Annals of Mathematics, **163** (2006), 969–1018

Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers

By Yann Bugeaud, Maurice Mignotte, and Samir Siksek*

Abstract

This is the first in a series of papers whereby we combine the classical approach to exponential Diophantine equations (linear forms in logarithms, Thue equations, etc.) with a modular approach based on some of the ideas of the proof of Fermat's Last Theorem. In this paper we give new improved bounds for linear forms in three logarithms. We also apply a combination of classical techniques with the modular approach to show that the only perfect powers in the Fibonacci sequence are 0, 1, 8 and 144 and the only perfect powers in the Lucas sequence are 1 and 4.

1. Introduction

Wiles' proof of Fermat's Last Theorem [53], [49] is certainly the most spectacular recent achievement in the field of Diophantine equations. The proof uses what may be called the 'modular' approach, initiated by Frey ([19], [20]), which has since been applied to many other Diophantine equations; mostly—though not exclusively—of the form

(1)
$$ax^p + by^p = cz^p, \qquad ax^p + by^p = cz^2, \qquad ax^p + by^p = cz^3, \ \ldots \quad (p \text{ prime}).$$

The strategy of the modular approach is simple enough: associate to a putative solution of such a Diophantine equation an elliptic curve, called a Frey curve, in a way that the discriminant is a p-th power up to a factor which depends only on the equation being studied, and not on the solution. Next apply Ribet's level-lowering theorem [43] to show that the Galois representation on the p-torsion of the Frey curve arises from a newform of weight 2 and a fairly small level N say. If there are no such newforms then there are no nontrivial solutions to the original Diophantine equation. (A solution is said to be trivial

*S. Siksek's work is funded by a grant from Sultan Qaboos University (IG/SCI/DOMS/02/06).

if the corresponding Frey curve is singular.) Occasionally, even when one has newforms of the predicted level there is still a possibility of showing that it is incompatible with the original Galois representation (see for example [18], [5], [21]), though there does not seem to be a general strategy that is guaranteed to succeed.

A fact that has been underexploited is that the modular approach yields a tremendous amount of local information about the solutions of the Diophantine equations. For equations of the form (1) it is perhaps difficult to exploit this information successfully since we neither know of a bound for the exponent p, nor for the variables x, y, z. This suggests that the modular approach should be applied to exponential Diophantine equations; for example, equations of the form

$$ax^p + by^p = c, \qquad ax^2 + b = cy^p, \ \ldots \quad (p \text{ prime}).$$

For such equations, Baker's theory of linear forms in logarithms (see the book of Shorey and Tijdeman [46]) gives bounds for both the exponent p and the variables x, y. This approach through linear forms in logarithms and Thue equations, which we term the 'classical' approach, has undergone substantial refinements, though often it still yields bounds that can only be described as 'number theoretical'.

The present paper is the first in a series of papers whose aims are the following:

(I) To present theoretical improvements to various aspects of the classical approach.

(II) To show how local information obtained through the modular approach can be used to reduce the size of the bounds, both for exponents and for variables, of solutions to exponential Diophantine equations.

(III) To show how local information obtained through the modular approach can be pieced together to provide a proof that there are no missing solutions less than the bounds obtained in (I), (II).

(IV) To solve various outstanding exponential Diophantine equations.

Our theoretical improvement in this paper is a new and powerful lower bound for linear forms in three logarithms. Such a lower bound is often the key to bounding the exponent in an exponential Diophantine equation. This is our choice for (I). Our choice for (IV) is the infamous problem of determining all perfect powers in the Fibonacci and Lucas sequences. Items (II), (III) will be present in this paper only in the context of solving this problem. A sequel combining the classical and modular approaches for Diophantine equations of the form $x^2 + D = y^p$ has just been completed [13].

We delay presenting our lower bound for linear forms in three logarithms until Section 12, as this is somewhat technical. Regarding the Fibonacci and Lucas sequences we prove the following theorems.

THEOREM 1. *Let F_n be the n-th term of the Fibonacci sequence defined by*

$$F_0 = 0,\ F_1 = 1 \quad \textit{and} \quad F_{n+2} = F_{n+1} + F_n \textit{ for } n \geq 0.$$

The only perfect powers in this sequence are $F_0 = 0$, $F_1 = 1$, $F_2 = 1$, $F_6 = 8$ and $F_{12} = 144$.

THEOREM 2. *Let L_n be the n-th term of the Lucas sequence defined by*

$$L_0 = 2,\ L_1 = 1 \quad \textit{and} \quad L_{n+2} = L_{n+1} + L_n \textit{ for } n \geq 0.$$

The only perfect powers in this sequence are $L_1 = 1$ and $L_3 = 4$.

It is appropriate to point out that equations $F_n = y^p$ and $L_n = y^p$ have previously been solved for small values of the exponent p by various authors. We present a brief survey of known results in Section 2.

The main steps in the proofs of Theorems 1 and 2 are as follows:

(i) We associate Frey curves to putative solutions of the equations $F_n = y^p$ and $L_n = y^p$ with even index n to Frey curves and apply level-lowering. This, together with some elementary arguments, is used to reduce to the case where the index n satisfies $n \equiv \pm 1 \pmod 6$.

(ii) Then we may suppose that the index n in the equations $F_n = y^p$ and $L_n = y^p$ is prime. In the Fibonacci case this is essentially a result proved first by Pethő [40] and Robbins [44] (independently).

(iii) We apply level-lowering again under the assumption that the index n is odd. We are able to show using this that $n \equiv \pm 1 \pmod p$ for $p < 2 \times 10^8$ in the Fibonacci case. In the Lucas case we prove that $n \equiv \pm 1 \pmod p$ unconditionally.

(iv) We show how to reduce the equations $F_n = y^p$ and $L_n = y^p$ to Thue equations. We do not solve these Thue equations completely, but compute explicit upper bounds for their solutions using classical methods (see for example [10]). This provides us with upper bounds for n in terms of p. In the Lucas case we need the fact that $n \equiv \pm 1 \pmod p$ to obtain a simpler equation of Thue type.

(v) We show how the results of the level-lowering of step (iii) can be used, with the aid of a computer program, to produce extremely stringent congruence conditions on n. For $p \leq 733$ in the Fibonacci case, and for $p \leq 281$ in the Lucas case, the congruences obtained are so strong that,

when combined with the upper bounds for n in terms of p obtained in (iv), they give a complete resolution for $F_n = y^p$ and $L_n = y^p$.

(vi) It is known that the equation $L_n = y^p$ yields a linear form in two logarithms. Applying the bounds of Laurent, Mignotte and Nesterenko [27] we show that $p \leq 281$ in the Lucas case. This completes the determination of perfect powers in the Lucas sequences.

(vii) The equation $F_n = y^p$ yields a linear form in three logarithms. However if $p < 2 \times 10^8$ then by step (iii) we know that $n \equiv \pm 1 \pmod{p}$. We show how in this case the linear form in three logarithms may be rewritten as a linear form in two logarithms. Applying [27] we deduce that $p \leq 733$, which is the case we have already solved in step (v).

(viii) To complete the resolution of $F_n = y^p$ it is enough to show that $p < 2 \times 10^8$. We present a powerful improvement to known bounds for linear forms in three logarithms. Applying our result shows indeed that $p < 2 \times 10^8$ and this completes the determination of perfect powers in the Fibonacci sequence.

Let us make some brief comments.

The condition $n \equiv \pm 1 \pmod{p}$ obtained after step (iii) cannot be strengthened. Indeed, we may define F_n and L_n for negative n by the recursion formulae $F_{n+2} = F_{n+1} + F_n$ and $L_{n+2} = L_{n+1} + L_n$. We then observe that $F_{-1} = 1$ and $L_{-1} = -1$. Consequently, F_{-1}, F_1, L_{-1} and L_1 are p-th powers for any odd prime p. Thus equations $F_n = y^p$ and $L_n = y^p$ do have solutions with $n \equiv \pm 1 \pmod{p}$.

