Publ. Math. Debrecen
71/3-4 (2007), 349–374

Solutions of some generalized Ramanujan–Nagell equations via binary quadratic forms

By N. SARADHA (Mumbai) and ANITHA SRINIVASAN (Mumbai)

Abstract. Let h be the class number of binary quadratic forms of discriminant $-4d$, where d is odd and I is the identity form $x^2 + dy^2$. Let λk^n be represented by I, where λ is a prime power represented by I and k is prime. Then we show that k^r is represented by I for some r dividing h and representations of λk^n by I arise out of the representations by I of λ and k^r. As an application we solve several generalized Ramanujan–Nagell equations of the type $x^2 + d = \lambda k^n$.

1. Introduction

For any integer n let $\omega(n)$ denote the number of distinct prime divisors of n where $\omega(\pm 1)$ is 0. Let $\nu_p(n)$ denote the exact power of the prime p in n with $\nu_p(\pm 1) = 0$ and $\nu_p(0) = \infty$. Throughout this paper λ, d, k are odd integers such that $\lambda \geq 1, d, k > 1$, $\gcd(\lambda, k) = \gcd(\lambda k, d) = 1$ and d is not a perfect square. A binary quadratic form of discriminant D is a function $ax^2 + bxy + cy^2$ with $b^2 - 4ac = D$. We can define an equivalence relation on the set of all binary quadratic forms of a given discriminant so that the equivalence classes form a group known as the *class group.* The *order* of the class group is denoted by $h(D)$. The form $x^2 + dy^2$ is the *identity form* which belongs to the identity class. An integer m is said to be *represented* by the form $ax^2 + bxy + cy^2$, if there exist coprime positive integers x_0 and y_0 such that $m = ax_0^2 + bx_0y_0 + cy_0^2$. A classical problem in the theory of quadratic forms is the following.

Mathematics Subject Classification: 11D61.
Key words and phrases: Ramanujan–Nagell equation, binary quadratic forms, class number.

Given integers m and $D, D \equiv 0$ or $1 \pmod 4$ does there exist a representation of m by some form of discriminant D, in particular, by the identity form ?

See [11] for other fundamental problems. We consider the problem of when the identity form can represent powers of a given integer $k > 1$. In other words, we ask for solutions of the Diophantine equation

$$x^2 + dy^2 = k^z \text{ in integers } x, y, z \text{ with } \gcd(x, y) = 1 \quad \text{and } z > 1. \tag{1.1}$$

See Nagell ([10], Chapter VI) for various results on the identity form representing a prime or a prime power. See also Hua ([6], Chapter 12) for results on the number of such representations. In [8], Le uses the class group structure to classify all solutions of $D_1x^2 - D_2y^2$ with $D_1 > 0$ and D_1D_2 not a square ($D_1 = 1, D_2 = -d$ gives (1.1)). He gives explicit formulas for these solutions that have a natural form. Later Heuberger and Le [5] elaborated and clarified certain ambiguities in the works of Le. Bugeaud and Shorey [2] proved numerous results on equations similar to (1.1) using Le's classification. (Their work depends also on the work of Bilu, Hanrot and Voutier [1] on primitive divisors of Lucas and Lehmer sequences.)

In this paper we consider the equation

$$x^2 + dy^2 = \lambda k^z \text{ in integers } x, y, z \text{ with } \gcd(x, y) = 1 \quad \text{and } z > 1. \tag{1.2}$$

From the theory of binary quadratic forms it is known that if an odd integer m is represented by a form of discriminant $-4d$ then all its divisors are also represented by *some* form of the same discriminant. Hence we may assume that λ and k are represented by *some* form (not necessarily the same one) of discriminant $-4d$.

Using the class group structure of forms, we prove the following result when λ and k are prime powers.

Theorem 1.1. *Suppose q_1 and q_2 are distinct primes not dividing d. Let f and g be classes that represent q_1 and q_2 respectively with corresponding orders r_1 and r_2. Then the equation*

$$x^2 + dy^2 = q_1^m q_2^n, \quad \gcd(x, y) = 1, \ m, n \geq 1 \tag{1.3}$$

implies that

$$r_1 \gcd(n, r_2) = r_2 \gcd(m, r_1). \tag{1.4}$$

In particular,

$$r_1 \mid m \text{ if and only if } r_2 \mid n. \tag{1.5}$$

Further if $\gcd(r_1, r_2) = 1$, then $r_1 \mid m$ and $r_2 \mid n$. If q_1 and q_2 are represented by the same class, then $r_1 = r_2 = r$ and (1.3) has a solution if and only if $r \mid (m+n)$ or $r \mid (m-n)$.

Remark 1.1. The integers r_1 and r_2 in Theorem 1.1 are uniquely determined by the primes q_1 and q_2 respectively. This is because a prime is represented by at-most two classes and these two classes are inverses of each other (see Lemma 3.9).

Note that (1.3) has no solution if either $r_1 \mid m$ and $r_2 \nmid n$ or $r_1 \nmid m$ and $r_2 \mid n$. It has solutions if $r_1 \mid m$ and $r_2 \mid n$. We illustrate the theorem with the following examples. Consider

$$x^2 + 31y^2 = 5^m 7^n.$$

Here $d = 31$, $q_1 = 5$ and $q_2 = 7$. Note that $h(-31) = h(-4 \cdot 31) = 3$. The three inequivalent classes have their representative forms as $e = 8x^2 + xy + y^2$, $f = 4x^2 + xy + 2y^2$ and $g = 5x^2 + 3xy + 2y^2$ with $f^3 \sim g^3 \sim e$ and $f^2 \sim g$. Here e represents the identity class. We see that 5 and 7 are both represented by f and hence also by $g = f^{-1}$. Thus $r_1 = r_2 = 3$ and by Theorem 1.1, we have $3 \mid (m+n)$ or $3 \mid (m-n)$. These conditions are equivalent to either $3 \mid m$, $3 \mid n$ or $3 \nmid m$, $3 \nmid n$. Note that if these conditions are satisfied the equation under consideration has solutions. For example,

$$5^3 = 1 + 31 \cdot 2^2;\ 7^3 = 8^2 + 31 \cdot 3^2 \text{ and } 5^3 \cdot 7^3 = 194^2 + 31 \cdot 13^2 \text{ or } 178^2 + 31 \cdot 19^2;$$

$$5 \cdot 7 = 2^2 + 31;\ 5 \cdot 7^2 = 11^2 + 31 \cdot 2^2;\ 5^2 \cdot 7 = 12^2 + 31;\ 5^2 \cdot 7^2 = 27^2 + 31 \cdot 4^2.$$

Also the equation has no solution if $3 \mid m$ and $3 \nmid n$ or $3 \nmid m$ and $3 \mid n$.

Next consider

$$x^2 + 17y^2 = 3^m 53^n.$$

Here $53 = 6^2 + 17$ and $3^4 = 8^2 + 17$. Note that $h(-4 \cdot 17) = 4$. Also $q_1 = 3$, $r_1 = 4$, $q_2 = 53$, $r_2 = 1$. By Theorem 1.1, this equation has no solution whenever $m \not\equiv 0 \pmod 4$.

If λ is represented *only* by the identity class, then it follows that k^z is also represented by the identity class and (1.2) has solutions. In fact, all the solutions of (1.2) can be put into $N_\lambda 2^{\omega(k)-1}$ classes where N_λ denotes the number of representations (up to signs) of λ by the identity form (see Section 4, Proposition 4.1). This generalizes Le's result on (1.1) as 1 is represented *only* by the identity class. Our work is based on the theory of binary quadratic forms. We point out here that our representation is similar to that of Yuan [13]. Indeed he gives the representations of solutions of a more general equation than (1.2) namely of

$$ax^2 + by^2 = ck^n \text{ with } \gcd(ax, by) = 1 \text{ in positive integers } x, y \text{ and } n.$$

He uses the structure of abelian groups and ideal theory of quadratic fields.

In the case when λ is a prime power represented by the identity class and k is a prime, there is *only one* class of solutions of (1.2) which we present in Theorem 1.2 below. We point out that all the theorems below assume these conditions on λ and k, namely,

$$\textit{λ is a prime power represented by the identity class and k is a prime.} \tag{1.6}$$

Theorem 1.2. *Assume* (1.6). *Then there exists a unique positive integer $r \mid h(-4d)$ and unique (up to signs) representations of λ and k^r by the identity form such that the following holds. If (x', y', z) is a solution of* (1.2) *then $z = rt$ for some $t \geq 1$ and $x' = \pm x, y' = \pm y$ where*

$$x + y\sqrt{-d} = (x_0 + y_0\sqrt{-d}\,)(x_1 + y_1\sqrt{-d}\,)^t \tag{1.7}$$

with $x_0^2 + dy_0^2 = \lambda, x_1^2 + dy_1^2 = k^r$.

We observe that if x and y satisfy (1.7) for some $t \geq 1$, then (x, y, rt) is a solution to (1.2). When $y = \pm 1$ in (1.2) we get the so called generalized Ramanujan–Nagell equations of the form

$$x^2 + d = \lambda k^n \text{ in integers } x \text{ and } n > 2. \tag{1.8}$$

From the theory of linear forms in logarithms, it is known that (1.8) has only finitely many solutions. There are several results in the literature on the number of solutions of (1.8), especially when $\lambda = 1$ and k is prime. See for instance [2]. We note that (1.8) has a solution if and only if (1.2) has a solution with $y = \pm 1$. If (1.6) holds then by Theorem 1.2, (1.8) has a solution if and only if (1.7) has a solution with $y = \pm 1$. In the following Theorems 1.3–1.6 we present conditions under which (1.7) does not hold with $y = \pm 1$. Thus we are able to completely solve some generalized Ramanujan–Nagell equations of type (1.8).

