ^2 = Y^N \]

can be put in at most \( 2^{\omega(Y)-1} \) classes where \( \omega(Y) \) denotes the number of distinct prime divisors of \( Y \). Further in each class there is a unique solution \((X_1, Z_1, N_1)\) with \( X_1 > 0, Y_1 > 0 \) and \( N_1 \) minimal among the solutions in the class. This minimal solution satisfies \( N_1 \) divides \( h(-4D) \), where \( h(-4D) \) equals the class number of the unique quadratic order of discriminant \(-4D \). Further \( N_1 = 1 \) if \( D = 1 \) or 3.

We observe that if (1) has a solution \((x, y, n)\) then it corresponds to a solution \((X, Z, N) = (x, 1, n)\) of (5). Suppose \((x, 1, n)\) is in some class, then it can be shown that the minimal solution of (5) in that class is of the form \((X_1, 1, N_1)\) of (5). See [7, Lemma 1 and pp. 67–68]. If \((x, 1, n)\) is the minimal solution, then \( n | h(-4D) \), by Lemma 2. Suppose \((x, 1, n)\) is not the minimal solution. Then this class has two solutions. The following lemma is a special case of [7, Theorem 2].

**Lemma 3.** If Eq. (1) has two solutions in one class then \((D, y) \in \mathcal{H}^0\) where

\[ \mathcal{H}^0 = \{ (D, y) \mid \text{there exist positive integers } r \text{ and } s \text{ such that} \]

\[ s^2 + D = y^r \text{ and } 3s^2 - D = \pm 1 \]

or

\[ (D, y) \in \{ (19, 55), (341, 377) \} \]

in which case Eq. (1) has exactly two solutions.

When \((D, y) = (19, 55), (341, 377)\), we find that \((x, n) = (6, 1), (22434, 5) \text{ and} (6, 1), (2759646, 5)\) are the solutions of (1), respectively. When \((D, y) \in \mathcal{H}^0\), then \((x, n) = (s, r) \text{ and} (8s^3 \pm 3s, 3r)\) are solutions of (1). Since \( n \) is an odd prime, in the latter case we get \( n = 3 \). Thus we conclude that

106
Lemma 4. Suppose \((x, y, n)\) is a solution of (1). Then either \(n = 3\) or \(n\) divides \(h(-4D)\).

In the next lemma we compute \(h(-4D)\). Let

\[
D_0 = -4D_s, \quad D_1 = D_t \quad \text{if} \quad D_s \equiv 1 \pmod{4}
\]

and

\[
D_0 = -D_s, \quad D_1 = 2D_t \quad \text{if} \quad D_s \equiv 3 \pmod{4}.
\]

Then

\[
D_0 \equiv 0, 1 \pmod{4} \quad \text{and} \quad -4D = D_0D_1^2.
\]

Note that \(D_0\) is the fundamental discriminant associated to the discriminant \(-4D\).

We have

Lemma 5. Let \(D\) be odd. Suppose

\[
\mu = \prod_{\substack{p|D_1 \\text{ and } p \neq 2 \\text{ or } \text{p is prime to } 2 |D_1 | \text{ and } \text{p is prime to } 2}} \left(1 - \frac{D_0}{p}\right).
\]

Then

\[
h(-4D) = 3^\delta D_1 \mu h(D_0)
\]

where \(\delta = 0\) if either \(D_s \equiv 1 \pmod{4}\) or \(D_s \equiv 7 \pmod{8}\) or \(D_s = 3\); \(\delta = 1\) if \(D_s \equiv 3 \pmod{8}\) and \(D_s \neq 3\).

Proof. We have (see [18, pp. 25–26])

\[
h(-4D) = h(D_0)\frac{\psi}{u}
\]

where

\[
\psi = D_1 \prod_{p|D_1} \left(1 - \frac{D_0}{p}\right)
\]

with \((\cdot)\) denoting the Kronecker symbol and \(u = 3\) when \(D_s = 3\) and 1 otherwise. By the definition of Kronecker symbol we have

\[
\left(\frac{D_0}{2}\right) = \begin{cases} 
1 & \text{if } D_0 \equiv 1 \pmod{8}, \\
-1 & \text{if } D_0 \equiv 5 \pmod{8}
\end{cases}
\]
and
\[ \left( \frac{D_0}{p} \right) = 0 \quad \text{if } p \mid D_0. \]