The strategy of combining explicit upper bounds for the solutions of Thue equations with a sieve has already been applied successfully in [12]. The idea of combining explicit upper bounds with the modular approach was first tentatively floated in [48].

A crucial observation for the proof of Theorem 1 is the fact that, with a modicum of computation, we can indeed use linear forms in two logarithms, and then get a much smaller upper bound for the exponent p.

The present paper is organised as follows. Section 2 is devoted to a survey of previous results. Sections 3 and 4 are concerned with useful preliminaries. Steps (i) and (ii) are treated in Sections 5 and 6, respectively. Sections 7 and 8 are devoted to step (iii). Sections 9 and 10 are concerned with Steps (iv) and (v). Section 11 deals with steps (vi) and (vii), and finishes the proof of Theorem 2. Finally, the proof of Theorem 1 is completed in Section 13, which deals with step (viii), by applying estimates for linear forms in three logarithms proved in Section 12.

The computations in the paper were performed using the computer packages `PARI/GP` [2] and `MAGMA` [7]. The total running time for the various compu-

tational parts of the proof of Theorem 1 is roughly 158 hours on a 1.7 GHz Intel Pentium 4. By contrast, the total time for the corresponding computational parts of the proof of Theorem 2 is roughly six hours.

2. A brief survey of previous results

In this section we would like to place our Theorems 1 and 2 in the context of other exponential Diophantine equations. We also give a very brief survey of results known to us on the problem of perfect powers in the Fibonacci and Lucas sequences, though we make no claim that our survey is exhaustive.

Thanks to Baker's theory of linear forms in logarithms, we know (see for example the book of Shorey and Tijdeman [46]) that many families of Diophantine equations have finitely many integer solutions, and that one can even compute upper bounds for their absolute values. These upper bounds are however huge and do not enable us to provide complete lists of solutions by brutal enumeration. During the last decade, thanks to important progress in computational number theory (such as the LLL-algorithm) and also in the theory of linear forms in logarithms (the numerical constants have been substantially reduced in comparison to Baker's first papers), we are now able to solve completely some exponential Diophantine equations. Perhaps the most striking achievement obtained via techniques from Diophantine approximation is a result of Bennett [4], asserting that, for any integers a, b and $p \geq 3$ with $a > b \geq 1$, the Diophantine equation

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

has at most one solution in positive integers X and Y.

Among other results in this area obtained thanks to (at least in part) the theory of linear forms in logarithms, we note that Bugeaud and Mignotte [11] proved that the equation $(10^n - 1)/(10 - 1) = y^p$ has no solution with $y > 1$, and that Bilu, Hanrot and Voutier [6] solved the long-standing problem of the existence of primitive divisors of Lucas–Lehmer sequences.

Despite substantial theoretical progress and the use of techniques coming from arithmetic geometry and developed in connection with Fermat's Last Theorem (see for example the paper of Bennett and Skinner [5]), some celebrated Diophantine equations are still unsolved. We would particularly like to draw the reader's attention to the following three equations:

$$x^2 + 7 = y^p, \qquad p \geq 3, \tag{2}$$

$$x^2 - 2 = y^p, \qquad p \geq 3, \tag{3}$$

and

$$F_n = y^p, \qquad n \geq 0 \text{ and } p \geq 2, \tag{4}$$

where F_n is the n-th term in the Fibonacci sequence. Let us explain the difficulties encountered with equations (2), (3) and (4). Classically, we first use estimates for linear forms in logarithms in order to bound the exponent p, and then we use a sieve. Equations (2) and (4) yield linear forms in three logarithms, and thus upper bounds for p of the order of 10^{13}, at present far too large to allow the complete resolution of (2) and (4) by classical methods (however, a promising attempt at equation (2) is made in [48]). The case of (3) is different, since estimates for linear forms in two logarithms yield that n is at most 164969 [22], an upper bound which can certainly be (at least) slightly improved. There is however a notorious difficulty in (3) and (4), namely the existence of solutions $1^2 - 2 = (-1)^p$ and $F_1 = 1^p$ for each value of the exponent p. These small solutions prevent us from using a sieve as efficient as the one used for (2). A natural way to overcome this is to derive, from (3) and (4), Thue equations, though these are of degree far too large to allow for a complete resolution by classical methods alone.

As explained in the introduction, the present work is devoted to equation (4), and to the analogous equation for the Lucas sequence.

As for general results, Pethő [39] and, independently, Shorey and Stewart [45] proved that there are only finitely many perfect powers in any nontrivial binary recurrence sequence. Their proofs, based on Baker's theory of linear forms in logarithms, are effective but yield huge bounds. We now turn to specific results on the Fibonacci and Lucas sequences.

- The only perfect squares in the Fibonacci sequence are $F_0 = 0$, $F_1 = F_2 = 1$ and $F_{12} = 144$; this is a straightforward consequence of two papers by Ljunggren [29], [30], [32]. This has been rediscovered by Cohn [14] (see the Introduction to [31]) and Wyler [54].

- London and Finkelstein [33] showed that the only perfect cubes in the Fibonacci sequence are $F_0 = 0$, $F_1 = F_2 = 1$ and $F_6 = 8$. This was reproved by Pethő [40], using a linear form in logarithms and congruence conditions.

- For $m = 5$, 7, 11, 13, 17, the only m-th powers are $F_0 = 0$, $F_1 = F_2 = 1$. The case $m = 5$ is due to Pethő [41], using the method described in [40]. It has been reproved by McLaughlin [34] by using a linear form in logarithms together with the LLL algorithm. The other cases are solved in [34] with this method.

- If $n > 2$ and $F_n = y^p$ then $p < 5.1 \times 10^{17}$; this was proved by Pethő using a linear form in three logarithms [42]. In the same paper he also showed that if $n > 2$ and $L_n = y^p$ then $p < 13222$ using a linear form in two logarithms.

- Another result which is particularly relevant to us is the following: If $p \geq 3$ and $F_n = y^p$ for integer y then either $n = 0$, 1, 2, 6 or there is a prime $q \mid n$ such that $F_q = y_1^p$, for some integer y_1. This result was established by Pethő [40] and Robbins [44] independently.
- Cohn [15] proved that $L_1 = 1$ and $L_3 = 4$ are the only squares in the Lucas sequence.
- London and Finkelstein [33] proved that $L_1 = 1$ is the only cube in the Lucas sequence.

3. Preliminaries

We collect in this section various results which will be useful throughout this paper. Our problem of determining the perfect powers in the Fibonacci and Lucas sequences naturally reduces to the problem of solving the following pair of equations:

$$F_n = y^p, \qquad n \geq 0, \text{ and } p \text{ prime}, \tag{5}$$

and

$$L_n = y^p, \qquad n \geq 0, \text{ and } p \text{ prime}. \tag{6}$$

Throughout this paper we will use the facts that

$$F_n = \frac{\omega^n - \tau^n}{\sqrt{5}}, \qquad L_n = \omega^n + \tau^n, \tag{7}$$

where

$$\omega = \frac{1+\sqrt{5}}{2}, \qquad \tau = \frac{1-\sqrt{5}}{2}. \tag{8}$$

This quickly leads us to associate the equations $F_n = y^p$ and $L_n = y^p$ with auxiliary equations as the following two lemmas show.

LEMMA 3.1. *Suppose that $F_n = y^p$. If n is odd then*

$$5y^{2p} = L_n^2 + 4, \tag{9}$$

and if n is even then

$$5y^{2p} = L_n^2 - 4. \tag{10}$$

LEMMA 3.2. *Suppose that $L_n = y^p$. If n is odd then*

$$y^{2p} = 5F_n^2 - 4, \tag{11}$$

and if n is even then

$$y^{2p} = 5F_n^2 + 4. \tag{12}$$

For a prime $l \neq 5$ define

$$M(l) = \begin{cases} l-1, & \text{if } l \equiv \pm 1 \pmod 5, \\ 2(l+1), & \text{if } l \equiv \pm 2 \pmod 5. \end{cases} \tag{13}$$

We will need the following two lemmas.

