On the period of the continued fraction expansion of $\sqrt{2^{2n+1}+1}$

Yann Bugeaud
Université Louis Pasteur
UFR de mathématiques
7 rue René Descartes, 67084 Strasbourg, France
bugeaud@math.u-strasbg.fr

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58180, Morelia, Michoacán, México
fluca@matmor.unam.mx

August 21, 2004

Abstract

We prove a general result which implies that the period of the continued fraction expansion of $\sqrt{2^{2n+1}+1}$ tends to infinity when n tends to infinity.

1 Introduction

Given a parametrized, infinite family of rational numbers, it is, in general, very hard to predict whether the lengths of their continued fraction expansions are uniformly bounded. However, for a rational function $p(X)/q(X)$, Schinzel [13] (see also Mendès France [9] for a more precise statement) established that the maximum of the lengths of the continued fraction expansions of the rational numbers $p(n)/q(n)$ is finite, when n runs through the set of positive integers. As proved recently by Corvaja and Zannier [3], quite the opposite happens when the rational function $p(X)/q(X)$ is replaced by a quotient of power sums f/g which satisfy certain assumptions. Recall that

a power sum f is a function defined on the set of positive integers and of the form

$$f(n) = a_1 b_1^n + \ldots + a_\ell b_\ell^n,$$

where $\ell \geq 1$ is an arbitrary integer, the a_i's are non-zero rational numbers and the b_i's are distinct positive integers. The main result from [3] is that if f and g satisfy certain very mild (albeit necessary) assumptions, then the length of the continued fraction of the rational number $f(n)/g(n)$ tends to infinity with n.

It is well-known that the continued fraction expansion of $\sqrt{d}$, where d is a positive integer which is not a square, is of the form $[c_0; \overline{c_1, \ldots, c_{r-1}, 2c_0}]$, where $\{\overline{\cdot}\}$ is used to emphasize the period of the expansion. Furthermore, we recall that $c_1, \ldots, c_{r-1}$ is a palindrome; i.e., $c_i = c_{r-i}$ holds for all $i = 1, \ldots, r-1$. The length r of the period is at least 1 (and this is achieved, for example, for square free numbers d of the form $k^2 + 1$ for some positive integer k), and it satisfies $r \ll \sqrt{d} \log d$ (see [7]). Here, and in all what follows, we use the Vinogradov symbols $\ll$ and $\gg$, as well as the Landau symbols O and o, with their usual meanings.

The aforementioned results from [3] and [13] suggest to us to investigate the following question: given a parametrized, infinite family of quadratic numbers, what can be said about the lengths of the periods of their continued fraction expansions? This was first studied by Schinzel (see [12], [13]), who proved that, if $p(X)$ is a non constant polynomial with integer coefficients and positive leading term satisfying certain assumptions (for example, of odd degree, or of even degree but of which the leading term is not a square of a positive integer), then the length of the continued fraction expansion of $\sqrt{p(n)}$ can become arbitrarily large as n goes to infinity. In the present work, we replace the polynomial $p(X)$ by a power sum f. Among other results, we establish that the length of the period of the continued fraction expansion of $\sqrt{2^{2n+1} + 1}$ tends to infinity when n tends to infinity. Our main result, which is Theorem 2.1, provides a partial affirmative answer to a question specifically raised at the end of [3], where it was conjectured that the period of the continued fraction expansions of $\sqrt{f(n)}$ tends to infinity with n if f satisfies certain technical assumptions. As predicted by the concluding remarks of [3], the proof of our main theorem uses the Schmidt Subspace Theorem, much in the spirit of the papers [2] and [3]. We point out that a complete characterization of those power sums f such that the period of the continued fraction expansion of $\sqrt{f(n)}$ does not tend to infinity with n has been obtained recently by Scremin (see [17] and the last section of the present paper).

Acknowledgments. Both authors thank Pietro Corvaja and Umberto Zannier for a copy of [3]. They also thank the referee for his very careful reading of a first version of the present text. This paper was written during a visit of the first author at the Mathematical Institute of the UNAM in Morelia in January 2004. He warmly thanks this Institute for its hospitality. Both authors were supported in part by the joint Project France-Mexico ANUIES-ECOS M01-M02.

2 Results

First, we introduce our notation. Let $\ell \geq 1$, a_i and b_i be non zero integers for $i = 1, \ldots, \ell$, with $b_1 > b_2 > \cdots > b_\ell \geq 1$, and set

$$f(n) = \sum_{i=1}^{\ell} a_i b_i^n, \qquad (n \geq 1). \tag{1}$$

We call $b_1, \ldots, b_\ell$ the *roots* of the form f and $a_1, \ldots, a_\ell$ its *coefficients*. To follow standard notation (see e.g. [2]), we write $\mathcal{E}_{\mathbb{Z}}$ for the ring of all such forms together with the constant 0 form. If R is any subring of $\mathbb{C}$, we write $R\mathcal{E}_{\mathbb{Z}}$ for the ring $R \otimes_{\mathbb{Z}} \mathcal{E}_{\mathbb{Z}}$, which is the ring of power sums f given by formula (1), but where the coefficients a_i are allowed to be in R. As usual, we write $\overline{\mathbb{Q}}$ for the field of algebraic numbers. In order to prove our main result, we shall assume that our form f is in $\mathbb{Q}\mathcal{E}_{\mathbb{Z}}$ and satisfies the following condition:

Condition $(*)$**.** *There do not exist an integer $j \in \{0, 1\}$, a number $\delta < 1/2$, and forms g and h in $\mathbb{Q}\mathcal{E}_{\mathbb{Z}}$, such that both the relation*

$$f(2n + j) = h(n)^2 + g(n)$$

and the estimate

$$|g(n)| \ll |f(n)|^\delta$$

hold for all positive integers n.

In this paper, we prove the following result.

