Generalized Lebesgue-Ramanujan-Nagell Equations

N. Saradha and Anitha Srinivasan

Dedicated to Professor T. N. Shorey on his 60th birthday

1 Prelude

For any positive integer $\nu > 1$, let $P(\nu)$ and $\omega(\nu)$ denote the greatest prime factor and the number of distinct prime factors of ν, respectively. Let $P(1) = 1$ and $\omega(1) = 0$. Throughout the paper D_1, D_2 and λ denote positive integers such that $\gcd(D_1, D_2) = 1$. We are interested in the equation

$$D_1 x^2 + D_2 = \lambda y^n \tag{1.1}$$

in positive integers x, y and $n > 1$. This equation has a rich history and it has attracted the attention of several great mathematicians. Several papers have been written on this topic, specially for particular values of D_1, D_2 and λ. Detailed surveys on this equation can be found in papers such as [Sh] and [BMS].

2 The Ramanujan-Nagell type equations

When $D_1 = 1,\ D_2 = D, \lambda$ and $y = k$ are fixed in (1.1), the resulting equation is called a Ramanujan-Nagell type equation, namely

$$x^2 + D = \lambda k^n. \tag{2.1}$$

The following result of Siegel [Si] shows that the number of solutions (x, n) of (2.1) is finite.

If $f(x) \in \mathbb{Z}[X]$ has at least two distinct roots then $P(f(x)) \to \infty$ as $\mid x \mid \to \infty$.

The famous Ramanujan-Nagell equation is a particular case of (2.1) when $D = 7,\ \lambda = 1$ and $k = 2$. In 1913, Ramanujan [Ra] conjectured that all the solutions (x, n) of the equation

$$x^2 + 7 = 2^n$$

are given by

$$(x, n) \in \{(1, 3), (3, 4), (5, 5), (11, 7), (181, 15)\}. \tag{2.2}$$

Ljunggren posed the same problem in 1943 and Nagell solved it in 1948. His proof in English was published in 1961, see [Na1]. Subsequently, alternative proofs have been given by various authors. For instance Chowla, Lewis and Skolem [CLS] used Skolem's p-adic method in their proof.

In 1960, Apéry [Ap] considered (2.1) with $\lambda = 4$ and $k = 2$. He showed that

$$x^2 + D = 2^{n+2}, D \neq 7 \tag{2.3}$$

has at most two solutions. In particular,

$$\begin{aligned} &(x, n) \in \{(3, 5), (45, 11)\} \text{ if } D = 23 \text{ and} \\ &(x, n) \in \{(1, m), (2^m - 1, 2m - 1)\} \text{ if } D = 2^m - 1 \text{ with } m \geq 4. \end{aligned} \tag{2.4}$$

Thus there are infinitely many D for which (2.3) has precisely two solutions. In 1980, Beukers (see [Beu1] and [Beu2]) showed that apart from the values of D given by (2.4), equation (2.3) has at most one solution, thereby confirming a conjecture of Browkin and Schinzel. Apéry also considered (2.1) with $\lambda = 1,\ k = p$, an odd prime, i.e.,

$$x^2 + D = p^n,\ p \nmid D. \tag{2.5}$$

He showed that (2.5) has at most two solutions. Further Beukers proved that (2.5) has at most one solution except when $(p, D) = (3, 2)$ or $(p, D) = (4t^2 + 1, 3t^2 + 1)$ for a positive integer t. In these exceptional cases there are exactly two solutions. Beukers used hyper-geometric methods for proving these results.

In a series of papers, Le (see [Le1] to [Le5]) considered the following form of equation (1.1) with $y = p$, a prime, namely

$$D_1 x^2 + D_2 = \eta^2 p^n \text{ with } \eta \in \{1, \sqrt{2}, 2\}. \tag{2.6}$$

He showed that (2.6) has at most two solutions except in the following four cases :

$$\begin{aligned} &x^2+7=4\cdot 2^n \Rightarrow (x,n) \text{ as in (2.2)},\\ &3x^2+5=4\cdot 2^n \Rightarrow (x,n)\in\{(1,1),(3,3),(13,7)\},\\ &x^2+11=4\cdot 3^n \Rightarrow (x,n)\in\{(1,1),(5,2),(31,5)\},\\ &x^2+19=4\cdot 5^n \Rightarrow (x,n)\in\{(1,1),(9,2),(559,7)\}. \end{aligned} \tag{2.7}$$

Bugeaud and Shorey [BuS] improved the above result of Le as follows:

Equation (2.6) *has at most one solution except in the cases given by* (2.7), (2.8) *and the three infinite families* G, H *and* I *given below .*

$$\begin{aligned} &2x^2+1=3^n \Rightarrow (x,n)\in\{(1,1),(2,2),(11,5)\},\\ &x^2+1=2\cdot 5^n \Rightarrow (x,n)\in\{(3,1),(7,2)\},\\ &x^2+1=2\cdot 13^n \Rightarrow (x,n)\in\{(5,1),(239,4)\},\\ &7x^2+11=2\cdot 3^n \Rightarrow (x,n)\in\{(1,2),(1169,14)\},\\ &13x^2=3=4\cdot 2^n \Rightarrow (x,n),\in\{(1,2),(71,14)\},\\ &7x^2+1=4\cdot 2^n \Rightarrow (x,n)\in\{(1,1),(3,4)\},\\ &x^2+3=4\cdot 7^n \Rightarrow (x,n)\in\{(5,1),(37,3)\},\\ &6x^2+1=7^n \Rightarrow (x,n)\in\{(1,1),(20,4)\}. \end{aligned} \tag{2.8}$$