Hence
\[ \psi \mu = 3^\delta \mu \]

where \( \delta = 1 \) if \( D_0 \equiv 5 \pmod{8} \) and \( D_0 \neq -3 \); \( \delta = 0 \) if \( D_0 \equiv 1, 4 \pmod{8} \) or \( D_0 = -3 \). \( \square \)

We observe that \( \mu = 1 \) if every odd prime dividing \( D_1 \) divides \( D_0 \), since then \( \left( \frac{D_0}{p} \right) = 0 \). Now the sets of odd primes dividing \( D_1 \) and \( D_0 \) are the same as the sets of odd primes dividing \( D_t \) and \( D_s \), respectively. Hence we find that whenever all \( \alpha_i \)'s are odd, any prime dividing \( D_t \) divides \( D_s \), which, in turn, implies that any odd prime dividing \( D_1 \) divides \( D_0 \). Hence we get \( \mu = 1 \). This leads to the following corollary.

**Corollary 3.** Suppose \( D \) given by (2) is such that all \( \alpha_i \)'s are odd. Then
\[ h(-4D) = 3^\delta h(D_0)D_t \]

where
\[ \delta = \begin{cases} 0 & \text{if } D_s \equiv 1, 5, 7 \pmod{8} \text{ or } D_s = 3, \\ 1 & \text{if } D_s \equiv 3 \pmod{8}, \ D_s \neq 3. \end{cases} \]

**Lemma 6.** Suppose Eq. (1) holds. Let \( h_0 \) be the class number of the quadratic field \( \mathbb{Q}(\sqrt{-D_s}) \). Suppose \( \gcd(n, h_0) = 1 \). Then there are integers \( a, b \) satisfying \( \gcd(a, D_s) = 1 \) and
\[ 2^n g D_t = \left( \frac{n}{1} \right) a^{n-1} - \left( \frac{n}{3} \right) a^{n-3}b^2D_s + \cdots + (-1)^{(n-1)/2}b^{n-1}D_s^{(n-1)/2} \]

where \( g = 0 \) or 1. Also if \( g = 1 \), then \( a \) and \( b \) are both odd.

**Proof.** Eq. (1) is
\[ x^2 + D_sD_t^2 = y^n. \]

Thus
\[ (x + D_t\sqrt{-D_s})(x - D_t\sqrt{-D_s}) = y^n. \]

Thus we have the ideal equation
\[ [x + D_t\sqrt{-D_s}][x - D_t\sqrt{-D_s}] = [y]^n. \]
Raising both sides to the power $h_0$ we see that
\[ [\alpha][\overline{\alpha}] = [\alpha^{h_0}]^n \]
where $[\alpha] = [x + D_t \sqrt{-D_s}]^{h_0}$; $[\overline{\alpha}] = [x - D_t \sqrt{-D_s}]^{h_0}$. The ideals $[x + D_t \sqrt{-D_s}]$ and $[x - D_t \sqrt{-D_s}]$ are co-prime since $y$ is odd and $\gcd(x, y) = 1$. Thus we get
\[ [\alpha] = [y_1]^n; \quad [\overline{\alpha}] = [\overline{y}_1]^n \]
for some $y_1$ in the ring of integers of $\mathbb{Q}(\sqrt{-D_s})$. Thus
\[ (x + D_t \sqrt{-D_s})^{h_0} = y_1^n; \quad (x - D_t \sqrt{-D_s})^{h_0} = \overline{y}_1^n. \]
Since $\gcd(n, h_0) = 1$, we get
\[ (6) \quad x + D_t \sqrt{-D_s} = y_2^n; \quad x - D_t \sqrt{-D_s} = \overline{y}_2^n \]
for some $y_2$ in the ring of integers of $\mathbb{Q}(\sqrt{-D_s})$. We know that there exist integers $a, b$ such that $y_2 = a + b \sqrt{-D_s}$ or $(a + b \sqrt{-D_s})/2$ with $a \equiv b \pmod{2}$. Thus $y_2 = (a + b \sqrt{-D_s})/2^g$ with $g = 0$ or 1. Further $g = 1$ if $a$ and $b$ are both odd. By comparing the real part in (6), we get
\[ x = \frac{1}{2^{ng}} \left( \frac{n}{2} \right) a^{n-2} b^2 (-D_s) + \left( \frac{n}{4} \right) a^{n-4} b^4 (-D_s)^2 \]
\[ + \cdots + \left( \frac{n}{n-1} \right) a b^{n-1} (-D_s)^{(n-1)/2} \]  
(7)
Thus $\gcd(a, D_s) = 1$ since $\gcd(x, D) = 1$. We compare the imaginary parts in (6) to get
\[ D_t = \frac{1}{2^{ng}} \left( \frac{n}{1} \right) a^{n-1} b - \left( \frac{n}{3} \right) a^{n-3} b^3 D_s + \cdots + (-1)^{(n-1)/2} b^{n-2} D_s^{(n-1)/2} \]
Now the lemma follows. \[ \square \]

