ON PERFECT POWERS IN LUCAS SEQUENCES

YANN BUGEAUD, FLORIAN LUCA, MAURICE MIGNOTTE, SAMIR SIKSEK

Abstract. Let $(u_n)_{n\geq 0}$ be the binary recurrent sequence of integers given by $u_0 = 0,\ u_1 = 1$ and $u_{n+2} = 2(u_{n+1} + u_n)$. We show that the only positive perfect powers in this sequence are $u_1 = 1$ and $u_4 = 16$.

We also discuss the problem of determining perfect powers in Lucas sequences in general.

1. Introduction and Results

Recently, Bugeaud, Mignotte and Siksek [7] showed that if $(F_n)_{n\geq 0}$ is the Fibonacci sequence given by $F_0 = 0,\ F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for $n \geq 0$, then F_n is a perfect power only for $n = 0,\ 1,\ 2,\ 6$ and 12; equivalently $F_n \in \{0, 1, 8, 144\}$. Their method combines the classical approach to Diophantine equations via linear forms in logarithms with the modular approach via Frey curves. This method applies to a large class of Diophantine problems including the determination of all the perfect powers in the set of values taken by quadratic polynomials (see [8], for example).

The five main steps used in [7] to solve the equation

$$F_n = y^p, \quad n > 2, \quad p > 3,$$

are the following (we simplify a little):

Step 1. Using some (new) lower bounds for linear forms in three logarithms one gets an upper bound on the (prime) exponent p, say

$$p < 2 \times 10^8;$$

Step 2. The modular method is used for all $p < 2 \times 10^8$ to prove the congruence

$$n \equiv \pm 1 \pmod{p},$$

(the computer time was around 50 hours);

Step 3. The previous condition allows us to view the initial linear form in three logarithms as a linear form in two logarithms, which leads to the important progress

$$p \leq 733;$$

Step 4. A detailed study of the family of Thue equations corresponding to the range $5 \leq p \leq 733$ leads to the condition

$$n < 10^{9000},$$

(recall that n is an index!);

Step 5. Using once more the modular method one proves that there is no solution for $5 \leq p \leq 733$ (the computer time was less than 100 hours). The proof is complete since the solutions for $p = 2$ and $p = 3$ were known for many years.

Date: April 11, 2006.

The principal goal of this note is to show that this method works—at least in principle—for a larger family of equations, namely that it can be applied to determine the complete list of perfect powers in a wide class of Lucas sequences.

Definition. A Lucas pair is a pair (α, β) of algebraic integers such that $\alpha+\beta$ and $\alpha\beta$ are non-zero rational integers and α/β is not a root of unity. For a given Lucas pair (α, β), one defines the corresponding *Lucas sequence* by

$$u_n = u_n(\alpha, \beta) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad (n = 0, 1, 2, \ldots).$$

The Fibonacci sequence is clearly the Lucas sequence corresponding to the Lucas pair $((1+\sqrt{5})/2, (1-\sqrt{5})/2)$. We study the equation

$$u_n = y^p,$$

in integers $n \geq 0$, y and prime exponent $p \geq 2$. For any p, it has the trivial solution $u_1 = 1^p$, and also sometimes the trivial solution $u_{-1} = \pm 1^p$ (exactly when $\alpha\beta = \pm 1$). The existence of solutions for any p makes its complete resolution very difficult, since one can no longer hope to solve it by only using congruences to suitable moduli. One important step is to prove, for large n, that

$$n \equiv 1 \pmod{p} \quad \text{or} \quad n \equiv \pm 1 \pmod{p},$$

respectively. This was a difficult part of the proof for the Fibonacci case, which corresponds to Steps 1 and 2 above. Here, we present an example where this part is rather easy. Moreover, for this example we try to minimize the time of computer verification.

Theorem 1. *Let $(u_n)_{n\geq 0}$ be the binary recurrent sequence defined by the initial values $u_0 = 0$, $u_1 = 1$ and the recurrence $u_{n+2} = 2(u_{n+1} + u_n)$. The only positive perfect powers in the sequence $(u_n)_{n\geq 0}$ are $u_1 = 1$ and $u_4 = 16$.*

The sequence (u_n) appearing in Theorem 1 is in fact the Lucas sequence corresponding to the Lucas pair $(1+\sqrt{3}, 1-\sqrt{3})$. As shown by the proof of Theorem 1, the method used in [7] can be simplified for many Lucas sequences $(u_n)_{n\geq 0}$. Roughly speaking, for a certain class of Lucas sequences, one can skip or significantly simplify the first two steps of the above proof-scheme and begin directly with the study of a linear form in two logarithms, which leads of course to rather good upper bounds for the exponent p in the equation $u_n = y^p$. This is precisely the case for the sequence considered in Theorem 1. This is also the case with the Nagell–Ljunggren equation

$$\frac{x^n - 1}{x - 1} = y^p$$

(see the survey [6]).

We postpone to Section 8 more information on the class of Lucas sequences $(u_n)_{n\geq 0}$ for which it is possible to avoid or significantly simplify the first two steps of the above proof-scheme. Some related open problems are briefly evoked in Section 9. Sections 2 to 7 are devoted to the proof of Theorem 1. More precisely, Sections 2 and 3 (resp. Section 4, Section 5, Sections 6 to 7) correspond to Steps 1 and 2 (resp. Step 3, Step 4, Step 5) of the above scheme of proof.

Throughout this paper, for a prime number p and a positive integer m we write $\mathrm{ord}_p(m)$ for the order at which p appears in the factorization of m. For a positive real number x, we write $\lfloor x \rfloor$ for the largest positive integer smaller than or equal to x, the 'floor' function, whereas $\lceil x \rceil$ is the 'ceiling' function, that is the smallest positive integer greater than or equal to x.

Throughout Sections 2 to 7, we let $(u_n)_{n\geq 0}$ be the binary recurrent sequence given by $u_0 = 0,\ u_1 = 1$ and $u_{n+2} = 2(u_{n+1} + u_n)$ for $n \geq 0$.

Acknowledgments. This paper was initiated during a visit of the second author at the Université Louis Pasteur, Strasbourg, in September 2004. He warmly thanks the Mathematical Department for its hospitality. The first three authors were supported in part by the joint Project France-Mexico ANUIES-ECOS M01-M02.

The authors warmly thank the referee for several useful comments.

2. Preliminary Results

We start with the following elementary result.

Lemma 2.1. *If* $n \geq 1$, *then*

$$\operatorname{ord}_2(u_n) = \lfloor n/2 \rfloor + \operatorname{ord}_2(n) + \delta_n, \tag{1}$$

where $\delta_n = 0$ *if* n *is odd or if* 4 *divides* n, *and* $\delta_n = -1$ *otherwise.*

Proof. The characteristic equation of the sequence $(u_n)_{n\geq 0}$ is

$$x^2 - 2x - 2 = 0.$$

Its roots are $\alpha = 1 + \sqrt{3}$ and $\beta = 1 - \sqrt{3}$, thus the general term of the sequence $(u_n)_{n\geq 0}$ is given by

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{1}{2\sqrt{3}}\left(\alpha^n - \beta^n\right). \tag{2}$$

Setting $\alpha_1 = \alpha/\sqrt{2}$ and $\beta_1 = \beta/\sqrt{2}$, we get

$$u_n = \frac{2^{n/2}}{2\sqrt{3}}\left(\alpha_1^n - \beta_1^n\right).$$

Note that α_1 and β_1 are algebraic integers which are biquadratic units. Assume first that n is odd. Then

$$u_n = 2^{\lfloor n/2 \rfloor}\left(\frac{\alpha_1^n - \beta_1^n}{\alpha_1 - \beta_1}\right).$$

One checks easily that the numbers

$$\tilde{u}_k = \frac{\alpha_1^{2k+1} - \beta_1^{2k+1}}{\alpha_1 - \beta_1} = \frac{\alpha \cdot (2+\sqrt{3})^k - \beta \cdot (2-\sqrt{3})^k}{\alpha - \beta}$$

are all odd integers for $k = 0, 1, \ldots$ In fact, $\tilde{u}_0 = 1$, $\tilde{u}_1 = 3$ are both odd and the recurrence

$$\tilde{u}_{k+2} = 4\tilde{u}_{k+1} - \tilde{u}_k$$

holds for all $k \geq 0$ (notice that $2 \pm \sqrt{3}$ are the roots of the polynomial $X^2 - 4X + 1$). Clearly, $\tilde{u}_{k+2} \equiv \tilde{u}_k \pmod 2$, and by induction on the parameter k, we get that indeed $\tilde{u}_k$ is odd for all $k \geq 0$. Hence, formula (1) holds for odd values of n.

