Revista Colombiana de Matemáticas
Volumen 43(2009)1, páginas 71-86

Perfect powers in solutions to Pell equations

Potencias perfectas en soluciones a las ecuaciones de Pell

KALYAN CHAKRABORTY[1], FLORIAN LUCA[2]

[1]Harish-Chandra Research Institute, Allahabad, India

[2]UNAM, Morelia, Mexico

ABSTRACT. In this paper, we study the appearance of perfect powers in the first component of a non-minimal solution of a Pell equation. We give an upper bound on the counting function of the positive integers n having the property that some power of it (of exponent larger than 1) is the first component of a non-minimal solution of a Pell equation, and we present a Diophantine application.

Key words and phrases. Pell equation.

2000 Mathematics Subject Classification. 11R58, 11R29.

RESUMEN. En este trabajo, investigamos la aparición de las potencias perfectas en la primera componente de una solución no minimal de una ecuación de Pell. Damos una cota superior sobre la función de conteo del conjunto de los enteros positivos n tal que alguna potencia suya con exponente mayor que 1 es la primera componente de una solución no-minimal de una ecuación de Pell y presentamos una aplicación Diofántica.

Palabras y frases clave. Ecuación de Pell.

1. Introduction

Given a positive integer U, we can always write each one of the numbers U^2+1 or U^2-1 as dV^2, where d and V are integers and d is square-free. Conversely, given any square-free number $d > 1$, the equation

$$U^2 - dV^2 = \pm 1\,, \tag{1}$$

usually referred to as the Pell equation has infinitely many positive integer solutions (U, V). Let (U_1, V_1) be the minimal positive integer solution of the above equation (1). Put

$$\alpha = U_1 + \sqrt{d}V_1\,, \tag{2}$$

and for each integer $t \geq 1$ write

$$\alpha^t = U_t + \sqrt{d}V_t\,, \tag{3}$$

with positive integers U_t and V_t. Then all positive integer solutions (U, V) of equation (1) are of the form $(U, V) = (U_t, V_t)$ for some $t \geq 1$ (see, for example, Theorem 8.2.9 on page 110 in [7]). Equation (1) has a solution with the sign -1 in the right hand side if and only if $U_1^2 - dV_1^2 = -1$, and in this case $U_t^2 - dV_t^2 = (-1)^t$. Otherwise, all positive integer solutions of equation (1) have the sign $+1$ in the right hand side.

Given d, the problem of determining all the perfect powers in either the sequence $(U_t)_{t\geq 1}$ or $(V_t)_{t\geq 1}$ has received a lot of interest. For example, when $U_1^2 - dV_1^2 = 1$, then from the combined work of Ljunggren [9] and Cohn [6] it follows that if U_t is a square, then either $t = 1$ or $t = 2$, and U_t is a square for both $t = 1$ and 2 only when $d = 1785$. More general results on polynomial values in linear recurrence sequences have been proved by Nemes and Pethő [11], and also by Shorey and Stewart [13]. It follows from the above mentioned results that there are only finitely many perfect powers in each of the two sequences $(U_t)_{t\geq 1}$ and $(V_t)_{t\geq 1}$.

Here, we assume that $U_1^2 - dV_1^2 = -1$ and we take a different point of view concerning the equation $U_t = n^g$ for some positive integers n and g with $g > 1$. We fix neither d nor g, but rather take a positive integer n and ask whether or not $n^g = U_t$ holds for some positive integers $g > 1$ and $t > 1$. In other words, we ask whether there exists a positive integer $g > 1$ such that when writing

$$n^{2g} + 1 = dv^2,$$

with integers d and v such that d is square-free; the pair (n^g, v) is *not* the minimal solution of the Pell equation $U^2 - dV^2 = -1$. In what follows, we write $\mathcal{A}$ for the set of such positive integers n. For a positive real number x we put $\mathcal{A}(x) = \mathcal{A} \cap [1, x]$. In this note, we give an upper bound for $\#\mathcal{A}(x)$ as $x \to \infty$.

Before mentioning our main result we point out that the set $\mathcal{A}(x)$ has already been investigated in our previous paper [5]. In that paper, we showed that the estimate

$$\#\mathcal{A}(x) \leq x^{(c_0+o(1))(\log\log\log\log\log x/\log\log\log\log\log x)^{1/3}}, \tag{4}$$

holds as $x \to \infty$, where $c_0 = 2(10/3)^{1/3}$. Here and in what follows, we use $\log x$ for the natural logarithm of x. Under the ABC-conjecture, it was also shown that $\mathcal{A}$ is finite. The above results are Lemma 3 in [5].

In this paper, we improve upon the upper bound (4) on the cardinality of $\mathcal{A}(x)$. Our main result is as follows.

Theorem 1. *The estimate*

$$\#\mathcal{A}(x) \leq \exp\left((c_1 + o(1))\sqrt{\log x \log\log x}\right),$$

holds as $x \to \infty$, *where* $c_1 = \sqrt{13/2}$.