In the theorems below we use the following notation. If p is a prime dividing $d - 1$ we write

$$d = p^\theta f + 1 \text{ with } p \nmid f \text{ and } \theta > 0. \tag{1.9}$$

We begin with the case $\lambda = 1$. As mentioned earlier, 1 is represented *only* by the identity class.

Theorem 1.3. *Assume* (1.6). *Let d satisfy* (1.9) *with $\theta > 1$ if $p = 2$. Suppose $x_0 = 1$, $y_0 = 0$ and $\theta < 2\nu_p(x_1)$. Then* (1.8) *has no solution except possibly when $n = r$ where r is as given in Theorem 1.2.*

For example, the equation

$$x^2 + 105 = 11^n \quad \text{with} \quad n > 2$$

has no solution. Here $p = 2, \theta = 3$, $\lambda = 1$ and $k = 11$. Also $r = 2$ as $11^2 = 4^2 + 105$. Therefore $x_1 = 4, \nu_2(x_1) = 2$. By Theorem 1.2, we find that $n = 2t$. Since $\theta < 2\nu_2(x_1)$, by Theorem 1.3, we see that the equation has no solution for $n > 2$. Here we note that (1.8) with $d \leq 100, \lambda = 1$ has been completely solved in x, k and n by Bugeaud, Mignotte and Siksek [3]. See also [4] and [7].

We assume henceforth that x_0, y_0, x_1, y_1 are all non-zero integers. It is clear from the expression for y (see Section 5) that $y \neq \pm 1$ if any of $\gcd(x_0, y_0)$, $\gcd(y_0, y_1)$ and $\gcd(x_1, y_1)$ exceeds 1. In Theorems 1.4–1.6, we consider the cases $\gcd(y_0, x_1) > 1$, $\gcd(x_0, x_1) > 1$ and $\gcd(x_0, y_1) > 1$.

Theorem 1.4. *Assume* (1.6). *Let* (1.9) *hold with* $p = 2$ *and* $\theta > 1$. *Suppose* $2 \mid \gcd(y_0, x_1)$ *and* $x_0, y_1 \in \{-1, 1\}$. *Further let*

$$\nu_2(y_0) + \nu_2(x_1) < \min(\theta, 2\nu_2(x_1)).$$

Then (1.8) *has no solution.*

As an example let $(\lambda, d, k) = (3301, 33, 7)$. Then $\theta = 5$ and $r = 2$. Moreover as $\lambda = 3301 = 1 + 33 \cdot 10^2$ and $k^r = 7^2 = 4^2 + 33$, we have $\nu_2(y_0) = 1, \nu_2(x_1) = 2$. Note that 3301 is a prime. Thus all the conditions of Theorem 1.4 are satisfied. Therefore the equation

$$x^2 + 33 = 3301 \cdot 7^n$$

has no solution.

Theorem 1.5. *Assume* (1.6). *Let* $y_0, y_1 \in \{-1, 1\}$. *Suppose that there exists a prime* p *such that* $p \mid \gcd(x_0, x_1)$ *and* (1.9) *holds. Suppose further that either*

(i) $\quad \nu_p(x_0) < \nu_p(x_1)$ *and* $\theta \neq \nu_p(x_0) + \nu_p(x_1)$ *if* $p \geq 3$

or

(ii) $\quad p = 2,\ \theta > 1,\ \nu_2(x_0) + 1 \neq \nu_2(x_1)$ *and* $\theta \neq \nu_2^* + \nu_2(x_1)$

or

(iii) $\quad p = 2,\ \theta > 1,\ \nu_2(x_0) + 1 = \nu_2(x_1)$ *and* $\theta \leq \nu_2(x_0) + \nu_2(x_1) + 1$

where $\nu_2^* = \min(\nu_2(x_0) + 1, \nu_2(x_1))$ *holds. Then* (1.8) *has no solution.*

Observe that if $\nu_2(x_1) = 1$ and $\theta \geq 3$, then condition (ii) above is satisfied. For example,

$$x^2 + 33 = 7^2 \cdot 37^n$$

has no solution since $7^2 = 4^2 + 33$ and $37 = 2^2 + 33$, hence condition (ii) is satisfied with $(\lambda, d, k) = (7^2, 33, 37)$. Similarly using condition (iii) in Theorem 1.5 we see that

$$x^2 + 33 = 7^2 \cdot 97^n$$

has no solution. The equation

$$x^2 + 7 = 43 \cdot 331^n$$

has no solution by Theorem 1.5(i) with $p = 3$.

Theorem 1.6. *Assume* (1.6). *Suppose* $y_0, x_1 \in \{-1, 1\}$. *Assume that there exists a prime* p *such that* $p \mid \gcd(x_0, y_1)$ *and* (1.9) *holds. Suppose further that*

$$\nu_p(x_0) + \epsilon < \nu_p(y_1)$$

where $\epsilon = 0$ *if* $p \geq 3$ *and* $\epsilon = 1$ *if* $p = 2$. *Then* (1.8) *has no solution.*

Consider $(\lambda, d, k^r) = (7, 3, 97^2)$. Then $\lambda = 7 = 2^2+3$ and $k^r = 97^2 = 1+3\cdot 56^2$ with $\nu_2(x_0) = 1$ and $\nu_2(y_1) = 3$. Hence by Theorem 1.6,

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

has no solution.

The plan of the paper is as follows. In Section 2 we present the basic definitions and notations of binary quadratic forms. In Section 3 we present proofs of certain results on binary quadratic forms. Section 4 contains the main lemmas and proofs of Theorems 1.1 and 1.2. Lemmas 4.4 and 4.5 also appear in [7]. Apart from the above two mentioned lemmas the remaining lemmas in Section 4 state results that while most certainly are not new, are not very well known. The proof of Theorem 1.2 depends only on these fundamental results on binary quadratic forms. In Section 5 we use combinatorial arguments which lead to the proofs of Theorems 1.3–1.6. The results of this paper can be generalized to the cases when d is negative. Moreover the restriction that λ and k be odd can also be relaxed. These cases will be treated in another article.

We refer to Hua [6], Ribenboim [11] and Rose [12] for the theory of binary quadratic forms. Also Appendix E in [9] is a compact and useful reference for results on binary quadratic forms.

2. Binary quadratic forms

A *binary quadratic form* $f = (a, b, c)$ of discriminant D is a function $f(x, y) = ax^2 + bxy + cy^2$, where a, b, c are integers such that $D = b^2 - 4ac$. Sometimes we write a binary quadratic form of discriminant D simply as (a, b), as the third coefficient c is determined by the discriminant equation above. A binary quadratic form (a, b, c) is called *primitive* if $\gcd(a, b, c) = 1$. Henceforth, we shall consider only primitive binary quadratic forms. Let $f = (a, b, c)$ be a form of discriminant D. Then $b^2 \equiv D \pmod{4a}$. Thus b and D are of the same parity. The forms $f = (a, b, c)$ and $f' = (a', b', c')$ are said to be *equivalent*, written as $f \sim f'$ if there exists a transformation

$$x = \alpha X + \beta Y, y = \gamma X + \delta Y$$

with $\alpha\delta - \gamma\beta = 1$ and $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ that takes f to f', i.e.

$$ax^2 + bxy + cy^2 = a'X^2 + b'XY + c'Y^2.$$

Note that

$$a' = f(\alpha, \gamma), \quad b' = b(\alpha\delta + \beta\gamma) + 2(a\alpha\beta + c\gamma\delta), \quad c' = f(\beta, \delta). \tag{2.1}$$

The matrix $A = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ is called the *transformation matrix* which takes f to f'. It is easily seen that equivalent forms represent the same integers.

The Composition formula. Let $f = (a_1, b_1, c_1)$ and $h = (a_2, b_2, c_2)$ be two forms. Then the composition $f \circ h$ is the form (a', b', c') obtained as follows. Let $g = \gcd(a_1, a_2, \frac{b_1+b_2}{2})$ and let $v_1, v_2, w \in \mathbb{Z}$ be integers that satisfy

$$v_1 a_1 + v_2 a_2 + w\frac{b_1 + b_2}{2} = g.$$

Then a', b' and c' are given as follows:

$$\begin{aligned} a' &= \frac{a_1 a_2}{g^2}, \\ b' &\equiv b_2 + \frac{2a_2}{g}\left(\frac{b_1 - b_2}{2}v_2 - c_2 w\right) \pmod{2a'}, \quad 1 \le b' \le 2a', \\ c' &= \frac{(b')^2 - D}{4a'}. \end{aligned}$$

We observe that if $f \sim f'$ and $g \sim g'$, then $f \circ g \sim f' \circ g'$. By f^n or $(a, b, c)^n$ we mean composition of the form f with itself n times.

The *class number* $h(D)$ is the number of *equivalence classes* of primitive binary quadratic forms of discriminant D. The equivalence classes of primitive binary quadratic forms form an abelian group called the *class group* with composition of forms as the group law. The *identity class* is the class of the *identity form*, which is defined as the form $e = (1, 0, \frac{-D}{4})$ or $(1, 1, \frac{1-D}{4})$ depending on whether D is even or odd respectively. The *inverse* of $f = (a, b, c)$ denoted by f^{-1} is given by $(a, -b, c)$. We denote the *order* of the form f in the class group by $\mathrm{ord}(f)$.