Theorem 2.1. *Assume that f in $\mathcal{E}_{\mathbb{Z}}$ satisfies Condition $(*)$. Then $\sqrt{f(n)}$ is a rational number for at most finitely many positive integers n. Moreover, the length $r(n)$ of the period of the continued fraction expansion of $\sqrt{f(n)}$ tends to infinity with n.*

It is likely that Theorem 2.1 remains true even for certain forms f in $\mathcal{E}_{\mathbb{Z}}$ (or $\mathbb{Q}\mathcal{E}_{\mathbb{Z}}$) which do not satisfy the above Condition $(*)$. However, some restrictions must be imposed as, for example, $\sqrt{h(n)^2+1} = [h(n); \overline{2h(n)}]$ holds for all forms h in $\mathcal{E}_{\mathbb{Z}}$ whose coefficients a_i are positive for $i = 1, \ldots, \ell$, while the example $f(n) = h(n)^2$ with h in $\mathbb{Q}\mathcal{E}_{\mathbb{Z}}$ shows that $\sqrt{f(n)}$ can be a rational number with a bounded denominator for all positive integers n. See Section 5 for further remarks.

While the above Condition $(*)$ seems cumbersome to verify for a given power sum f, we display an immediate consequence of Theorem 2.1.

Corollary 2.2. *Let $\ell \geq 1$, a_i and b_i be non-zero integers for $i = 1, \ldots, \ell$, with $b_1 > b_2 > \cdots > b_\ell \geq 1$. Assume that neither a_1 nor $a_1 b_1$ is a square and set*

$$f(n) = \sum_{i=1}^{\ell} a_i b_i^n, \qquad (n \geq 1).$$

Then $\sqrt{f(n)}$ is a rational number for at most finitely many positive integers n. Moreover, the length $r(n)$ of the period of the continued fraction expansion of $\sqrt{f(n)}$ tends to infinity with n.

It follows, from Corollary 2.2 applied to the form $f(n) = 2 \cdot 4^n + 1$, that the length of the period of the continued fraction expansion of $\sqrt{2^{2n+1}+1}$ tends to infinity when n tends to infinity. We emphasize that Corollary 2.2 applies to a much wider class of power sums.

3 Preparations

In this section, we review some standard notions of algebraic number theory (see, for example, [1, 10, 18]) and of Diophantine approximation.

Let $\mathbb{L}$ be an algebraic number field of degree D over $\mathbb{Q}$. Denote its ring of integers by $O_{\mathbb{L}}$ and its collection of places by $\mathcal{M}_{\mathbb{L}}$. For a fractional ideal $\mathcal{I}$ of $\mathbb{L}$, we denote by $\mathrm{Nm}_{\mathbb{L}}(\mathcal{I})$ its norm. We recall that $\mathrm{Nm}_{\mathbb{L}}(\mathcal{I}) = \#(O_{\mathbb{L}}/\mathcal{I})$ if $\mathcal{I}$ is an ideal of $O_{\mathbb{L}}$, and the norm map is extended multiplicatively (using unique factorization) to all the fractional ideals of $\mathbb{L}$.

For a prime ideal $\mathcal{P}$, we denote by $\mathrm{ord}_{\mathcal{P}}(x)$ the order at which it appears in the factorization of the principal ideal $[x]$ generated by x inside $\mathbb{L}$.

For $\mu \in \mathcal{M}_{\mathbb{L}}$ and $x \in \mathbb{L}$, we define the absolute value $|x|_\mu$ as follows:

(i) $|x|_\mu = |\sigma(x)|^{1/D}$ if μ corresponds to the embedding $\sigma : \mathbb{L} \mapsto \mathbb{R}$;

(ii) $|x|_\mu = |\sigma(x)|^{2/D} = |\overline{\sigma}(x)|^{2/D}$ if μ corresponds to the pair of complex conjugate embeddings $\sigma, \overline{\sigma} : \mathbb{L} \mapsto \mathbb{C}$;

(iii) $|x|_\mu = \mathrm{Nm}_{\mathbb{L}}(\mathcal{P})^{-\mathrm{ord}_{\mathcal{P}}(x)}$ if μ corresponds to the nonzero prime ideal $\mathcal{P}$ of $O_{\mathbb{L}}$.

In case (i) or (ii) we say that μ is *real infinite* or *complex infinite*, respectively; in case (iii) we say that μ is *finite*.

These absolute values satisfy the *product formula*

$$\prod_{\mu \in \mathcal{M}_{\mathbb{L}}} |x|_\mu = 1, \qquad \text{for all } x \in \mathbb{L}^*.$$

Our basic tool is the following simplified version of a result of Schlickewei (see [14], [15]), which is commonly known as the Subspace Theorem.

Lemma 3.1. *Let $\mathbb{L}$ be an algebraic number field of degree D. Let $\mathcal{S}$ be a finite set of places of $\mathbb{L}$ containing all the infinite places. Let $\{L_{1,\mu}, \ldots, L_{M,\mu}\}$ for $\mu \in \mathcal{S}$ be linearly independent sets of linear forms in M variables with coefficients in $\mathbb{L}$. Then, for every fixed $0 < \varepsilon < 1$, the set of solutions $\mathbf{x} = (x_1, \ldots, x_M) \in \mathbb{Z}^M \backslash \{0\}$ to the inequality*

$$\prod_{\mu \in \mathcal{S}} \prod_{i=1}^{M} |L_{i,\mu}(\mathbf{x})|_\mu < \max\{|x_i| \mid i = 1, \ldots, M\}^{-\varepsilon} \tag{2}$$

is contained in finitely many proper linear subspaces of $\mathbb{Q}^M$.

4 Proofs

Throughout this section, $C_1, C_2, \ldots$ are effectively computable constants which are either absolute, or depend on the given data (usually, a form f in $\mathcal{E}_{\mathbb{Z}}$).