As applications, in [5] the positive integers n not in $\mathcal{A}$ were used to construct quadratic fields having class number divisible by any given positive integer g. Namely, it was shown that for $x > x_0$, there are are at least $x^{1/g}/5$ real quadratic fields $\mathbb{K}$ of discriminant $\Delta_{\mathbb{K}} < x$ whose class group has an element of order g (even), and this holds uniformly for even positive integers $g \leq (\log\log x)/(8\log\log\log x)$.

Furthermore, consider the equation

$$(x^m + 1)(y^n + 1) = z^2, \tag{5}$$

in positive integer unknowns (x, y, m, n, z) with $x^m > y^n$. In [10], it was shown that the ABC-conjecture implies that equation (5) has only finitely many solutions with $\min\{m, n\} \geq 4$. Note that for each solution of equation (5) there exists a square-free integer d and integers v and w such that $x^m + 1 = dv^2$, $x^n + 1 = dw^2$. When $m \geq 2$ and $n \geq 2$ are both even, it follows that both $(U, V) = \left(x^{m/2}, v\right)$, $\left(y^{n/2}, w\right)$ are solutions to the Pell equation $U^2 - dV^2 = -1$. Since $x^{m/2} > y^{n/2}$, we get that $x^{m/2} = U_t$ for some $t > 1$. In particular, $x \in \mathcal{A}$ for $m > 2$, therefore our result can be used to yield an unconditional upper bound on the number of solutions (x, y, m, n, z) to equation (5) with $\max\{x, y\} \leq X$ below some fixed upper bound X. We record this as

Corollary 1. *Let* $\mathcal{B}(X)$ *be the set of quintuples* (x, y, m, n, z) *of positive integers satisfying equation* (5) *with* $x^m > y^n$, m, n *even,* $\min\{m, n\} \geq 4$ *and* $\max\{x, y\} \leq X$. *Then*

$$\#\mathcal{B}(X) \leq \exp\left((c_1 + o(1))\sqrt{\log X \log\log X}\right)$$

as $X \to \infty$.

2. Proof of Theorem 1

For any odd positive integer m, let

$$P_m(X) = \frac{\left(X + \sqrt{X^2+1}\right)^m + \left(X - \sqrt{X^2+1}\right)^m}{2} \in \mathbb{Z}[X]. \tag{6}$$

For example, $P_1(X) = X$ and $P_3(X) = 4X^3 + 3X$, etc. It is known and easy to check that $P_{mn}(X) = P_m(P_n(X))$ holds for all odd positive integers m and

n. It is also well-known, and it can be immediately deduced from formulas (2) and (3) that if $U_1^2 - dV_1^2 = -1$, then $U_t = P_t(U_1)$.

Hence, if $n \in \mathcal{A}(x)$, then $n^{2g} + 1 = dv^2$, where d is square-free, and so $n^g = U_t = P_t(U_1)$ holds with some integer $t \geq 2$. Furthermore, since $U_t^2 - dV_t^2 = (-1)^t$, it follows that t is odd. Using the fact that $P_{mn}(X) = P_m(P_n(X))$, it follows that we may replace t by any prime factor p of it (necessarily odd) and U_1 by $u = U_{t/p} = P_{t/p}(U_1)$, and thus assume that

$$n^g = P_p(u). \tag{7}$$

Thus, it remains to count the number of positive integers $n \leq x$ such that relation (7) is satisfied for some integers $g > 1$, $u \geq 1$ and prime $p \geq 3$.

Some of the following arguments have already appeared in [5]. We review them here in order to make this paper self contained.

The structure of n.

If $u = 1$, we then get that

$$n^g = P_p(1) = \frac{(1+\sqrt{2})^p + (1-\sqrt{2})^p}{2}.$$

Since $g > 1$, we get that $P_p(1)$ is a perfect power. Since non-degenerate binary recurrent sequences contain only finitely many perfect powers (see [11], or Theorem 9.6 on page 152 in [14], for example), we get that the number of such exponents p is $O(1)$. From now on, we assume that $u > 1$. In this case,

$$\frac{(2u)^p - 1}{2} < \frac{\left(u + \sqrt{u^2+1}\right)^p + \left(u - \sqrt{u^2+1}\right)^p}{2} < \frac{(2u+1)^p}{2}. \tag{8}$$

Let us take a closer look at the polynomial $P_p(X)$. Its roots are $z_j = i \sin((2j+1)\pi/p)$, $j \in \{0, 1, \ldots, p-1\}$. In particular, $P_p(X)$ has no double roots. Hence, from known results about perfect power values of polynomials (see Theorems 10.1 on page 169 and 8.1 on page 141 in [14]), we deduce that for any fixed $p \geq 3$, the equation

$$P_p(u) = n^g,$$

has only finitely many positive integer solutions (u, n, g). From now on, we assume that $p > 100$.

Now note that $u \mid P_p(u)$. Further, it is known that $\gcd(u, P_p(u)/u) \mid p$, and that if this greatest common divisor is p, then $p \parallel P_p(u)/u$ (see [5]). Hence, from the equation

$$n^g = P_p(u),$$

we deduce that either

$$u = n_1^g, \qquad P_p(u)/u = n_2^g, \qquad \text{and} \qquad n_1 n_2 = n,$$

or

$$u = p^{g-1} n_1^g, \qquad P_p(u)/u = p n_2^g, \qquad \text{and} \qquad p n_1 n_2 = n.$$

Bounding n_1 and p.