We note here that the solution $(x,n)=(11,5)$ for the equation $2x^2+1=3^n$ in (2.8) was found by Leu and Li [LL]. The last equation and its solutions were added by Mollin [Mo2]. The three infinite families are

$$\begin{aligned} G &= \{(D_1,D_2,p)=(1,4p^r-1,p)\mid p\geq 2, r\geq 1, \eta=2\},\\ H &= \{(D_1,D_2,p)\mid \exists\ r,s, D_1s^2+D_2=\eta^2p^r, 3D_1s^2-D_2=\pm\eta^2\} \end{aligned}$$

and

$$I=\{(F_{p-2\varepsilon},L_{p+\varepsilon},F_p)\mid p\geq 2,\ \varepsilon\in\{\pm 1\},\eta=2\},$$

where

$$F_0=0,\ F_1=1,\ F_k=F_{k-1}+F_{k-2} \text{ for } k\geq 2$$

and

$$L_0=2,\ L_1=1,\ L_k=L_{k-1}+L_{k-2} \text{ for } k\geq 2.$$

The two solutions in each case are given by

$$(x,n) \in \begin{cases} \{(1,r),(2p^r-1,2r)\} \text{ for } G, \\ \{(s,r),(\frac{3D_1s^2}{\eta^2} \mp 3s, 3r)\} \text{ for } H, \\ \{(1,1),(\frac{9F_{2p+1}-F_{2p-5}-6}{10},5)\} \text{ for } I \text{ if } \varepsilon = 1, \\ \{(1,1),(\frac{9F_{2p-1}-F_{2p-7}+6}{10},5)\} \text{ for } I \text{ if } \varepsilon = -1. \end{cases}$$

The results of Le, Bugeaud and Shorey mentioned above are based on the work of Bilu, Hanrot and Voutier [BHV] on primitive divisors of Lucas and Lehmer sequences. The relevance of these recurrence sequences was noted by Beukers back in 1980, when he observed that distinct solutions of (2.5) in positive integers (x,n) correspond to integers $l \geq 2$ for which

$$\frac{\xi^l - \bar{\xi}^l}{\xi - \bar{\xi}} = \pm 1 \text{ where } \xi \in \mathbb{Q}(\sqrt{-D}).$$

Let D_1 be odd and $\gcd(D_1D_2,k)=1$. Consider the equation

$$D_1x^2 + D_2 = \eta^2 k^n \text{ with } \eta \in \{1,\sqrt{2},2\}. \tag{2.9}$$

In [BuS], some equations of the form (2.9) with k composite were solved. For instance, it was shown that

$$\begin{aligned} x^2+19 = 55^n &\Rightarrow (x,n) \in \{(6,1),(22434,5)\}, \\ x^2+341 = 377^n &\Rightarrow (x,n) \in \{(6,1),(2759646,5)\}. \end{aligned} \tag{2.10}$$

The following result is obtained from the works of Le, Bugeaud and Shorey.

The solutions of (2.9) *can be put into at most* $2^{\omega(k)-1}$ *classes. Suppose that* (2.9) *is not any of the equations occurring in* (2.7),(2.8) *and* (2.10). *Then in each class there is at most one solution except when* (D_1,D_2,k) *belongs to* G *or* H *or* I, *in which case the equation has two solutions in one class and at most one solution in any other class.*

Bugeaud and Shorey applied their result to solve (2.9) for several values of D_1, D_2 and n a prime. Apart from the Ramanujan-Nagell equation, there are values of D, λ, k for which equation (2.1) has many solutions. For example, Stiller [St] showed that the equation

$$x^2 + 119 = 15 \cdot 2^n$$

has six solutions given by

$$(x, n) \in \{(1, 3), (11, 4), (19, 5), (29, 6), (61, 8), (701, 15)\}.$$

In the language of binary quadratic forms, equation (2.1) can be considered as a representation of the integer λk^n by the identity form $x^2 + Dz^2$. Using this approach in [SA2] we solved completely several generalized Ramanujan-Nagell equations. A typical result therein is mentioned below. Let $\mathrm{ord}_p(x)$ denote the highest power of p in x.

Proposition 2.1 *Suppose D is of the form $p^\theta f + 1$ with p prime, $p \nmid f$ and $\theta > 0$. Assume that $\lambda = x_0^2 + D$ and $k^r = 1 + Dy_1^2$ for some integers x_0, y_1 and $r \geq 1$ such that $p \mid \gcd(x_0, y_1)$. Suppose further that*

$$\mathrm{ord}_p\ (x_0) + \varepsilon < \mathrm{ord}_p\ (y_1)$$

where $\varepsilon = 0$ if $p \geq 3$ and $\varepsilon = 1$ if $p = 2$. Then equation (2.1) does not hold.

As an application, we see that the equation

$$x^2 + 3 = 7 \cdot 97^n,\ n > 1$$

has no solution. Using similar criteria as in Proposition 2.1, we were able to solve (2.1) for several values of D, λ and k.