LEMMA 3.3. *Suppose that $l \neq 5$ is a prime and $n \equiv m \pmod{M(l)}$. Then*

$$F_n \equiv F_m \pmod l \quad \text{and} \quad L_n \equiv L_m \pmod l.$$

Proof. Write $\mathcal{O}$ for the ring of integers of the field $\mathbb{Q}(\sqrt{5})$. Recall, by (7), that F_n and L_n are expressed in terms of ω, τ. Let π be a prime in $\mathcal{O}$ dividing l. To prove the lemma all we need to show is that

$$\omega^{M(l)} \equiv \tau^{M(l)} \equiv 1 \pmod \pi.$$

If $l \equiv \pm 1 \pmod 5$ then 5 is a quadratic residue modulo l. The lemma follows immediately in this case from the fact that $(\mathcal{O}/\pi\mathcal{O})^* \cong \mathbb{F}_l^*$ and so has order $l-1$.

Now suppose that $l \equiv \pm 2 \pmod 5$. Note that

$$\omega^l \equiv \frac{1^l + 5^{\frac{l-1}{2}}\sqrt{5}}{2^l} \equiv \frac{1-\sqrt{5}}{2} \equiv \tau \pmod \pi,$$

since 5 is a quadratic nonresidue modulo l. Thus

$$\omega^{M(l)} \equiv \omega^{2(l+1)} \equiv (\omega\tau)^2 \equiv 1 \pmod \pi,$$

and similarly for τ. □

LEMMA 3.4. *The residues of L_n, F_n modulo 4 depend only on the residue of n modulo 6, and are given by the following table*

	$L_n \pmod 4$	$F_n \pmod 4$
$n \equiv 0 \pmod 6$	2	0
$n \equiv 1 \pmod 6$	1	1
$n \equiv 2 \pmod 6$	3	1
$n \equiv 3 \pmod 6$	0	2
$n \equiv 4 \pmod 6$	3	3
$n \equiv 5 \pmod 6$	3	1

Proof. The lemma is proved by a straightforward induction, using the recurrence relations defining F_n and L_n. □

4. Eliminating small exponents and indices

We will later need to assume that the exponent p and the index n in the equations (5) and (6) are not too small. More precisely, in this section, we prove the following pair of propositions.

PROPOSITION 4.1. *If there is a perfect power in the Fibonacci sequence not listed in Theorem* 1 *then there is a solution to the equation*

$$F_n = y^p, \qquad n > 25000 \text{ and } p \geq 7 \text{ is prime.} \tag{14}$$

PROPOSITION 4.2. *If there is a perfect power in the Lucas sequence not listed in Theorem* 2 *then there is a solution to the equation*

$$L_n = y^p, \qquad n > 25000 \text{ and } p \geq 7 \text{ is prime.} \tag{15}$$

The propositions follow from the results on Fibonacci perfect powers quoted in Section 2 together with Lemmas 4.3 and 4.4 below.

4.1. *Ruling out small values of the index* n.

LEMMA 4.3. *For no integer* $13 \leq n \leq 25000$ *is* F_n *a perfect power. For no integer* $4 \leq n \leq 25000$ *is* L_n *a perfect power.*

Proof. Suppose $F_n = y^p$ where p is some prime and n is in the range $13 \leq n \leq 25000$. It is easy to see from (7), (8) that $2 \leq p \leq n \log(\omega)/\log(2)$. Now fix n, p. We would like to show that F_n is not a p-th power.

Suppose l is a prime satisfying $l \equiv \pm 1 \pmod 5$ and $l \equiv 1 \pmod p$. The condition $l \equiv \pm 1 \pmod 5$ ensures that 5 is a quadratic residue modulo l. Then one can easily compute F_n modulo l using (7) (without having to write down F_n). Now let $k = (l-1)/p$. If $F_n^k \not\equiv 1 \pmod l$ then we know that F_n is not a p-th power.

We wrote a short `PARI/GP` program to check for n in the above range, and for each prime $2 \leq p \leq n \log(\omega)/\log(2)$ that there exists a prime l proving that F_n is not a p-th power, using the above idea. This took roughly 15 minutes on a 1.7 GHz Pentium 4.

The corresponding result for the Lucas sequence is proved in exactly the same way, with the program taking roughly 16 minutes to run on the same machine. □

4.2. *Solutions with exponent* $p = 2, 3, 5$. Later on when we come to apply level-lowering we will need to assume that $p \geq 7$. It is straightforward to solve equations (5) and (6) for $p = 2, 3, 5$ with the help of the computer algebra package `MAGMA`. We give the details for the Lucas case; the Fibonacci case is similar. Alternatively we could quote the known results surveyed in Section 2, although $p = 5$ for the Lucas case does not seem to be covered by the literature.

LEMMA 4.4. *The only solutions to the equation* (6) *with* $p = 2, 3, 5$ *are* $(n, y, p) = (1, 1, p)$ *and* $(3, 2, 2)$.

Proof. Suppose first that n is even. By Lemma 3.2 it is enough to show that (12) does not have a solution. Suppose that (n, y, p) is a solution to (12). Clearly F_n and y are odd, and y is not divisible by 5. Thus we have

$$(2 + F_n\sqrt{-5}) = \mathfrak{a}^{2p}$$

for some ideal $\mathfrak{a}$ of $\mathbb{Z}[\sqrt{-5}]$. Now the class number of $\mathbb{Z}[\sqrt{-5}]$ is 2, and hence $\mathfrak{a}^2$ is a principal ideal. It follows that

$$2 + F_n\sqrt{-5} = \epsilon(u + v\sqrt{-5})^p$$

for some integers u, v, where $\epsilon = \pm 1$ if $p = 2$ and $\epsilon = 1$ otherwise. If $p = 2$ then we get $\pm 2 = u^2 - 5v^2$ which is impossible modulo 5. If $p = 3$ then

$$2 = u(u^2 - 15v^2),$$

and if $p = 5$ then

$$2 = u(u^4 - 50u^2v^2 + 125v^4).$$

It is easy to see that both of these are impossible. Next we turn to the case where n is odd. Again by Lemma 3.2 it is enough to solve the equation (11). Suppose first that $p = 3$, 5. If (n, y, p) is any solution to equation (11) then we quickly see that y must be odd and

$$2 + \sqrt{5}F_n = \left(\frac{1 + \sqrt{5}}{2}\right)^r (u + v\sqrt{5})^p.$$

For some $r = 0, \ldots, p - 1$ we see that u and v are both integers or both halves of odd integers. The computer algebra package `MAGMA` quickly solves all the resulting Thue equations showing that $y = \pm 1$. This implies that for $p = 3$, 5 the only solution to equation (6) is the trivial one $(1, 1, p)$.

Finally to deal with $p = 2$ we note that if (n, y) satisfies (11) then $(X, Y) = (5y^2, 25F_n y)$ is an integral point on the elliptic curve $Y^2 = X^3 + 100X$. Again `MAGMA` quickly computes all integral points on this curve: these are $(X, Y) = (0, 0)$, $(5, \pm 25)$, $(20, \pm 100)$, which yield the solutions $(n, y) = (1, 1)$, $(3, 2)$. This completes the proof of the lemma. □

5. Reducing to the case $n \equiv \pm 1 \pmod 6$

In this section we would like to reduce the study of equations (5) and (6) to the special case where the index n satisfies $n \equiv \pm 1 \pmod 6$. For Fibonacci we show that if there is some solution (n, y, p) to (5) then there is another solution with the same exponent p such that the index n satisfies the above condition. For the Lucas sequence we prove the following stronger result.

LEMMA 5.1. *If (n, y, p) is a solution to the equation (6) with $p \geq 7$ then $n \equiv \pm 1 \pmod 6$.*

For Fibonacci our result is weaker but still useful.