Suppose an integer m and a form f are given. We say that the equality $f(x, y) = m$ is a *representation* (of m) if the integers x and y are coprime.

3. Basic lemmas on binary quadratic forms

The results in this section are well known. However, we provide proofs for the sake of completeness.

Definition 3.1. If a transformation matrix A takes the form f to the form f' we write $T_A(f) = f'$.

The following lemma may be verified easily.

Lemma 3.1. *If f_1, f_2 and f_3 are forms such that $T_A(f_1) = f_2$ and $T_B(f_2) = f_3$, then $T_{AB}(f_1) = f_3$.*

Lemma 3.2. *The form (a, b, c) is equivalent to the form $(a, b + 2a\delta)$ for any integer δ.*

Proof. The equivalence follows via the matrix $\begin{pmatrix} 1 & \delta \\ 0 & 1 \end{pmatrix}$. □

Lemma 3.3. *Let f and h be two forms. Then there exists a unique form F such that $f \circ h = F$.*

Proof. Let $f = (a_1, b_1, c_1)$ and $h = (a_2, b_2, c_2)$. Let $\gcd(a_1, a_2, \frac{b_1+b_2}{2})$ be denoted by g with $a_1 = ga_1'$, $a_2 = ga_2'$ and $\frac{b_1+b_2}{2} = gB$. Let integers v_1, v_2, w and v_1', v_2', w' satisfy

$$v_1 a_1 + v_2 a_2 + w\frac{b_1 + b_2}{2} = g = v_1' a_1 + v_2' a_2 + w'\frac{b_1 + b_2}{2}.$$

Let (a, ϕ) and (a, ϕ') be the corresponding forms obtained by the composition formula. We have

$$v_1 a_1' + v_2 a_2' + wB = 1 = v_1' a_1' + v_2' a_2' + w'B.$$

Thus

$$(v_2 - v_2')a_2' \equiv -(w - w')\left(\frac{b_1 + b_2}{2g}\right) \pmod{a_1'},$$

and hence

$$(v_2 - v_2')\left(\frac{b_1 - b_2}{2}\right)a_2' \equiv -(w - w')\left(\frac{b_1^2 - b_2^2}{4g}\right) \pmod{a_1'}.$$

Since $D = b_1^2 - 4a_1c_1 = b_2^2 - 4a_2c_2$, we have $\frac{b_1^2 - b_2^2}{4} = a_1c_1 - a_2c_2$ implying that

$$\frac{b_1^2 - b_2^2}{4g} \equiv -c_2a_2' \pmod{a_1'}.$$

Therefore

$$\frac{b_1 - b_2}{2}(v_2 - v_2') \equiv c_2(w - w') \pmod{a_1'}.$$

It follows that

$$\phi - \phi' = 2a_2'\left(\frac{b_1 - b_2}{2}(v_2 - v_2') - c_2(w - w')\right) \equiv 0 \pmod{2a_1'a_2'}$$

which gives $\phi = \phi'$ since by definition, $1 \leq \phi,\ \phi' \leq 2a_1'a_2'$. Hence $(a, \phi) = (a, \phi')$. □

Lemma 3.4. *Let (a_1, b_1, c_1) and (a_2, b_2, c_2) be two forms. For $i = 1, 2$ let (a_i, b_i', c_i') be forms such that $b_i \equiv b_i' \pmod{2a_i}$. Then the compositions $(a_1, b_1, c_1) \circ (a_2, b_2, c_2)$ and $(a_1, b_1', c_1') \circ (a_2, b_2', c_2')$ are equal.*

Proof. Let $b_i' = b_i + 2a_ik_i$ for $i = 1, 2$. Then $c_i' = c_i + a_ik_i^2 + b_ik_i$. Let $g = \gcd(a_1, a_2, \frac{b_1+b_2}{2})$. Note that $g = \gcd(a_1, a_2, \frac{b_1'+b_2'}{2})$. Let the two compositions in the lemma be $(\frac{a_1a_2}{g^2}, \phi_i)$ for $i = 1, 2$, where $v_1,\ v_2, w$ and $v_1',\ v_2', w'$ are chosen such that

$$v_1a_1 + v_2a_2 + w\frac{b_1 + b_2}{2} = g \tag{3.1}$$

and

$$v_1'a_1 + v_2'a_2 + w'\frac{b_1' + b_2'}{2} = g. \tag{3.2}$$

Equation (3.2) above gives $a_1(v_1' + w'k_1) + a_2(v_2' + w'k_2) + w'\frac{b_1+b_2}{2} = g$. Observe that if we set $w' = w$, $v_1' = v_1 - wk_1$ and $v_2' = v_2 - wk_2$, then (3.2) is satisfied. By the composition formula, $\left(\bmod \frac{2a_1a_2}{g^2}\right)$ we have

$$\phi_1 \equiv b_2 + \frac{2a_2}{g}\left(v_2\frac{b_1 - b_2}{2} - c_2w\right) \quad \text{and} \quad \phi_2 \equiv b_2' + \frac{2a_2}{g}\left(v_2'\frac{b_1' - b_2'}{2} - c_2'w\right).$$

Therefore

$$\begin{aligned}
\phi_2 &\equiv b_2 + 2a_2k_2 \\
&\quad + \frac{2a_2}{g}\left((v_2 - wk_2)\Big(\frac{b_1-b_2}{2} + a_1k_1 - a_2k_2\Big) - w\left(c_2 + a_2k_2^2 + b_2k_2\right)\right) \\
&\equiv \phi_1 + 2a_2k_2 + \frac{2a_2}{g}\left(a_1k_1v_2 - a_2k_2v_2 - k_2w\frac{b_1+b_2}{2} - k_2wa_1k_1\right) \\
&\equiv \phi_1 + 2a_2k_2 + \frac{2a_2}{g}\big(a_1k_1v_2 - k_2(g - v_1a_1) - k_2wa_1k_1\big).
\end{aligned}$$

The last congruence above follows from (3.1). As a result we have

$$\phi_2 \equiv \phi_1 + \frac{2a_1a_2}{g}(k_1v_2 + v_1k_2 - wk_1k_2) \left(\mathrm{mod}\ \frac{2a_1a_2}{g^2}\right),$$

and hence $\phi_2 \equiv \phi_1 \left(\mathrm{mod}\ \frac{2a_1a_2}{g^2}\right)$. Therefore $\phi_1 = \phi_2$ and the two compositions are equal. □

Lemma 3.5. *Let $f(x,y) = n$ be a representation. Then there exist unique integers x_1 and y_1 with $xy_1 - x_1y = 1$ such that if $A = \left(\begin{smallmatrix} x & x_1 \\ y & y_1 \end{smallmatrix}\right)$, then $T_A(f) = (n, \phi)$ with $1 \le \phi \le 2n$.*

Proof. Let integers x_0 and y_0 be such that $xy_0 - yx_0 = 1$. Let $A' = \left(\begin{smallmatrix} x & x_0 \\ y & y_0 \end{smallmatrix}\right)$ and $T_{A'}(f) = (n, \phi')$. If $B' = \left(\begin{smallmatrix} 1 & \delta \\ 0 & 1 \end{smallmatrix}\right)$, then $T_{B'}(n, \phi') = (n, \phi' + 2n\delta)$. We may choose δ so that $\phi = \phi' + 2n\delta$ satisfies $1 \le \phi \le 2n$. Now let $A = A'B' = \left(\begin{smallmatrix} x & x_1 \\ y & y_1 \end{smallmatrix}\right)$. Then $T_A(f) = (n, \phi)$. Suppose $B = \left(\begin{smallmatrix} x & x_2 \\ y & y_2 \end{smallmatrix}\right)$ is such that $T_B(f) = (n, \phi')$ with $1 \le \phi' \le 2n$. Since $xy_2 - yx_2 = 1$, we observe that $x_2 = x_1 + hx, y_2 = y_1 + hy$ for some integer h. Using the expression for ϕ and ϕ' from (2.1) we have

$$\begin{aligned}
\phi - \phi' &= b(xy_1 + yx_1 - xy_2 - yx_2) + 2(axx_1 + cyy_1 - axx_2 - cyy_2) \\
&= -2hbxy - 2ahx^2 - 2chy^2 = -2hn.
\end{aligned}$$

Since $1 \le \phi, \phi' \le 2n$ we conclude that $\phi = \phi'$ and $x_2 = x_1$ and $y_2 = y_1$. □

Henceforth we assume that the discriminant $D = -4d$. Hence the identity form $e = (1, 0, d)$ and b is even in any form $f = (a, b, c)$. We note that there is a binary quadratic form of discriminant $-4d$ that represents an odd integer k if and only if the congruence $x^2 \equiv -d \pmod{k}$ has a solution.

Definition 3.2. Let $e(x,y)=n$ be a representation. Define $T(x,y)=T_A(e)=(n,2\phi)$ where $1\le\phi\le n$ and A is the unique transformation matrix as in Lemma 3.5 above.