The following result is a variation of Lemma 1 from [2].

Lemma 4.1. *If the positive integer b and the power sum f in $\mathcal{E}_{\mathbb{Z}}$ (not necessarily satisfying Condition $(*)$) are such that for infinitely many positive integers n the denominator of the rational number $f(n)/b^n$ is less than $2^{n/2}$, then $b \mid b_i$ for all $i = 1, \ldots, \ell$.*

Proof. Without any loss of generality, we may assume that $\gcd(b_1, \ldots, b_\ell) = 1$. We then have to prove that $b = 1$. Assume that this is not so, and assume further that b is prime (if not, we replace b by a prime factor of it). Finally,

it is clear that we may assume that none of the roots of f is a multiple of b, for, if not, we may replace $f(n)$ by

$$\sum_{\substack{1\le i\le \ell\\ b\not| b_i}} a_i b_i^n.$$

We now apply Lemma 3.1 as in the proof of Lemma 1 in [2]. We let $\mathbb{L}=\mathbb{Q}$, $M=\ell$, and $\mathcal{S}$ be the set of places of $\mathbb{L}$ consisting of ∞, b, and all prime factors of b_i for $i=1,\dots,\ell$. For $\mu\in\mathcal{S}\backslash\{b\}$ and a vector $\mathbf{x}=(x_1,\dots,x_\ell)$ we put $L_{i,\mu}(\mathbf{x})=x_i$ for $i=1,\dots,\ell$, while for $\mu=b$ we put $L_{1,b}(\mathbf{x})=\sum_{i=1}^{\ell}a_ix_i$ and $L_{i,b}(\mathbf{x})=x_i$ for $i=2,\dots,\ell$. We evaluate the double product appearing in the statement of Lemma 3.1 for $\mathbf{x}=(b_1^n,\dots,b_\ell^n)$. We note that x_i are integers for all $i=1,\dots,\ell$. Our assumption and the calculation from page 322 in [2] show that, for infinitely many positive integers n, we have

$$\prod_{\mu\in\mathcal{S}}\prod_{i=1}^{\ell}|L_{i,\mu}(\mathbf{x})|_\mu=|L_{1,b}(\mathbf{x})|_b\le b^{-n}\cdot 2^{n/2}\le b^{-n/2}=(b_1^n)^{-\varepsilon_0},\tag{3}$$

where $\varepsilon_0=(\log b)/(2\log b_1)$. Since $b_1^n=\max\{|x_i|\mid i=1,\dots,\ell\}$, it follows easily that the above inequality (3) implies that our points $\mathbf{x}$ and linear forms $L_{i,\mu}$ for $i=1,\dots,\ell$, and $\mu\in\mathcal{S}$ fulfill inequality (2) with $\varepsilon=\varepsilon_0$. Now Lemma 3.1 asserts that there are only finitely many proper subspaces of $\mathbb{Q}^\ell$ of equations of the form $\sum_{i=1}^{\ell}c_ix_i=0$ with $c_i\in\mathbb{Q}$ for $i=1,\dots,\ell$, not all zero, such that every point $\mathbf{x}\in\mathbb{Z}^\ell$ satisfying the above inequality (3) lies on one of these subspaces. This in turns gives us equations of the form

$$\sum_{i=1}^{\ell}c_ib_i^n=0.\tag{4}$$

Since each one of the above equations gives the set of zeros of a linear recurrent sequence having a dominant root (note that at least one of the coefficients c_i is non zero), it follows that each one of these equations can have only finitely many positive integer solutions n. This contradiction shows that b must be equal to 1 and proves the lemma. □

Let f be a form in $\mathbb{Q}\mathcal{E}_{\mathbb{Z}}$, not necessarily satisfying Condition $(*)$. Replacing $f(n)$ by $f(2n+j)$ for $j=\{0,1\}$, it follows that we may replace b_i by b_i^2 and a_i by $a_ib_i^j$ for $i=1,\dots,\ell$. In particular, we may assume that b_1 is a square throughout this section.

Lemma 4.2. *Let f be a form in $\mathbb{Q}\mathcal{E}_{\mathbb{Z}}$ satisfying Condition $(*)$. Then there exists a computable positive constant C_1, depending only on f, such that if C_2 is any fixed constant and if $X(n)$, $Y(n)$ are positive integers such that the inequality*

$$|X(n)^2 - f(n)Y(n)^2| < C_2$$

holds, then $Y(n) > \exp(C_1 n)$ holds for all positive integers n with only finitely many exceptions.

Proof. We write $f(n) = a_1 b_1^n (1 + \delta(n))$, where

$$\delta(n) = \sum_{i=2}^{\ell} \frac{a_i}{a_1} \left(\frac{b_i}{b_1}\right)^n.$$

Note that $\delta(n) \equiv 0$ in $\mathbb{Q}\mathcal{E}_{\mathbb{Z}}$ if, and only if, $\ell = 1$. If $\ell \geq 2$, we then let $\beta = b_1/b_2$, and observe that $\beta > 1$ and that $\delta(n) = O(\beta^{-n})$. We let k be a positive integer such that $\beta^k > b_1$. Clearly, we can choose $k = \lfloor \log b_1 / \log \beta \rfloor + 1$. Writing $\alpha = \sqrt{a_1}$, we note that we have the approximation

$$\begin{aligned}
\sqrt{f(n)} &= \alpha b_1^{n/2} \sqrt{1 + \delta(n)} \\
&= \alpha b_1^{n/2} \left(\sum_{i=0}^{k} \binom{1/2}{i} \delta(n)^i + O(\delta(n)^{k+1}) \right) \\
&= \alpha b_1^{n/2} \sum_{i=0}^{k} \binom{1/2}{i} \delta(n)^i + O\left(b_1^{-n/2} \beta^{-n} \right).
\end{aligned}$$