3 Lebesgue-Nagell type equations

Lebesgue-Nagell type equations are of the form

$$x^2 + D = \lambda y^n, \tag{3.1}$$

where λ and D are fixed and a solution is given by a triple (x, y, n) of positive integers. From Theorem 10.6 of [ST] it follows that the number of solutions of (3.1) is finite. The following results were proved for $\lambda = 1$. In 1850, Lebesgue [Leb] showed that equation (3.1) with $D = 1$ has no solution. In 1928, Nagell [Na2] solved the equation with $D = 3, 5$. Cohn [Co] solved (3.1) for 77 values of $D \leq 100$. For $D = 74, 86$ the equation was solved by Mignotte and de Weger [MW] using linear forms in logarithms and Bennett and Skinner [BeS] solved it for $D = 55, 95$. For the remaining 19 values of $D \leq 100$ equation (3.1) was solved by Bugeaud, Mignotte and Siksek

[BMS]. The proofs of their results depend heavily on the theory of Galois representation of modular forms.

In the above results, D is fixed, (in fact $D \leq 100$). Let the prime factorization of D be written as

$$D = p_1^{\alpha_1} \dots p_r^{\alpha_r}, \tag{3.2}$$

where $p_1, \dots, p_r$ are primes and $\alpha_1, \dots, \alpha_r$ are positive integers. We consider the primes $p_1, \dots, p_r$ to be fixed and allow $\alpha_1, \dots, \alpha_r$ to vary in the equation

$$x^2 + D = y^n. \tag{3.3}$$

Using [BHV], Luca [Lu] solved (3.3) completely for $r = 2,\ p_1 = 2,\ p_2 = 3$. Let $h(d)$ denote the class number of binary quadratic forms of discriminant d. Also $h_0 = h_0(d)$ denotes the class number of the quadratic field $\mathbb{Q}(\sqrt{d})$. In [SA1] (Corollary 1), we proved a result on (3.3) that is not complete. Below we give the complete and corrected result.

Proposition 3.1 *Let* (3.2) *and* (3.3) *hold with* $n > 2$ *and* $D \equiv 3 (\mathrm{mod}\ 4)$. *Suppose that each* α_i *is odd and each* $p_i \equiv 3 \pmod 4$. *Further assume that* y *is odd if* $D \equiv 7 (\mathrm{mod}\ 8)$. *Then* n *is odd and every prime divisor of* n *divides* $3h_0$. *Also if* $\gcd(n, h_0) = 1$ *and* $3 \nmid h_0$, *then there exists an integer* a *such that one of the following holds.*

1. $3 \nmid D$ *and* $D = 3a^2 - 1$ *or* $3a^2 \pm 8$.
2. $\mathrm{ord}_3(D) = 3$ *and* $D = 27(a^2 - 8)$.
3. $\mathrm{ord}_3(D) = 2h + 1$ *with* $h > 1$ *and one of the following holds.*
   (a) $D/27 = a^2 + 8$.
   (b) $D/3^{2h+1} = a^2 - 3^{h-1}$ *and* h *is even.*
   (c) $D/3^{2h+1} = a^2 \pm 8 \cdot 3^{h-1}$.

Proposition 3.1 is a corollary to Theorem 4.2. As mentioned above, Proposition 3.1 is a corrected version of a result in [SA1], where part 3 of Proposition 3.1 was not included. Due to these extra possibilities the sets of values of D given by S_2, S_3 and S_5 in Corollary 4 of [SA1] need to be altered while S_1 and S_4 remain unaltered. We present in Section 7, a new set of values of

D for which equation (3.3) can be completely solved. As a consequence of Proposition 3.1, we are able to show that the equation

$$x^2 + 3^3 \cdot 11^{\alpha_2} \cdot 19^{\alpha_3} = y^n, \ \alpha_2, \alpha_3 \text{ odd} \tag{3.4}$$

has no solution. Now we consider (3.3) with $r = 1$, i.e.,

$$x^2 + p^\ell = y^n, \ n \geq 3 \text{ with } \gcd(x, y) = 1. \tag{3.5}$$

By a result of Darmon and Granville [DG], equation (3.5) with $\ell > 6$ has only finitely many solutions. Arif & Murifah [AM] and Luca [Lu] solved (3.5) with $p = 3$ without any gcd condition. They found two families of solutions viz.,

$$(x, y, \ell, n) \in \{(10 \cdot 3^{3t}, 7 \cdot 3^{3t}, 5 + 6t, 3), (46 \cdot 3^{3t}, 13 \cdot 3^{2t}, 4 + 6t, 3)\}.$$

Bugeaud [Bu] proved that (3.5) with $p = 7$ and $y = 2$ has exactly six solutions. Bennett and Skinner [BeS] have also made partial contributions on (3.5). In [SA1], we showed the following result on (3.5).

Proposition 3.2 *Suppose* (3.5) *holds with* $p \in \{11, 19, 43, 67, 163\}$ *and* ℓ *is odd. Then* $\ell = 3^\beta 5^\gamma$ *for some non-negative integers* β *and* γ*. In particular if* $\ell = 1$*, then the solutions are given by* $(x, y, p, n) \in S$ *where* S *is as follows.*

$$S = \{(4, 3, 11, 3), (58, 15, 11, 3), (18, 7, 19, 3), (22434, 55, 19, 5), (110, 23, 67, 3)\}.$$

Moreover if ℓ *is an odd prime, then* $(x, y, p^\ell, n) = (9324, 443, 11^3, 3)$*. In the case when* $p = 7$ *and* y *is odd there is no solution.*

Note that $h_0 = 1$ for these values of p. In the following sections, we extend Proposition 3.1 to a larger set of values of D. We also present a result that furthers the result of Proposition 3.2 in that for the values of p considered therein, we solve (3.5) for all values of ℓ.