Assume first that $n_1 = 1$. Then, since $u > 1$, we have that $u = p^{g-1}$, and $pn_2^g = P_p(u)/u$. Hence,

$$x^g \geq n^g = P_p(u) \geq u^p/2 = p^{p(g-1)}/2 \geq p^{p(g-1)/2} \geq p^{pg/4},$$

therefore

$$g \log x \gg pg \log p,$$

giving $p \ll \log x / \log\log x$.

Next, assume that $n_1 > 1$. Then $\log u \geq g \log n_1$, while

$$\begin{aligned} p \log u - \log 2 = \log(u^p/2) < \log\left(P_p(u)/u\right) &\leq \log\left(n_2^g p\right) \\ &\leq g \log n_2 + \log p, \end{aligned}$$

therefore

$$p - 1 \leq \frac{p \log u - \log 2}{\log u} \leq \frac{\log n_2 + (\log p)/g}{\log n_1}. \tag{9}$$

Since $g \geq 2$ and $n_2 \leq x/n_1$, it follows, from (9), that

$$(p-1) \log n_1 \leq \log x - \log n_1 + (\log p)/2,$$

giving $n_1^p \leq p^{1/2} x$, which implies

$$n_1 \ll x^{1/p}. \tag{10}$$

Further, since $n_1 \geq 2$, $g \geq 2$ and $n_2 \leq x$, we have

$$p - 1 \leq \frac{\log n_2 + (\log p)/2}{\log 2} \leq 2 \log x + \log p.$$

Since $\log p < p/2 - 1$ when $p > 100$, we get that $p \leq 4 \log x$. Thus, in both cases when $n_1 = 1$ or $n_1 > 1$, we have that

$$p \leq 4 \log x, \tag{11}$$

provided that $x > x_0$ is sufficiently large.

Bounding g.

We now deal with the more difficult task of bounding g. It is known that $2P_p(X) = Q_p(2X)$, where $Q_p(X) \in \mathbb{Z}[X]$ is a monic polynomial. A quick way to prove this fact is to first notice, by comparing leading terms, that $Q_p(X) \in \mathbb{Q}[X]$ is monic, and next to notice that the roots of $Q_p(X)$:

$$2z_j = 2i\sin((2j+1)\pi/p) = e^{(2j+1)i\pi/p} - e^{-(2j+1)i\pi/p}, \qquad j = 0, \ldots, p-1,$$

are all algebraic integers and Galois conjugates; thus, $Q_p(X) \in \mathbb{Q}[X]$ is, in fact, a polynomial with integer coefficients. Hence, the equation $P_p(u) = n^g$ is equivalent to $Q_p(2u) = 2n^g$.

At this stage, we record a result of Bugeaud from [2].

Lemma 1. *Let $f(X) = X^d + a_1X^{d-1} + \cdots + a_d \in \mathbb{Z}[X]$ be a monic polynomial of degree $d \geq 2$ with integer coefficients without multiple roots. Assume that $a \neq 0$ and u are integers such that $f(u) = av^m$. Then, either $m \leq 2d\log(2H+3)$ or*

$$m \leq 2^{15(d+6)}d^{7d}|D|^{3/2}\left(\log|D|\right)^{3d}\left(\log(3|a|)\right)^2\log\log\left(27|a|\right),$$

where D is the discriminant of f and $H = \max\{|a_1|, \ldots, |a_d|\}$ is the naive height of f.

We apply Lemma 1 to bound the number g in terms of x. For this, we need upper bounds for the parameters H and $|D|$ associated to the polynomial $Q_p(X)$. Since $Q_p(X)$ has only nonnegative coefficients, it follows that

$$H = H\left(Q_p\right) \leq H\left(P_p\right) \leq 1 + \sum_{i=1}^{p} a_i = P_p(1) < \frac{\left(1+\sqrt{2}\right)^p}{2}.$$

Here, $P_p(X) = 2^{p-1}X^p + a_1X^{p-1} + \cdots + a_p \in \mathbb{Z}[X]$.

As for the discriminant D of $Q_p(X)$, note that

$$|D| = \prod_{j=0}^{p-1}\left|Q_p'(2z_j)\right| = \prod_{j=0}^{p-1}\left|P_p'(z_j)\right|,$$

where again $z_j = i\sin((2j+1)\pi/p)$, $j = 0, \ldots, p-1$ are the roots of $P_p(X)$. Here, we used the fact that $Q_p'(2X) = P_p'(X)$, which follows with the chain rule from the fact that $Q_p(2X) = 2P_p(X)$. Since

$$P_p'(X) = \frac{p}{2\sqrt{X^2+1}}\left[\left(X+\sqrt{X^2+1}\right)^p - \left(X-\sqrt{X^2+1}\right)^p\right], \tag{12}$$

one checks easily that

$$P_p'(z_j) = \frac{\pm p}{\cos((2j+1)\pi/p)}, \qquad \text{for } j = 0, \ldots, p-1.$$