Note that

$$\alpha b_1^{n/2} \sum_{i=0}^{k} \binom{1/2}{i} \delta(n)^i = \alpha \cdot \frac{f_1(n)}{b_1^{(k-1/2)n}},$$

where f_1 is in $\mathbb{Q}\mathcal{E}_{\mathbb{Z}}$. Thus, we may write

$$\sqrt{f(n)} = \alpha \frac{f_1(n)}{b_1^{(k-1/2)n}} + O(b_1^{-n/2} \beta^{-n}), \tag{5}$$

where we take $f_1(n) \equiv 0$ if $\ell = 1$. Note also that all the prime factors of the roots of f_1 are among the prime factors of the roots of f. Assume now that C_2 is some fixed positive constant and that $(X(n), Y(n))$ is a pair of positive integers such that

$$|X(n)^2 - f(n)Y(n)^2| < C_2. \tag{6}$$

Then, since

$$f(n) = \left(\alpha \frac{f_1(n)}{b_1^{(k-1/2)n}} + O(b_1^{-n/2}\beta^{-n}) \right)^2 = \alpha^2 \left(\frac{f_1(n)}{b_1^{(k-1/2)n}} \right)^2 + O\left(\beta^{-n}\right),$$

we get that

$$X(n)^2 - f(n)Y(n)^2 = X(n)^2 - \alpha^2 \left(\frac{f_1(n)}{b_1^{(k-1/2)n}} \right)^2 Y(n)^2 + O\left(Y(n)^2\beta^{-n}\right).$$

We choose $C_1 < (\log \beta)/2$, and we infer that, if $Y(n) < \exp(C_1 n)$, then inequality (6) leads to the conclusion that the inequality

$$\left| X(n)^2 - \alpha^2 \left(\frac{f_1(n)}{b_1^{(k-1/2)n}} \right)^2 Y(n)^2 \right| < 2C_2$$

holds for all but finitely many positive integers n. In turn, the above inequality implies that

$$\left| X(n) - \frac{\alpha f_1(n)}{b_1^{(k-1/2)n}} Y(n) \right| \ll \frac{1}{b_1^{n/2} Y(n)}. \tag{7}$$

The constant understood in $\ll$ above depends on C_2 and on the form f. The above inequality (7) is equivalent to

$$\left| b_1^{(k-1/2)n} X(n) - \alpha f_1(n) Y(n) \right| \ll \frac{b_1^{(k-1)n}}{Y(n)}. \tag{8}$$

We now write

$$f_1(n) = \sum_{i=1}^{\ell'} a_i' (b_i')^n,$$

where $b_1' > b_2' > \cdots > b_{\ell'} \geq 1$. Note that $1 \leq \ell' \leq 1 + (\ell - 1) + \cdots + (\ell - 1)^k$, and that $b_1' = b_1^k$ (recall that b_1 is a square). We are now all set to apply Lemma 3.1. We choose $\mathbb{L} = \mathbb{Q}(\alpha)$, $M = 1 + \ell'$, and $\mathcal{S}$ to be the set of all places of $\mathbb{L}$ (which is either $\mathbb{Q}$, or a real quadratic field, respectively) consisting of the infinite ones (one, or two of them, respectively), and the finite ones corresponding to primes in $\mathbb{L}$ lying above the prime factors of the product $b_1 \dots b_\ell$. Note that all the prime factors of the b_i''s are among the prime factors of the b_i's. Denote by D the degree of $\mathbb{L}$ ($D = 1$ or

$D = 2$, respectively). When $\mu \in \mathcal{S}$ is finite, we then put $L_{i,\mu}(\mathbf{x}) = x_i$ for $i = 1, \dots, M$, while if μ is infinite corresponding to the real embedding $\sigma : \mathbb{L} \mapsto \mathbb{R}$, we then put $L_{i,\mu} = x_i$ if $i \neq 2$, and $L_{i,\mu} = x_1 - \sigma^{-1}(\alpha)(a'_1 x_2 + \cdots + a'_{\ell'} x_{\ell'+1})$ if $i = 2$. Note that if x_i are rational integers, then $|L_{i,\mu}(\mathbf{x})|_\mu = |x_1 - \alpha(a'_1 x_2 + \cdots + a'_{\ell'} x_{\ell'+1})|^{1/D}$ holds for all the infinite places $\mu \in \mathcal{S}$. We begin by verifying that if we take $\mathbf{x} = (x_1, \dots, x_M)$ as $x_1 = b_1^{(k-1/2)n} X(n)$, and $x_i = (b'_{i-1})^n Y(n)$ for $i = 2, \dots, M$, then inequality (8) implies that the inequality

$$\prod_{\mu \in \mathcal{S}} \prod_{i=1}^{M} |L_{i,\mu}(\mathbf{x})|_\mu \ll \frac{Y(n)^{M-1}}{b_1^{n/2}} \tag{9}$$

holds. To this end, observe first that if $i \neq 2$, then

$$\prod_{\mu \in \mathcal{S}} |L_{i,\mu}(\mathbf{x})|_\mu = \prod_{\mu \in \mathcal{S}} |x_i|_\mu,$$

and by the product formula, the fact that $x_i \in \mathbb{Z}^*$ for all $i = 1, \dots, M$, and the fact that $\mathcal{S}$ contains all infinite places and all the places corresponding to all the prime divisors of b_1 and of b'_j for $j = 2, \dots, \ell'$, it follows easily from (6) and the definition of f that

$$\prod_{\mu \in \mathcal{S}} |L_{1,\mu}(\mathbf{x})|_\mu = \prod_{\mu \in \mathcal{S}} |x_1|_\mu \leq X(n) \ll b_1^{n/2} Y(n), \tag{10}$$

while

$$\prod_{\mu \in \mathcal{S}} |L_{i,\mu}(\mathbf{x})|_\mu = \prod_{\mu \in \mathcal{S}} |x_i|_\mu \leq Y(n) \qquad \text{for } i = 3, \dots, M. \tag{11}$$