4 Statements of the theorems

Let $\left(\frac{\cdot}{\cdot}\right)$ denote the Legendre Symbol.

Theorem 4.1 *Let*

$$x^2 + D = y^n \tag{4.1}$$

hold with $n > 2$ *and* $D \equiv 3 (\mathrm{mod}\ 4)$. *Also let* y *be odd if* $D \equiv 7 (\mathrm{mod}\ 8)$. *Suppose that*

$$D = D_s D_t^2 E^2$$

where D_s *and* E *are square free with* $\gcd(E, D_s) = 1$ *and* $D_s > 3$. *Assume that*

$$D_s D_t^2 = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

where each α_i *is odd and each* $p_i \equiv 3 (\mathrm{mod}\ 4)$. *Further assume that each prime* $q \mid E$ *satisfies*

$$q \neq 3,\ q = 2^{\alpha} 3^{\beta} + \left(\frac{-D_s}{q} \right) \tag{4.2}$$

and every divisor $e > 1$ *of* E *satisfies*

$$2^g e \not\equiv \pm 1 (\mathrm{mod}\ p) \text{ where } g \in \{0, 1\} \tag{4.3}$$

for any prime $p > 3$ *dividing* D_t. *Then every prime divisor of* n *divides* $3h_0$.

As a consequence of Theorem 4.1 we obtain the following result.

Theorem 4.2 *Suppose* $x^2 + D = y^n$ *and let all the hypotheses of Theorem* 4.1 *hold. Further assume that* $\gcd(n, h_0) = 1$ *and* $3 \nmid h_0$. *Let* $g \in \{0, 1\}$. *Then there exists a divisor* e *of* E *and an integer* a *with* $\gcd\ (a, D_s) = 1$ *such that one of the following holds.*

1. $3 \nmid D$ *and* $D = e^2(3a^2 \pm 8^g e)$.
2. $\mathrm{ord}_3(D) = 3$ *and* $D/27 = e^2(a^2 \pm 8^g e)$.
3. $\mathrm{ord}_3(D) = 2h + 1$ *where* $h > 1$ *and one of the following holds.*
   (a) $D/27 = e^2(a^2 \pm 8^g e)$.
   (b) $D/3^{2h+1} = e^2(a^2 \pm 8^g 3^{h-1} e)$.

Observe that while the primes dividing D_s and D_t are congruent to 3 mod 4 (as in Proposition 3.1), the primes dividing E can be congruent to 1 or 3 (mod 4). Note that Proposition 3.1 corresponds to the case $E = 1$ in Theorem 4.2. As seen earlier we used Proposition 3.1 to solve equation (3.4). By applying Theorems 4.1 and 4.2 we can extend the values of D. For instance, we can show that the equation

$$x^2 + 3^3\ 11^{\alpha_2}\ 19^{\alpha_3}\ E^2 = y^n, \quad \alpha_2,\ \alpha_3 \text{ odd}$$

with

$$E \in \{7, 31, 107\}$$

has no solution. For every prime $q|E$ for E in the above set, we observe that

$$\left(\frac{-3 \cdot 11 \cdot 19}{q}\right) = -1.$$

Further $q - \left(\frac{-3\cdot 11\cdot 19}{q}\right)$ is of the form $2^\alpha 3^\beta$ for non-negative integers α and β. Moreover (4.3) is satisfied. Hence by Theorem 4.1 every prime divisor of n divides $3h_0 = 12$. Thus we may suppose that $n = 3$. By Theorem 4.2 part 2, we have

$$11^{\alpha_2} 19^{\alpha_3} E^2 = a^2 \pm 8$$

or

$$11^{\alpha_2} 19^{\alpha_3} = a^2 \pm 8^g E$$

since E is a prime. These equalities are excluded using congruence argument modulo the primes 3,11 and 19.

Theorem 4.3 *Suppose equation* (3.5) *holds with* $p \in \{11, 19, 43, 67, 163\}$ *and* ℓ *is odd. Then all the solutions of* (3.5) *are given in Proposition* 3.2.

5 Lemmas

The following is [SA1, Lemma 4].

Lemma 5.1 *Let* d *be a positive integer. Then the equation*

$$x^2 + d = y^p \text{ with } \gcd(x, d) = 1 \tag{5.1}$$

in positive integers x, y *and* p *prime implies that either* $p = 3$ *or*

$$p \mid h(-4d).$$

The next lemma connects $h(-4D)$ with the class number h_0 of the quadratic field $\mathbb{Q}(\sqrt{-4D})$ where D is given in Theorem 4.1.

Lemma 5.2 *Let* D *be as given in Theorem* 4.1. *Then*

$$h(-4D) = 2^{\alpha_0} 3^{\beta_0+\delta} D_t h_0$$

where α_0 *and* β_0 *are non-negative integers,* $\delta = 0$ *if* $D_s \equiv 7 (\mathrm{mod}\ 8)$ *or* $D_s = 3$; $\delta = 1$ *if* $D_s \equiv 3 (\mathrm{mod}\ 8)$ *and* $D_s \neq 3$.