From now on, we assume that $n = 2k$ is even. Let $\alpha_2 = \alpha_1^2 = 2 + \sqrt{3}$ and $\beta_2 = \beta_1^2 = 2 - \sqrt{3}$. Then

$$u_{2k} = 2^k \left(\frac{\alpha_2^k - \beta_2^k}{\alpha_2 - \beta_2}\right) = 2^{n/2} w_k, \qquad \text{where } w_k = \frac{\alpha_2^k - \beta_2^k}{\alpha_2 - \beta_2}.$$

It remains to show that $\mathrm{ord}_2(w_k) = \mathrm{ord}_2(n) + \delta_n = \mathrm{ord}_2(k) + \delta_{2k} + 1$. We first prove that this is the case when $k = 2^s$ for some integer $s \geq 0$, and we shall treat the general case later. For $s \geq 0$, we let $z_s = \alpha_2^{2^s} + \beta_2^{2^s}$. It is clear that z_s is an integer. Note that $w_{2^0} = w_1 = 1$, $w_{2^1} = z_0 = \alpha_2 + \beta_2 = 4$, and

$$w_{2^s} = \prod_{0 \leq k \leq s-1} z_k$$

for all $s \geq 1$. Furthermore, if $s \geq 1$, then

$$z_s = \alpha_2^{2^s} + \beta_2^{2^s} = \left(\alpha_2^{2^{s-1}} + \beta_2^{2^{s-1}}\right)^2 - 2(\alpha_2\beta_2)^{2^{s-1}} = z_{s-1}^2 - 2.$$

Reducing the above relation modulo 4, since $z_0 = 4$, we get, by induction on $s \geq 1$, that $\mathrm{ord}_2(z_s) = 1$ for all $s \geq 1$. Hence, $\mathrm{ord}_2(w_{2^s}) = s + 1$ if $s \geq 1$ and is 0 if $s = 0$. Thus, formula (1) holds when $n = 2k$ and $k = 2^s$ for some $s \geq 0$. In now suffices to prove it when $n = 2k$ and $k = 2^s m$, where $m \geq 3$ is some odd integer. In this case,

$$u_{2k} = 2^k w_k = 2^k w_{2^s} \left(\frac{w_{2^s m}}{w_{2^s}}\right).$$

It suffices to show that the quotient in the right-hand side is an odd integer. However,

$$\frac{w_{2^s m}}{w_{2^s}} = \frac{\alpha_2^{2^s m} - \beta_2^{2^s m}}{\alpha_2^{2^s} - \beta_2^{2^s}} = \sum_{t=0}^{m-1} \alpha_2^{2^s t} \beta_2^{2^s(m-t-1)}.$$

Clearly,

$$\alpha_2^{2^s t} = \left(z_s - \beta_2^{2^s}\right)^t \equiv (-1)^t \beta_2^{2^s t} \pmod{2}$$

(here, we say that two algebraic integers λ and μ are congruent modulo 2 if $(\lambda - \mu)/2$ is also an algebraic integer). Thus,

$$\sum_{t=0}^{m-1} \alpha_2^{2^s t} \beta_2^{2^s(m-1-t)} \equiv \sum_{t=0}^{m-1} (-1)^t \beta_2^{2^s(m-1)} \equiv m\beta_2^{2^s(m-1)} \equiv \beta_2^{2^s(m-1)} \pmod{2},$$

as m is odd. Since β_2 is a unit, it follows that the integer $w_{2^s m}/w_{2^s}$ is odd. The lemma is therefore proved. □

Classically, we introduce the (Lucas) companion sequence to $(u_n)_{n\geq 0}$, that is the sequence $(v_n)_{n\geq 0}$ defined by

$$v_n = \alpha^n + \beta^n, \qquad (n \geq 0),$$

so that

$$v_0 = 2, \ v_1 = 2, \ v_{n+2} = 2(v_{n+1} + v_n) \quad \text{for } n \geq 0.$$

Then, one checks easily that

$$12\, u_n^2 - v_n^2 = -(-2)^{n+2}, \tag{3}$$

and that

$$u_{2n} = u_n v_n \tag{4}$$

hold for any $n \geq 0$.

Corollary 2.2. *The sequence $v_n = \alpha^n + \beta^n$, where $\alpha = 1 + \sqrt{3}$ and $\beta = 1 - \sqrt{3}$, satisfies*

$$\mathrm{ord}_2(v_n) = \begin{cases} \lceil n/2 \rceil, & \text{if } n \text{ is odd,} \\ 2 + n/2, & \text{if } 2 \mid\mid n, \\ 1 + n/2, & \text{if } 4 \mid n. \end{cases}$$

Proof. We use the relation $12u_n^2 - v_n^2 = \pm 2^{n+2}$ and the above Lemma 2.1.

If n is odd, then $2^{n+1} \mid\mid 12u_n^2$, and we get easily that $2^{n+1} \mid\mid v_n^2$; hence, the result in this case.

If $2 \mid\mid n$, then $2^{n+2} \mid\mid 12u_n^2$ and

$$v_n^2 = 12u_n^2 + 2^{n+2} \equiv 2^{n+4} \pmod{2^{n+5}},$$

and we see that $2^{2+n/2} \mid\mid v_n$.

If n is a multiple of 4, then 2^{n+4} divides $12u_n^2$ and

$$v_n^2 = 12u_n^2 + 2^{n+2} \equiv 2^{n+2} \pmod{2^{n+4}},$$

and the asserted result follows. □

3. Reductions

In this section, we prove the following result.

Proposition 3.1. *Let $(u_n)_{n\geq 0}$ be the binary recurrent sequence given by $u_0 = 0$, $u_1 = 1$ and $u_{n+2} = 2(u_{n+1} + u_n)$.*

The only squares in this sequence are $u_0 = 0$, $u_1 = 1$ and $u_4 = 16$.

The equation

$$u_n = y^p, \quad \text{for } p \text{ prime } \geq 3,$$

has only the solution $n = 0$ for n even. If n is odd and greater than 1, then $n > 100$ and $p \geq 41$, and if such a solution exists, then there exists at least one solution with n prime.

Proof. Firstly, we determine the squares among the sequence $(u_n)_{n\geq 0}$. Suppose that u_n is a square, say $u_n = z^2$. Then the relation (3) implies

$$12z^4 - v_n^2 = -(-2)^{n+2}.$$

If n is odd, then $\mathrm{ord}_2(u_n^2) = n - 1$ and $\mathrm{ord}_2(v_n^2) = n + 1$. Thus, we get a relation of the form

$$3X^4 = Y^2 + 2.$$

Working in the imaginary quadratic field $\mathbb{Q}(\sqrt{-2})$, we easily see that this relation leads to the Thue equation

$$a^4 + 4a^3b - 12a^2b^2 - 8ab^3 + 4b^4 = \pm 1.$$

Using PARI, in less than 0.1 second we get that the only solutions are the trivial ones, namely $(a, b) = (\pm 1, 0)$. This implies that $u_n = 2^{(n-1)/2}$. Considering the rate of growth of u_n that is immediate from equation (2), we deduce that $n = 1$.

If n is even then, using Lemma 2.1, we see that $\nu := \mathrm{ord}_2(n)$ must be even and the relation (3) implies now

$$3 \cdot 2^{n+2\nu+2} \cdot X^4 - 2^{n+2}Y^2 = -2^{n+2},$$

where X and Y are odd integers. After simplification, we get a relation of the form

$$3Z^4 - Y^2 = -1.$$

This kind of equation has been studied by Ljunggren [18], who proved that it cannot have more than two solutions in positive integers. Since $(Z, Y) = (1, 2)$ and $(2, 7)$ are two positive solutions, there are no other ones. Consequently, the only positive squares in the sequence $(u_n)_{n\geq 0}$ are $u_1 = 1$ and $u_4 = 16$.

Suppose now that $u_n = y^p$ where p is prime and $n = 2m$ is even. Then, by the two above formulas (3) for the index n and (4), there are positive odd numbers X and Y such that

$$u_m = 2^r X^p, \quad v_m = 2^s Y^p$$

for some non negative integers r and s, and (3) — now for the index m — gives

$$12 \cdot 2^{2r} X^{2p} - 2^{2s} Y^{2p} = -(-2)^{m+2}.$$

If m is odd, by Lemma 2.1 and Corollary 2.2, the previous relation becomes

$$3\, X^{2p} - Y^{2p} = 2.$$

By a result of Bennett [2] this implies $X^2 = Y^2 = 1$, which gives no solutions for $u_n = y^p$ in this case (that is, when $\mathrm{ord}_2(n) = 1$).