LEMMA 5.2. *If (n, y, p) is a solution to equation (5) with $p \geq 7$ then either $n = 0$ or $n \equiv \pm 1 \pmod 6$ or else $n = 2k$ with*

(a) $k \equiv \pm 1 \pmod 6$.

(b) $F_k = U^p$ *and* $L_k = V^p$ *for some positive integers* U *and* V.

The proofs of both Lemmas 5.1 and 5.2 make use of Frey curves and level-lowering. Here and elsewhere where we make use of these tools, we do not directly apply the original results in this field (Ribet's level-lowering Theorem [43], modularity of elliptic curves by Wiles and others [53], [8], irreducibility of Galois representations by Mazur and others [36], etc.). We will instead quote directly from the excellent recent paper of Bennett and Skinner [5], which is concerned with equations of the form $Ax^n + By^n = Cz^2$. In every instance we will put our equation in this form before applying the results of [5].

Proof of Lemma 5.1. Suppose that (n, y, p) is a solution to equation (6) with $p \geq 7$. We observe first that $n \not\equiv 0, 3 \pmod 6$. For in this case Lemma 3.4 implies that both F_n and L_n are even, and hence by Lemma 3.2 either 5 or -5 is a 2-adic square, which is not the case.

We now restrict our attention to $n \equiv 2,\ 4 \pmod 6$ and $p \geq 7$ and show that this leads to a contradiction. This is enough to prove the lemma. Let

$$G_n = \begin{cases} -F_n & \text{if } n \equiv 2 \pmod 6 \\ F_n & \text{if } n \equiv 4 \pmod 6. \end{cases}$$

It follows from Lemma 3.2 that

$$y^{2p} = 5{G_n}^2 + 4.$$

We associate to our solution (n, y, p) of (6) with $n \equiv 2,\ 4 \pmod 6$ the Frey curve

$$E_n : \qquad Y^2 = X^3 + 5G_nX^2 - 5X. \tag{16}$$

Let E be the elliptic curve 100A1 in Cremona's tables [17]; E has the following model:

$$E : \quad Y^2 = X^3 - X^2 - 33X + 62.$$

Write $\rho_p(E)$ for the Galois representation

$$\rho_p(E) : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[p])$$

on the p-torsion of E, and let $\rho_p(E_n)$ be the corresponding Galois representation for E_n.

Applying the results of [5, §§2, 3], we see that $\rho_p(E_n)$ arises from a cuspidal newform of weight 2, level 100, and trivial Nebentypus character. However

using the computer algebra package MAGMA we find that the dimension of newforms of weight 2 and level 100 is one. Moreover the curve E above is (up to isogeny) the unique elliptic curve of conductor 100. Thus $\rho_p(E_n)$ and $\rho_p(E)$ are isomorphic. It follows from this, by [5, Prop. 4.4], that 5 does not divide the denominator of the j-invariant of E. This is not true as $j(E) = 16384/5$, giving us a contradiction.

For the convenience of the reader we point out that in Bennett and Skinner's notation:

$$A = 1, \quad B = -4, \quad C = 5, \quad a = y^2, \quad b = 1, \quad c = G_n.$$

Lemma 3.4 and our definition of G_n above imply that $c \equiv 3 \pmod 4$ which is needed to apply the results of Bennett and Skinner. This completes our proof of Lemma 5.1. □

Proof of Lemma 5.2. Suppose that (n, y, p) is a solution to equation (5) with $n \neq 0$ and $p \geq 7$. By Lemma 3.4 we see that $n \not\equiv 3 \pmod 6$. Suppose then that $n \not\equiv \pm 1 \pmod 6$. Clearly $n = 2k$ for some integer k. It is well-known and easy to see from (7) that $F_n = F_{2k} = F_k L_k$. It is also easy to see that the greatest common divisor of F_k and L_k is either 1 or 2. The crux of the proof is to show that if $F_n = y^p$ then F_n is odd.

Thus suppose that F_n (and hence y) is even. Lemma 3.2 tells us that $5y^{2p} + 4 = L_n^2$. Since y even, we see that $2 \,\|\, L_n$. Let $z = y/2$ and

$$x = \begin{cases} L_n/2, & \text{if } L_n \equiv 2 \pmod 8, \\ -L_n/2, & \text{if } L_n \equiv 6 \pmod 8 . \end{cases}$$

Thus $x \equiv 1 \pmod 4$ and

$$2^{2p-2} \cdot 5z^{2p} + 1 = x^2.$$

Following [5, §2] we associate to this equation the Frey curve

$$Y^2 + XY = X^3 + \left(\frac{x-1}{4}\right) X^2 + 2^{2p-8} \cdot 5z^{2p} X.$$

Applying level-lowering [5, §3] shows that the Galois representation arises from a cusp form of weight 2 and level 10. Since there are no such cusp forms we get a contradiction. (This is essentially the same argument used in the proof of Fermat's Last Theorem.) It is noted that the argument here fails for $n = 0$ since in this case the Frey curve is singular.

We deduce that F_n is odd, so that $F_k = U^p$ and $L_k = V^p$ for some positive integers U, V. By Lemma 5.1 we know that $k \equiv \pm 1 \pmod 6$. This completes the proof of Lemma 5.2. □

6. Reduction to the prime index case

In this section we reduce our problem to the assumption that the index n is prime, as in the following pair of propositions.

PROPOSITION 6.1. *If there is a perfect power in the Fibonacci sequence not listed in Theorem* 1 *then there is a solution to the equation*

$$F_n = y^p, \qquad n > 25000,\ p \geq 7 \text{ with } n,\ p \text{ prime.} \tag{17}$$

PROPOSITION 6.2. *If there is a perfect power in the Lucas sequence not listed in Theorem* 2 *then there is a solution to the equation*

$$L_n = y^p, \qquad n > 25000,\ p \geq 7 \text{ with } n,\ p \text{ prime.} \tag{18}$$

After we prove these two propositions the remainder of this paper will be devoted to showing that there are no solutions to equations (17) and (18).

Proof of Proposition 6.1. If $F_n = y^p$ with n odd then this is just the result of Pethő and Robbins quoted in Section 2 together with our Proposition 4.1. Suppose $n = 2k$. By Lemma 5.2 we know that k is odd and $F_k = U^p$ for some integer U. Now simply apply the result of Pethő and Robbins again, together with Proposition 4.1. □

Proof of Proposition 6.2. Suppose that $L_n = y^p$ where $n \neq 1,\ 3$ and $p \geq 7$. By Lemma 5.1 we know that $n \equiv \pm 1 \pmod 6$, and so n is odd. If n is prime then the result follows from Proposition 4.2. Thus suppose that n is composite and let q be its smallest prime factor. Write $n = kq$, where $k > 1$. Then $L_n = y^p$ can be rewritten as

$$(\omega^k - \omega^{-k})(\omega^{k(q-1)} + \omega^{k(q-3)} + \cdots + \omega^{-k(q-3)} + \omega^{-k(q-1)}) = \omega^n - \omega^{-n} = y^p. \tag{19}$$

It is straightforward to see that the two factors on the left-hand side are in $\mathbb{Z}$ and that their greatest common factor divides q. [Proof: If this gcd is d then $\omega^{2k} \equiv 1 \pmod d$ and $\omega^{k(q-1)} + \cdots + \omega^{-k(q-1)} \equiv q \equiv 0 \pmod d$, which shows that d divides q.] Suppose that q divides the two factors. Then we see that

$$\omega^{2k} \equiv 1 \pmod \pi$$

for some prime π of $\mathcal{O}$ lying above q. But $\omega^2 - 1 = \omega$ and so $\omega^2 \not\equiv 1 \pmod \pi$. Therefore, the order of the image of ω^2 in $(\mathcal{O}/\pi)^*$ is not 1 and that it divides k and hence n. But $\#(\mathcal{O}/\pi)^*$ is either $q-1$ or q^2-1. Therefore, some nontrivial factor of n divides $(q-1)(q+1)$. Moreover, n is odd, and all odd prime factors of $(q-1)(q+1)$ are smaller than q. This contradicts the assumption that q is the smallest prime factor of n.