Proof. We refer to Mollin [Mo1] for the formula of $h(-4D)$ used in the proof below. As in [SA1, Lemma 5], we see that

$$h(-4D) = 3^{\delta} D_t E \mu h_0 \tag{5.2}$$

where

$$\mu = \prod_{\substack{p|D_t E \\ p \neq 2}} \left(1 - \frac{\left(\frac{-D_s}{p}\right)}{p}\right).$$

Since E is square-free and (4.2) holds there exist non-negative integers α_0 and β_0 such that

$$\mu = \prod_{p|E} (1 - \frac{\left(\frac{-D_s}{p}\right)}{p}) = \frac{2^{\alpha_0} 3^{\beta_0}}{E}. \tag{5.3}$$

The lemma follows from (5.2) and (5.3).

□

The following is [SA1, Lemma 6].

Lemma 5.3 *Let $D = D_s D_t^2 E^2$ where D_s is square-free. Suppose $x^2 + D = y^n$ with $n > 2$ and $\gcd(n, h_0) = 1$. Then there are integers a, b satisfying $\gcd(a, D_s) = 1$ and*

$$\frac{2^{ng} D_t E}{b} = \binom{n}{1} a^{n-1} - \binom{n}{3} a^{n-3} b^2 D_s + \ldots + (-1)^{\frac{n-1}{2}} b^{n-1} D_s^{\frac{n-1}{2}}$$

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

The last lemma below is based on congruence arguments. This is used in the proof of Theorem 4.3.

Lemma 5.4 *Let α, β, p, q and ℓ be given non-zero integers with ℓ odd, $p \nmid \alpha$ and $q|\ell$. Suppose there exist integers a, a_0 such that*

$$\alpha a^2 + \beta = p^{\ell} \text{ and } \alpha a_0^2 + \beta = p^q g \text{ with } g \geq 1. \tag{5.4}$$

Let $p^{2q} \equiv \pm 1 (\mathrm{mod}\ f)$ for some positive integer f. Then there exists an integer h with $0 \leq h < f$ such that

$$\alpha p^q h^2 + 2\alpha a_0 h + g \equiv \begin{cases} 1 (\mathrm{mod}\ f) & if\ p^{2q} \equiv 1 (\mathrm{mod}\ f) \\ \pm 1 (\mathrm{mod}\ f) & if\ p^{2q} \equiv -1 (\mathrm{mod}\ f). \end{cases}$$

Proof. Suppose (5.4) holds. Then

$$a \equiv \pm a_0 \pmod{p^q}.$$

Thus $a = p^q h' \pm a_0$ for some integer h'. Hence

$$p^\ell = \alpha a^2 + \beta = \alpha p^{2q} h'^2 \pm 2\alpha a_0 p^q h' + \alpha a_0^2 + \beta$$

which gives

$$\alpha p^q h'^2 \pm 2\alpha a_0 h' + g = p^{\ell - q}.$$

Since $\ell - q \equiv 0 \pmod{2q}$, we get for some h with $0 \leq h < f$,

$$\alpha p^q h^2 \pm 2\alpha a_0 h + g \equiv \begin{cases} 1 \pmod{f} & \text{if } p^{2q} \equiv 1 \pmod{f} \\ \pm 1 \pmod{f} & \text{if } p^{2q} \equiv -1 \pmod{f} \end{cases}$$

which proves the lemma.

□

6 Proofs of Theorems

Proof of Theorem 4.1. Let $n \neq 3$ and gcd $(n, h_0) = 1$. Since n is odd, we may assume that $n = p$ is a prime. By Lemmas 5.1 and 5.2, we get

$$p \mid D_t. \tag{6.1}$$

Hence $p | D_s$. From Lemma 5.3 we see that b is odd and for any prime q,

$$\mathrm{ord}_q(\frac{D_t}{p}) = \mathrm{ord}_q(b) \text{ and } \mathrm{ord}_q(E) \geq \mathrm{ord}_q(b).$$

Therefore $2^{pg} D_t E = \pm 2^{pg} pbe$ for some divisor e of E. Thus

$$\pm 2^{pg} e = a^{p-1} - \binom{p}{3} a^{p-3} b^2 \frac{D_s}{p} + \ldots + (-1)^{\frac{p-1}{2}} b^{p-1} \frac{D_s^{\frac{p-1}{2}}}{p}.$$

Considering the above equality mod p and using (4.3), we see that the left hand side is equal to 1. Thus $g = 0, e = 1$ and $D_t E = pb$. Now reducing the

equality mod 2 we conclude that a is an even integer with $\gcd(a, D_s) = 1$ such that

$$1 = a^{p-1} - \binom{p}{3} a^{p-3}\frac{D}{p^3} + \ldots + (-1)^{\frac{p-1}{2}}\frac{D^{\frac{p-1}{2}}}{p^p}.$$

Hence

$$(-1)^{\frac{p-1}{2}} D_s^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} D^{\frac{p-1}{2}} \equiv p \pmod 4.$$

As each $p_i \equiv 3 (\mathrm{mod}\ 4)$, we have

$$D_s \equiv 1 (\mathrm{mod}\ 4).$$

This is a contradiction since $D_s \equiv D \equiv 3 \pmod 4$ which proves the theorem.