Finally, when $i = 2$, and $D = 1$, we have, by inequality (8), that

$$\prod_{\substack{\mu \in \mathcal{S} \\ \mu < \infty}} |L_{2,\mu}(\mathbf{x})|_\mu \cdot |L_{2,\infty}(\mathbf{x})|_\infty \leq \frac{1}{(b'_1)^n} \cdot \frac{b_1^{(k-1)n}}{Y(n)} \leq \frac{1}{b_1^n}, \tag{12}$$

because $b'_1 = b_1^k$, while when $i = 2$ and $D = 2$, we have, again by inequality (8), that

$$\prod_{\substack{\mu \in \mathcal{S} \\ \mu < \infty}} |L_{2,\mu}(\mathbf{x})|_\mu \cdot |L_{2,\infty_1}(\mathbf{x})|_{\infty_1} \cdot |L_{2,\infty_2}(\mathbf{x})|_{\infty_2}$$

$$\leq \frac{1}{b_1^{kn}} \cdot \left(\frac{b_1^{(k-1)n}}{Y(n)} \right)^{1/2} \cdot \left(\frac{b_1^{(k-1)n}}{Y(n)} \right)^{1/2} \leq \frac{1}{b_1^n},$$

which is again inequality (12) but for the case $D = 2$. Inequality (9) follows now easily by multiplying inequalities (10), (11) and (12). We now choose $C_1 < (\log b_1)/(4(M-1))$, and conclude that if $Y(n) < \exp(C_1 n)$, then $Y(n)^{M-1} \leq b_1^{n/4}$, and therefore inequality (9) implies that the inequality

$$\prod_{\mu \in \mathcal{S}} \prod_{i=1}^{M} |L_{i,\mu}(\mathbf{x})|_\mu \ll \frac{1}{b_1^{n/4}} \tag{13}$$

holds. Since $C_1 < k \log b_1$, we get that

$$\max\{|x_i| \mid i = 1, \ldots, M\} \ll b_1^{kn} Y(n) \leq b_1^{2kn} = (b_1^{n/4})^{8k}.$$

Assume that we have $Y(n) < \exp(C_1 n)$ for infinitely many n. It follows easily that the above inequality (13) implies that Lemma 3.1 holds for our field $\mathbb{L}$, the points $\mathbf{x}$ corresponding to these values of n, the set of valuations $\mathcal{S}$ and the forms $L_{i,\mu}$ for $i = 1, \ldots, M$, and $\mu \in \mathcal{S}$, with $\varepsilon = 1/(8k+1)$. The conclusion of Lemma 3.1 is that there exist only finitely many proper subspaces of $\mathbb{Q}^M$ of equations $\sum_{i=1}^{M} c_i x_i = 0$, with not all the coefficients c_i being zero, and such that all points $\mathbf{x}$ satisfying the above inequality (13) belong to one of these subspaces.

Assume now that $\mathbf{x}$ is on one of these subspaces of equation $\sum_{i=1}^{M} c_i x_i = 0$. Suppose first that $c_1 = 0$. We then get the equation

$$\sum_{i=2}^{M} c_i (b'_{i-1})^n = 0,$$

which gives the set of zeros of a linear recurrence sequence having a dominant root (note that at least one c_i for $i \geq 2$ is nonzero), and as such it can have only finitely many positive integer solutions n.

Assume now that $c_1 \neq 0$. In this case, we get that

$$X(n) = \frac{f_2(n)}{b_1^{(k-1/2)n}} Y(n),$$

where f_2 is the form in $\mathbb{Q}\mathcal{E}_{\mathbb{Z}}$ given by

$$f_2(n) = -\sum_{i=2}^{M} c_i c_1^{-1} (b'_{i-1})^n.$$

Thus, if we write $b = b_1^{k-1/2}$, then $f_2(n)/b^n = X(n)/Y(n)$. Assume that $C_1 < (\log 2)/2$. Then, if $Y(n) < \exp(C_1 n)$, and if the above equation has

infinitely many positive integer solutions n, it follows, by Lemma 4.1, that b divides every root of $f_2(n)$. In particular, we get that $Y(n)$ is bounded. Since we are assuming that this is so for infinitely many values of n, it follows that there exists a constant value A such that $Y(n) = A$ holds for infinitely many values of the positive integer n. Since the inequality $|X(n)^2 - f(n)Y(n)^2| < C_2$ also holds for all these positive integers n, it follows that there exists a fixed integer B such that both relations $X(n)^2 - f(n)Y(n)^2 = B$ and $Y(n) = A$ hold. In particular, we conclude that the Diophantine equation $f(n) = x^2 - B/A^2$ admits infinitely many solutions (n, x), with a positive integer n, and a rational number x (namely, all the pairs $(n, x) = (n, X(n)/A)$). Then, by Theorem 3 from [2], the form f does not satisfy Condition $(*)$. This contradicts our assumption that $Y(n) < \exp(C_1 n)$ holds for infinitely many n.

The above argument does show that if we choose C_1 to be sufficiently small, then indeed, for every fixed value of the positive real number C_2, all positive integer solutions $(X(n), Y(n))$ of the inequality (6) have $Y(n) > \exp(C_1 n)$ for all but finitely many values of n. □

Remark. It is easy to see that Lemma 4.2 remains true even for forms f in $\mathbb{Q}\mathcal{E}_{\mathbb{Z}}$ satisfying a weaker hypothesis then Condition $(*)$, namely such that there do not exist j in $\{0, 1\}$, a form h in $\mathbb{Q}\mathcal{E}_{\mathbb{Z}}$ and a rational number λ such that $f(2n + j) = h(n)^2 + \lambda$ holds identically for all positive integers n.