3. PROOF OF THEOREM 1 AND COROLLARIES 1 AND 2

**Proof of Theorem 1.** Let $n \neq 3$ with $\gcd(n, h_0) = 1$. Assume that $D$ satisfies the assumptions of Theorem 1. By Lemma 4, we see that $n$ divides $h(-4D)$. By Corollary 3, we get
\[ n \mid h(D_0)D_t. \]
Since $D_0$ is the fundamental discriminant associated with $D$, we see that $h_0 = h(D_0)$. As $\gcd(n, h_0) = 1$, we find that $n \mid D_t$. Since $\alpha_1, \ldots, \alpha_r$ are odd, the set of primes dividing $D_t$ is a subset of the set of primes dividing $D_s$. Thus $n \mid D_s$. By Lemma 6, we get integers $a, b, g$ with $\gcd(a, D_s) = 1$ such that
\[ (8) \quad 2^{ng} \frac{D_t}{n} = a^{n-1} b - \left( \frac{n}{3} \right) a^{n-3} b^3 \frac{D_s}{n} + \cdots + (-1)^{(n-1)/2} b^{n-2} \frac{D_s^{(n-1)/2}}{n}. \]
From this we see that

\[ \text{ord}_p(b) = \text{ord}_p \left( \frac{D_t}{n} \right) \quad \text{for every prime } p \mid b, \ p \neq 2. \]

Let \( g = 1 \). In this case both \( a \) and \( b \) are odd. Hence from (8) and (9) we get \( b = \pm D_t/n \) and

\[ \pm 2^n \equiv a^{n-1} \equiv 1 \pmod{n}. \]

This is not possible since \( n \neq 3 \). Let \( g = 0 \). Again from (8) and (9) we get \( b = \pm D_t/n \). Reducing both sides of (8) modulo \( n \) we get \( a^{n-1} \equiv \pm 1 \pmod{n} \) which shows that we need to consider only the + sign. Now we get from (8) and (9) that

\[ 1 = a^{n-1} - \left( \frac{n}{3} \right) a^{n-3} \left( \frac{D}{n^3} \right) + \left( \frac{n}{5} \right) a^{n-5} \left( \frac{D^2}{n^5} \right) - \cdots \]

\[ + \frac{(-1)^{(n-1)/2} D^{(n-1)/2}}{n^n}. \]

Suppose \( a \) is odd. Reducing mod 8 we get

\[ \left( \left( \frac{n}{3} \right) + \left( \frac{n}{7} \right) + \cdots \right) D \equiv \left( \left( \frac{n}{5} \right) + \left( \frac{n}{9} \right) + \cdots \right) \pmod{8}, \]

i.e.,

\[ \left( \left( \frac{n}{3} \right) + \left( \frac{n}{7} \right) + \cdots \right) D_s \equiv \left( \left( \frac{n}{5} \right) + \left( \frac{n}{9} \right) + \cdots \right) \pmod{8} \]

which gives

\[ \left( \left( \frac{n}{3} \right) + \left( \frac{n}{5} \right) + \cdots + \left( \frac{n}{n} \right) \right) = 0 \pmod{2}. \]

On the other hand, it is well known that

\[ \left( \frac{n}{1} \right) + \left( \frac{n}{3} \right) + \cdots + \left( \frac{n}{n} \right) = 2^{n-1}. \]

Thus

\[ \left( \frac{n}{3} \right) + \cdots + \left( \frac{n}{n} \right) = 2^{n-1} - n \equiv 1 \pmod{2} \]

which contradicts (11). Thus \( a \) is even. Then from (10) we get

\[ (-1)^{(n-1)/2} D_s \equiv (-1)^{(n-1)/2} D^{(n-1)/2} \equiv n \pmod{4}. \]

Since each \( p_i \equiv 3 \pmod{4} \) and \( n \) is one of these \( p_i \)'s we get

\[ D_s \equiv 1 \pmod{4}. \]
This is a contradiction since $D_s \equiv D \equiv 3 \pmod{4}$. This proves Theorem 1. \hfill \Box

**Proof of Corollary 1.** By Theorem 1, we need to take only the case $n = 3$. We show that there exists an integer $a$ with $\gcd(a, D) = 1$ satisfying the following properties.