Since

$$|\cos((2j+1)\pi/p)| = |\sin((p-2(2j+1))\pi/(2p))| \geq \sin(\pi/(2p)) \geq 1/p,$$

for all $j = 0, \ldots, p-1$, and $p \geq 3$, we get that

$$|D| \leq p^{2p}.$$

Thus, from Lemma 1 with $a = 2$ and $f(X) = Q_p(X)$, we conclude that either

$$g \leq 2p \log\left(\left(1+\sqrt{2}\right)^p + 3\right) \ll p^2,$$

or

$$g \leq 2^{15(p+6)} p^{7p} p^{3p} (2p \log p)^{3p} (\log 6)^2 \log\log 54.$$

In both cases,

$$g \leq \exp(13p(\log p + O(\log\log p))). \tag{13}$$

We define $y = c_2\sqrt{\log x/\log\log x}$, where $c_2 = \sqrt{2/13}$. If $p \leq y$, then $\log p < (1/2 + o(1))\log\log x$ as $x \to \infty$, and the above inequality (13) immediately implies that the inequality

$$g < \exp((c_3 + o(1))\sqrt{\log x \log\log x}) \tag{14}$$

holds as $x \to \infty$, where $c_3 = \sqrt{13/2}$.

We now look at the case when $p > y$. Estimate (10) implies that

$$n_1 \ll x^{1/y} = \exp\left((c_3 + o(1))\sqrt{\log x \log\log x}\right). \tag{15}$$

Further, the constant term a_{p-1} of $P_p(u)/u = Q_p(2u)/(2u)$ is p. This can be noticed by observing that this constant term is

$$a_{p-1} = \lim_{t\to 0} \frac{P_p(t)}{t} = P_p'(s)\Big|_{s=0} = p \qquad \text{(cf. formula (12))}.$$

Since $u \mid P_p(u)/u - a_{p-1}$, we get that $n_1^g \mid n_2^g - p$, or $p^{g-1}n_1^g \mid pn_2^g - p$, according to whether $u = n_1^g$ or $p^{g-1}n_1^g$.

Assume first that $n_1 = 1$. Then $p^{g-2} \mid n_2^g - 1$. It then follows easily that

$$\begin{aligned} g - 2 \leq \mathrm{ord}_p(n_2^g - 1) &\leq (p-1)\frac{\log n_2}{\log p} + \frac{\log g}{\log p} \\ &< p\log x + \log g < 4(\log x)^2 + \log g. \end{aligned}$$

This shows that $g \ll (\log x)^2$ in this case. Hence, inequality (14) holds in this case as well if x is large.

Assume now that $n_1 > 1$. Then $n_1^g \mid n_2^g - \delta$, where $\delta \in \{1, p\}$. Let q be the smallest prime factor of n_1. Applying a linear form in q-adic logarithms (see, for example, [3]), we get that

$$g \leq \mathrm{ord}_q\,(n_2^g - \delta) \ll \frac{q}{\log q} \log n_2 \log p \log g \ll n_1 \log x \log\log x \log g\,,$$

which together with inequality (15) implies easily that inequality (14) holds in this instance also.

Comparing inequalities (14) and (16), we conclude that estimate

$$g < \exp\left((c_3 + o(1))\sqrt{\log x \log\log x}\right) \qquad \text{holds as } x \to \infty\,. \tag{16}$$

Let $\mathcal{A}_p(x)$ be the number of $n \leq x$ corresponding to the same value for p. Since n_1 and g are bounded as in (10), and (16), and since n_2 is determined in at most two ways once n_1, p and g are fixed, we deduce that if p is fixed then

$$\begin{aligned} \#\mathcal{A}_p(x) &\ll \#\{\text{choices for } n_1\} \times \#\{\text{choices for } g\} \\ &\ll x^{1/p} \exp((c_3 + o(1))\sqrt{\log x \log\log x}) \end{aligned} \tag{17}$$

as $x \to \infty$. Furthermore, if $n_1 \leq p$, then the number of choices for the pair (n_1, p) is $O\left((\log x)^2\right)$. Writing $\mathcal{M}(x)$ for the set of $n \leq x$ for which $n_1 \leq p$, we get that

$$\begin{aligned} \#\mathcal{M}(x) &\ll \#\{\text{choices for } g\} \times (\log x)^2 \\ &\leq \exp((c_3 + o(1))\sqrt{\log x \log\log x})\,. \end{aligned} \tag{18}$$

Thus, from now on we assume that $n_1 > p$.

We now distinguish two cases according to whether g is much larger than p or not.

The case when $g > 5p$.