Assume now that f in $\mathbb{Q}\mathcal{E}_{\mathbb{Z}}$ satisfies Condition $(*)$. For every positive integer n, we write $\sqrt{f(n)} = [a_0(n); \ldots, a_j(n), \ldots]$ for the continued fraction expansion of $\sqrt{f(n)}$. We also write $p_j(n)/q_j(n)$ for the jth convergent of $\sqrt{f(n)}$. The next Lemma is the key ingredient of the proof of our Theorem 2.1, as it will show that the first 'sufficiently many' partial quotients $a_j(n)$ are 'small' for all but finitely many positive integers n.

Lemma 4.3. *Let f be a form in $\mathbb{Q}\mathcal{E}_{\mathbb{Z}}$ satisfying Condition $(*)$. Then there exist positive computable positive constants $C_3 < 0.3$ and $C_4 \geq 3$ depending only on f, such that the following holds.*

Assume that $\varepsilon \in (0, C_3)$ is fixed. Let j be a positive integer.

(i) If $q_j(n) < \exp(C_3 \varepsilon n)$, then the inequality

$$\left| \sqrt{f(n)} - \frac{p_j(n)}{q_j(n)} \right| \geq \frac{1}{q_j^2(n) \exp(\varepsilon n)} \tag{14}$$

holds with at most finitely many exceptions in the positive integer n (depending on ε).

(ii) If $\exp(C_3\varepsilon n) \le q_j(n) < \exp(C_3 n)$*, then the inequality*

$$\left|\sqrt{f(n)} - \frac{p_j(n)}{q_j(n)}\right| \ge \frac{1}{q_j(n)^{C_4}} \tag{15}$$

holds with at most finitely many exceptions in the positive integer n *(depending on* ε*).*

Proof. We will deal with both inequalities (14) and (15) simultaneously. We write $Q_j(n) = q_j(n)\exp(\varepsilon n)$ in case (i) and $Q_j(n) = q_j(n)^{C_4-1}$ in case (ii). With the notations from Lemma 4.2, we established (see (5)) in the course of its proof that

$$\sqrt{f(n)} = \alpha\frac{f_1(n)}{b_1^{(k-1/2)n}} + O(b_1^{-n/2}\beta^{-n}).$$

Thus, the inequality

$$\left|\sqrt{f(n)} - \frac{p_j(n)}{q_j(n)}\right| < \frac{1}{q_j(n)Q_j(n)}$$

leads to the inequality

$$\left|\alpha\frac{f_1(n)}{b_1^{(k-1/2)n}} - \frac{p_j(n)}{q_j(n)}\right| \ll \frac{1}{q_j(n)Q_j(n)}, \tag{16}$$

provided that the inequality $(b_1^{1/2}\beta)^n > q_j(n)Q_j(n)$ holds. In case (i) this last inequality is satisfied if $(2C_3+1)\varepsilon < \log(b_1^{1/2}\beta)$ and in case (ii) it is satisfied if $C_3C_4 < \log(b_1^{1/2}\beta)$. Since $\varepsilon < C_3 < 1$, it follows that in the first case the inequality is fulfilled if $3C_3 < \log(b_1^{1/2}\beta)$, and, since $C_4 \ge 3$, we see that it suffices that the inequality $C_3C_4 < \log(b_1^{1/2}\beta)$ holds. ¿From (16), we get the inequality

$$\left|b_1^{(k-1/2)n}p_j(n) - \alpha f_1(n)q_j(n)\right| \ll \frac{b_1^{(k-1/2)n}}{Q_j(n)}. \tag{17}$$

Comparing (17) with (8), we see that (17) is obtained from (8) by replacing $X(n)$ and $Y(n)$ by $p_j(n)$ and $q_j(n)$, respectively, and the upper bound $b_1^{(k-1)n}/Y(n)$ on (8) by the upper bound $b_1^{(k-1/2)n}/Q_j(n)$. We now apply again Lemma 3.1 with the same choices of field $\mathbb{L}$, set of places $\mathcal{S}$, forms

$L_{i,\mu}$, and integer indeterminates vector $\mathbf{x}$, as in the proof of Lemma 4.2. Inequality (9) now becomes

$$\prod_{\mu\in\mathcal{S}}\prod_{i=1}^{M}|L_{i,\mu}(\mathbf{x})|_\mu \ll \frac{q_j(n)^M}{Q_j(n)}. \tag{18}$$

In case (i), the right hand side of (18) is $q_j(n)^{M-1}/\exp(\varepsilon n)$. Imposing that $C_3 < 1/(2(M-1))$, then $q_j(n)^{M-1} < \exp(\varepsilon n/2)$, and therefore the above inequality (18) becomes

$$\prod_{\mu\in\mathcal{S}}\prod_{i=1}^{M}|L_{i,\mu}(\mathbf{x})|_\mu \ll \frac{1}{\exp(\varepsilon n/2)}. \tag{19}$$

Assume that ε is such that $C_3\varepsilon < k\log b_1$. Since $\varepsilon < C_3$, it suffices that $C_3^2 < k\log b_1$. In this case, since $q_j(n) < \exp(C_3\varepsilon n) < b_1^{kn}$, we get that

$$\max\{|x_i| \mid i=1,\dots,M\} \ll q_j(n)b_1^{kn} \ll b_1^{2kn} = \exp(\varepsilon n/2)^{\varepsilon^{-1}C_5}, \tag{20}$$

where $C_5 = 4k\log b_1$. Hence, from inequalities (19) and (20), we get

$$\prod_{\mu\in\mathcal{S}}\prod_{i=1}^{M}|L_{i,\mu}(\mathbf{x})|_\mu \ll \frac{1}{\exp(\varepsilon n/2)} \ll \max\{|x_i| \mid i=1,\dots,M\}^{-\varepsilon C_6}, \tag{21}$$

where $C_6 = C_5^{-1}$.