If $\mathrm{ord}_2(m) = 1$, then equation (3), for the index m, gives after simplification

$$3\, X^{2p} - 4Y^{2p} = -1.$$

By another result of Bennett [1], this implies again $X = Y = 1$, which gives again no solutions for $u_n = y^p$ in this case (that is when $\mathrm{ord}_2(n) = 2$).

If $4 \mid m$, then, putting $\gamma = \mathrm{ord}_2(m)$ so that $\gamma \geq 2$, we get

$$3 \cdot 2^{2\gamma} X^{2p} - Y^{2p} = -1.$$

By Theorem 1.5 of Bennett and Skinner [3], this equation has no nontrivial solution if $p \geq 7$ and $\gamma \geq 3$. But in this case, we can also proceed as follows. Put $m = 2k$. Then $v_k = 2^t Z^p$, where Z is some positive odd integer and

$$v_k^2 = v_m + 2^{k+1}.$$

If $2 \mid\mid k$ (that is, if $\gamma = 2$), then, after simplification, we get

$$8Z^{2p} = Y^p + 1,$$

where $v_k = 2^t Z^p$ for some positive integers t and Z with Z odd, and Theorem 1.2 of Bennett and Skinner [3] says that this equation has no nontrivial solution if $p \geq 7$. If $4 \mid k$, then the simplification gives

$$2Z^{2p} = Y^p + 1,$$

and a theorem of Darmon and Merel [11] implies that there is no nontrivial solution (that is with $|YZ| > 1$) for $p \geq 3$. To summarize, the only remaining cases (for n even) correspond to the solutions of the Diophantine equation

$$8Z^{2p} - Y^p = 1, \qquad p < 7.$$

It is easy to see that this equation has no nontrivial solution for $p = 3$ [use the factorization $8Z^3 - Y^6 = (2Z - Y^2)(4Z^2 + 2ZY^2 + Y^4)$], and a direct application of `PARI` (to the Thue equation $8X^p - Y^p = 1$), for $p = 5$ proves that there is no solutions for $u_n = y^p$ (with $8 \mid n$) for $p = 5$.

Moreover, a short and easy computation (a few seconds with PARI) shows that for a prime $p \geq 3$,

$$u_n = y^p \implies n \leq 4 \text{ or } n > 100.$$

Finally, when $n > 1$ is odd, considering the Thue equations associated to the equations $u_n = y^p$ for $p \in \{3, 5, \dots, , 37\}$, using PARI (the time of computation being around 30 minutes), we see that there is no solution for these exponents. We are very grateful to Guillaume Hanrot who wrote an extension of PARI, Version 2.2.8 (development CHANGES-1.1035), which contains a new treatment of Thue equations based on his paper [12]. In this paper, he showed that the knowledge of a subgroup of finite index in the full group of units is actually sufficient to solve a Thue equation (one bottleneck of the classical algorithm is the computation of the unit group of the field). With this new software, we can solve Thue equations of rather large degree in a reasonable time and get a **guaranteed** result (the older version used GRH to give a fast non-guaranteed result and the algorithm without assuming GRH was terribly slow for medium size examples).

Applying also an argument found independently by Pethő [24] and Robbins [26] (see also the proof of Proposition 6.2 of [7]), we can prove that if there is a solution of $u_n = y^p$ for $n > 1$ odd, then there is also such a solution with $n > 1$ and prime. This completes the proof of the proposition. □

To prove Theorem 1, we need some estimates from the theory of lower bounds for linear forms in logarithms of algebraic numbers.

Let α_1 and α_2 be algebraic numbers. Write $\mathbb{L} = \mathbb{Q}[\alpha_1, \alpha_2]$ and D for the degree of $\mathbb{L}$ over $\mathbb{Q}$. We write A_1 and A_2 for positive integers such that

$$\log A_i \geq \max\left\{ \mathrm{h}(\alpha_i), \frac{|\log \alpha_i|}{D}, \frac{1}{D} \right\} \qquad (i = 1,\, 2). \tag{5}$$

Here, for an algebraic number α whose minimal polynomial over $\mathbb{Z}$ is of the form $P(X) = a\prod_{i=1}^{d}(X - \alpha^{(i)})$, we write $\mathrm{h}(\alpha)$ for its logarithmic height given by

$$\mathrm{h}(\alpha) = \frac{1}{d}\left(\log|a| + \sum_{i=1}^{d} \log\left(\max\{1, |\alpha^{(i)}|\} \right) \right).$$

In other words,

$$\mathrm{h}(\alpha) = \frac{1}{d}\log \mathrm{M}(\alpha),$$

where $\mathrm{M}(\alpha) := \mathrm{M}(P)$ is the Mahler measure of the minimal polynomial of α over the rational integers.

Let b_1 and b_2 be positive integers and put

$$\Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1$$

and

$$b' = \frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1}.$$

The next result is Corollaire 2 on page 288 in [16] and gives a lower bound for $\log|\Lambda|$.

Theorem 2. *Assume that α_1 and α_2 are real, positive, and multiplicatively independent. Then*

$$\log|\Lambda| > -24.34\,D^4 \left(\max\left\{\log b' + 0.14, \frac{21}{D}, \frac{1}{2}\right\}\right)^2 \log A_1 \log A_2.$$

We point out that in the next section we do not use the Theorem 2 as given above but a sharper (and technically more involved) version of it for which we will refer the reader to [16].

In the sequel, we will use the following (equivalent) definition of $\mathrm{h}(\alpha)$, due to André Weil. Let $\alpha \in \mathbb{K}$ where $\mathbb{K}$ is a number field of degree D over the rationals. Then one defines the archimedean (normalized) valuations of $\mathbb{K}$ as follows; if Σ is the set of different embeddings

$$\sigma : \mathbb{K} \to \mathbb{C}$$

of $\mathbb{K}$ into the field of complex numbers, then one puts

$$|\alpha|_\sigma = \begin{cases} |\sigma\alpha|, & \text{if } \sigma\mathbb{K} \subset \mathbb{R}, \\ |\sigma\alpha|^2, & \text{otherwise,} \end{cases}$$

where $|\cdot|$ is the usual absolute value in $\mathbb{C}$.

Any finite valuation of $\mathbb{K}$ corresponds to a prime ideal $\mathfrak{l}$ of $\mathbb{K}$, which is over a prime rational integer ℓ. If e and f are the index of ramification and the residual degree of $\mathfrak{l}$, respectively, then one puts $|\alpha|_\mathfrak{l} = 0$ is $\alpha = 0$, and for $\alpha \neq 0$,

$$|\alpha|_\mathfrak{l} = \ell^{-f\operatorname{ord}_\mathfrak{l}(\alpha)/e},$$

where $\operatorname{ord}_\mathfrak{l}(\alpha)$ is the integer ν defined by the conditions

$$\alpha \in \mathfrak{l}^\nu, \quad \alpha \notin \mathfrak{l}^{\nu+1}.$$

Then, the other definition of $\mathrm{h}(\alpha)$ is

$$\mathrm{h}(\alpha) = \frac{1}{d}\left(\sum_\sigma \log^+|\alpha|_\sigma + \sum_\mathfrak{l} \log^+|\alpha|_\mathfrak{l}\right),$$

where

$$\log^+ x = \log\max\{1, x\}, \quad \text{for } x > 0.$$

4. A bound for p

The main result of this section is the following.

Proposition 4.1. *Let $(u_n)_{n\geq 0}$ be the sequence appearing in Proposition 3.1. If $u_n = y^p$, where $p > 2$ is prime and $n > 1$ is odd, then $p < 200$.*

We shall first give a complete argument based on Theorem 2 which shows that $p \leq 257$. The proof of the above proposition is achieved in the same way by appealing to the main theorem of [16] instead of Theorem 2.

Consider the equation $u_n = y^p$. By Proposition 3.1, we can assume that n is odd and > 100, and also that $p \geq 41$. Set $m := \operatorname{ord}_2(y)$ and put

$$y = 2^m z.$$

Thus, z is odd. Then the order at which 2 divides the right hand side of the above equation is mp, while the order at which 2 divides the left-hand side of the above equation is, by Lemma 2.1, equal to $(n-1)/2$. Thus we have

$$n = 2mp + 1.$$

In other words, in this simple case we have proved in an **elementary** way that

$$n \equiv 1 \mod p.$$

This corresponds to the congruence $n \equiv \pm 1 \bmod p$ proved in [7] for the case of Fibonacci numbers (notice that both results are best possible since $u_1 = 1$, $u_{-1} = 1/2$, whereas $F_1 = F_{-1} = 1$).