Proof of Theorem 4.2. We observe that Theorem 4.1 is valid. We may assume that n is prime and since $\gcd(n, h_0) = 1$, we need only consider the case $n = 3$. Also by Lemma 5.3 there exists an integer a with $\gcd(a, D_s) = 1$ such that

$$8^g D_t E = b(3a^2 - b^2 D_s). \tag{6.2}$$

Note that b is odd. Suppose $3 \nmid D$. Then $3a^2 - b^2 D_s$ and D_t are coprime (as $\gcd(a, D_s) = 1$) and hence

$$3a^2 - b^2 D_s = 8^g e \tag{6.3}$$

and

$$b = \pm D_t e',$$

where $E = ee'$. Therefore from (6.2),

$$\pm 8^g e = 3a^2 - D/e^2,$$

that is

$$D = e^2(3a^2 \pm 8^g e).$$

Suppose $3|D$. By assumption $3 \nmid E$. If $3||D$, then $3|D_s$ but $3 \nmid D_t$. This contradicts (6.2). Hence $\mathrm{ord}_3(D) \geq 3$. Let $D = 3^{2h+1} Q_s Q_t^2 E^2$ where $D_s = 3Q_s, D_t = 3^h Q_t, h \geq 1$ and $3 \nmid Q_s Q_t$. Then (6.2) gives

$$8^g 3^{h-1} Q_t E = b(a^2 - b^2 Q_s), \tag{6.4}$$

which implies that

$$a^2 - b^2 Q_s = \pm 8^g 3^\alpha e \text{ and } b = \pm Q_t e' 3^\beta, \tag{6.5}$$

where $E = ee'$ and $\alpha, \beta \geq 0$ with $\alpha + \beta = h - 1$. Moreover $\alpha \cdot \beta = 0$ as $3 \nmid a$. Combining the two equations in (6.5) we get

$$D = 3^{2h+1-2\beta} e^2 (a^2 \pm 8^g 3^\alpha e). \tag{6.6}$$

If $h = 1$ then $\alpha = \beta = 0$ and (6.6) gives

$$D/27 = e^2(a^2 \pm 8^g e).$$

For $h > 1$ observe that parts 3(a) and 3(b) of Theorem 4.2 correspond to $\alpha = 0$ and $\beta = 0$ respectively.

Proof of Proposition 3.1. We observe that Proposition 3.1 corresponds to the case $E = 1$ and hence $e = 1$ in Theorem 4.2.

Suppose $3 \nmid D$. By reducing the equality in part 1 of Theorem 4.2 modulo 8, we note that $D \neq 3a^2 + 1$ and hence part 1 of Proposition 3.1 follows.

Now let $3|D$ with $\mathrm{ord}_3(D) = 3$. Then the equation in part 2 of Theorem 4.2 holds. Suppose $g = 0$. Then a is even and $D/27 \neq a^2 - 1$ since $D/27 \equiv 1$ or $5 (\mathrm{mod}\ 8)$. Since $D_s > 3$ and $D/27$ has prime factors $\equiv 3 (\mathrm{mod}\ 4)$ dividing to an odd power, $D/27$ cannot be equal to a sum of two squares. Hence $D/27 \neq a^2 + 1$. Thus $g \neq 0$. Since $D/27$ is not divisible by 3, it is not equal to $a^2 + 8$. Now the second part of the proposition follows.

Next let $h > 1$. Then by part 3 of Theorem 4.2

$$D/27 = a^2 \pm 8^g \text{ or } D/3^{2h+1} = a^2 \pm 8^g 3^{h-1}. \tag{6.7}$$

First we consider

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

Reducing the above equation modulo 3 and modulo 8 and observing $D/27 \equiv 0 (\mathrm{mod}\ 3)$ and 1 or 5 $(\mathrm{mod}\ 8)$, we obtain

$$D/27 = a^2 + 8. \tag{6.8}$$

Next consider

$$D/3^{2h+1} = a^2 \pm 8^g 3^{h-1}. \tag{6.9}$$

Let $g = 0$. Since each prime factor of D is congruent to $\equiv 3 (\mathrm{mod}\ 4)$ and occurs with an odd exponent, we have

$$D/3^{2h+1} = a^2 - 3^{h-1} \text{ with } h \text{ even}. \tag{6.10}$$

This concludes the proof of part 3 of Proposition 3.1.

Proof of Theorem 4.3. Let $p \in \{11, 19, 43, 67, 163\}$. By Proposition 3.2 we have $\ell = 3^\alpha 5^\beta > 5$. By Proposition 3.1, there exists an integer a such that

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

or

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

Consider

$$3a^2 - 1 = 11^\ell \text{ or } 3a^2 + 8 = 11^\ell. \tag{6.11}$$

Reducing ℓ modulo 3, we obtain elliptic equations of the form

$$Y^2 = X^3 + k \tag{6.12}$$

with $k \in \{3^3, 3^3 \cdot 11^2, 3^3 \cdot 11^4, -8 \cdot 3^3, -8 \cdot 3^3 \cdot 11^2, -8 \cdot 3^3 \cdot 11^4\}$. We find all the integral solutions using MAGMA and verify that they do not satisfy (6.11). Thus $p \neq 11$.

Next consider $p = 43$. Then

$$3a^2 - 8 = 43^\ell$$

which is not satisfied modulo 7. Thus $p \neq 43$. Finally consider

$$p \in \{19, 67, 163\}.$$

We have

$$3a^2 - 8 = p^\ell. \tag{6.13}$$

We provide here a simple congruence argument based on Lemma 5.4 to rule out these cases.