Lemma 3.6. *Suppose $e(x_1,y_1)=e(x_2,y_2)=n$ are representations. If $T(x_1,y_1)=T(x_2,y_2)$ then $x_2+y_2\sqrt{-d}=\pm(x_1+y_1\sqrt{-d}\,)$.*

Proof. It follows by definition that there exist matrices A and B with $A=\left(\begin{smallmatrix}x_1 & t_1\\ y_1 & s_1\end{smallmatrix}\right)$ and $B=\left(\begin{smallmatrix}x_2 & t_2\\ y_2 & s_2\end{smallmatrix}\right)$ such that $T_A(e)=T(x_1,y_1)=(n,2\phi_1)$ and $T_B(e)=T(x_2,y_2)=(n,2\phi_2)$. Since $T(x_1,y_1)=T(x_2,y_2)$, we have

$$x_1t_1+dy_1s_1=\phi_1=\phi_2=x_2t_2+dy_2s_2.$$

Let $\phi=\phi_1=\phi_2$. We define two rational numbers u and v as

$$nu=x_1x_2+dy_1y_2 \quad\text{and}\quad nv=x_1y_2-x_2y_1.$$

We have

$$\begin{aligned}x_1&=x_1(x_1s_1-y_1t_1)=x_1^2s_1-\phi y_1+dy_1^2s_1\\ &=s_1(x_1^2+dy_1^2)-\phi y_1=ns_1-\phi y_1\end{aligned}$$

that gives $x_1=ns_1-\phi y_1$. Similarly $x_2=ns_2-\phi y_2$. Hence $nv=x_1y_2-x_2y_1=ns_1y_2-ns_2y_1$ implying that $v=s_1y_2-s_2y_1$. Thus v is an integer. Now

$$(u^2+dv^2)n^2=x_1^2x_2^2+d^2y_1^2y_2^2+dx_2^2y_1^2+dx_1^2y_2^2=(x_1^2+dy_1^2)(x_2^2+dy_2^2)=n^2.$$

Hence $u^2+dv^2=1$ and we conclude that $u=\pm1$ and $v=0$. Therefore $n=\pm(x_1x_2+dy_1y_2)$ and $x_1y_2=x_2y_1$. We have now

$$\begin{aligned}x_1&=\pm(x_1^2x_2+dx_1y_1y_2)/n=\pm(x_1^2x_2+dx_2y_1^2)/n=\pm x_2,\\ y_1&=\pm(-x_1x_2y_1+dy_1^2y_2)/n=\pm(x_1^2y_2+dy_1^2y_2)/n=\pm y_2\end{aligned}$$

which proves the lemma. □

Lemma 3.7. *Let h be a positive integer. Suppose $e(a_i,b_i)=p_i^{r_i}$ is a representation, where p_i is an odd prime and r_i is a positive integer for every i with $1\le i\le h$. Then the identity class is the only class that represents $P=p_1^{r_1}\cdots p_h^{r_h}$. Moreover, if $P=p^\alpha$ for an odd prime p and a positive integer α and $e(a,b)=e(m,n)=p^\alpha$ are two representations, then $m=\pm a$ and $n=\pm b$.*

Proof. By Lemma 3.5 for each $1 \le i \le h$ there exists $1 \le \phi_i \le p_i^{r_i}$ such that $e \sim (p_i^{r_i}, 2\phi_i)$. By composition of the forms $(p_i^{r_i}, 2\phi_i)$ it follows that P is represented by the identity class. Suppose a form f represents P. Again by Lemma 3.5, we have $f \sim (P, 2\xi)$ for some ξ with $1 \le \xi \le P$. Let $\xi \equiv \xi_i \pmod{p_i^{r_i}}$ with $1 \le \xi_i \le p_i^{r_i}$. Then $\xi_i^2 \equiv -d \pmod{p_i^{r_i}}$. Hence $\phi_i \equiv \pm\xi_i \pmod{p_i^{r_i}}$. By Lemma 3.2, for all i we obtain

$$(p_i^{r_i}, 2\xi_i) \sim (p_i^{r_i}, \pm 2\phi_i) \sim e.$$

Once again by resorting to Lemma 3.2 we have $(p_i^{r_i}, 2\xi_i) \sim (p_i^{r_i}, 2\xi)$. It follows now by composition that

$$e \sim (p_1^{r_1}, 2\xi) \circ \cdots \circ (p_h^{r_h}, 2\xi) \sim (P, 2\xi)$$

which proves the first assertion.

Let $T(a,b) = (p^\alpha, 2\eta_1)$ and $T(m,n) = (p^\alpha, 2\eta_2)$. We reason as above to conclude that $\eta_2 = \eta_1$ or $\eta_2 = p^\alpha - \eta_1$. Now $T(-a,b) = T(a,-b) = (p^\alpha, 2(p^\alpha - \eta_1))$. Thus $T(a,b) = T(m,n)$ or $T(-a,b) = T(a,-b) = T(m,n)$. By Lemma 3.6 we have $m = \pm a, n = \pm b$. $\square$

Remark 3.1. The converse of the above lemma is not always true. For instance, let $d = 31$. As seen following Theorem 1.1 in the Introduction, there are three inequivalent representative forms namely $e(x,y) = x^2 + 31y^2$, $f(x,y) = 4x^2 + xy + 2y^2$ and $g(x,y) = 5x^2 + 3xy + 2y^2$. Now $f(1,-1) = g(1,0) = 5$; $f(1,1) = g(1,-2) = 7$; $e(2,1) = 35$. Clearly 5 and 7 are not represented by e. If f or g represents 35 then $|x| \le 3, |y| \le 5$. It may be verified that for these values of x and y, neither $f(x,y)$ nor $g(x,y)$ is equal to 35. Thus 35 is represented only by e but its prime factors are not represented by e.

Lemma 3.8. *Let (a,b,c) be a form such that r is the highest power of a that divides c. Then for $1 \le i \le r+1$ we have $(a,b,c)^i \sim (a^i, b, \frac{c}{a^{i-1}})$.*

Proof. By the composition formula, as $\gcd(a,b) = 1$, it follows immediately that $(a,b,c)^2 \sim (a^2, b, \frac{c}{a})$. Similarly for $2 \le i \le r$ it follows by induction that

$$(a,b,c)^{i+1} \sim (a,b,c) \circ \left(a^i, b, \frac{c}{a^{i-1}}\right) \sim \left(a^{i+1}, b, \frac{c}{a^i}\right). \qquad \square$$

Lemma 3.9. *Let p be an odd prime that is represented by a class f. If f' is any other class that represents p, then either $f' = f$ or $f' = f^{-1}$.*

Proof. As f represents p, there exist coprime integers α and β such that $f(\alpha,\beta) = p$. It follows from (2.1) that there exists a form (p,b,c) with $f \sim (p,b,c)$. Note that b is a solution of the congruence $x^2 \equiv -4d \pmod{4p}$. Also, modulo

$2p$ this congruence has only two solutions, namely b and $-b$. Therefore from Lemma 3.2 it follows that there are only two classes that represent p, namely the classes of the forms (p, b, c) and $(p, -b, c)$. It is easily seen that these forms are inverses of each other. $\square$

4. Proofs of Theorems 1.1 and 1.2

Lemma 4.1. *Let m and n be positive integers such that $\gcd(mn, d) = 1$. Assume that m is represented only by the identity class. Let $e(x, y) = mn$ and $T(x, y) = (mn, 2\phi)$. Then n is represented by the identity class and there exist representations $e(x_0, y_0) = m$ and $e(x_1, y_1) = n$ such that $T(x_0, y_0) = (m, 2\phi_0)$, $T(x_1, y_1) = (n, 2\phi_1)$ and $T(x, y) = T(x_0, y_0) \circ T(x_1, y_1)$ where $\phi \equiv \phi_0 \pmod{m}$ and $\phi \equiv \phi_1 \pmod{n}$.*

Proof. We have $\phi^2 \equiv -d \pmod{mn}$. If $\phi \equiv \phi_0 \pmod{m}$ then $\phi_0^2 \equiv -d \pmod{m}$ and we obtain the form $(m, 2\phi_0, \frac{\phi_0^2+d}{m}) = (m, 2\phi_0)$ of discriminant $-4d$. By Lemma 3.2, $(m, 2\phi) \sim (m, 2\phi_0)$. Similarly if $\phi \equiv \phi_1 \pmod{n}$ we have $(n, 2\phi) \sim (n, 2\phi_1)$. As the identity class is the only class that represents m, we have $e \sim (m, 2\phi_0)$. Moreover by composition and Lemma 3.4 we have $e \sim (mn, 2\phi) = (m, 2\phi) \circ (n, 2\phi) = (m, 2\phi_0) \circ (n, 2\phi_1) \sim (n, 2\phi_1)$. Therefore $(n, 2\phi_1)$ is equivalent to e and hence n is represented by the identity class. Moreover there exist representations $e(x_0, y_0) = m$ and $e(x_1, y_1) = n$ such that $T(x_0, y_0) = (m, 2\phi_0)$ and $T(x_1, y_1) = (n, 2\phi_1)$ as $e \sim (m, 2\phi_0) \sim (n, 2\phi_1)$. By Lemma 3.4 we have

$$T(x_0, y_0) \circ T(x_1, y_1) = (m, 2\phi) \circ (n, 2\phi) = (mn, 2\phi) = T(x, y). \qquad \square$$

Lemma 4.2. *Let $e(x_0, y_0) = m, e(x_1, y_1) = n$ be representations of coprime integers m, n with $\gcd(mn, d) = 1$. Let $x + y\sqrt{-d} = (x_0 + y_0\sqrt{-d})(x_1 + y_1\sqrt{-d})$. Then $\gcd(x, y) = 1$ and $e(x, y) = mn$. Moreover $T(x, y) = T(x_0, y_0) \circ T(x_1, y_1)$.*

Proof. We have $x = x_0x_1 - dy_0y_1$ and $y = x_0y_1 + x_1y_0$. Suppose g divides x and y. Then $x_1y - xy_1 = y_0(x_1^2 + dy_1^2) = y_0n$ is divisible by g. Similarly $g \mid x_0n$ and hence $g \mid n$ since $\gcd(x_0, y_0) = 1$. In the same manner we can show that $g \mid m$ and thus $\gcd(x, y) = 1$. We observe that

$$\begin{aligned} e(x, y) &= x^2 + dy^2 = (x_0^2 + dy_0^2)(x_1^2 + dy_1^2) \\ &= e(x_0, y_0)e(x_1, y_1) = mn. \end{aligned}$$