We write $\mathcal{N}(x)$ for the set of such $n \leq x$. We treat in detail the case when $n = n_1 n_2$, and later on we shall indicate the minor adjustments needed to deal with the case when $n = p n_1 n_2$. We then have $u = n_1^g$, and

$$n_2^g = \frac{P_p(u)}{u} = 2^{p-1}u^{p-1} + a_1 u^{p-2} + \cdots + a_{p-1}\,.$$

Replacing u by n_1^g we get,

$$n_2^g = 2^{p-1} n_1^{g(p-1)} + a_1 n_1^{g(p-2)} + \cdots + a_{p-1}\,.$$

We divide both sides of the above equation by $n_1^{g(p-1)}$ and obtain

$$\left|\left(\frac{n_2}{n_1^{p-1}}\right)^g - 2^{p-1}\right| < \frac{a_1 + a_2 + \cdots + a_{p-1}}{n_1^g}. \tag{19}$$

Recall that $a_1, \ldots, a_{p-1}$ are nonnegative coefficients. Since the roots $z_j = i\sin((2j+1)\pi/p)$ for $j = 1, \ldots, p-1$, of the polynomial $P_p(X)/X$ are all at most 1 in absolute value, and the first coefficient of this polynomial is 2^{p-1}, it follows, from the Viète relations, that

$$a_k < 2^{p-1}\binom{p-1}{k} < 4^p, \qquad \text{for all } k = 1, \ldots, p-1.$$

Thus, inequality (19) implies that

$$\left|\left(\frac{n_2}{n_1^{p-1}}\right)^g - 2^{p-1}\right| < \frac{4^p p}{n_1^g}. \tag{20}$$

One checks immediately that the inequality

$$\frac{4^p p}{n_1^g} < \frac{1}{2n_1^{2(p-1)}}$$

holds, since it is implied by $n_1^{g-2p} > (2p)4^p$, which is true when $g > 5p$ and $n_1 > p > 100$. Thus, inequality (19) leads to

$$\left|\frac{n_2}{n_1^{p-1}} - 2^{(p-1)/g}\right|\left|\left(\frac{n_2}{n_1^{p-1}}\right)^{g-1} + \cdots + 2^{(p-1)(g-1)/g}\right| < \frac{1}{2n_1^{2(p-1)}}.$$

Since n_2 and n_1 are positive and $(p-1)(g-1)/g > 1$, the second factor in the left hand side above is larger than 1. Hence, the last inequality above leads to

$$\left|\frac{n_2}{n_1^{p-1}} - 2^{(p-1)/g}\right| < \frac{1}{2n_1^{2(p-1)}}.$$

Note that $2^{(p-1)/g}$ is irrational since $g > 5p$. By a classical result from the theory of continued fractions (see Theorem 8.2.4b on page 108 in [7]), we conclude that n_2/n_1^{p-1} is a convergent of $2^{(p-1)/g}$. Since $n_2 \leq n \leq x$ and the sequence $\{p_k/q_k\}_{k\geq 0}$ of convergents to the irrational number $2^{(p-1)/g}$ has the property that $\{p_k\}_{k\geq 0}$ has exponential growth (in fact, $p_k \geq F_k$ for all $k \geq 0$, where F_k is the kth Fibonacci number), we get that the number of possibilities for $n \leq x$ once p and g are fixed such that $g > 5p$ is $O(\log x)$.

The same argument applies in the case $n = pn_1n_2$, except that now we get that $n_2/(pn_1)^{p-1}$ is a convergent to $(2^{p-1}/p^p)^{1/g}$. Thus, in both instances when

$n = n_1 n_2$ or $n = p n_1 n_2$, we get that the number of possibilities for $n \in \mathcal{N}(x)$ is at most

$$\begin{aligned} \#\mathcal{N}(x) &\ll \#\{\text{choices for } p\} \times \#\{\text{choices for } g\} \times \log x \\ &\le \exp((c_3 + o(1))\sqrt{\log x \log\log x}), \qquad \text{as } x \to \infty. \end{aligned} \tag{21}$$

The case when $g \le 5p$.

As a first remark, we observe that inequalities (10) and (17) together with the fact that $g \ll p \ll \log x$, show that

$$\#\mathcal{A}_p(x) \ll x^{1/p} \log x. \tag{22}$$

Next, we digress a bit in order to state a particular version of a result of Evertse and Silverman, which is useful for our purpose.

Let $\mathbb{L}$ be an algebraic number field of degree ℓ and class number $h(\mathbb{L})$. Assume that $f(X) \in \mathbb{Z}[X]$ is a polynomial of degree p having only simple roots. With these notations, Evertse and Silverman proved the following result (see [8], or Theorem 5A on page 142 of [12]).

Lemma 2. *Consider the equation*

$$y^g = f(x), \qquad \text{with } x \in \mathbb{Z} \text{ and } y \in \mathbb{Q}^*. \tag{23}$$