We deduce that q does not divide the factors on the right-hand side of (19). Hence $L_k = \omega^k - \omega^{-k} = y_1^p$ for some integer y_1. If k is prime then the proof is complete by Proposition 4.2. Otherwise we apply the above argument recursively. □

7. Level-lowering for Fibonacci — The odd index case

Previously we used a Frey curve and level-lowering to obtain information about solutions of $F_n = y^p$ for even n. In this section we associate a Frey curve to any solution of equation (17).

Suppose that (n, y, p) is a solution to (17). Thus n and p are primes with $p \geq 7$ and $n > 25000$. Let

$$H_n = \begin{cases} L_n, & \text{if } n \equiv 1 \pmod 6, \\ -L_n, & \text{if } n \equiv 5 \pmod 6. \end{cases} \tag{20}$$

LEMMA 7.1. *With notation as above,* $H_n \equiv 1 \pmod 4$ *and*

$$5y^{2p} - 4 = H_n^2. \tag{21}$$

The lemma follows immediately from Lemma 3.1 and Lemma 3.4.

We associate to the solution (n, y, p) the Frey curve

$$E_n : \qquad Y^2 = X^3 + H_n X^2 - X. \tag{22}$$

We now come to level-lowering. Let E be the following elliptic curve over $\mathbb{Q}$:

$$E : \quad Y^2 = X^3 + X^2 - X; \tag{23}$$

this is curve 20A2 in Cremona's tables [17]. As before, write $\rho_p(E)$ for the Galois representation on the p-torsion of E, and let $\rho_p(E_n)$ be the corresponding Galois representation on the p-torsion of E_n. If l is a prime, let $a_l(E)$ be the trace of the Frobenius of the curve E at l, and let $a_l(E_n)$ denote the corresponding trace of the Frobenius of E_n.

PROPOSITION 7.2. *Suppose that* (n, y, p) *is a solution to* (17). *With notation as above, the Galois representations* $\rho_p(E_n)$, $\rho_p(E)$ *are isomorphic. Moreover, for any prime* $l \neq 2, 5$,

(i) $a_l(E_n) \equiv a_l(E) \pmod p$ *if* $l \nmid y$,

(ii) $l + 1 \equiv \pm a_l(E) \pmod p$ *if* $l \mid y$.

Proof. First we apply the results of [5, §§2,3]. From these we know that $\rho_p(E_n)$ arises from a cuspidal newform of weight 2, level 20, and trivial Nebentypus character. (In applying the results of [5] we need Lemma 7.1.) However

$S_2(\Gamma_0(20))$ has dimension 1. Moreover, the curve E is (up to isogeny) the unique curve of conductor 20. It follows that $\rho_p(E)$ and $\rho_p(E_n)$ are isomorphic.

The rest of the proposition follows from [24, Prop. 3], and the fact that if $l \neq 2$, 5 and $l \mid y$ then l is a prime of multiplicative reduction for E_n and so $a_l(E_n) = \pm 1$. □

Proposition 7.2 is useful in several stages of our proof of Theorem 1. The following proposition is needed later, and follows from Proposition 7.2 and some computational work.

PROPOSITION 7.3. *If (n, y, p) is any solution to equation (17) with $p < 2 \times 10^8$ then $n \equiv \pm 1 \pmod{p}$.*

The idea behind the proof is inspired by a method of Kraus (see [23] or [48]) but there are added complications in our situation: for any prime p the equation $F_n = y^p$ has the solution $(n, y) = (1, 1)$, and also the solution $(n, y) = (-1, 1)$ (obtained by extrapolating the definition of the Fibonacci sequence backwards).

Before proving Proposition 7.3 we start with a little motivation. Suppose that $p \geq 7$ is a prime, and we find some small positive integer k such that $l = 2kp + 1$ is prime, and $l \equiv \pm 1 \pmod{5}$. It follows that 5 is a quadratic residue modulo l, and we choose an element in $\mathbb{F}_l$ which we conveniently denote by $\sqrt{5}$, satisfying $(\sqrt{5})^2 \equiv 5 \pmod{l}$. We may then consider ω, τ (defined in (8)) as elements of $\mathbb{F}_l$.

Consider the equation $F_n = y^p$. Now $l - 1 = 2kp$, with k small. This means that y^p comes from a small subset of $\mathbb{F}_l$. We can now use the level-lowering to predict the values of y^p. Hopefully, we may find that the only value of y^p modulo l predicted by the level-lowering and also belonging to our small subset are ± 1. Under a further minor hypothesis we can show that this implies that $n \equiv \pm 1 \pmod{p}$. If a particular value of k does not work, we may continue trying until a suitable k is found.

We make all this precise. Suppose as above that l, p are primes with $l = 2kp + 1$ and $l \equiv \pm 1 \pmod{5}$. Define

$$A(p, k) = \left\{ \zeta \in (\mathbb{F}_l^*)^{2p} \setminus \{1\} \ : \quad \left(\frac{5\zeta - 4}{l} \right) = 0 \text{ or } 1 \right\}.$$

For each $\zeta \in A(p, k)$, choose an integer δ_ζ such that

$$\delta_\zeta^2 \equiv 5\zeta - 4 \pmod{l}.$$

Let

$$E^\zeta \ : \quad Y^2 = X^3 + \delta_\zeta X^2 - X.$$

As above, E will denote the elliptic curve 20A2.

LEMMA 7.4. *Suppose $p \geq 7$ is a prime. Suppose there exists an integer k satisfying the following conditions:*

(a) *The integer $l = 2kp + 1$ is prime, and $l \equiv \pm 1 \pmod 5$.*

(b) *The order of ω modulo l is divisible by p; equivalently $\omega^{2k} \not\equiv 1 \pmod l$.*

(c) *For all $\zeta \in A(p, k)$,*

$$a_l(E^\zeta)^2 \not\equiv a_l(E)^2 \pmod p.$$

Then any solution to the equation (17) must satisfy $n \equiv \pm 1 \pmod p$.

Proof. Suppose p, k satisfy the conditions of the lemma, and that (n, y, p) is a solution to equation (17). Let H_n and E_n be as above. Thus H_n satisfies (21).

We will prove first that $l \nmid y$. Suppose that $l \mid y$. Then $(\omega^n + \omega^{-n})/\sqrt{5} = F_n = y^p \equiv 0 \pmod l$ and so $\omega^{4n} \equiv 1 \pmod l$. From (b) we deduce that $p \mid 4n$. However, the integer n is prime, and so $p = n$. This is impossible, since otherwise $F_p = y^p$ and clearly $1 < F_p < 2^p$. Hence $l \nmid y$.

Next we will show that $y^{2p} \equiv 1 \pmod l$. Thus suppose that $y^{2p} \not\equiv 1 \pmod l$. By Lemma 7.1 there is some $\zeta \in A(p, k)$ such that $y^{2p} \equiv \zeta \pmod l$. Further $\delta_\zeta \equiv \pm H_n \pmod l$. It follows that $a_l(E^\zeta) = \pm a_l(E_n)$. Applying Proposition 7.2 again, we see that $a_l(E_n) \equiv a_l(E) \pmod p$. These congruences now contradict condition (c).

We have finally proved that $y^{2p} \equiv 1 \pmod l$. By equation (21) we see that $H_n \equiv \pm 1 \pmod l$. Since n is odd (in fact an odd prime), and $\tau = -\omega^{-1}$, we get from the definition of H_n that $\omega^{2n} \pm \omega^n - 1 \equiv 0 \pmod l$. Solving this we find that $\omega^n \equiv \pm\omega^{\pm 1} \pmod l$. Thus

$$\omega^{2(n+1)} \equiv 1 \pmod l \qquad \text{or} \qquad \omega^{2(n-1)} \equiv 1 \pmod l.$$

However, condition (b) of the lemma assures us that the order of ω modulo l is divisible by p. This immediately shows that $n \equiv \pm 1 \pmod p$ as required. □

Proof of Proposition 7.3. We used a `PARI/GP` program to check that for each prime in the range $7 \leq p < 2 \times 10^8$, there is some k satisfying conditions (a), (b) and (c) of Lemma 7.4. This took approximately 41 hours on a 1.7 GHz Pentium 4. This proves the proposition. □

8. Level-lowering for Lucas — The odd-index case

In this section we associate a Frey curve to solutions of (18) and apply level-lowering. Our objective is to give the Lucas analogue of Propositions 7.2 and 7.3.