Let $T(x_0, y_0) = (m, 2\phi_0)$, $T(x_1, y_1) = (n, 2\phi_1)$ and $T(x, y) = (mn, 2\phi)$. Let

$$A = \begin{pmatrix} x_0 & a_0 \\ y_0 & b_0 \end{pmatrix}, \; B = \begin{pmatrix} x_1 & a_1 \\ y_1 & b_1 \end{pmatrix}, \; C = \begin{pmatrix} x & a \\ y & b \end{pmatrix}$$

be such that $T_A(e) = (m, 2\phi_0), T_B(e) = (n, 2\phi_1)$ and $T_C(e) = (mn, 2\phi)$. We will show that $\phi \equiv \phi_0 \pmod{m}$ and $\phi \equiv \phi_1 \pmod{n}$. By equation (2.1), $\phi = xa + dyb$ and for $i = 0, 1$, $\phi_i = x_i a_i + dy_i b_i$. We have

$$\begin{aligned}\phi - \phi_1 &= xa + dyb - x_1 a_1 - dy_1 b_1 \\ &= (x_0 x_1 - dy_0 y_1)a + db(x_0 y_1 + x_1 y_0) - x_1 a_1 - dy_1 b_1 \\ &= x_1(x_0 a + dby_0 - a_1) + dy_1(-y_0 a + bx_0 - b_1).\end{aligned}$$

Multiplying by $x_1 y_1$ we have

$$x_1 y_1(\phi - \phi_1) = x_1^2(x_0 a + dby_0 - a_1)y_1 + dy_1^2(-y_0 a + bx_0 - b_1)x_1.$$

Observe that

$$\begin{aligned}&(x_0 a + dby_0 - a_1)y_1 - (-y_0 a + bx_0 - b_1)x_1 \\ &= a(x_0 y_1 + x_1 y_0) + b_1 x_1 - a_1 y_1 + b(dy_0 y_1 - x_0 x_1) = 1 + ay + b(-x) = 0.\end{aligned}$$

Hence

$$x_1 y_1(\phi - \phi_1) = (x_1^2 + dy_1^2)(x_0 a + dby_0 - a_1)y_1 \equiv 0 \pmod{n}.$$

As $\gcd(x_1 y_1, n) = 1$, it follows that $\phi \equiv \phi_1 \pmod{n}$. Similarly $\phi \equiv \phi_0 \pmod{m}$. Therefore by Lemma 3.4 we have

$$T(x_0, y_0) \circ T(x_1, y_1) = (m, 2\phi) \circ (n, 2\phi) = (mn, 2\phi) = T(x, y),$$

which completes the proof of the lemma. □

Lemma 4.3. *Let $\gcd(m, n) = \gcd(mn, d) = 1$. Assume that m and mn are represented by the identity class. Further assume that m is represented only by the identity class. Let $e(x, y) = mn$ be a representation. Then there exist representations $e(x_0, y_0) = m$ and $e(x_1, y_1) = n$ such that*

$$x + y\sqrt{-d} = \pm(x_0 + y_0\sqrt{-d})(x_1 + y_1\sqrt{-d}).$$

Proof. Let $T(x, y) = (mn, 2\phi)$. By Lemma 4.1 there exist pairs (x_0, y_0) and (x_1, y_1) such that $T(x, y) = T(x_0, y_0) \circ T(x_1, y_1)$. Moreover we have $T(x_0, y_0) = (m, 2\phi_0)$ and $T(x_1, y_1) = (n, 2\phi_1)$ where $\phi \equiv \phi_0 \pmod{m}$ and $\phi \equiv \phi_1 \pmod{n}$.

Also by Lemma 4.2 we have $T(x_0, y_0) \circ T(x_1, y_1) = T(x', y')$ where $x' + y'\sqrt{-d} = (x_0 + y_0\sqrt{-d}\,)(x_1 + y_1\sqrt{-d}\,)$. Hence $T(x, y) = T(x', y')$ and by Lemma 3.6, the assertion follows. $\square$

Lemma 4.4. *Let* $\gcd(x_0, y_0) = 1$ *and* $e(x_0, y_0) = k^r$ *for some positive integer* r. *Let* $(x_0 + y_0\sqrt{-d}\,)^t = x_t + y_t\sqrt{-d}$ *for some* $t \geq 0$. *Then* $\gcd(x_t, y_t) = 1$ *and* $e(x_t, y_t) = k^{rt}$. *Moreover* $T(x_t, y_t) = T(x_0, y_0)^t$.

Proof. Let $T(x_0, y_0) = (k^r, 2\phi_0)$. We have

$$x_t = \sum_{i=0}^{[\frac{t}{2}]} \binom{t}{2i} x_0^{t-2i} y_0^{2i} (-d)^i$$

and

$$y_t = \sum_{i=0}^{[\frac{t-1}{2}]} \binom{t}{2i+1} x_0^{t-2i-1} y_0^{2i+1} (-d)^i.$$

As $x_0^2 + dy_0^2 = k^r$ we have

$$x_t \equiv x_0^t \sum_{i=0}^{[\frac{t}{2}]} \binom{t}{2i} = 2^{t-1} x_0^t \pmod{k^r}$$

and

$$y_t \equiv x_0^{t-1} y_0 \sum_{i=0}^{[\frac{t-1}{2}]} \binom{t}{2i+1} = 2^{t-1} x_0^{t-1} y_0 \pmod{k^r}.$$

Note that $x_t^2 + dy_t^2 = k^{rt}$. Hence if a prime p divides x_t and y_t then p divides k. As $\gcd(x_0 y_0, k) = 1$ and k is odd it follows from the above two congruences that $\gcd(x_t, y_t) = 1$. Moreover $y_0 x_t - x_0 y_t \equiv 0 \pmod{k^r}$. Thus

$$\frac{x_t}{y_t} \equiv \frac{x_0}{y_0} \pmod{k^r}. \tag{4.1}$$

Let $A = \left(\begin{smallmatrix} x_0 & a_0 \\ y_0 & b_0 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} x_t & a_t \\ y_t & b_t \end{smallmatrix}\right)$ be such that $T_A(e) = T(x_0, y_0) = (k^r, 2\phi_0)$ and $T_B(e) = T(x_t, y_t) = (k^{rt}, 2\phi_t)$, where $1 \leq \phi_0 \leq k^r$ and $1 \leq \phi_t \leq k^{rt}$. Observe that

$$\phi_t^2 + d \equiv 0 \pmod{k^{rt}}. \tag{4.2}$$

By (2.1), $\phi_i = x_i a_i + db_i y_i$, $i = 0, t$, which gives $x_i + y_i\phi_i = b_i(x_i^2 + dy_i^2)$, that is

$$\frac{x_i}{y_i} \equiv -\phi_i \pmod{k^r}.$$

Using (4.1) we have

$$\phi_0 \equiv \phi_t \pmod{k^r}.$$

By Lemma 3.4, $(k^r, 2\phi_0)^t = (k^r, 2\phi_t)^t$ and so $T(x_0, y_0)^t = (k^r, 2\phi_0)^t = (k^r, 2\phi_t)^t$. Note that $(k^r, 2\phi_t) = (k^r, 2\phi_t, c_1)$ where $c_1 = \frac{\phi_t^2+d}{k^r}$. Now c_1 is divisible by $k^{r(t-1)}$ from (4.2) and hence by Lemma 3.8 $(k^r, 2\phi_t)^t = (k^{rt}, 2\phi_t) = T(x_t, y_t)$. Thus $T(x_0, y_0)^t = T(x_t, y_t)$. □

Note that the congruence

$$x^2 \equiv -d \pmod{k}$$

has $2^{\omega(k)}$ solutions. Let $x_1, \cdots, x_{2^{\omega(k)}}$ be the solutions with $1 \leq x_i \leq k$. Corresponding to each x_i, we have a form $(k, 2x_i)$. Now the forms $(k, 2x_i)$ and $(k, 2(k-x_i))$ are inverses and hence have the same order. For $1 \leq i \leq 2^{\omega(k)-1}$ we now define $f_i = (k, 2\ell_i)$, where ℓ_i is chosen to be either x_i or $k - x_i$. Let r_i be the order of f_i in the class group. Let $f_i^{r_i} = (k^{r_i}, 2L_i)$ with $1 \leq L_i \leq k^{r_i}$. Since $f_i^{r_i} \sim e$, there exist coprime integers α_i, β_i such that $T(\alpha_i, \beta_i) = (k^{r_i}, 2L_i)$, which gives $T(-\alpha_i, \beta_i) = T(\alpha_i, -\beta_i) = (k^{r_i}, 2(k^{r_i} - L_i))$. In conclusion we have

Lemma 4.5. *Let k be an odd integer such that $\gcd(k,d) = 1$. Assume that k is represented by some form of discriminant $-4d$. Then for every i with $1 \leq i \leq 2^{\omega(k)-1}$, there exists an integer r_i dividing $h(-4d)$ and integral tuples (α_i, β_i, L_i) such that*

$$1 \leq L_i \leq k^{r_i}, \alpha_i, \beta_i \geq 0 \quad \text{with} \quad \gcd(\alpha_i, \beta_i) = 1$$

and

$$(k^{r_i}, 2L_i) = T(\alpha_i, \beta_i) \quad \text{or} \quad (k^{r_i}, 2L_i) = T(\alpha_i, -\beta_i).$$