(i) Suppose $g \ge 3$, $p \ge 2$, and $\mathbb{L}$ contains at least two roots of $f(x)$. Then the number of solutions of (23) is bounded by

$$17^{7\ell} g^{2\ell} h(\mathbb{L}).$$

(ii) Suppose $g = 2$, $p \ge 3$ and $\mathbb{L}$ contain at least three roots of $f(x)$. Then the number of solutions of (23) is bounded by

$$7^{13\ell} h(\mathbb{L})^2.$$

We apply Lemma 2 above to our equation

$$n^g = P_p(u). \tag{24}$$

Fix the prime p and let $f(X) = P_p(X) \in \mathbb{Q}[X]$. We may take $\mathbb{L} = \mathbb{Q}\left[e^{2\pi i/2p}\right]$ to be the cyclotomic field of degree $\ell = \phi(2p) = p - 1$, which contains the splitting field of $f(X)$. Since the discriminant $\Delta_{\mathbb{L}}$ of $\mathbb{L}$ is $\pm p^{p-2}$, and by a classical result of Landau $h(\mathbb{L}) \ll \sqrt{|\Delta_{\mathbb{L}}|}(\log|\Delta_{\mathbb{L}}|)^{\ell-1}$, we get that

$$h(\mathbb{L}) \le \exp((3/2 + o(1))p \log p),$$

as $p \to \infty$. By Lemma 2 and the fact that $g \leq 5p$, we get at once that the number of solutions of (24) for p fixed is at most

$$\#\mathcal{A}_p(x) \leq \exp\left((7/2 + o(1))p \log p\right), \tag{25}$$

when $p \to \infty$. Inequalities (22), (18), (21) and (25), imply immediately that

$$\begin{aligned}\#\mathcal{A}(x) &\leq \#\mathcal{M}(x) + \#\mathcal{N}(x) + \sum_{p \leq 4 \log x} \#\mathcal{A}_p(x) \\ &\ll \exp\left((c_3 + o(1))\sqrt{\log x \log\log x}\right) \\ &\quad + \sum_{p \leq 4 \log x} \min\left\{x^{1/p} \log x,\ \exp((7/2 + o(1))p \log p)\right\},\end{aligned}$$

as $x \to \infty$. A quick computation reveals that

$$\min\left\{\frac{\log x}{p}, (7/2 + o(1))p \log p\right\} \leq (c_4 + o(1))\sqrt{\log x \log\log x},$$

as $x \to \infty$, where $c_4 = \sqrt{7}/2$. Since $c_3 > c_4$, we get the desired inequality upon ignoring lower order factors and noticing that $c_3 = c_1$.

3. Proof of Corollary 1

Let X be large and $(x, y, m, n, z) \in \mathcal{B}(X)$. Then $x^{m/2} = U_t$ and $y^{n/2} = U_s$ for some positive integers $s < t$. Clearly, $x \in \mathcal{A}(X)$. Observe that $z > 0$ is uniquely determined by (x, y, m, n), so it suffices to count the number of such quadruples. Let us assume that $x \leq X$ is fixed.

We first bound the number of choices for t. By the primitive divisor theorem for Lucas sequences (see [4], for example), for each odd $k > 3$, the number U_k has a *primitive prime factor* p_k, which is an odd prime not dividing $dU_1U_2 \cdots U_{k-1}$. It is known that such a prime is congruent to $(d|p_k) \in \{\pm 1\}$, where for an odd prime p we use $(\bullet|p)$ for the Legendre symbol with respect to p. In particular, writing

$$t = r_1^{\alpha_1} \cdots r_s^{\alpha_s},$$

we observe that for all divisors $k > 3$ of t we have that $U_k \mid U_t$ and that U_k has a primitive prime factor p_k. Clearly, $p_k \mid x$ and $k \mid p_k \pm 1$. This shows that

$$t^{\tau(t)/2} = \prod_{k \mid t} k \ll \prod_{\substack{3 < k \\ k \mid t}} (p_k + 1) \ll \prod_{p \mid x} (p + 1) \ll x \log\log x.$$

Here, we write $\tau(t)$, $\omega(t)$ and $\Omega(t)$ for number of divisors, prime divisors, and prime power divisors of t (> 1), respectively. Since $t \geq 2^{\Omega(t)}$, we get that

$$2^{\Omega(t)\tau(t)/2} \ll x \log\log x,$$

yielding $\Omega(t)\tau(t) < 4\log x$ once x is sufficiently large. Since $\tau(t) \geq 2^{\omega(t)}$, we get that $2^{\omega(t)} \leq 4\log x$, therefore $s = \omega(t) \leq 2\log\log x$ once x is sufficiently large. Note that all prime factors of t divide

$$\prod_{\substack{3\leq p,\ p|x \\ p\not|d}} (p - (d|p)),$$

which is a number having at most $\log x$ distinct prime factors for large enough values of x. Furthermore, the multiplicity α_i of each prime factor r_i of t is at most $\Omega(t) < 4\log x$. Thus, the number of possibilities for t once x is fixed is at most

$$(4\log x)^{2\log\log x}\binom{\lfloor \log x \rfloor}{\lfloor 2\log\log x \rfloor} < \exp\left(5\,(\log\log X)^2\right), \tag{26}$$

for sufficiently large values of X. From now on, we assume that both x and t are fixed. Observe that, by the primitive divisor theorem again, if $t > 3$, then $t \mid (p \pm 1)$ for some prime factor p of x, and, in particular, $t \leq x + 1$.

Observe that the count (26) on t is already of order $\exp(o(\sqrt{\log X}))$ as $X \to \infty$. In what follows, we will show that the count on n is of order at most polynomial in $\log X$. This would later imply that the counts on t, s and m are also bounded polynomially in $\log X$, which will then complete the proof of this corollary.