Suppose then that (n, y, p) is a solution to (18), and associate to this solution the Frey curve

$$E_n : \qquad Y^2 = X^3 - 5F_nX^2 + 5X. \tag{24}$$

Let E be the elliptic curve $200B1$ in Cremona's tables [17]. This has the model

$$E : \quad Y^2 = X^3 + X^2 - 3X - 2. \tag{25}$$

PROPOSITION 8.1. *Suppose that (n, y, p) is a solution to* (18). *With notation as above, the Galois representations $\rho_p(E_n)$, $\rho_p(E)$ are isomorphic. Moreover, for any prime $l \neq 2, 5$*

(i) $a_l(E_n) \equiv a_l(E) \pmod{p}$ *if* $l \nmid y$,

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

PROPOSITION 8.2. *If (n, y, p) is any solution to equation* (18) *then* $n \equiv \pm 1 \pmod{p}$.

The proof of Proposition 8.1 is by no means as simple as the proof of the corresponding proposition for Fibonacci. However, given Proposition 8.1, the proof of Proposition 8.2 is a fairly trivial modification of the proof of Proposition 7.3 and we omit it. The reader will notice that in Proposition 7.3 (the Fibonacci case) we suppose that $p < 2 \times 10^8$, but in the Lucas case above there is no such assumption. This is because we know by a result of Pethő quoted in Section 2 that $p < 13222$, which also means that our program for the proof of Proposition 8.2 takes only a few seconds. Later on we will prove a much better bound for p in the Lucas case, namely $p \leq 283$, but we do not need such a good bound for the proof of Proposition 8.2.

8.1. *Level-lowering.* Let $E^1, \ldots, E^5$ be the elliptic curves 200A1, 200B1, 200C1, 200D1, 200E1 in Cremona's tables [17]. Note that E^2 is just our elliptic curve E defined above. We follow the notation of previous sections with regard to Galois representations and traces of Frobenius.

LEMMA 8.3. *Suppose (n, y, p) is a solution to equation* (18). *With notation as above, the Galois representation $\rho_p(E_n)$ is isomorphic to one of the Galois representations $\rho_p(E^1), \ldots, \rho_p(E^5)$. Moreover, if $\rho_p(E_n)$ is isomorphic to $\rho_p(E^i)$ then, for any prime $l \neq 2, 5$,*

(i) $a_l(E_n) \equiv a_l(E^i) \pmod{p}$ *if* $l \nmid y$.

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

Proof. By the results of [5, §§2, 3], $\rho_p(E_n)$ arises from a cuspidal newform of weight 2, level 200, and trivial Nebentypus character. For this we need Lemma 3.2 and using `MAGMA` we find that the dimension of newforms of weight 2 and level 200 is 5 and there are (up to isogeny) exactly five elliptic curves of conductor 200, and these are the curves $E^1, \ldots, E^5$ above.

The rest of the lemma follows from [24, Prop. 3], and the fact that if $l \neq 2$, 5 and $l \mid y$ then l is a prime of multiplicative reduction for E_n and so $a_l(E_n) = \pm 1$. □

8.2. *Eliminating newforms.* Lemma 8.3 relates the Galois representation of E_n to too many Galois representations. We now eliminate all but one of them.

Suppose $l \neq 2, 5$ is a prime. Define $d_l(E_n, E^i) = a_l(E_n) - a_l(E^i)$. Let $M(l)$ be given by (13). Recall that (Lemma 3.3) the residue class of F_n modulo l, and hence the Frey curve E_n modulo l, depends only on the residue class of n modulo $M(l)$. We see that the following definitions make sense: let

$$\mathcal{T}_l(E^i) = \left\{ m \in \mathbb{Z}/M(l) : d_l(E_m, E^i) = 0 \right\},$$

$$g_l(E^i) = \operatorname{lcm} \left\{ d_l(E_m, E^i) : m \in \mathbb{Z}/M(l), \quad m \notin \mathcal{T}_l(E^i) \right\},$$

and

$$h_l(E^i) = \begin{cases} g_l(E^i), & \text{if } l \equiv \pm 2 \pmod 5, \\ \operatorname{lcm}(g_l(E^i), l + 1 - a_l(E^i), l + 1 + a_l(E^i)), & \text{if } l \equiv \pm 1 \pmod 5. \end{cases}$$

LEMMA 8.4. *Suppose that $l \neq 2$, 5 is a prime. If $\rho_p(E_n)$ is isomorphic to $\rho_p(E^{(i)})$ then either the reduction of n modulo $M(l)$ belongs to $\mathcal{T}_l(E^i)$ or else p divides $h_l(E^i)$.*

Proof. Recall that by Lemma 3.2, $y^{2p} = 5F_n^2 - 4$. Thus if $l \equiv \pm 2 \pmod 5$ then l does not divide y. The lemma now follows from Lemma 8.3. □

Given two positive integers M_1, M_2, and two sets $T_1 \subset \mathbb{Z}/M_1$ and $T_2 \subset \mathbb{Z}/M_2$ we loosely define their 'intersection' $T_1 \cap T_2$ to be the set of all elements of $\mathbb{Z}/\operatorname{lcm}(M_1, M_2)$ whose reduction modulo M_1 and M_2 is respectively in T_1 and T_2.

We are now ready to prove Proposition 8.1.

Proof of Proposition 8.1. Suppose that (n, y, p) is a solution to (18). Thus $p \geq 7$ and $n \equiv \pm 1 \pmod 6$. We recall that the elliptic curves E and E^2 are one and the same. Thus the proposition follows from Lemma 8.3 if we can demonstrate that $\rho_p(E_n)$ cannot be isomorphic to the corresponding representation for E^1, E^3, E^4 and E^5. Fix i one of 1, 3, 4, 5. By the above lemma, to show that the Galois representations of E_n and E^i are not isomorphic it is enough to produce a set of primes $S = \{l_1, \ldots, l_r\}$ all neither 2 nor 5 satisfying

(1) For every $l \in S$ the integer $h_l(E^i)$ is not divisible by any prime number greater than 5,

(2) $\left(\cap_{l\in S}\mathcal{T}_l(E^i)\right) \cap \mathcal{T}_0 = \emptyset$,

where $\mathcal{T}_0 = \left\{\overline{1}, \overline{5}\right\} \subseteq \mathbb{Z}/6Z$. With the help of a short `PARI/GP` program we find that we can take $S = \{3\}$ to eliminate E^1, E^3, E^5 and $S = \{3, 7, 11, 13, 17, 19, 23\}$ to eliminate E^4.

We note in passing that the j-invariant of the curve E^3 is $55296/5$, and so the argument used in the proof of Lemma 5.1 also shows that the Galois representation $\rho_p(E^3)$ is not isomorphic to $\rho(E_n)$. This argument does not apply to the Galois representations of E^1, E^4, E^5 as these have integral j-invariants. □

9. Bounds for n in terms of p

Our objective in this section is to obtain bounds for n in terms of p for solutions to (17) and (18). It follows from Baker's theory of linear forms in logarithms (see for example the book of Shorey and Tijdeman [46]) that the sizes of n and y are bounded in terms of p. Unfortunately, these bounds are huge, and there is no hope to complete the resolution of our equations by proceeding in that way. We however recall, by Lemma 3.1 (and 3.2), that it is sufficient to obtain upper bounds for the size of integer solutions to the equation $x^2 + 4 = 5y^{2p}$ (and one like it in the Lucas case). As is explained below, this equation easily reduces to a Thue equation, and we may apply the results of Bugeaud and Győry [10] to get an upper bound for x and y. However, it is of much interest to rework the proof of Bugeaud and Győry in our particular context. On the one hand, our particular equation has some nice properties not taken into account in the general result of [10], and, on the other hand, there has been an important improvement, due to Matveev, in the theory of linear forms in logarithms since [10] has appeared. Altogether we actually compute a much better upper bound than the one obtained by applying the main result of [10] directly.