As a consequence of the above lemma, we have

Lemma 4.6. *Let k be an odd integer such that $\gcd(k,d) = 1$. Assume that k is represented by some form of discriminant $-4d$. Suppose that $e(x,y) = k^n$ is a representation with $T(x,y) = (k^n, 2\phi)$. Then for some i with $1 \leq i \leq 2^{\omega(k)-1}$, there exists an integer $t_i > 0$ such that $n = r_i t_i$ and $T(x,y) = T(\alpha_i, \beta_i)^{t_i}$ or $T(x,y) = T(\alpha_i, -\beta_i)^{t_i}$ where r_i, α_i, β_i are given by Lemma 4.5.*

Proof. By Lemma 3.8 we have $e \sim (k^n, 2\phi) = (k, 2\phi)^n$. Hence if $f = (k, 2\phi)$ then $\operatorname{ord}(f) \mid n$. Note that $\phi^2 \equiv -d \pmod{k}$. Let $\phi \equiv \ell_i \pmod{k}$ for some $1 \leq i \leq 2^{\omega(k)}$. Then $f \sim f_i$ and $\operatorname{ord}(f) = r_i$. Thus $n = r_i t_i$ for some integer $t_i \geq 1$ and $T(x,y) = (k^{r_i t_i}, 2\phi) = (k, 2\phi)^{r_i t_i} = (k, 2\ell_i)^{r_i t_i} = (k^{r_i}, 2L_i)^{t_i} = T(\alpha_i, \pm\beta_i)^{t_i}$ by Lemmas 3.4 and 4.5 above. □

Proposition 4.1. *Suppose* (1.2) *holds where* λ *is represented only by the identity class. Then for* $1 \le i \le 2^{\omega(k)-1}$ *there exist positive integers* $r_i \mid h(-4d)$ *and representations* $e(\alpha_i, \beta_i) = k^{r_i}$*, such that the solutions* (x, y, z) *of* (1.2) *can be put into classes as given below. To each integer* r_i *as above and to each representation* $e(\gamma, \delta) = \lambda$*, we have* $x = \pm x', y = \pm y'$ *and* $z = r_i t_i$*, where*

$$x' + y'\sqrt{-d} = (\gamma + \delta\sqrt{-d}\,)(\alpha_i + \beta_i\sqrt{-d}\,)^{t_i}$$

and $t_i \ge 0$ *is any integer. Conversely each triple* (x', y', z) *given as above satisfies equation* (1.2).

Proof. We have $e(x, y) = \lambda k^n$. By Lemma 4.3, there exist representations $e(\gamma, \delta) = \lambda$ and $e(\alpha, \beta) = k^n$ such that $(x + y\sqrt{-d}\,) = (\gamma + \delta\sqrt{-d}\,)(\alpha + \beta\sqrt{-d}\,)$. Let $T(\alpha, \beta) = (k^n, 2\phi)$. By Lemma 4.6, for some i with $1 \le i \le 2^{\omega(k)-1}$ there exists $t_i > 0$ such that $n = r_i t_i$ and $T(\alpha, \beta) = T(\alpha_i, \pm\beta_i)^{t_i}$. By Lemma 4.4, we have $T(\alpha_i, \pm\beta_i)^{t_i} = T(\alpha_{it_i}, \pm\beta_{it_i})$ where $(\alpha_i \pm \beta_i\sqrt{-d}\,)^{t_i} = \alpha_{it_i} \pm \beta_{it_i}\sqrt{-d}$. Thus $T(\alpha, \beta) = T(\alpha_{it_i}, \pm\beta_{it_i})$ which by Lemma 3.6, implies that

$$(\alpha + \beta\sqrt{-d}\,) = \pm(\alpha_i \pm \beta_i\sqrt{-d}\,)^{t_i}.$$

Therefore for some $1 \le i \le 2^{\omega(k)-1}$, we have

$$x+y\sqrt{-d} = \pm(\gamma+\delta\sqrt{-d}\,)(\alpha_i\pm\beta_i\sqrt{-d}\,)^{t_i} = \pm(\gamma+\delta\sqrt{-d}\,)(\alpha_{it_i}\pm\beta_{it_i}\sqrt{-d}\,). \quad (4.3)$$

Now for any integers p, q, r and s, let

$$(x_1 + y_1\sqrt{-d}\,) = (|p| + |q|\sqrt{-d}\,)(|r| + |s|\sqrt{-d}\,)$$

and

$$(x_2 + y_2\sqrt{-d}\,) = (|p| + |q|\sqrt{-d}\,)(|r| - |s|\sqrt{-d}\,).$$

It can be seen easily that if

$$(x_0 + y_0\sqrt{-d}\,) = (p + q\sqrt{-d}\,)(r + s\sqrt{-d}\,)$$

then $x_0 = \pm x_1$, $y_0 = \pm y_1$ or $x_0 = \pm x_2$, $y_0 = \pm y_2$. The proposition now follows from (4.3). The converse follows by Lemma 4.2. □

Proof of Theorem 1.1. Let f and g be forms that represent the primes q_1 and q_2 with orders, $\mathrm{ord}(f) = r_1$ and $\mathrm{ord}(g) = r_2$. It is easy to see that

$$\mathrm{ord}(f^m) = \frac{r_1}{\gcd(r_1, m)}, \quad \mathrm{ord}(g^n) = \frac{r_2}{\gcd(r_2, n)}.$$

By (1.3), we have $e \sim T(x,y) = (q_1^m q_2^n, 2b) = (q_1^m, 2b) \circ (q_2^n, 2b)$. By Lemmas 3.8 and 3.9 we have $(q_1^m, 2b) \sim (q_1, 2b)^m \sim f^m$ or f^{-m}. Similarly $(q_2^n, 2b) \sim g^n$ or g^{-n}. Hence $f^m \sim g^n$ or $f^m \sim g^{-n}$. Thus $\mathrm{ord}(f^m) = \mathrm{ord}(g^n)$ which yields (1.4). The assertion (1.5) is immediate from (1.4). Suppose $\gcd(r_1, r_2) = 1$. Then by (1.4), $r_1 \mid \gcd(m, r_1)$ and $r_2 \mid \gcd(n, r_2)$. Hence $r_1 \mid m$ and $r_2 \mid n$. Suppose q_1 and q_2 are represented by the same class. Then $f \sim g$ or $f \sim g^{-1}$. Hence $r_1 = r_2 = r$. By hypothesis, $e \sim f^m \circ g^n \sim f^{m+n}$ or f^{m-n}. Hence $r \mid (m+n)$ or $r \mid (m-n)$. Conversely, suppose $m + n = rh$. Then $f^{m+n} = (f^r)^h \sim e$. By composition $f^{m+n} = (q_1^m q_2^n, 2b_1)$ for some integer b_1. Thus $e \sim (q_1^m q_2^n, 2b_1)$ and so there exists a representation $e(x,y) = q_1^m q_2^n$. Hence equation (1.3) has a solution. The case $r \mid (m-n)$ is similar. □

Proof of Theorem 1.2. If k is prime, then by Proposition 4.1 there exists a unique integer $r \geq 1$ such that $r \mid h(-4d)$ and a unique (up to signs) representation $e(\alpha_1, \beta_1) = k^r$. Moreover by Lemma 3.7, as representations of prime powers by the identity form are unique, there exists a unique (up to signs) representation $e(\gamma_1, \delta_1) = \lambda$. Hence solutions of (1.2) can be put into one class, given by

$$x + y\sqrt{-d} = (\gamma_1 + \delta_1\sqrt{-d})(\alpha_1 + \beta_1\sqrt{-d})^t \quad \text{where } t > 0.$$

Taking $x_0 = \pm|\gamma_1|$, $y_0 = \pm|\delta_1|$ and $x_1 = \pm|\alpha_1|$, $y_1 = \pm|\beta_1|$ we have (1.7). □

5. Proofs of Theorems 1.3–1.6

The lemmas in this section leading to the proofs of Theorems 1.3–1.6 are combinatorial in nature and are of independent interest. We consider the equality (1.7) viz.,

$$(x + y\sqrt{-d}\,) = (x_0 + y_0\sqrt{-d}\,)(x_1 + y_1\sqrt{-d}\,)^t.$$

Using binomial expansion and equating real and imaginary parts we get

$$y = \sum_{i=0}^{h} P_i \quad \text{if} \quad t = 2h+1 \tag{5.1}$$

where

$$P_i = (-d)^{h-i} x_1^{2i} y_1^{2h-2i} \left(x_0 y_1 \binom{2h+1}{2i} + x_1 y_0 \binom{2h+1}{2i+1} \right)$$

and

$$y = \sum_{i=1}^{h} Q_i + y_0 y_1^{2h} (-d)^h \text{ if } t = 2h \tag{5.2}$$

where

$$Q_i = (-d)^{h-i} x_1^{2i-1} y_1^{2h-2i} \left(x_0 y_1 \binom{2h}{2i-1} + x_1 y_0 \binom{2h}{2i} \right).$$

Our aim is to determine when $y = \pm 1$. From the above two expressions for y it is clear that $y \neq \pm 1$ whenever any one of $\gcd(y_0, y_1), \gcd(x_0, y_0)$ and $\gcd(x_1, y_1)$ exceeds 1. Hence we assume throughout this section that

$$\gcd(y_0, y_1) = \gcd(x_0, y_0) = \gcd(x_1, y_1) = 1. \tag{5.3}$$

Let p be a prime and suppose that

$$d = p^\theta f + g \quad \text{with } \theta \geq 1,\ p \nmid f,\ 0 < g < p. \tag{5.4}$$

Then we see that

$$\nu_p(d - g) = \theta. \tag{5.5}$$

In the following lemma we compute $\nu_p(d^h - g^h)$ for any positive integer h.