So, let us look at n and let us assume that $n > 20\log X$. Write

$$x^{n/2} = U_1\left(\frac{U_t}{U_1}\right).$$

It is well-known that if a prime q divides both U_1 and U_t/U_1, then q divides t. Furthermore, if $q^\beta \| U_1$ and $q^\gamma \| t$, then $q^{\beta+\gamma} \| U_t$. Armed with these facts, we first conclude that if $q \not| t$, then $(n/2) \mid \beta$. If on the other hand $q \mid t$, then $q^\gamma \mid t$, and $\beta + \gamma$ is a multiple of $n/2$. To summarize, there exists a positive integer x_1 dividing x such that

$$U_1 = \frac{x_1^{n/2}}{\ell},$$

where ℓ is a divisor of t. We may also assume that $x_1 > 1$, since otherwise $U_1 = 1$, therefore $x^{n/2} = U_t$ and $y^{m/2} = U_s$ are both perfect powers of exponents $n/2$ and $m/2$, respectively (both larger than 1), in the recurrence of general term

$$U_k = \frac{\left(1+\sqrt{2}\right)^k + \left(1-\sqrt{2}\right)^k}{2}, \qquad \text{for } k = 1, 2, \ldots,$$

and as we have already mentioned it is known that there are only finitely many such possibilities for the quadruple (x, y, m, n).

Putting now $x_2 = x/x_1$, we get

$$x_2^{n/2} = \frac{P_t(U_1)}{U_1} = 2^{t-1}U_1^{t-1} + \cdots + a_{t-1}\,, \tag{27}$$

where we again use

$$\begin{aligned}\frac{P_t(X)}{X} &= \frac{\left(X+\sqrt{X^2+1}\right)^t + \left(X-\sqrt{X^2+1}\right)^t}{2X} \\ &= 2^{t-1}X^{t-1} + \cdots + a_{t-1} \in \mathbb{Z}[X]\,. \end{aligned} \tag{28}$$

We rewrite relation (27) as

$$\left|\frac{x_2^{n/2}}{2^{t-1}U_1^{t-1}} - 1\right| = \frac{a_1U_1^{t-2} + \cdots + a_{t-1}}{2^{t-1}U_1^{t-1}}\,.$$

Replacing U_1 by $x_1^{n/2}/\ell$ in the left hand side of the above expression, and using the formula (28) for $P_t(U_1)$ to rewrite the right hand side of the above expression, we get

$$\left|\frac{x_2^{n/2}(\ell/2)^{t-1}}{x_1^{(t-1)n/2}} - 1\right| < \left(\frac{U_1+\sqrt{U_1^2+1}}{2U_1}\right)^t + \left(\frac{U_1-\sqrt{U_1^2+1}}{2U_1}\right)^t - 1\,. \tag{29}$$

We now study the right hand side of the above expression. Observe that

$$\begin{aligned}\left(\frac{U_1+\sqrt{U_1^2+1}}{2U_1}\right)^t &= \left(1+\frac{1}{2}\left(\sqrt{1+\frac{1}{U_1^2}}-1\right)\right)^t \\ &= \left(1+O\left(\frac{1}{U_1^2}\right)\right)^t = \exp\left(O\left(\frac{t}{U_1^2}\right)\right). \end{aligned} \tag{30}$$

Observe further that

$$\frac{t}{U_1^2} \le \frac{t}{U_1} = \frac{t\ell}{x_1^{n/2}} \ll \frac{x^2}{x_1^{n/2}} \ll \frac{1}{x_1^{n/4}}\,, \tag{31}$$

where the last inequality follows because it is implied by $x_1^{n/4} \ge x^2$, which is implied by $2^n \ge x^8$, which in turn holds because $n \ge 20\log X$.

Next observe that

$$\left(\frac{U_1-\sqrt{U_1^2+1}}{2U_1}\right)^t < \frac{1}{U_1} \ll \frac{1}{x_1^{n/4}}\,. \tag{32}$$

Thus, from estimates (30), (31) and (32), we get that

$$\begin{aligned}\left(\frac{U_1+\sqrt{U_1^2+1}}{2U_1}\right)^t &+ \left(\frac{U_1-\sqrt{U_1^2+1}}{2U_1}\right)^t - 1 \\ &\ll \left(\exp\left(O\left(\frac{1}{x_1^{n/4}}\right)\right)-1\right)+\frac{1}{x_1^{n/4}} \\ &\ll \frac{1}{x_1^{n/4}},\end{aligned}$$

which together with estimate (29) leads to

$$\left|x_2^{n/2}(\ell/2)^{t-1}x_1^{-(t-1)n/2}-1\right| \ll \frac{1}{x_1^{n/4}}. \tag{33}$$