With $\alpha = 1+\sqrt{3}$ and $\beta = 1-\sqrt{3}$ as in Section 2, we rewrite the given equation $u_n = y^p$ as

$$\alpha^n - 2\sqrt{3}y^p = \beta^n,$$

or

$$\left(\frac{\alpha^{2m}}{y}\right)^p - \frac{2\sqrt{3}}{\alpha} = \frac{1}{\alpha}\,\frac{\beta^n}{y^p},$$

which implies that

$$\left|\left(\frac{\alpha^{2m}}{y}\right)^p - \frac{2\sqrt{3}}{\alpha}\right| = \frac{2\sqrt{3}}{\alpha}\,\frac{|\beta|^n}{\alpha^n - \beta^n} < 1.27\,(2/\alpha^2)^n.$$

Now we put

$$\Lambda = p\log\bigl(\alpha^{2m}/y\bigr) - \log\bigl(2\sqrt{3}/\alpha\bigr).$$

This is a linear form in two logarithms. Forgetting our initial notation and using the notation of Theorem 2 we have

$$b_1 = p,\ \ \alpha_1 = \alpha^{2m}/y = (2+\sqrt{3})^m/z, \quad b_2 = 1,\ \ \alpha_2 = 2\sqrt{3}/\alpha.$$

We have

$$n = 2mp + 1,$$

and

$$1.26 < \left(\frac{\alpha^{2m}}{y}\right)^p < 1.28,$$

hence

$$0 < \log\left(\frac{\alpha^{2m}}{y}\right) < \frac{0.25}{p}.$$

By the definition of the Weil logarithmic height,

$$2\,\mathrm{h}\bigl(\alpha^{2m}/y\bigr) = 2\,\mathrm{h}\bigl((2+\sqrt{3})^m/z\bigr) = \log^+\bigl(\alpha^{2m}/y\bigr) + \log^+(|\beta|^{2m}/y) + 2\log z,$$

(notice that the algebraic number $2+\sqrt{3}$ is a unit so it has a trivial valuation for any finite place), so that

$$\mathrm{h}\bigl(\alpha^{2m}/y\bigr) = \frac{1}{2}\log^+\bigl(\alpha^{2m}/y\bigr) + \log z < \frac{0.13}{p} + \log z.$$

Concerning α_2, we obtain

$$\alpha_2 = \frac{2\sqrt{3}}{1+\sqrt{3}} = \sqrt{3}(\sqrt{3}-1) = 3-\sqrt{3},$$

which shows that the minimal polynomial of α_2 over $\mathbb{Z}$ is $X^2 - 6X + 6$ and that

$$\mathrm{h}(\alpha_2) = \frac{1}{2}\,\mathrm{M}(X^2 - 6X + 6) = \frac{\log 6}{2}.$$

Moreover

$$\log \alpha_2 = \log(3 - \sqrt{3}).$$

Finally, it is easy to see that, for $n > 10$,

$$|\log \alpha_1| \leq \frac{1}{p}\,(0.01 + |\log \alpha_2|).$$

It follows that we can take here

$$\log A_1 = \frac{0.13}{p} + \log z,$$

and

$$\log A_2 = \frac{\log 6}{2}.$$

Thus,

$$b' \leq \frac{2p}{\log 6} + \frac{1}{2\,\log z}.$$

Notice also that

$$\frac{\alpha^{n-1}}{1.27} < u_n = 2^{(n-1)/2} z^p = y^p < \frac{\alpha^{n-1}}{1.26}.$$

Since

$$\frac{\log z}{\log y} = 1 - \frac{(n-1)\log 2}{2p \log y},$$

it follows that

$$1 - \frac{\log 2}{2 \log \alpha} < \frac{\log z}{\log y} < 1 - \frac{\log y - (\log 1.27)/p}{2 \log \alpha\, \log y} \log 2 < 1 + \frac{0.09}{p \log y} - \frac{\log 2}{2 \log \alpha},$$

and, for $p \geq 199$ we get

$$1 - \frac{\log 2}{2 \log \alpha} < \frac{\log z}{\log y} < 1.001 - \frac{\log 2}{2 \log \alpha},$$

and

$$0.6551\, \log y < \log z < 0.6553\, \log y,$$

where indeed the first inequality is true for all $n > 0$ and all p.

By (3), Lemma 2.1 and Corollary 2.2, we get the relation

$$x^2 + 2 = 3z^{2p},$$

where $x := 2^{-(n+1)/2} v_n$ is an integer. This shows that -2 is a quadratic residue for any prime divisor q of z. Hence, $q \equiv 1$ or $3 \bmod 8$.

One may also notice that

$$z < (\alpha/\sqrt{2})^{2m}.$$

Moreover, since n is prime, for any prime divisor q of z, the period of the zeros of the recursive sequence $(u_n)_{n \geq 0}$ modulo q is equal to n. Since this period is a divisor of $q \pm 1$, this implies

$$z \geq q \geq 2n - 1 = 4mp + 1.$$

It is easy to see that the two previous inequalities imply $m \geq 6$ for $p \geq 209$, hence

$$z \geq 24p + 1 \quad \text{and} \quad y \geq 2^6\,(24p + 1) \qquad \text{for } p \geq 209.$$

With the above corollary of [16], we get $p < 19232$.

But it is much more efficient to use the main theorem of [16]. We assume

$$p \geq 263, \quad \text{then} \quad y \geq e^{12.9}.$$

In this case, we apply this theorem with the choices

$$L = 8, \quad R_1 = 1, \quad S_1 = 8, \quad R_2 = 19, \quad S_2 = 75,$$

and

$$\mathrm{m} = 0.0766857, \quad \rho = 22,$$

and we get a contradiction. Thus,

$$p \leq 257.$$

In the same way, we can prove that:

- $p \leq 251$ if $y \geq e^{20}$,
- $p \leq 211$ if $y \geq e^{50}$,
- $p \leq 199$ if $y \geq e^{90}$.

To prove a better lower bound on m (for $2 < p < 1000$), we proceed as follows. From the relation

$$u_n = \frac{\alpha^n - \beta^n}{2\sqrt{3}} = y^p = 2^{mp} z^p$$

(recall that $n = 2mp + 1$), we get

$$z > \left(\frac{\alpha^2}{2}\right)^m \left(\frac{\alpha}{2\sqrt{3}}\right)^{1/p},$$

and

$$z < \left(\frac{\alpha^2}{2}\right)^m \left(\frac{\alpha + (2/\alpha^2)^{2mp}}{2\sqrt{3}}\right)^{1/p} < \left(\frac{\alpha^2}{2}\right)^m \left(\frac{\alpha}{2\sqrt{3}}\right)^{1/p} \left(1 + (2/\alpha^2)^{mp}\right).$$

Hence,

$$\left| z - \left(\frac{\alpha^2}{2}\right)^m \left(\frac{\alpha}{2\sqrt{3}}\right)^{1/p} \right| < \left(\frac{2}{\alpha^2}\right)^{m(p-1)} < 10^{-50},$$

using only the fact that $n > 100$.

We have tested this inequality for $2 < p < 1000$ and $1 \leq m \leq 100$, with 10^{-50} replaced by 10^{-5} — using a real precision of 1000 decimal digits — and we found no solution (after a few seconds of computation with PARI). Thus, for $p > 2$ we have

$$m > 100,$$

which implies

$$\log y > 200\,(\log \alpha) - 1 > 200.$$

We now apply [16] with the choices

$$L = 8, \quad R_1 = 1, \quad S_1 = 8, \quad R_2 = 17, \quad S_2 = 992,$$

and

$$\mathrm{m} = 0.057046, \quad \rho = 23,$$

and we get

$$p \leq 199.$$

5. Bounds for n in terms of p

Here, we follow the same strategy as in § 9 of [7].

Our objective is to obtain bounds for n (for n odd) in terms of p for the solutions of the equation

$$u_n = y^p.$$

We obtain the following result, in which $C_{\mathbb{K}}(\cdot)$ is as in Lemma 9.1 from [7].

Proposition 5.1. *Suppose $p \geq 11$ is prime. Let θ be any root of the polynomial*

$$P(X) := \sum_{k=0}^{p} (-2)^{\lfloor (p-k)/2 \rfloor} \binom{p}{k} X^k, \tag{6}$$

and let $\mathbb{K} = \mathbb{Q}(\theta)$. Let

$$\Theta = 5 \cdot 30^{p+3}\, p^{13/2}\, (p-1)^{p+1} \left((p-1)!\right)^2 (3p+2) \left(1 + \log(p(p-1))\right) C_{\mathbb{K}}(10^{p-1} p^p).$$

If (n, y, p) satisfies the equation $u_n = y^p$ with n odd, then $n < \mathcal{M}_p$ where $\mathcal{M}_p = 1.5\, p\, \Theta \log \Theta$.