Lemma 5.1. *Let d be given by (5.4). Then for any integer $h \geq 1$, we have*

$$\nu_p(d^h - g^h) = \theta + \nu_p(h) \tag{5.6}$$

except when $d = 2f + 1$ and h is even in which case

$$\nu_2(d^h - 1) \geq 1 + \nu_2(h).$$

Proof. Let

$$L_i = \binom{h}{i} (p^\theta f)^i g^{h-i} \quad \text{for } 0 \leq i \leq h.$$

Then

$$d^h - g^h = \sum_{i=1}^{h} L_i. \tag{5.7}$$

Now for any i with $1 \leq i \leq h$,

$$\nu_p(L_i) = \nu_p \left(\binom{h}{i} (p^\theta f)^i g^{h-i} \right) = \theta i + \nu_p \left(\binom{h}{i} \right).$$

Assume that h is odd whenever $d = 2f + 1$. Then

$$\nu_p(L_1) = \theta + \nu_p(h), \tag{5.8}$$

$$\nu_p(L_2) = 2\theta + \nu_p\left(\binom{h}{2}\right) = 2\theta + \nu_p(h) + \nu_p(h-1) - \nu_p(2) > \theta + \nu_p(h) \quad (5.9)$$

and for $i \geq 3$,

$$\nu_p(L_i) \geq \theta i + \nu_p(h) - \nu_p(i) \geq \theta i + \nu_p(h) - \frac{\log\ i}{\log\ p} > \theta + \nu_p(h).$$

Now the assertion follows from (5.5)–(5.9). In the case when h is even and $d = 2f+1$, we have

$$\nu_2(L_2) = 2 + \nu_2\binom{h}{2} = 1 + \nu_2(h) = \nu_2(L_1)$$

and for $i \geq 3$,

$$\nu_2(L_i) > 1 + \nu_2(h)$$

which gives the assertion on using (5.7). □

Lemma 5.2. *Suppose* (1.7) *holds with* $x_0 = 1$, $y_0 = 0$. *Let* p *be a prime such that* $p \mid x_1$. *Further let* d *be given by* (5.4). *Then* $y \equiv 0 \pmod p$ *if* $t = 2h$. *When* $t = 2h+1$ *and* $\theta < 2\nu_p(x_1)$, *we have*

$$\nu_p(y - (-g)^h) = \theta + \nu_p(h).$$

Proof. We note that $y_1 = \pm 1$ by (5.3) as $y_0 = 0$. The assertion for $t = 2h$ is clear from (5.2). Let $t = 2h+1$. Using (5.1), we see that

$$y - (-g)^h = \pm(d^h - g^h) + \sum_{i=1}^{h} P_i. \quad (5.10)$$

By Lemma 5.1, we have $\nu_p(d^h - g^h) = \theta + \nu_p(h)$. Also

$$\begin{aligned}\nu_p(P_i) &= \nu_p\left((-d)^{h-i}x_1^{2i}y_1^{2h-2i+1}\binom{2h+1}{2i}\right)\\ &\geq 2i\nu_p(x_1) + \nu_p(h(2h+1)) - \nu_p(i(2i-1))\\ &\geq 2i\nu_p(x_1) + \nu_p(h) - \max(\nu_p(i), \nu_p(2i-1))\\ &\geq 2i\nu_p(x_1) + \nu_p(h) - \frac{\log(2i-1)}{\log\ p} \geq 2\nu_p(x_1) + \nu_p(h).\end{aligned}$$

Thus

$$\nu_p\left(\sum_{i=1}^{h} P_i\right) \geq 2\nu_p(x_1) + \nu_p(h).$$

Now the assertion follows from (5.10) since $\theta < 2\nu_p(x_1)$. □

Next, we consider the case when $2 \mid \gcd(y_0, x_1)$.

Lemma 5.3. *Suppose* (1.7) *holds. Let* (5.4) *be satisfied with* $p = 2$. *Assume that* $2 \mid \gcd(y_0, x_1)$. *Then* y *is even if* $t = 2h$. *If* $t = 2h + 1$ *and*

$$\nu_2(y_0) + \nu_2(x_1) < \min(\theta, 2\nu_2(x_1)),$$

then

$$\nu_2(y - (-g)^h x_0 y_1^{2h+1}) = \nu_2(y_0) + \nu_2(x_1).$$

Proof. If $t = 2h$ then from (5.2) we observe that as x_1 and y_0 are even, y is even. From (5.1) when $t = 2h + 1$, we have

$$\begin{aligned} y - (-g)^h x_0 y_1^{2h+1} &= (-d)^h x_1 y_0 y_1^{2h}(2h + 1) \\ &\quad + (-1)^h x_0 y_1^{2h+1}(d^h - g^h) + \sum_{i=1}^{h} P_i. \end{aligned} \tag{5.11}$$

Note that $\nu_2((-d)^h x_1 y_0 y_1^{2h}(2h + 1)) = \nu_2(x_1) + \nu_2(y_0)$ since y_1 is odd. By Lemma 5.1, we have $\nu_2((-1)^h x_0 y_1^{2h+1}(d^h - g^h)) = \theta + \nu_2(h)$ since x_0 and y_1 are odd. Also for $i \ge 1$ as x_1 is even, $\nu_2(P_i) \ge 2\nu_2(x_1) > \nu_2(x_1) + \nu_2(y_0)$, by hypothesis. Now the assertion of the lemma follows from (5.11). □

In the next lemma we deal with the case when $p \mid \gcd(x_0, x_1)$.

Lemma 5.4. *Suppose* (1.7) *holds and* d *satisfies* (5.4). *Let* p *be a prime such that* $p \mid \gcd(x_0, x_1)$. *Further if* $p = 2$, *let* $\nu_2^* = \min(\nu_2(x_0)+1, \nu_2(x_1))$. *Then* $y \equiv 0 \pmod p$ *if* $t = 2h + 1$. *Let* $t = 2h$. *Then the following assertions hold.*

(i) *Suppose* $p \ge 3$ *and* $\nu_p(x_0) < \nu_p(x_1)$. *Let* $\theta \ne \nu_p(x_0) + \nu_p(x_1)$. *Then*

$$\nu_p(y - (-g)^h y_0 y_1^{2h}) = \min(\theta, \nu_p(x_0) + \nu_p(x_1)) + \nu_p(h).$$

(ii) *Let* $p = 2$ *and* $d \ne 2f + 1$. *Assume that* $\nu_2(x_0) + 1 \ne \nu_2(x_1)$ *and* $\theta \ne \nu_2^* + \nu_2(x_1)$. *Then*

$$\nu_2(y - (-g)^h y_0 y_1^{2h}) = \min(\theta, \nu_2^* + \nu_2(x_1)) + \nu_2(h).$$

(iii) *Let* $d \ne 2f+1$. *Assume that* $\nu_2(x_0)+1 = \nu_2(x_1)$ *and* $\theta \le \nu_2(x_0)+\nu_2(x_1)+1$. *Then*

$$\nu_2(y - (-g)^h y_0 y_1^{2h}) = \theta + \nu_2(h).$$

Proof. From the expression for y in (5.1), we see that

$$y \equiv 0 \pmod{p} \text{ if } \ t = 2h+1.$$

Let $t = 2h$. Then from (5.2), we have

$$y - (-g)^h y_0 y_1^{2h} = \sum_{i=1}^{h} Q_i + (-1)^h y_0 y_1^{2h}(d^h - g^h). \tag{5.12}$$

As

$$Q_1 = (-d)^{h-1} x_1 y_1^{2h-2}(2x_0 y_1 h + h(2h-1)x_1 y_0), \tag{5.13}$$

we have

$$\nu_p(Q_1) = \nu_p(x_1) + \nu_p(h) + \nu_p\left(2A_1 p^{\nu_p(x_0)} + A_2 p^{\nu_p(x_1)+\nu_p(2h-1)}\right)$$

for some integers A_1, A_2 with $p \nmid A_1 A_2$. Let $p \geq 3$. By hypothesis, $\nu_p(x_0) < \nu_p(x_1)$. It follows that

$$\nu_p(Q_1) = \nu_p(x_0) + \nu_p(x_1) + \nu_p(h). \tag{5.14}$$

Let $i \geq 2$. Then

$$\nu_p(Q_i) = (2i-1)\nu_p(x_1) + \nu_p\left(x_0 y_1 \frac{2h}{2i-1}\binom{2h-1}{2i-2} + x_1 y_0 \frac{h}{i}\binom{2h-1}{2i-1}\right)$$

which gives

$$\begin{aligned}\nu_p(Q_i) &\geq (2i-1)\nu_p(x_1) + \nu_p(h) + \nu_p(x_0) - \frac{\log(2i-1)}{\log\ p} \\ &> \nu_p(x_0) + \nu_p(x_1) + \nu_p(h).\end{aligned} \tag{5.15}$$

From (5.14) and (5.15), it follows that

$$\nu_p\left(\sum_{i=1}^{h} Q_i\right) = \nu_p(x_0) + \nu_p(x_1) + \nu_p(h) \quad \text{if } p \geq 3. \tag{5.16}$$

Using (5.12), Lemma 5.1 and (5.16) we obtain assertion (i) of the lemma.