In case (ii), we may choose $C_4 = M+2$, and then inequality (18) becomes

$$\prod_{\mu\in\mathcal{S}}\prod_{i=1}^{M}|L_{i,\mu}(\mathbf{x})|_\mu \ll \frac{1}{q_j(n)} \le \frac{1}{\exp(C_3\varepsilon n)}. \tag{22}$$

Since $C_3 < k\log b_1$, for any positive integer n with $q_j(n) < \exp(C_3 n)$, we have

$$\max\{|x_i| \mid i=1,\dots,M\} \ll b_1^{kn}q_j(n) \le b_1^{2kn} = \exp(C_3\varepsilon n)^{\varepsilon^{-1}C_7},$$

where $C_7 = (2k\log b_1)/C_3$. Thus, inequality (22) implies that the inequality

$$\prod_{\mu\in\mathcal{S}}\prod_{i=1}^{M}|L_{i,\mu}(\mathbf{x})|_\mu \ll \frac{1}{\exp(C_3\varepsilon n)} \ll \max\{|x_i| \mid i=1,\dots,M\}^{-\varepsilon C_8} \tag{23}$$

holds with $C_8 = C_7^{-1}$.

In either one of the two cases (i) or (ii) we may apply Lemma 3.1, and derive that there exist only finitely many subspaces of $\mathbb{Q}^M$ of equations $\sum_{i=1}^{M} c_i x_i = 0$, and not all the coefficients c_i being zero, and such that every point $\mathbf{x} \in \mathbb{Z}^M$ satisfying either inequality (21) or (23) lies on one of these subspaces. Consider now the subspace of equation $\sum_{i=1}^{M} c_i x_i = 0$. If $c_1 = 0$, we then get the equation $\sum_{i=2}^{M} c_i (b'_{i-1})^n = 0$, which has only finitely many positive integer solutions n because at least one of the coefficients c_i is non-zero for $i = 2, \ldots, M$. Assume now that $c_1 \neq 0$. In this case, we get that

$$\frac{p_j(n)}{q_j(n)} = \frac{f_2(n)}{b^n},$$

where $b = b_1^{(k-1/2)}$, and $f_2(n) = \sum_{i=2}^{M} c_i c_1^{-1} (b'_{i-1})^n$. Since $C_3 < (\log 2)/2$, if the above equation has infinitely many positive integer solutions n, then Lemma 4.1 implies that $q_j(n)$ is bounded for all such n and thus, for large n, we are in case (i). It now follows that there exists a constant A such that $q_j(n) = A$ holds for infinitely many n, and we are therefore led to the conclusion that the inequality

$$\left| \sqrt{f(n)} - \frac{p_j(n)}{A} \right| \ll \frac{1}{\exp(\varepsilon n)}$$

holds for infinitely many positive integers n. Theorem 3 from [2] tells us that f does not satisfy Condition $(*)$. This proves that (14) (resp. (15)) holds with only finitely many exceptions. □

We can now prove our Theorem 2.1.

Proof of Theorem 2.1. We assume again that b_1 is a perfect square. We keep the notation C_1, C_3, C_4 for the constants appearing in the statements of Lemmas 4.1, 4.2 and 4.3, respectively. We first note that if $\sqrt{f(n)}$ is a rational number for infinitely many values of the positive integer n, then, by Theorem 3 from [2], that there exists a form h in $\mathbb{Q}\mathcal{E}_{\mathbb{Z}}$ such that $f(n) = h(n)^2$. In particular, f does not satisfy Condition $(*)$. Assume now that $f(n)$ is not a square of an integer. In this case, $\sqrt{f(n)} = [a_0(n); \overline{a_1(n), \ldots, a_{r(n)-1}, 2a_0(n)}]$. Assume that $r(n)$ does not tend to infinity. Then there exists a fixed positive integer r such that $r = r(n)$ holds for infinitely many positive integers n. It is known that $p_{r-1}(n)/q_{r-1}(n)$ gives the fundamental unit in the quadratic order $\mathbb{Q}[\sqrt{f(n)}]$. In particular, we have the equation $p_{r-1}(n)^2 - f(n) q_{r-1}(n)^2 = \pm 1$. By Lemma 4.2 with $C_2 = 1.5$, it follows that infinitely many positive integers n exist such that $q_{r-1}(n) > \exp(C_1 n)$. Let ε be a very small number in the interval $(0, C_3)$ to

be chosen later. Let $m \leq r-1$ be the largest index such that the inequality $q_m(n) < \exp(C_3\varepsilon n)$ holds. Since r is fixed and we have infinitely many values for n, we may assume that m is also fixed. In this case, by inequality (14), we get that $q_{m+1}(n) \leq q_m(n)\exp(\varepsilon n) < \exp((C_3+1)\varepsilon n)$, but by the definition of m, we also have $q_{m+1}(n) \geq \exp(C_3\varepsilon n)$. By inequality (15), we get that the inequality $q_{m+2} \leq q_{m+1}^{C_4-1}$ holds once ε is sufficiently small, and, in general, that the inequality $q_{m+s+1}(n) \leq q_{m+s}(n)^{C_4-1}$ holds provided that $q_{m+s}(n) < \exp(C_3 n)$. Assuming therefore that $q_{m+s}(n) < \exp(C_3 n)$, we get that $q_{m+s+1}(n) \leq q_{m+1}(n)^{(C_4-1)^s} \leq \exp((C_4-1)^s(C_3+1)\varepsilon n)$. Taking $s = r-1$, we get that the inequality

$$q_r(n) \leq q_{m+(r-1)+1}(n) \leq \exp\left((C_4-1)^{r-1}(C_3+1)\varepsilon n\right)$$

holds, provided that $(C_4-1)^{r-1}(C_3+1)\varepsilon < C_3$. Thus, it suffices to choose ε such that this last inequality is fulfilled. However, we also know that $q_r(n) > q_{r-1}(n) \geq \exp(C_1 n)$. Hence, if we choose ε such that the inequality $(C_4-1)^{r-1}(C_3+1)\varepsilon < C_1$ holds as well, we then obtain a contradiction.