Observe that the numerical result is very similar to Proposition 9.2 from [7], the only changes being 5 instead of 3.9 in the definition of Θ and 1.5 instead of 2. in that of $\mathcal{M}_p$. Clearly, the present upper bound for n is only slightly smaller than the one obtained in Proposition 9.2 from [7] in the case of the Fibonacci sequence.

In the sequel, we only point out the (small) changes with the proof of Proposition 9.2 from [7].

By (3), Lemma 2.1 and Corollary 2.2, a solution to $u_n = y^q$ with n odd yields a solution in positive integers x and y to the superelliptic equation

$$x^2 + 2 = 3y^{2p}.$$

Set $\omega = \sqrt{-2}$. Factorizing the left-hand side of the above equation over $\mathbb{Z}[\omega]$, we deduce the existence of rational integers a and b with $a^2 + 2b^2 = y^2$ (notice that y being odd, the same holds for a; hence, b must be even). Using the relation $3 = (1+\omega)(1-\omega)$, we see that

$$(x+\omega)(x-\omega) = (1+\omega)(1-\omega)(a+\omega b)^p (a-\omega b)^p.$$

We thus obtain

$$\pm 2\omega = (1+\omega)(a+\omega b)^p - (1-\omega)(a-\omega b)^p. \tag{7}$$

Dividing by 2ω, we get

$$\begin{aligned} \pm 1 = &\sum_{k=0}^{\lfloor p/2 \rfloor} \binom{p}{2k} a^{2k}\, (-2)^{(p-2k-1)/2}\, b^{p-2k} \\ &+ \sum_{k=0}^{\lfloor p/2 \rfloor} \binom{p}{2k+1} a^{2k+1}\, (-2)^{(p-2k-1)/2}\, b^{p-2k-1}. \end{aligned}$$

Consequently, (a, b) is an integer solution of the Thue equation

$$\sum_{k=0}^{p} (-2)^{\lfloor (p-k)/2 \rfloor} \binom{p}{k} X^k\, Y^{p-k} = \pm 1. \tag{8}$$

Remark. Our above computation works for the more general equation

$$x^2 + D = Cy^{2p},$$

where C and D are positive rational integers, with D squarefree.

To bound the size of the solutions of (8), we follow the general scheme of [5]. Let $P(X)$ and θ and $\mathbb{K}$ be as in Proposition 5.1; we note that $P(X)$ is the polynomial naturally associated to the Thue equation (8). We first need information on the number field $\mathbb{K}$ and its Galois closure.

Lemma 5.2. *The field $\mathbb{K} = \mathbb{Q}(\theta)$ is totally real and its Galois closure $\mathbb{L}$ has degree $p(p-1)$ over $\mathbb{Q}$. Furthermore, for $p \geq 11$, the absolute value of the discriminant of $\mathbb{K}$ is bounded by $10^{p-1}p^p$.*

Proof. Observe that any root of the polynomial

$$Q(X) := \frac{1}{2\omega} \cdot \big((1+\omega)(X+\omega)^p - (1-\omega)(X-\omega)^p\big) = X^p P(1/X).$$

satisfies $|X + \omega| = |X - \omega|$, and so must be real. Hence, $\mathbb{K}$ is a totally real field. (Observe that this argument uses only the fact that ω is purely imaginary.) Furthermore, $\mathbb{L}(\omega)/\mathbb{Q}(\omega)$ is a Kummer extension obtained by adjoining the p-th roots of unity and the p-th roots of $(1+\omega)/(1-\omega)$. Hence, this extension has degree $p(p-1)$, and this is the same for $\mathbb{L}/\mathbb{Q}$.

Observe now that $\mathbb{K}(\omega)$ is generated over $\mathbb{Q}(\omega)$ by any root of either of the following two monic polynomials with coefficients in $\mathbb{Z}[\omega]$: namely, $Y^p - (1+\omega)(1-\omega)^{p-1}$, and $Y^p - (1-\omega)(1+\omega)^{p-1}$. Since the discriminant D_1 (viewed as an algebraic integer in $\mathbb{Z}[\omega]$ and not as an ideal) of the extension $\mathbb{K}(\omega)/\mathbb{Q}(\omega)$ divides the discriminant of each of these polynomials, D_1 divides $p^p 3^{p-1}(1+\omega)^{(p-1)(p-2)}$ and $p^p 3^{p-1}(1-\omega)^{(p-1)(p-2)}$. As $1+\omega$ and $1-\omega$ are relatively prime, D_1 divides $3^{p-1}p^p$. Furthermore, estimating the discriminant of $\mathbb{K}(\omega)/\mathbb{Q}$ in two different ways thanks to Lemma 9.7 from [7] gives

$$|D_{\mathbb{K}(\omega)}| = 8^p D_1^2 = |D_{\mathbb{K}}|^2 \cdot |\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(D_{\mathbb{K}(\omega)/\mathbb{K}})|. \tag{9}$$

Consequently, $|D_{\mathbb{K}}|$ divides $3^{p-1}(2\sqrt{2}p)^p$, therefore $|D_{\mathbb{K}}|$ is less than $10^{p-1}p^p$, since $p \geq 11$. □

The above lemma provides the same upper bound for the discriminant of the associated number field as in the Fibonacci case. We now keep the notation from Proposition 9.2 of [7]. We have to estimate the modified height of the quotient $(\alpha_2 - \alpha_1)/(\alpha_3 - \alpha_1)$, where α_1, α_2 and α_3 are roots of $P(X)$. We proceed as follows. Let $\mathrm{M}(P)$ denote the Mahler measure of $P(X)$ and $\|P\|_2$ denotes its quadratic norm, that is, if $P(X) = \sum_{k\geq 0} a_k X^k$, then $\|P\|_2 = \big(\sum |a_k|^2\big)^{1/2}$. It is then well-known that

$$\mathrm{M}(P) \leq \|P\|_2,$$

(this is just Landau's inequality from [14]; see also [21]). In the present case, we have

$$\|P\|_2{}^2 < \sum_{k=0}^{p} 2^{p-k}\binom{p}{k}^2 \leq \sum_{k=0}^{p} 2^{2p-k}\binom{p}{k} = 6^p,$$

whence

$$\mathrm{M}(P) < 6^{p/2} \quad \text{and} \quad \mathrm{h}(\theta) \leq \frac{\log \mathrm{M}(P)}{p} < \frac{1}{2}\log 6.$$

Hence, with the modified height h' related to the field $\mathbb{L}$ defined in Lemma 5.2, we have

$$\mathrm{h}'\left(\frac{\alpha_2-\alpha_1}{\alpha_3-\alpha_1}\right) \leq 5\,p(p-1).$$

This explains the constant 5 instead of 3.9 in the definition of Θ.

Finally, we observe that if u_n is a p-th power for some odd n, then there are integers X and Y such that (X,Y) is a solution of the Thue equation (8) and $u_n^{2/p} = 2^{(n-1)/p}(X^2+2Y^2)$. Since $|X| \leq 1+3^p|Y|$ and $u_n \geq 2.5^n$ (for $n \geq 100$), we derive, exactly as in [7], that $n < 1.1\,p\log|Y|$. It then follows that (very roughly!)

$$n < 1.5\,p\,\Theta\log\Theta,$$

with

$$\Theta = 5\cdot 30^{p+3}\,p^{13/2}\,(p-1)^{p+1}\,(3p+2)\,\big((p-1)!\big)^2\,\big(1+\log(p(p-1))\big)\,C_{\mathbb{K}}(10^{p-1}p^p).$$

This proves Proposition 5.1.

6. Level-lowering

Recall our earlier notation $\alpha = 1+\sqrt{3}$, $\beta = 1-\sqrt{3}$. It is convenient to define

$$U_k = \frac{\alpha^{2k+1}-\beta^{2k+1}}{2^{k+1}\sqrt{3}}, \qquad V_k = \frac{\alpha^{2k+1}+\beta^{2k+1}}{2^{k+1}}, \qquad (k \geq 0).$$

Note that if $n = 2k+1$ then $u_n = 2^kU_k$. If $u_n = y^p$ with $n = 2k+1$ odd, then we have shown that $p \mid k$. So, we also know that

$$U_k = y'^p, \tag{10}$$

and therefore that

$$V_k^2 + 2 = 3y'^{2p}. \tag{11}$$

Our task is to prove that $k = 0$, which we do in this and the next section using the modular approach and the information obtained thus far by classical methods. In particular we assume that $41 \leq p \leq 199$. Our first step is to associate a putative solution to equation (10) to the Frey curve

$$E_k \;:\quad Y^2 = X^3 + 2V_kX^2 - 2X.$$

In this, we follow the recipe given by the paper of Bennet and Skinner [3]. From the result of Sections 2, 3 of that paper we deduce the following Lemma.