(12) Suppose $3 \not| D$. Then $D = 3a^2 - 1$ or $3a^2 \pm 8$.

(13) Suppose $3 | D$. Then $\mathrm{ord}_3(D) \geq 3$ and $D = 27(a^2 \pm 8)$.

Since $3 \not| h_0$, by Lemma 6, we find that there are integers $a, b$ satisfying $\gcd(a, D_s) = 1$ and

(14) $8^s \frac{D_t}{b} = 3a^2 - b^2 D_s$.

Suppose $3 \not| D$. Then $b = \pm D_t$. Then $\pm 8^s = 3a^2 - D$. Reducing mod 8, $3a^2 - D \neq -1$. This proves (12).

Suppose $3 | D$. Then we see that 3 divides the right-hand side of (14) since $3 | D_s$. But 3 does not divide the left-hand side of (14), a contradiction. Thus $\mathrm{ord}_3(D) \geq 3$ if $3 | D$. Then we get

$$8^s \frac{D_t/3}{b} = a^2 - b^2 (D_s/3)$$

implying $b = \pm D_t/3$. Thus we get

$$\pm 8^s = a^2 - D/27.$$  

Reducing the above equation mod 8 we see that $a^2 - D/27 \neq 1$. Also $a^2 - D/27 \neq -1$, since the primes in $D$ are congruent to 3 (mod 4) and occur with an odd power. This proves (13). The assertion of Corollary 1 follows immediately from (12) and (13). \hfill \Box

**Proof of Corollary 2.** Let $D = p^\ell$, $p \in \{7, 11, 19, 43, 67, 163\}$ with $\ell$ odd and we suppose $y$ odd if $p = 7$. By Theorem 1 and Corollary 1, we get $n = 3, D = 3a^2 - 1$ or $3a^2 \pm 8$. Reducing mod 3, we see that

$$11^\ell = 3a^2 - 1 \text{ or } 3a^2 + 8;$$

$$p^\ell = 3a^2 - 8 \quad \text{for } p \in \{7, 19, 43, 67, 163\}.$$  

We check that $7^\ell = 3a^2 - 8$ is not possible using congruence mod 7. This proves Corollary 2 when $D = 7^\ell$. Next we consider $p \neq 7$. Then we get an equation of the form

$$z_1^\ell + 8^\delta z_2^\ell = 3a^2 \quad \text{with } z_2 = \pm 1, \delta = 0, 1.$$  

Now we apply Lemma 1 to conclude that $\ell = 3^\beta 5^\gamma$ for some non-negative integers $\beta$ and $\gamma$.  

111
Let $\ell = 1$. By the result of [8] we have the solutions given by (4) for $D \neq 163$. Let now $D = 163$. We check that 163 is not of the form $3a^2 - 1$ or $3a^2 \pm 8$. Thus $\ell \neq 1$. Suppose $\ell$ is an odd prime. Then $\ell = 3, 5$. We find that the only possible value is $D = 11^3 = 3 \cdot 21^2 + 8$ i.e., $a = 21$. Further from Lemma 6, we see that $b = -11$ and using (7), we get $x = 9324$ which gives $y = 443$. □

4. EXAMPLES

In this section we list several values of $D$ with $D_x \leq 10000$ and $h_0 > 1$ a power of 2. We show in Corollary 4 below that conditions (ii) or (iii) of Corollary 1 is satisfied for these values of $D$. Hence by Corollary 1, Eq. (1) has no solution when $D$ takes one of these values. We set $D = p_1^\alpha p_2^\beta p_3^\gamma$ where $\alpha, \beta, \gamma$ are odd integers and $p_1, p_2, p_3$ are given as follows. Let $S_1$ be the set of values of $D$ with $(p_1, p_2) = (3, 3)$ and

\[(p_2, p_3) \in \{(11, 19), (11, 59), (11, 67), (11, 83), (19, 59),
(11, 107), (19, 67), (11, 131), (11, 179), (19, 107),
(11, 227), (19, 139), (11, 251), (43, 67), (19, 163)\}.