Before giving a precise statement of the main results of this section, we need an upper bound for the regulators of number fields. Several explicit upper bounds for regulators of a number field are available in the literature; see for example [28] and [47]. We have however found it best to use a result of Landau.

LEMMA 9.1. *Let $\mathbb{K}$ be a number field with degree $d = r_1 + 2r_2$ where r_1 and r_2 are numbers of real and complex embeddings. Denote the discriminant by $D_{\mathbb{K}}$ and the regulator by $R_{\mathbb{K}}$, and the number of roots of unity in $\mathbb{K}$ by w. Suppose, moreover, that L is a real number such that $D_{\mathbb{K}} \leq L$. Let*

$$a = 2^{-r_2}\,\pi^{-d/2}\,\sqrt{L}.$$

Define the function $f_{\mathbb{K}}(L,s)$ *by*

$$f_{\mathbb{K}}(L,s) = 2^{-r_1}\, w\, a^s \left(\Gamma(s/2)\right)^{r_1} \left(\Gamma(s)\right)^{r_2} s^{d+1}\, (s-1)^{1-d},$$

and let $C_{\mathbb{K}}(L) = \min\{f_K(L, 2 - t/1000) \ : t = 0, 1, \ldots, 999\}$. *Then* $R_{\mathbb{K}} < C_{\mathbb{K}}(L)$.

Proof. Landau [25] proved the inequality $R_{\mathbb{K}} < f_{\mathbb{K}}(D_{\mathbb{K}}, s)$ for all $s > 1$. It is thus clear that $R_{\mathbb{K}} < C_{\mathbb{K}}(L)$.

Perhaps a comment is in order. For a complicated number field of high degree it is difficult to calculate the discriminant $D_{\mathbb{K}}$ exactly, though it is easy to give an upper bound L for its size. It is also difficult to minimise the function $f_{\mathbb{K}}(L,s)$ analytically, but we have found that the above gives an accurate enough result, which is easy to calculate on a computer. □

We are now ready to state our upper bound for n in terms of p for the Fibonacci and Lucas cases.

PROPOSITION 9.2. *Suppose* $p \geq 7$ *is prime. Let* α *be any root of the polynomial*

$$P(X) := \sum_{k=0}^{p} (-4)^{[(p-k)/2]} \binom{p}{k} X^k, \tag{26}$$

and let $\mathbb{K} = \mathbb{Q}(\alpha)$. *Let* $C_{\mathbb{K}}(\cdot)$ *be as in Lemma* 9.1 *and*

$$\Theta = 3.9 \cdot 30^{p+3}\, p^{13/2}\, (p-1)^{p+1} \left((p-1)!\right)^2 (3p+2) \left(1+\log(p(p-1))\right) C_{\mathbb{K}}(10^{p-1}p^p).$$

If (n, y, p) *satisfies the equation and conditions* (17) *then* $n < 2.5p\Theta \log \Theta$.

PROPOSITION 9.3. *Suppose* $p \geq 7$ *is prime. Denote by* $\sqrt[p]{\omega}$ *the real* p*-th root of* ω *(where* ω *is given by* (8)*) and set* $\mathbb{K} = \mathbb{Q}(\sqrt{5}, \sqrt[p]{\omega})$, *and let* $C_{\mathbb{K}}(\cdot)$ *be as in Lemma* 9.1. *Let*

$$\Theta = 67 \cdot 30^{p+5}(p-1)^{p+2} p^3\, (p+2)^{5.5}\, (p!)^2 \left(1 + \log(2p(p-1))\right) C_{\mathbb{K}}(5^p p^{2p}).$$

If (n, y, p) *satisfies the equation and conditions* (18) *then* $n < 2.5\, p\, \Theta \log \Theta$.

9.1. *Preliminaries.* We first need a lower bound for linear forms in logarithms due to Matveev. Let $\mathbb{L}$ be a number field of degree D, let $\alpha_1, \ldots, \alpha_n$ be nonzero elements of $\mathbb{L}$ and $b_1, \ldots, b_n$ be rational integers. Set

$$B = \max\{|b_1|, \ldots, |b_n|\},$$

and

$$\Lambda = \alpha_1^{b_1} \ldots \alpha_n^{b_n} - 1.$$

Let h denote the absolute logarithmic height and let $A_1, \ldots, A_n$ be real numbers with

$$A_j \geq \mathrm{h}'(\alpha_j) := \max\{D\, \mathrm{h}(\alpha_j), |\log \alpha_j|, 0.16\}, \quad 1 \leq j \leq n.$$

We call h' the modified height (with respect to the field $\mathbb{L}$). With this notation, the main result of Matveev [35] implies the following estimate.

THEOREM 9.4. *Assume that Λ is nonzero. Then*

$$\log|\Lambda| > -3\cdot 30^{n+4}\,(n+1)^{5.5}\,D^2\,(1+\log D)\,(1+\log nB)\,A_1\ldots A_n.$$

Furthermore, if $\mathbb{L}$ is real,

$$\log|\Lambda| > -1.4\cdot 30^{n+3}\,n^{4.5}\,D^2\,(1+\log D)\,(1+\log B)\,A_1\ldots A_n.$$

Proof. Denote by log the principal determination of the logarithm. If $|\Lambda| < 1/3$, then there exists an integer b_0, with $|b_0| \le n\,B$, such that

$$\Omega := |b_0\log(-1) + b_1\log\alpha_1 + \ldots + b_n\log\alpha_n|$$

satisfies $|\Lambda| \ge \Omega/2$. Noticing that $\mathrm{h}'(-1) = \pi$, and that $b_0 = 0$ if $\mathbb{L}$ is real, we deduce our lower bounds from Corollary 2.3 of Matveev [35]. □

We also need some precise results from algebraic number theory. In the rest of this section, let $\mathbb{K}$ denote a number field of degree $d = r_1 + 2r_2$ and unit rank $r = r_1 + r_2 - 1$ with $r > 0$. Let $R_{\mathbb{K}}$ and $D_{\mathbb{K}}$ be its regulator and discriminant, respectively. Let w denote the number of roots of unity in $\mathbb{K}$. Observe that $w = 2$ if $r_1 > 0$.

LEMMA 9.5. *For every algebraic integer η which generates $\mathbb{K}$,*

$$d\,\mathrm{h}(\eta) \ge \frac{\log|D_{\mathbb{K}}| - d\,\log d}{2(d-1)}.$$

Proof. As in Mignotte [37], it follows from the Hadamard inequality that

$$|D_{\mathbb{K}}| \le \mathrm{Discr}(1,\eta,\ldots,\eta^{d-1})^2 \le d^d\,\mathrm{M}(\eta)^{2(d-1)},$$

where $\mathrm{M}(\eta)$ is the Mahler measure of η. Since $d\log\mathrm{M}(\eta) = \mathrm{h}(\eta)$, the lemma is proved. □

In the course of our proof, we use fundamental systems of units in $\mathbb{K}$ with specific properties.

LEMMA 9.6. *There exists in $\mathbb{K}$ a fundamental system $\{\varepsilon_1,\ldots,\varepsilon_r\}$ of units such that*

$$\prod_{i=1}^{r}\mathrm{h}(\varepsilon_i) \le 2^{1-r}\,(r!)^2\,d^{-r}\,R_{\mathbb{K}},$$

and the absolute values of the entries of the inverse matrix of $(\log|\varepsilon_i|_{v_j})_{i,j=1,\ldots,r}$ do not exceed $(r!)^2\,2^{-r}\,(\log(3d))^3$.