Lemma 6.1. *Let $E^1,\ldots,E^8$ be the elliptic curve 384A1, 384B1, ..., 384H1 (in Cremona's tables* [10]*). Suppose (k,y,p) is a solution to equation (10). With notation as above, the Galois representation on the p-torsion of E_k is isomorphic to the Galois representation on the p-torsion of one of the elliptic curve $E^1,\ldots,E^8$, in which case, for any prime $l \neq 2$, 3,*

(i) $a_l(E_k) \equiv a_l(E^i) \pmod{p}$ *if* $l \nmid y$.
(ii) $l+1 \equiv \pm a_l(E^i) \pmod{p}$ *if* $l \mid y$.

Proof. The results of [3] show that the Galois representation on the p-torsion of E_k arises from a newform of weight 2 and level 384. Using the computer algebra system `MAGMA` we compute the newforms at level 384 and find that these are all rational and correspond to the elliptic curves 384A1, 384B1, ..., 384H1 in Cremona's tables [10]. □

Our first task is to eliminate all of $E^1, \ldots, E^8$ except for one.

Lemma 6.2. *Suppose $l \neq 2, 3$ is a prime. The residue class of V_k modulo l depends only on the residue class of k modulo K_l, where*

$$K_l = \begin{cases} l-1 & \text{if } l \equiv \pm 1 \pmod{12}, \\ l+1 & \text{otherwise.} \end{cases} \tag{12}$$

Proof. The condition $l \equiv \pm 1 \pmod{12}$ is equivalent to the condition that 3 is a quadratic residue modulo l. If 3 is a quadratic residue modulo l, then the Lemma follows from Fermat's Little Theorem. Thus, suppose that 3 is a quadratic non-residue modulo l, and write $K_l = l + 1$. It is sufficient to show that

$$\frac{\alpha^{2K_l}}{2^{K_l}} \equiv 1 \pmod{l}, \qquad \frac{\beta^{2K_l}}{2^{K_l}} \equiv 1 \pmod{l}.$$

Now the Frobenius automorphism generates the Galois group of the algebraic closure of $\mathbb{F}_l$, and so $\alpha^l \equiv \beta \pmod{l}$. Hence, since $K_l = l + 1$, we see that

$$\frac{\alpha^{2K_l}}{2^{K_l}} \equiv \frac{\alpha^2\beta^2}{2^2} \equiv 1 \pmod{l},$$

and similarly for β instead of α. □

6.1. **Eliminating Newforms.** Lemma 6.1 relates the Galois representation of E_k to too many Galois representations. We now eliminate all but one of them.

Fix a prime $41 \leq p \leq 199$. Suppose $l \neq 2, 3$ is a prime. Let K_l be given by (12). Recall that (Lemma 6.2) the residue class of V_k modulo l, and hence the Frey curve E_k modulo l, depends only on the residue class of k modulo K_l. We see that the following definitions make sense: let $\mathcal{N}_p(l, E^i)$ to be the subset of $\kappa \in \mathbb{Z}/K_l$ such that

- either $V_\kappa^2 + 2 \not\equiv 0 \pmod{l}$, and $a_l(E_\kappa) \equiv a_l(E^i) \pmod{p}$,
- or $V_\kappa^2 + 2 \equiv 0 \pmod{l}$ and $l + 1 \equiv \pm a_l(E^i) \pmod{p}$.

Lemma 6.3. *Suppose (k, y, p) is a solution to equation (10), where $41 \leq p \leq 199$ is prime. Suppose that the Galois representation on the p-torsion of E_k is isomorphic to the corresponding representation for E^i. If $l \neq 2, 3$ is a prime then the reduction of k modulo K_l belongs to $\mathcal{N}_p(l, E^i)$.*

Proof. The Lemma follows from Lemma 6.1. □

Given two positive integers K_1, K_2, and two sets $\mathcal{N}_1 \subset \mathbb{Z}/K_1$ and $\mathcal{N}_2 \subset \mathbb{Z}/K_2$ we loosely define their 'intersection' $\mathcal{N}_1 \cap \mathcal{N}_2$ to be the set of all elements of $\mathbb{Z}/\mathrm{lcm}(K_1, K_2)$ whose reduction modulo K_1 and K_2 is respectively in $\mathcal{N}_1$ and $\mathcal{N}_2$.

Lemma 6.4. *Suppose (k, y, p) is a solution to equation (10), where $41 \leq p \leq 199$ is prime. Let*

$$E \ : \quad Y^2 = X^3 - X^2 - 3X + 3. \tag{13}$$

(This is the elliptic curve 384D1 in the notation of [10].) Then the Galois representation on the p-torsion of E_k is isomorphic to the Galois representation on the p-torsion of E.

Proof. Suppose otherwise. We then know that the Galois representation on the p-torsion of E_k is isomorphic to the Galois representation on E^i for some $i \neq 4$ (note that E^4 is $384D1$). Now fix a prime $41 \leq p \leq 199$ and fix $i \neq 4$ and we explain how to derive a contradiction.

Recall that $k \equiv 0 \pmod{p}$. In other words, the reduction of k modulo p belongs to the set

$$\mathcal{N}' = \left\{ \overline{0} \in \mathbb{Z}/p \right\}.$$

Moreover, for any prime $l \neq 2$, 3, we know that the reduction of k modulo K_l belongs to $\mathcal{N}_p(l, E^i)$. To derive a contradiction, it is sufficient to produce a set S of primes $l \neq 2$, 3, such that

$$\mathcal{N}' \cap \bigcap_{l \in S} \mathcal{N}_p(l, E^i) = \emptyset.$$

We used a short `pari/gp` script which for each $i \neq 4$ and for each prime $41 \leq p \leq 199$ produces such set S. For example, to eliminate E^1, $p = 41$, our program found it sufficient to take

$$S = \{5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 53, 83, 163\}.$$

The computational part of the proof took just a few minutes. □

7. The Modular Sieve

In this section, we complete the proof that the only positive perfect powers in the sequence u_n are u_1 and u_4. We continue with the notation of the previous section. We have shown that if $u_n = y^p$ then $n = 2k + 1$ is odd and that $41 \leq p \leq 199$. Recall that our solution to $u_n = y^p$ with $n = 2k + 1$ gives a solution (k, y', p) to equation (10). Our task is to show that $k = 0$. Furthermore, Proposition 5.1 gives a bound for the index n in terms of the exponent p, say $n \leq \mathcal{M}_p$.

We continue to denote by E the elliptic curve $384D1$ given by (13).

Lemma 7.1. *Let $41 \leq p \leq 199$ be prime. Let $\mathcal{M}_p$ be as given by Proposition 5.1. Suppose that S is a set of primes $l \neq 2$, 3, and write*

$$K_S = \mathrm{lcm}_{l \in S} K_l, \qquad \mathcal{N}_p(S, E) = \bigcap_{l \in S} \mathcal{N}_p(l, E) \subset \mathbb{Z}/K_S.$$

Suppose that the following conditions are satisfied.

- $\mathcal{N}_p(S, E) = \left\{ \overline{0} \in \mathbb{Z}/K_S \right\}$.
- $K_S > \mathcal{M}_p$.

Then the only solution to the equation $u_n = y^p$ is $n = 1$.

Proof. Since $n = 2k + 1$ we need to prove that $k = 0$. It follows from Lemmas 6.3, 6.4 that the reduction of k modulo K_S belongs to $\mathcal{N}_p(S, E)$. If the conditions are satisfied, then K_S divides k and since $0 \leq k < n \leq \mathcal{M}_p$ the Lemma follows. □

7.1. **Completion of the the Proof of Theorem 1.**

Fix the prime exponent $41 \leq p \leq 199$. All we need to do is to find a set S satisfying the conditions of Lemma 7.1. For this, we wrote a `pari/gp` program, and we now describe the strategy of our program taking $p = 41$ for concreteness. Here, Proposition 5.1 shows that

$$k < n \leq \mathcal{M}_{41} \approx 5.5 \times 10^{321}.$$

Let

$$K = 6983776800 = 2^5 \times 3^3 \times 5^2 \times 7 \times 11 \times \cdots \times 19.$$

We start with $S = \{5\}$. We go through the set of primes $l \geq 5$ in order, and we pickout those that that satisfy $K_l \mid K$. If such a prime is found then we append it to S and compute $\mathcal{N}_p(S, E)$. The reader will no doubt expect that since most of our K_l are highly composite and have lots of common factors, the set $\mathcal{N}_p(S, E)$ will be a small set of congruences modulo a large modulus. After a few seconds we found that $K_S = K$ and $\mathcal{N}_p(S, E) = \{\overline{0} \in \mathbb{Z}/K\}$, where S is the set of the first 48 primes $l \neq 2$, 3, satisfying $K_l \mid K$. Finding such a set of primes S proves that K divides k.