Let $S_2$ be the set of values of $D$ with $p_1 = 3, \alpha > 3$ and

\[(p_2, p_3) \in \{(7, 23), (7, 47), (23, 31), (23, 47), (7, 167),
(23, 71), (31, 79), (7, 383), (31, 103)\}.

Let $S_3$ be the set of values of $D$ with $p_1 = 3$ and

\[(p_2, p_3) \in \{(7, 31), (7, 79), (7, 103), (7, 127), (7, 151), (7, 199),
(7, 223), (7, 367), (7, 439), (19, 43)\}.

Let $S_4$ be the set of values of $D$ with

\[(p_1, p_2, p_3) \in \{(7, 11, 23), (7, 19, 31), (7, 11, 71), (7, 23, 43),
(11, 23, 31), (11, 19, 43)\}.

Finally we set $S_5$ to be the set of values of $D$ with

\[(p_1, p_2, p_3) \in \{(3, 7, 19), (3, 7, 43), (3, 11, 31), (3, 7, 59), (7, 11, 19),
(3, 11, 47), (3, 19, 31), (3, 11, 71), (3, 7, 227), (3, 7, 251),
(3, 7, 283), (3, 31, 67), (3, 11, 199), (7, 11, 107), (3, 7, 467)\}.

Corollary 4. Let $n \geq 3$. Suppose $D$ is given by $S_1, S_2, S_3$ and $S_4$. Then (1) does not hold. Further suppose $y$ is odd. Then (1) does not hold with $D$ given by $S_5$.

Proof. Suppose (1) holds with $D$ given by $S_1, S_2, S_3$ and $S_4$. By Theorem 1, we may take $n = 3$. By Corollary 1, we may assume that if $3 \mid D$, then $\text{ord}_3(D) \geq 3$. 112
Also as in the proof of Corollary 1, there exists an integer $a$ with $\gcd(a, D) = 1$ satisfying condition (12) or (13). We show that no $D$ satisfies these two conditions.

Let $D = 3^\alpha 7^\beta p^\gamma$ with $\alpha \geq 3, \beta > 0$. We have $D = 27(a^2 \pm 8)$. Using mod 7, we find that $D = 27(a^2 - 8)$. Now we use mod 3 to conclude that $\alpha = 3$ and $p \equiv 2$ (mod 3). Thus $D \notin S_2$.

Let $D \in S_4$. We take $D = 7^\alpha p_1^\beta p_2^\gamma$. Further $D = 3a^2 - 1$ or $3a^2 \pm 8$. We reduce mod 7 to see that $D = 3a^2 + 8$ and using mod 3, we get $p_1 p_2 \equiv 2$ (mod 3). Thus

$$D \notin \{7 \cdot 11 \cdot 23, 7 \cdot 19 \cdot 31, 7 \cdot 11 \cdot 71\}.$$

Suppose $D = 7 \cdot 23 \cdot 43 = 3a^2 + 8$. This is not possible by reducing mod 23. Now we take $D = 11^\alpha 23^\beta 31^\gamma, 11^\alpha 19^\beta 43^\gamma$. Reducing mod 11, we see that $D = 3a^2 - 1, 3a^2 + 8$, respectively. Now we use mod 3 and mod 19, respectively to exclude the two values of $D$. Thus $D \notin S_4$.

Now we take a case belonging to $S_1$. Let $D = 3^3 \cdot 11^\beta 19^\gamma$. Then $D = 27(a^2 \pm 8)$. We use mod 11 to show that $D = 27(a^2 + 8)$. Now reading mod 3 we get a contradiction since $\text{ord}_3(D) = 3$ and $a^2 + 8$ is always divisible by 3. All other cases in $S_1$ are excluded similarly. Suppose $D$ is given by $S_2$. We show that $D = 27(a^2 - 8)$. Reading mod 3 this leads to a contradiction since $\text{ord}_3(D) > 3$.

Every case in $S_5$ is excluded using congruence argument as above with the primes $p_1, p_2, p_3$ in $D$.

ACKNOWLEDGEMENT

We thank the referee for many useful comments which helped us in giving a better presentation of the paper.

REFERENCES


(Received January 2005)