Thus, $r(n)$ tends to infinity with n and Theorem 2.1 is therefore proved. □

5 Comments and Remarks

We do not know whether Condition $(*)$ is needed, although it is clear that some assumption is necessary in order to get the conclusion of Theorem 2.1.

Indeed, it is easily checked that for v, w in $\mathcal{E}_{\mathbb{Z}}$ and $f(n) = v(n)^2w(n)^2 + 2w(n)$, the relation

$$\sqrt{f(n)} = [v(n)w(n); \overline{v(n), 2v(n)w(n)}]$$

holds for all sufficiently large positive integers n.

Scremin [17] showed that if $f \in \mathcal{E}_{\mathbb{Z}}$ is such that the length $r(n)$ of the period of the continued fraction expansion of $\sqrt{f(n)}$ remains bounded for infinitely many n, there must exist $j \in \{0,1\}$ and $f_0, \ldots, f_{r-1}$ in $\mathbb{Q}\mathcal{E}_{\mathbb{Z}}$ such that the relation

$$\sqrt{f(2n+j)} = [f_0(n); \overline{f_1(n), \ldots, f_{r-1}(n), 2f_0(n)}]$$

holds for all sufficiently large positive integers n (note that the above 'continued fraction' may differ from the actual continued fraction as $f_i(n)$ are rational numbers with bounded denominators, but not necessarily positive integers).

Very recently, Corvaja and Zannier [4] applied the Schmidt Subspace Theorem to prove that, under suitable (necessary) assumptions on the real quadratic number α, the length of the period of the continued fraction expansion of α^n tends to infinity with n.

In the literature, there exist explicit versions of Lemma 3.1 (see, for example, [5] and [6]), which bound the number of possible subspaces occurring in its conclusion. Usually, such a bound is of the form $C_9\delta^{-C_{10}}$. The constant C_{10} depends only on the number of indeterminates M, and the number of places $\#S$, while the constant C_9 depends also on the *heights* of the linear forms $L_{i,\mu}$ for $i = 1, \ldots, M$, and $\mu \in \mathcal{S}$.

It is likely that one could use such results instead of the present formulation of Lemma 3.1, in conjunction with upper bounds for the zero multiplicities of linearly recurrent sequences (such as the results from [11] and [16]), to get that there exists a function $X \mapsto g(X)$ tending to infinity with X, such that if f in $\mathcal{E}_{\mathbb{Z}}$ satisfies Condition $(*)$ and if X tends to infinity, then $r(n) \gg g(X)$ holds for all positive integers $n < X$ with $o(X)$ exceptions. We point out that a result establishing a lower bound for the exponent of the group $\mathbf{E}(\mathbb{F}_{q^n})$ of points on an elliptic curve $\mathbf{E}$ defined over the finite field with q elements $\mathbb{F}_q$, and valid for almost all n, has been recently established in [8] by a method similar to the one described above.

References

[1] H. Cohn, *A classical introduction to algebraic number theory and class fields*, Springer-Verlag, NY, 1978.

[2] P. Corvaja and U. Zannier, 'Diophantine equations with power sums and universal Hilbert sets', *Indag. Math. N.S.* **9** no. 3 (1998), 317–332.

[3] P. Corvaja and U. Zannier, 'On the length of the continued fraction for values of quotients of power sums', *J. Théor. Nombres Bordeaux*, to appear (available at `http://arxiv.org/ps/math.NT/0401362`).

[4] P. Corvaja and U. Zannier, 'On the rational approximations to the powers of an algebraic number', *Preprint*, available at `http://arxiv.org/ps/math.NT/0403522`.

[5] J.-H. Evertse, 'An improvement of the quantitative subspace theorem', *Compos. Math.* **101** (1996), 225–311.

[6] J.-H. Evertse and H. P. Schlickewei, 'A quantitative version of the absolute subspace theorem', *J. Reine Angew. Math.* **548** (2002), 21–127.

[7] L. K. Hua, 'On the least solution to Pell's equation', *Bull. Amer. Math. Soc.* **48** (1942), 731–735.

[8] F. Luca and I. E. Shparlinski, 'On the exponent of the group of points on elliptic curves in extension fields', *Preprint*, 2003.

[9] M. Mendès France, 'Quelques problèmes relatifs à la théorie des fractions continues limitées', Sém. Delange–Pisot–Poitou, 13ème année (1971/72), Théorie des Nombres, Exp. No. 2, Paris, 1973.

[10] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Polish Sci. Publ., Warszawa, 1990.

[11] A. J. van der Poorten and H. P. Schlickewei, 'Zeros of recurrence sequences', *Bull. Austral Math. Soc.* **44** (1991), 215-223.

[12] A. Schinzel, 'On some problems of the arithmetical theory of continued fractions', *Acta Arith.* **6** (1961), 393–413.

[13] A. Schinzel, 'On some problems of the arithmetical theory of continued fractions II', *Acta Arith.* **7** (1962), 287–298.

[14] W. M. Schmidt, *Diophantine Approximations*, Springer Verlag, LNM **785** (1980).

[15] W. M. Schmidt, *Diophantine Approximations and Diophantine Equations*, Springer Verlag, LNM **1467** (1991).

[16] H. P. Schlickewei and W. M.Schmidt, 'The number of solutions of polynomial-exponential equations', *Compos. Math.* **120** (2000), 193–225.

[17] A. Scremin, 'On the period of the continued fraction for values of the square root of power sums', *Preprint*, available at `http://arxiv.org/ps/math.NT/0405390`.

[18] I. Stewart and Tall, *Algebraic number theory and Fermat's last theorem*, A. K. Peters, Natick, MA, 2002.