Next let $p = 2$. We see from (5.13) that

$$\nu_2(Q_1) = \nu_2^* + \nu_2(x_1) + \nu_2(h) \quad \text{if } \nu_2(x_0) + 1 \neq \nu_2(x_1) \tag{5.17}$$

and

$$\nu_2(Q_1) \geq \nu_2(x_0) + \nu_2(x_1) + \nu_2(h) + 2 \quad \text{if } \nu_2(x_0) + 1 = \nu_2(x_1). \tag{5.18}$$

Further

$$\begin{aligned} \nu_2(Q_i) \geq (2i-1)\nu_2(x_1) + \nu_2(h) \\ +\nu_2\left(A_3 2^{\nu_2(x_0)+1}\binom{2h-1}{2i-2} + A_4 2^{\nu_2(x_1)}\binom{2h-1}{2i-1}\right) - \frac{\log i}{\log 2} \end{aligned}$$

for some integers A_3, A_4 with $2 \nmid A_3A_4$. Thus

$$\nu_2(Q_i) \geq \nu_2^* + \nu_2(x_1) + \nu_2(h) + 1 \quad \text{if } \nu_2(x_0) + 1 \neq \nu_2(x_1). \tag{5.19}$$

Suppose $\nu_2(x_0) + 1 = \nu_2(x_1)$. Then

$$\begin{aligned} \nu_2(Q_i) \geq \nu_2(x_1) + \nu_2(h) + 1 + \nu_2^* \\ +\nu_2\left(A_3(2i-1) + A_4(2h-2i+1)\right) + \nu_2\left(\frac{(2h-1)!}{(2i-1)!(2h-2i+1)!}\right) \\ \geq \nu_2^* + \nu_2(x_1) + \nu_2(h) + 2 + \nu_2\left(\frac{(2h-2)!}{(2i-1)!(2h-2i+1)!}\right). \end{aligned}$$

Thus when $\nu_2(x_0) + 1 = \nu_2(x_1)$ we have

$$\nu_2(Q_i) \geq \nu_2(x_0) + \nu_2(x_1) + \nu_2(h) + 3. \tag{5.20}$$

From (5.17) and (5.19), we have

$$\nu_2\left(\sum_{i=1}^{h} Q_i\right) \geq \nu_2^* + \nu_2(x_1) + \nu_2(h) \quad \text{if } \nu_2(x_0) \neq \nu_2(x_1) - 1. \tag{5.21}$$

From (5.18) and (5.20), we have

$$\nu_2\left(\sum_{i=1}^{h} Q_i\right) \geq \nu_2(x_0) + \nu_2(x_1) + \nu_2(h) + 2 \quad \text{if } \nu_2(x_0) + 1 = \nu_2(x_1). \tag{5.22}$$

Now combining (5.12), Lemma 5.1, (5.21) and (5.22) we have the assertions (ii) and (iii). □

Finally we consider the case $\gcd(x_0, y_1) > 1$. As this case is similar to Lemma 5.4, we omit the details.

Lemma 5.5. *Suppose* (1.7) *holds. Assume that* p *is a prime such that* $p \mid \gcd(x_0, y_1)$ *and* d *is given by* (5.4). *Let* $t = 2h+1$. *If* $\nu_p(x_0) < \nu_p(y_1)$, *then*

$$\nu_p(y - x_1^{2h+1} y_0) = \nu_p(x_0) + \nu_p(y_1) + \nu_p(2h+1).$$

Let $t = 2h$. *Suppose* $\epsilon = 0$ *if* $p \geq 3$ *and* $\epsilon = 1$ *if* $p = 2$. *If* $\nu_p(x_0) + \epsilon < \nu_p(y_1)$, *then*

$$\nu_p(y - x_1^{2h} y_0) = \nu_p(x_0) + \nu_p(y_1) + \nu_p(h) + \epsilon.$$

Proof. Let $t = 2h+1$. Then from (5.1), we have

$$y - x_1^{2h+1} y_0 = x_0 y_1 x_1^{2h}(2h+1) + \sum_{i=0}^{h-1} P_i.$$

Since

$$\nu_p(x_0 y_1 x_1^{2h}(2h+1)) = \nu_p(x_0) + \nu_p(y_1) + \nu_p(2h+1), \tag{5.23}$$

$$\nu_p\left(\sum_{i=0}^{h-1} P_i\right) = 2\nu_p(y_1) + \nu_p(h) + \nu_p(2h+1) \tag{5.24}$$

we have the required assertion.

Let $t = 2h$. Then from (5.2), we have

$$y - x_1^{2h} y_0 = 2h x_0 y_1 x_1^{2h-1} + y_0 y_1^{2h}(-d)^h + \sum_{i=1}^{h-1} Q_i.$$

As

$$\nu_p(2h x_0 y_1 x_1^{2h-1}) = \nu_p(x_0) + \nu_p(y_1) + \nu_p(h) + \epsilon, \nu_p(y_0 y_1^{2h}(-d)^h) = 2h\nu_p(y_1)$$

and

$$\nu_p\left(\sum_{i=1}^{h-1} Q_i\right) = 2\nu_p(y_1) + \nu_p(h) + \nu_p(2h-1),$$

the assertion of the lemma follows. □

We now present the proofs of Theorems 1.3 to 1.6.

By the hypotheses of Theorems 1.3-1.6, d satisfies (1.9). Therefore (5.4) is satisfied with $g = 1$.

Proof of Theorem 1.3. Suppose (1.7) holds with $y = \pm 1, x_0 = 1$ and $y_0 = 0$. Let d satisfy (1.9) with $\theta < 2\nu_p(x_1)$. By Lemma 5.2, we have $t = 2h + 1$ and

$$\nu_p(\pm 1 - (-1)^h) = \theta + \nu_p(h). \tag{5.25}$$

If $p \geq 3$, then the left hand side of (5.23) is either 0 or ∞ while the right hand side is a finite non-zero value. This is a contradiction. When $p = 2$, the left hand side of (5.23) is 1 or ∞ while the right hand side is $\geq \theta > 1$, by assumption. This is again a contradiction. □

As the proofs of the other theorems are similar, we give only the equalities corresponding to (5.23) in each case.

Proof of Theorem 1.4. By Lemma 5.3, we have $t = 2h + 1$ and

$$\nu_2(\pm 1 \pm (-1)^h) = \nu_2(y_0) + \nu_2(x_1).$$

The assertion follows by comparing the values on both sides of the above equation as in the proof of Theorem 1.3. □

Proof of Theorem 1.5. By Lemma 5.4, we have $t = 2h$,

$$\nu_p(\pm 1 \pm (-1)^h) = \nu_p(h) + \min(\theta, \nu_p(x_0) + \nu_p(x_1)) \text{ for } p \geq 3$$

and

$$\nu_2(\pm 1 \pm (-1)^h) = \nu_p(h) + \min(\theta, \nu_2^* + \nu_2(x_1))$$

in the case when $\nu_2(x_0)+1 \neq \nu_2(x_1)$ and $\theta \neq \nu_2^*+\nu_2(x_1)$. Moreover if $\nu_2(x_0)+1 = \nu_2(x_1)$ and $\theta \leq \nu_2(x_0) + \nu_2(x_1) + 1$, then

$$\nu_2(\pm 1 \pm (-1)^h) = \theta + \nu_2(h).$$

As in the proofs above, these lead to contradictions proving the assertion of the theorem. □

Proof of Theorem 1.6. By Lemma 5.5, we have the following. Let $t = 2h + 1$ and $\nu_p(x_0) < \nu_p(y_1)$. Then we have

$$\nu_p(\pm 1 \pm 1) = \nu_p(x_0) + \nu_p(y_1) + \nu_p(2h + 1).$$

If $t = 2h$ and $\nu_p(x_0) + \epsilon < \nu_p(y_1)$, then

$$\nu_p(\pm 1 \pm 1) = \nu_p(x_0) + \nu_p(y_1) + \nu_p(h) + \epsilon.$$

The result follows in the same manner as in the proof of Theorem 1.3 above. □

References

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

[2] 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.

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

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

[5] C. Heuberger and M. Le, On the generalized Ramanujan–Nagell equation $x^2 + D = p^z$, *J. Number Theory* **78** (1999), 312–331.

[6] L. K. Hua, Introduction to Number Theory, *Springer Verlag*, 1982.

[7] Maohua Le, On the number of solutions of the diophantine equation $x^2 + D = p^n$, *C. R. Acad Sci Paris Sér. A* **317** (1993), 135–138.

[8] Maohua Le, Some Exponential Diophantine Equations I. The Equation $D_1x^2 - D_2y^2 = \lambda k^z$, *J. Number Theory* **55** (1995), 209–221.

[9] R. A. Mollin, Quadratics, *CRC Press*, *New York*, 1996.

[10] T. Nagell, Introduction to Number Theory, *AMS Chelsea Publishing, Providence*, 1964.

[11] P. Ribenboim, My Numbers, My Friends, Popular Lectures on Number Theory, *Springer-Verlag*, 2000.

[12] H. E. Rose, A Course in Number Theory, *Clarendon Press*, *Oxford*, 1988.

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

N. SARADHA
SCHOOL OF MATHEMATICS
TIFR, MUMBAI
INDIA

E-mail: saradha@math.tifr.res.in
URL: http://www.math.tifr.res.in/ saradha

ANITHA SRINIVASAN
DEPARTMENT OF MATHEMATICS
IIT, MUMBAI
INDIA

E-mail: rsrinivasan.anitha@gmail.com

(Received March 28, 2006; revised September 15, 2006)