We now let $K' = K$. We look for primes l such that $23 \mid K_l$ and $K_l \mid K'$. We append them to our set S and continue in computing $\mathcal{N}_p(S, E)$ until we have shown that $K' \mid k$, etc.

The entire computation for $p = 41$ took just over a minute; at the end S had 353 elements and satisfied the conditions of Lemma 7.1 with

$$K_S = 2^5 \times 3^3 \times 5^2 \times 7 \times 11 \times \cdots \times 769 \approx 6.96 \times 10^{323}.$$

The entire computation for $41 \leq p \leq 199$ took about 9 hours on a 2.2 Mhz Intel Pentium.

There is an important optimization, worth mentioning, that was missed in [7]. Suppose we want to compute $\mathcal{N}_p(S, E) \cap \mathcal{N}_p(l, E)$, where we have already determined $\mathcal{N}_p(S, E)$. Suppose also that, in some previous step, we have shown that $L \mid k$ for some integer L (here L will be some divisor of K_S). To compute $\mathcal{N}_p(S, E) \cap \mathcal{N}_p(l, E)$, we need not determine $\mathcal{N}_p(l, E)$. We merely have to decide which elements $\kappa \in \mathbb{Z}/K_l$ satisfying $\kappa \equiv 0 \pmod{\operatorname{lcm}(L, K_l)}$ belong to $\mathcal{N}_p(l, E)$.

8. Discussion

In the sequel, we denote by (α, β) a given Lucas pair of *complex* numbers.

First, we consider the case when α and β are *real.* Without any loss of generality, we assume that we have $|\alpha| > |\beta|$. Furthermore, since

$$\frac{\alpha^n - \beta^n}{\alpha - \beta} = \pm \frac{(-\alpha)^n - (-\beta)^n}{(-\alpha) - (-\beta)},$$

we may further assume that β is positive. We consider the equation

$$u_n := \frac{\alpha^n - \beta^n}{\alpha - \beta} = y^p, \tag{14}$$

in integers n, y, p with p prime. We observe that $(n, y, p) = (1, 1, p)$ is a solution of (14) for any p. Furthermore, if $\alpha\beta = \pm 1$, then either $(-1, 1, p)$, or $(-1, -1, p)$ is also a solution. The existence of solutions for any p makes the complete resolution of (14) very difficult, since one can no longer hope to solve it by only using congruences to suitable moduli.

We now restrict our attention to solutions (n, y, p) of (14) with $|y| \geq 2$. Our first aim is to obtain a good upper bound for p. The existence of such an effective bound is due to Pethő [23] and, independently, to Shorey and Stewart [28].

Without any further assumption, we derive that

$$0 \neq |(\alpha - \beta) y^p \alpha^{-n} - 1| = |\alpha/\beta|^{-n}.$$

Using estimates for linear forms in *three* logarithms, we then get an upper bound for p, depending (of course!) on α and β.

However, we can do better in three situations, for which linear forms in *two* logarithms can be applied.

A first one is (trivially) when α and β differ by 1. In this case, both are integers, and, setting $x := \alpha = \beta + 1$, our equation can be rewritten as

$$x^n - (x-1)^n = y^p.$$

Then, an immediate application of estimates for linear forms in *two* logarithms yields a sharp upper bound for p.

A second one is when $\beta = 1$. In this case, α is an integer and, setting $x := \alpha$, our equation reduces to the Nagell–Ljunggren equation

$$\frac{x^n - 1}{x - 1} = y^p, \tag{15}$$

for which the following alternative approach has been developed (see [4] and the survey [6]). Rewrite (15) under the form

$$x^n = (x-1)y^p + 1,$$

We then take a prime divisor ℓ of x, and use estimates for linear forms in *two* ℓ-adic logarithms to get an upper bound for the ℓ-adic valuation $\mathrm{ord}_\ell(x^n)$ of $(x-1)y^p+1$. Basically, this yields the estimate $\mathrm{ord}_\ell(x^n) \ll (\log y)(\log p)$. On the other hand, we have trivially

$$\mathrm{ord}_\ell(x^n) \geq n \gg p \log y,$$

where, here and above, the numerical constant implied in $\ll$ depends only on ℓ. Hence, we get an upper bound for p, which is considerably better that what can be obtained using linear forms in *three* Archimedean logarithms.

A third one is described in the present Note. It is applicable, under some further assumption, when $\alpha + \beta$ and $\alpha\beta$ are not coprime.

Let $a \geq 1$, b and $t \geq 2$ be integers such that t divides no power of b and $a^2t^2 + 4bt$ is positive and not a perfect square. Consider the sequence defined by $u_0 = 0$, $u_1 = 1$ and

$$u_{n+2} = atu_{n+1} + btu_n.$$

An easy induction shows that, for any positive integer m, the integers u_{2m} and u_{2m+1} are divisible by t^m and that u_{2m+1} is congruent to b^mt^m modulo t^{m+1}. Consequently, when we consider the equation $u_n = y^p$ with n odd, denoting by ℓ the greatest integer for which t^ℓ divides y, we get that $(n-1)/2 = \ell p$; hence, that n is congruent to 1 modulo p. We then get an upper bound for p by using linear forms in *two* logarithms, exactly as in Theorem 1.

As we have seen in Sections 2 and 3, the case of even index yields further difficulties and requires a more precise analysis.

If one does not manage to get rid of linear forms in *three* logarithms, then the strategy is essentially the same as developed for the Fibonacci sequence. We try to use a sieve to prove that any solution to our equation $u_n = y^p$ must satisfy $n \equiv \pm 1 \pmod p$. Then, with ν such that $n = \nu p \pm 1$, we see that

$$|(\alpha-\beta)y^p(\alpha^{-\nu})^p\alpha^{\pm 1} - 1| = |(\alpha^{\pm 1}(\alpha-\beta)) \times (\alpha^{-\nu}y)^p - 1| = |\alpha/\beta|^{-n},$$

where the use of linear forms in *two* logarithms gives a very good upper bound for p.

Consequently, we can now assume that we have a *reasonable* upper bound for p. Obviously, it depends on the data, but, when $\alpha+\beta$ and $\alpha\beta$ are not too large, we get that p is less than a few hundreds. However, much work is still needed to achieve the resolution of the equation.

We continue the discussion by considering first, specifically, the case when $\beta = 1$, that is, equation (15).

A remarkable result of Bennett [1] asserts that for any given positive integers a, b and m, with $a > b$ and $m \geq 3$, the Diophantine equation

$$|aX^m - bY^m| = 1$$

has at most one solution in positive integers X and Y. This implies immediately that the Nagell–Ljunggren equation (15) has no solution (n, y, p) with $y \geq 2$ and $n \equiv 1 \pmod{p}$. For a fixed value of p, using an elementary sieve, it is then possible to prove that this equation has also no solution with $n \not\equiv 1 \pmod{p}$ (see [6]). Note that (15) has been solved for any value of x between -10^4 and 10^6.

We return to the quadratic case. We introduce the companion sequence of $(u_n)_{n\geq 0}$, namely the sequence $(v_n)_{n\geq 0}$ defined by

$$v_n = \alpha^n + \beta^n, \qquad (n \geq 0).$$

We observe that both sequences are related, for every $n \geq 0$, by

$$(\alpha-\beta)^2 u_n^2 = v_n^2 - 4(\alpha\beta)^n.$$

Assume first that α is a unit, that is, that $\alpha\beta = \pm 1$. With our assumptions on α and β, we see that α and β are roots of a polynomial

$$X^2 - tX + \varepsilon,$$

for some $\varepsilon = \pm 1$ and a positive integer t with $t \geq 3$ if $\varepsilon = 1$. Then, assuming that u_n is a p-th power and that $\varepsilon = -1$, we get the hyperelliptic equation

$$X^2 \pm 4 = (t^2+4)\, Y^{2p}. \tag{16}$$

We then proceed as in [7] to derive a Thue equation, from which we get an upper bound for X and Y; hence, for n. We mention that to any solution to (16) it corresponds a solution to the equation

$$(t+2i)W^p - (t-2i)Z^p = \pm 4i,$$

to be solved in Gaussian integers W and Z. It has the trivial solutions $(W, Z) = (1, 1)$ and $(-1, -1)$. It would be very nice to have an extension of Bennett's above result to the Gaussian field!