Let $p = 19$. Suppose $3 \mid \ell$. We apply Lemma 5.4 with $q = 3,\ \alpha = 3,\ \beta = -8$ and $f = 27$. We find that $19^6 \equiv 1 (\text{mod } 27)$ and $a_0 = 1466$. Hence $g = 940$. We check that

$$3 \cdot 19^3 h^2 + 6 \cdot 1466h + 940 \not\equiv 1 (\text{mod } 27) \text{ for } 0 \leq h < 27.$$

Hence by Lemma 5.4,

$$3a^2 - 8 \neq 19^\ell \text{ for any } \ell \text{ with } 3 \mid \ell. \tag{6.14}$$

Suppose $5 \mid \ell$. Then let $q = 5,\ \alpha = 3,\ \beta = -8$ and $f = 11$. We have $19^{10} \equiv 1 (\text{mod } 11)$ and $a_0 = 2278654$ and $g = 6290860$. We see that

$$3 \cdot 19^5 h^2 + 6 \cdot 2278654h + 6290860 \not\equiv 1 (\text{mod } 11) \text{ for } 0 \leq h < 11.$$

Hence by Lemma 5.4,

$$3a^2 - 8 \neq 19^\ell \text{ for any } \ell \text{ with } 5 \mid \ell. \tag{6.15}$$

We combine (6.14) and (6.15) to get the assertion of the theorem for $p = 19$. For $p = 67, 163$, we give the necessary parameters for the application of Lemma 5.4.

$p = 67;$ $\quad q = 3,\ a_0 = 203953,\ g = 414913,\ f = 7,$ if $3 \mid l$.
$\quad q = 5,\ a_0 = 620270116,\ g = 854887480,\ f = 25$ if $5 \mid l$.

$p = 163:$ $\quad q = 3,\ a_0 = 689427,\ g = 329257,\ f = 19$ if $3 \mid l$.
$\quad q = 5,\ a_0 = 40142383370,\ g = 42013565644,\ f = 27,$ if $5 \mid l$.

This completes the proof of Theorem 4.3.

□

We note here that we may reduce ℓ modulo 3 in (6.13) to get an elliptic curve as in the case $p = 11$ to find all integral solutions using MAGMA. However, it is not clear to us if MAGMA can solve all possible values. For instance, when $k = -8 \cdot 3^3 \cdot 67^4$ MAGMA did not return any result even after three hours. We also note that the case $p = 11$ can be excluded by using an old result of Walker [W] and a result on primitive divisors of Lucas and Lehmer sequences from [BHV].

Remark. We record here with thanks a simpler congruence argument given by the anonymous referee to exclude the cases $p = 19, 67$ and 163. Recall that 3 or 5 divides l. Let $p = 19$. From (6.13), we get modulo 27 that $l \equiv 1 (\text{mod } 3)$ and modulo 151 that $l \equiv 1, 2 (\text{mod } 5)$, a contradiction. Let $p = 67$. Then modulo 49, we have $l \equiv \pm 1 (\text{mod } 3)$ and modulo 761, $l \equiv \pm 1, \pm 2 (\text{mod } 5)$, again a contradiction. Finally (6.13) with $p = 163$ is not satisfied modulo 81.

7 Values of D for which there are no solutions

In [SA1] we presented certain sets of values of D for which (4.1) has no solution. As pointed out earlier in Section 3, some of these sets are not

correct as they relied upon an incomplete result which we have corrected in Proposition 3.1 We list below a new set of values of $D = D_s D_t^2 = p_1^\alpha p_2^\beta p_3^\gamma$ where α, β and γ are odd integers. For these values of D equation (4.1) has no solution by applying the three criteria in Proposition 3.1. and congruence arguments modulo 8 or some suitable prime.
Let U_1 be the set of values of D with $(p_1, \alpha) = (3, 3)$ and

$$(p_2, p_3) \in \{(7,19),(7,43),(7,283),(11,19),(11,47),(11,59),(11,67),$$

$$(11,71),(11,83),(11,107),(11,131),(11,179),(11,227),(11,251),(19,31),$$

$$(19,59),(19,67),(19,107),(19,139),(19,163),(31,67),(43,67)\}.$$

Let U_2 be the set of values of D with $p_1 = 3, \alpha > 3$ and

$$(p_2, p_3) \in \{(7,23),(7,47),(7,167),(7,383),(23,31).$$

Let U_3 be the set of values of D with

$$(p_1, p_2, p_3) \in \{(3,7,59),(3,7,227),(3,7,251),(3,7,467),(3,11,31),(3,11,199),$$

$$(7,11,19),(7,11,23),(7,11,71),(7,11,107),(7,19,31),(7,23,43),(11,23,31),(11,19,43)\}.$$

References

[Ap] R. Apéry, *Sur ue èquation diophantienne*, C.R. Acad. Sci. Paris Sér. A **251** (1960), 1263–1264 and 1451–1452.

[AM] S.A. Arif and F.S. Abu Muriefah, *The Diophantine equation* $x^2+3^m = y^n$, Int. J. Math. Sci **21** (1998), no.3, 619–620.

[BeS] M.A. Bennett and C.M. Skinner, *Ternary Diophantine equations via Galois representations and modular forms,* Canad. J. Math. **56** (2004), no. 1, 23-54.

[Beu1] F. Beukers, *On the generalized Ramanujan- Nagell Equations, I,* Acta Arith. **38** (1980/1981), 389-410.

[Beu2] F. Beukers, *On the generalized Ramanujan- Nagell Equations, II,* Acta Arith. **39** (1981), 113-123.