The left hand side above is nonzero, since if it were, then we would get that

$$\frac{P_t(U_1)}{U_1} = 2^{t-1}U_1^{t-1},$$

which is not possible for $t > 1$ since then the left hand side above is larger than the right hand side above. Applying now a lower bound for a linear form in logarithms *à la* Baker [1] to the nonzero expression

$$\left|\alpha_1^{b_1}\alpha_2^{b_2}\alpha_3^{b_3}-1\right|,$$

with $\alpha_1 = x_2$, $\alpha_2 = \ell/2$, $\alpha_3 = x_1$, $b_1 = n/2$, $b_2 = t-1$ and $b_3 = -(t-1)n/2$, we get that the left hand side above is bounded from below by

$$\exp\left(-c_5(\log X)^3\log(Xn)\right),$$

where c_5 is some positive constant. Thus, we get that

$$\exp\left(-c_5(\log X)^3\log(Xn)\right) \ll \frac{1}{x_1^{n/4}},$$

leading to

$$n\log 2 \le 4c_5\left(\log X\right)^3\log(Xn),$$

which yields $n \le c_6(\log X)^4$ for some absolute constant c_6. Hence, $x^{n/2} = \exp\left(O(\log X)^5\right)$. Since $x^{n/2} = U_t \gg (\sqrt{2}+1)^t$, we get that $t \ll (\log X)^5$, and since $s < t$, we get that $s \ll (\log X)^5$ also. Finally, having fixed $n \ll (\log X)^4$ and both t and s of sizes $O\left((\log X)^5\right)$, we have that $y^{m/2} = U_s$ is a fixed number on the scale $\exp\left(O((\log X)^5)\right)$. Since $y > 1$, we get that m can be fixed in

$O\left((\log X)^5\right)$ ways, after which y is uniquely determined. This argument shows that we have

$$\begin{aligned}\#\mathcal{B}(X) &\leq O(1) + \#\{\text{choices for } x\} \times \#\{\text{choices for } n\} \\ &\quad \times \#\{\text{choices for } t\} \times \#\{\text{choices for } s\} \times \#\{\text{choices for } m\} \\ &\ll \#\mathcal{A}(X) \times (\log X)^4 \times (\log X)^5 \times (\log X)^5 \times (\log X)^5 \\ &\leq \exp\left((c_1 + o(1))\sqrt{\log X \log\log X}\right),\end{aligned}$$

as $X \to \infty$, as desired. This completes the proof of Corollary 1.

Acknowledgements. We thank the referee for a careful reading of the manuscript. Work by F. L. started when he visited H. R. I. in Allahabad, India in January of 2008. He thanks the people of this Institute for their kind hospitality. F. L. was also supported in part by Grants SEP-CONACyT 79685 and PAPIIT 100508.

References

[1] A. Baker and G. Wüstholz, *Logarithmic forms and group varieties*, J. Reine Angew. Math. **442** (1993), 19-62.

[2] Y. Bugeaud, *Sur la distance entre deux puissances pures*, C.R. Acad. Sci. Paris Sèr. I Math. **332** (1996), 1119–1121 (fr).

[3] Y. Bugeaud and M. Laurent, *Minoration effective de la distance p-adique entre puissances de nombres algèbriques*, J. Number Theory **61** (1996), 311–342 (fr).

[4] R. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Ann. Math. **15** (1913), 30–70.

[5] K. Chakraborty, F. Luca, and A. Mukhopadhyay, *Exponents of class groups of real quadratic fields*, Int. J. Number Theory **4** (2008), 597–611.

[6] J. H. Cohn, *The Diophantine equation* $x^4 - Dy^2 = 1$ *II*, Acta Arith. **78** (1997), 401–403.

[7] J. Esmonde and M. R. Murty, *Problems in algebraic number theory*, Springer Verlag, New York, 1999.

[8] J. H. Evertse and J. H. Silverman, *Uniform bounds for the number of solutions to* $y^n = f(x)$, Math. Proc. Cambr. Phil. Soc. **100** (1986), 237–248.

[9] W. Ljunggren, *Über die gleichung* $x^4 - Dy^2 = 1$, Arch. Math. Naturv. **45** (1942), no. 5, 61–70 (al).

[10] F. Luca and P. G. Walsh, *The product of like-indexed terms in binary recurrences*, J. Number Theory **96** (2002), 152–173.

[11] I. Nemes and A. Petho, *Polynomial values in linear recurrences II*, J. Number Theory **24** (1986), 47–53.

[12] W. M. Schmidt, *Diophantine approximations and diophantine equations*, Springer Verlag, Berlin, 1991, Lecture Notes in Artificial Intelligence, 1467.

[13] T. N. Shorey and C. L. Stewart, *On the diophantine equation* $ax^{2t} + bx^t y + cy^2 = d$ *and pure powers in recurrence sequences*, Math. Scand. **52** (1983), 24–36.

[14] T. N. Shorey and R. Tijdeman, *Exponential diophantine equations*, Cambridge U. Press, Cambridge, 1986.

(Recibido en septiembre de 2008. Aceptado en enero de 2009)

INSTITUTE OF MATHEMATICS AND MATHEMATICAL PHYSICS
HARISH-CHANDRA RESEARCH INSTITUTE
CHHATNAG ROAD, JHUSI
ALLAHABAD 211 019, INDIA
e-mail: kalyan@mri.ernet.in

MATHEMATICAL INSTITUTE, UNAM
AP. POSTAL 61-3 (XANGARI), CP 58089
MORELIA, MICHOACÁN, MEXICO
e-mail: fluca@matmor.unam.mx