If $\varepsilon = 1$, we then get the hyperelliptic equation

$$X^2 \pm 4 = (t^2-4)\, Y^{2p} = (t+2)(t-2)\, Y^{2p}.$$

If α is not a unit, then the situation is not very clear, and we see no general method unless $(\alpha\beta)^n$ divides u_n^2 and v_n^2.

To conclude, we briefly discuss the case when α and β are complex conjugates. Thus, we consider the binary recurrence

$$u_0 = 0, \qquad u_1 = 1, \qquad u_{n+2} = au_{n+1} + bu_n,$$

with $(a, b) \neq (1, -1)$ (otherwise, α and β would be roots of unity) and $a^2 + 4b < 0$.

We can no longer use estimates for linear forms in complex logarithms in order to bound the exponent p.

Assume that there is a prime ℓ such that ℓ divides b but does not divide a. Then, there is an ideal $\mathfrak{l}$ in $\mathbb{Q}(\beta)$ such that $v_{\mathfrak{l}}(\beta) > 0$ and $v_{\mathfrak{l}}(\alpha) = 0$. Writing then

$$-(\beta/\alpha)^n = (\alpha - \beta)\alpha^{-n} y^p - 1,$$

we derive from known estimates for linear forms in *three* non-Archimedean logarithms (see e.g. [32]) an upper bound for p in terms of a and b.

We may then try to prove that n must be congruent to 1 modulo p in order to be able to apply estimates for linear forms in only *two* logarithms. However, there may be some additional difficulties. Consider for instance the recurrence given by $(a, b) = (1, -2)$. An easy calculation shows that, starting with u_0, we have the values

$$0, 1, 1, -1, -3, -1, 5, 7, -3, \ldots$$

Consequently, u_2, u_3 and u_5 are perfect p-th powers for any odd prime number p.

9. Related equations and open problems

The equations considered in the present paper are a particular class of the exponential Diophantine equation

$$u_n = y^q, \qquad \text{in } n, y, q \geq 2 \text{ integers with } |y| \geq 2,$$

where $(u_n)_{n\geq 0}$ is a given non-degenerated linear recurrent sequence of integers.

It is a well-known fact that, if the characteristic polynomial of the recurrence has only simple roots and has a dominant root, then the theory of linear forms in logarithms yields an effective upper bound for the exponent q (see, e.g. [25]). Under the same assumption, Pethő [25] applied results from Corvaja and Zannier [9] to get that the above equation has finitely many solutions for any fixed $q \geq 2$. Since the proof ultimately depend on the Schmidt Subspace Theorem, we have no algorithm to compute the set of perfect powers in (u_n).

Take for instance the Tribonacci sequence defined by the initial terms $T_0 = T_1 = 0$, $T_2 = 1$ and by the recursion $T_{n+3} = T_{n+2} + T_{n+1} + T_n$, for any $n \geq 0$. Since the above assumptions are clearly satisfied, we get that only finitely many Tribonacci numbers are perfect powers. However, we still do not know whether the only Tribonacci squares are $T_0 = T_1 = 0$, $T_2 = T_3 = 1$, $T_5 = 4$, $T_{10} = 81$, $T_{16} = 3136 = 56^2$ and $T_{18} = 10609 = 103^2$.

Let define the integers T_{-n} for $n \geq 1$ in such a way that the recursion formula holds for any integer. It is still an open question to decide whether there are only finitely perfect powers among the integers T_{-n}, $n \geq 1$.

References

[1] M. A. Bennett, *Rational approximation to algebraic number of small height: The Diophantine equation* $\mid ax^n - by^n \mid= 1$, J. reine angew. Math. 535 (2001), 1–49.

[2] M. A. Bennett, *Personal communication.*

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

[4] Y. Bugeaud, *Linear forms in p-adic logarithms and the Diophantine equation* $(x^n-1)/(x-1) = y^p$, Math. Proc. Cambridge Phil. Soc. **127** (1999), 373–381.

[5] Y. Bugeaud and K. Győry, *Bounds for the solutions of Thue-Mahler equations and norm form equations*, Acta. Arith. **74** (1996), 273–292.

[6] Y. Bugeaud and M. Mignotte, *L'équation de Nagell–Ljunggren* $(x^n - 1)/(x - 1) = y^p$, Enseign. Math. **48** (2002), 147–168.

[7] Y. Bugeaud, M. Mignotte and S. Siksek, *Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas powers*, Annals of Math., to appear.

[8] Y. Bugeaud, M. Mignotte and S. Siksek, *Classical and modular approaches to exponential Diophantine equations II. The Lebesque-Nagell equation*, Compositio Math., to appear.

[9] P. Corvaja and U. Zannier, *Some new applications of the subspace theorem*, Compositio Math. **131** (2002), 319–340.

[10] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd edition, Cambridge University Press, 1996.

[11] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's Last Theorem* J. reine angew. Math. **490** (1997), 81–100.

[12] G. Hanrot, *Solving Thue equations without the full unit group* Math. of Comp. **69**, no. 229, (1997), 3951–405.

[13] G. Hardy, J.E. Littlewood, and G. Polya, *Inequalities*, Cambridge University Press, Cambridge, 1934.

[14] E. Landau, *Sur quelques théorèmes de M. Petkovic̀ relatifs aux zéros des fonctions analytiques*, Bull. Soc. Math. France **33** (1905), 251–261.

[15] E. Landau, *Verallgemeinerung eines Pólyaschen Satzes auf algebraische Zahlkörper*, Nachr. Kgl. Ges. Wiss. Göttingen, Math.-Phys. Kl. (1918), 478–488.

[16] M. Laurent, M. Mignotte and Y. Nesterenko, 'Formes linéaires en deux logarithmes et déterminants d'interpolation,' *J. Number Theory* **55** (1995), 285–321.

[17] H. W. Lenstra, Jr., *Algorithms in algebraic number theory*, Bull. Amer. Math. Soc. **26** (1992), 211-244.

[18] W. Ljunggren, *Über die Gleichung* $x^2 = Dy^4 + 1$, Archiv. Math. Naturv. **45** (1942), Nr. 5.

[19] E. M. Matveev, *An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II*, Izv. Ross. Akad. Nauk Ser. Mat. **64** (2000), 125–180. English transl. in Izv. Math. **64** (2000), 1217–1269.

[20] M. Mignotte, *Entiers algébriques dont les conjugués sont proches du cercle unité*, Séminaire Delange–Pisot–Poitou, 19e année: 1977/78, Théorie des nombres, Fasc. 2, Exp. No. 39, 6 pp., Secrétariat Math., Paris, 1978.

[21] M. Mignotte, *Mathematics for Computer Algebra*, Springer-Verlag, New York, 1992.

[22] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers,* Springer-Verlag, Berlin, 1990.

[23] A. Pethő, *Perfect powers in second order linear recurrences*, J. Number Theory **15** (1982), no. 1, 5–13.

[24] A. Pethő, *Full cubes in the Fibonacci sequence*, Publ. Math. Debrecen **30** (1983), no. 1, 117–127.

[25] A. Pethő, *Diophantine properties of linear recursive sequences II*, Acta Math. Paedagogicae Nyíregyháziensis **17** (2001), 81–96.

[26] N. Robbins, *On Fibonacci numbers which are powers. II.* Fibonacci Quart. **21** (1983), no. 3, 215–218.

[27] A. Schinzel, *On the product of the conjugates outside of the unit circle of an algebraic number*, Acta Arith. **24** (1973), 385–399; Addendum **26** (1975), 329–331.

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

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

[30] C. L. Siegel, *Abschätzung von Einheiten*, Nachr. Akad. Wiss. Göttingen II, Math.-Phys. Kl., Nr. 9, (1969), 71–86.

[31] P. M. Voutier, *An effective lower bound for the height of algebraic numbers*, Acta Arith. **74** (1996), 81–95.

[32] Yu Kunrui, *p-adic logarithmic forms and group varieties. II.*, Acta Arith. **89** (1999), 337–378.

Yann Bugeaud, Université Louis Pasteur, U. F. R. de mathématiques, 7, rue René Descartes, 67084 Strasbourg Cedex, France
E-mail address: bugeaud@math.u-strasbg.fr

Florian Luca, Instituto de Matemáticas, Universidad Nacional Autónoma de México, C.P. 58089, Morelia, Michoacán, México
E-mail address: fluca@matmor.unam.mx

Maurice Mignotte, Université Louis Pasteur, U. F. R. de mathématiques, 7, rue René Descartes, 67084 Strasbourg Cedex, France
E-mail address: mignotte@math.u-strasbg.fr

Samir Siksek, Mathematics Institute, University of Warwick, Coventry, CV4 7AL, United Kingdom
E-mail address: siksek@maths.warwick.ac.uk