[BHV] Y. Bilu, G. Hanrot and P. Voutier (with an appendix by M. Mignotte), *Existence of primitive divisors of Lucas and Lehmer numbers,* J. reine angew. Math. **539** (2001), 75–122.

[BuS] Y. Bugeaud and T.N. Shorey, *On the number of solutions of the generalized Ramanujan-Nagell equation*, I.J. reine angew. Math. **539** (2001), 55–74.

[BMS] Y. Bugeaud, M. Mignotte and S. Siksek, *Classical and modular approaches to exponential and Diophantine equations II. The Lebesgue-Nagell equation,* Compos. Math. **142** (2006), no. 1, 31-62.

[Bu] Y. Bugeaud, *On some exponential Diophantine equations,* Monatsh. Math **132** (2001), 93-97.

[CLS] S. Chowla, D.J. Lewis and Th. Skolem, *The Diophantine equation* $2^{n+2}-7 = x^2$ *and related problems,* Proc. Amer. Math. Soc. **10** (1959), 250-257.

[Co] J.H.E. Cohn, *The Diophantine equation* $x^2 + C = y^n$*,* Acta Arith. **55** (1993), 367–381.

[DG] H. Darmon and A. Granville, *On the equations* $z^m = F(x, y)$ *and* $Ax^p + By^q = Cz^r$, Bull. London Math. Soc, **27** (1995), 513-543.

[Leb] V. A. Lebesgue, *Sur l'impossibilité en nombres entiers de l'équation* $x^m = y^2 + 1$, Nouvelles Annales des Mathématiques (1) **9** (1850), 178-181.

[Le1] Maohua Le, *The Diophantine Equation* $x^2 + D^m = p^n$, Acta Arith, **52** (1989), 255-265.

[Le2] Maohua Le, *On the Diophantine Equations* $d_1x^2 + d_2 = 4y^n$, Proc. Amer. Math.Soc, **118** (1993), 67-70.

[Le3] Maohua Le, *A note on the Diophantine Equation* $x^2 + 4D = y^p$, Monatsh Math, **116** (1993), 283-285.

[Le4] Maohua Le and T. Xu, *On the Diophantine Equation* $D_1x^2+D_2 = k^n$, Publ. Math. Debrecen, **47** (1995), 293-297.

[Le5] Maohua Le, *The Diophantine equation* $x^2 + 2^m = y^n$, Chinese Sci. Bull **42** (1997), 1515–1517.

[LL] Ming-Guang Leu and Guan-Wei Li, *The Diophantine equation* $2x^2 + 1 = 3^n$, Proc. Amer. Math. Soc. **131** (2003), no.12, 3643-3645.

[Lu] F. Luca, *On the equation* $x^2 + 2^a 3^b = y^n$, IJMMS **29** (2002), 239–244.

[Mo1] R.A. Mollin, *Quadratics*, CRC Press, New York, 1996, 387p.

[Mo2] R. A. Mollin, *A note on the Diophantine Equation* $D_1x^2 + D_2 = ak^n$, Acta Math. Acad. Pædagog. Nyházi(N.S.) **21** (2005), no.1, 21-24.

[MW] M. Mignotte and B.M.M de Weger, *On the equations* $x^2 + 74 = y^5$ *and* $x^2 + 86 = y^5$, Glasgow Math. J. **38**(1) (1996), 77-85.

[Na1] T. Nagell, *The Diophantine equation* $x^2+7 = 2^n$, Ark. Math.**4** (1960), 185-187.

[Na2] T. Nagell, *Darstellung ganzer Zahlen durch biná re kubische Formen mit negativer Diskriminante,* Math. Z. **28** (1928), no. 1, 10-29.

[Ra] S. Ramanujan, *Question 446*, J. Indian Math. Soc.**5** (1913), 120, Collected papers, Cambridge University Press (1927), 327.

[SA1] N. Saradha and Anitha Srinivasan, *Solutions of some generalized Ramanujan-Nagell equation*, Indag Mathem.N.S., **17** (1)(2006), 103-114.

[SA2] N. Saradha and Anitha Srinivasan, *Solutions of some generalized Ramanujan- Nagell equations via binary quadratic forms,* to appear in Publ.Math., Debrecen.

[ST] T. N. Shorey and R. Tijdeman, *Exponential Diophantine equations,* Cambridge Tracts in Mathematics **87**, Cambridge University Press, Cambridge, 1986.

[Sh] T. N. Shorey, *Diophantine approximations, Diophantine equations, Transcendence and Applications,* Indian Jour. of Pure and Applied Math., **37**(1) (2006), 9-39.

[Si] C. L. Siegel, *Approximation algebraischer Zahlen*, Math. Zeit. **10** (1921), 173-213.

[St] J. Stiller, *The Diophantine equation $x^2 + 119 = 15 \cdot 2^n$ has exactly six solutions,* Rocky Mountain J. math. **26** (1996), 295-298.

[W] D.T. Walker, *On the Diophantine Equation $mx^2 - ny^2 = \pm 1$,* Amer. Math. Monthly, **74** (1967), 504-513.

[Yu] P. Yuan, *On the Diophantine equation $ax^2 + by^2 = ck^n$*, Indag. Mathem. N.S., **16**(2), (2005), 301–320.

School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road
Mumbai-400005, India
e-mail: saradha@ math.tifr.res.in

Department of Mathematics
Indian Institute of Technology
Powai
Mumbai-400076, India
e-mail: anitha@ math.iitb.ac.in