Proof. This is Lemma 1 of [9] combined with a result of Voutier [50] (see [10]) giving a lower bound for the height of any nonzero algebraic number which is not a root of unity. □

Furthermore, we need sharp bounds for discriminants of number fields in a relative extension.

LEMMA 9.7. *Let $\mathbb{K}_1$ and $\mathbb{K}_2$ be number fields with $\mathbb{K}_1 \subseteq \mathbb{K}_2$ and denote the discriminant of the extension $\mathbb{K}_2/\mathbb{K}_1$ by $D_{\mathbb{K}_2/\mathbb{K}_1}$. Then*

$$|D_{\mathbb{K}_2}| = |D_{\mathbb{K}_1}|^{[\mathbb{K}_2:\mathbb{K}_1]} \, |\mathrm{N}_{\mathbb{K}_1/\mathbb{Q}}(D_{\mathbb{K}_2/\mathbb{K}_1})|.$$

Proof. This is Proposition 4.9 of [38]. □

9.2. *Proof of Proposition* 9.2. We now turn our attention to the proof of Proposition 9.2 and so to equation (17). Lemma 3.1 reduces the problem to solving the superelliptic equation $x^2 + 4 = 5y^{2p}$. Factoring the left-hand side over $\mathbb{Z}[i]$, we deduce the existence of integers a and b with $a^2 + b^2 = y^2$ and

$$\pm 4i = (2+i)(a+ib)^p - (2-i)(a-ib)^p. \tag{27}$$

Dividing by $2i$, we get

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

We infer that a is even. Consequently, $(b, a/2)$ is an integer solution of the Thue equation

$$\sum_{k=0}^{p} (-4)^{[(p-k)/2]} \binom{p}{k} X^k \, Y^{p-k} = \pm 1. \tag{28}$$

To bound the size of the solutions of (28) we follow the general scheme of [10], which was also used in [12]. Let $P(X)$ and α and $\mathbb{K}$ be as in Proposition 9.2; we note that $P(X)$ is the polynomial naturally associated to the Thue equation (28). We first need information on the number field $\mathbb{K}$ and its Galois closure. We would like to thank Mr. Julien Haristoy for his help in proving the following lemma.

LEMMA 9.8. *The field $\mathbb{K} = \mathbb{Q}(\alpha)$ is totally real and its Galois closure $\mathbb{L}$ has degree $p(p-1)$ over $\mathbb{Q}$. Furthermore, the discriminant of $\mathbb{K}$ divides $10^{p-1}p^p$.*

Proof. Observe that any root of the polynomial

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

satisfies $|X+i| = |X-i|$, and so must be real. Hence, $\mathbb{K}$ is a totally real field. Furthermore, $\mathbb{L}(i)/\mathbb{Q}(i)$ is a Kummer extension obtained by adjoining the p-th

roots of unity and the p-th roots of $(2+i)/(2-i)$. Hence, this extension has degree $p(p-1)$, and this is the same for $\mathbb{L}/\mathbb{Q}$.

Observe now that $\mathbb{K}(i)$ is generated over $\mathbb{Q}(i)$ by any root of either of the following two monic polynomials with coefficients in $\mathbb{Z}[i]$, namely $Y^p - (2+i)(2-i)^{p-1}$ and $Y^p - (2-i)(2+i)^{p-1}$. Since the discriminant D_1 (viewed as an algebraic integer in $\mathbb{Z}[i]$ and not as an ideal) of the extension $\mathbb{K}(i)/\mathbb{Q}(i)$ divides the discriminant of each of these polynomials, D_1 divides $p^p 5^{p-1}(2-i)^{(p-1)(p-2)}$ and $p^p 5^{p-1}(2+i)^{(p-1)(p-2)}$. However, $2+i$ and $2-i$ are relatively prime; thus D_1 divides $5^{p-1}p^p$. Furthermore, estimating the discriminant of $\mathbb{K}(i)/\mathbb{Q}$ in two different ways thanks to Lemma 9.7 gives

$$|D_{\mathbb{K}(i)}| = 4^p D_1^2 = |D_{\mathbb{K}}|^2 \cdot |\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(D_{\mathbb{K}(i)/\mathbb{K}})|. \tag{29}$$

Consequently, $|D_{\mathbb{K}}|$ divides $5^{p-1}(2p)^p$. We now refine this estimate by showing that 4 divides $|\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(D_{\mathbb{K}(i)/\mathbb{K}})|$.

Suppose that the decomposition of the ideal $2 \cdot \mathcal{O}_{\mathbb{K}}$ in $\mathbb{K}/\mathbb{Q}$ is given by

$$2 \cdot \mathcal{O}_{\mathbb{K}} = \mathcal{P}_1^{e_1} \dots \mathcal{P}_s^{e_s}.$$

At least one of the e_i is odd, since otherwise 2 would divide $\sum_{i=1}^{s} e_i f_i = p$. Thus, there is (at least) one prime $\mathcal{P}$ in $\mathcal{O}_{\mathbb{K}}$ lying above 2 whose ramification index e is odd: this prime must ramify in $\mathbb{K}(i)/\mathbb{K}$, since $2i = (1+i)^2$ in $\mathbb{K}(i)$. Thus $\mathcal{P}$ divides $D_{\mathbb{K}(i)/\mathbb{K}}$ and so $|\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(D_{\mathbb{K}(i)/\mathbb{K}})|$ is divisible by 2. However, by (29), we know that $|\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(D_{\mathbb{K}(i)/\mathbb{K}})|$ is a square and so must be divisible by 4. □

Remark. Based on computations for small p, it seems very likely that $10^{p-1}p^p$ is the exact value of $|D_{\mathbb{K}}|$ for most p.

Since we introduce many changes in the proof of [10], we give a complete proof, rather than only quoting [10].

Let $\alpha_1, \dots, \alpha_p$ be the roots of $P(X)$ and let (X, Y) be a solution of (28). Without any loss of generality, we assume that $\alpha = \alpha_1$ and $|X - \alpha_1 Y| = \min_{1 \le j \le p} |X - \alpha_j Y|$. We will make repeated use of the fact that $|\alpha_1|, \dots |\alpha_p|$ are neither greater than 4^p, nor smaller than 4^{-p} (since $4^p - 1$ is an upper bound for the absolute values of the coefficients of $P(X)$). Assuming that Y is large enough, namely that

$$\log |Y| \ge (30p)^p, \tag{30}$$

we get $|Y| \ge 2 \min_{2 \le j \le p} \{|\alpha_1 - \alpha_j|^{-1}\}$ and

$$|X - \alpha_1 Y| \le 2^{p-1} \prod_{2 \le j \le p} |\alpha_1 - \alpha_j| \, |Y|^{-p+1} \le 2^{2p^2} |Y|^{-p+1}, \tag{31}$$

since $|X - \alpha_j Y| \ge |\alpha_1 - \alpha_j| \cdot |Y|/2$ if $|X - \alpha_1 Y| \le |\alpha_1 - \alpha_j| \cdot |Y|/2$, for any $j = 2, \dots, p$.

From the 'Siegel identity',

$$(X-\alpha_1 Y)(\alpha_2-\alpha_3)+(X-\alpha_2 Y)(\alpha_3-\alpha_1)+(X-\alpha_3 Y)(\alpha_1-\alpha_2)=0,$$

we have

$$\Lambda := \frac{\alpha_2-\alpha_3}{\alpha_3-\alpha_1}\cdot\frac{X-\alpha_1 Y}{X-\alpha_2 Y} = \frac{X-\alpha_3 Y}{X-\alpha_2 Y}\cdot\frac{\alpha_2-\alpha_1}{\alpha_3-\alpha_1}-1.$$

Observe that the unit rank of $\mathbb{K}$ is $p-1$, since $\mathbb{K}$ is totally real. Let $\varepsilon_{1,1},\dots$ $\dots,\varepsilon_{1,p-1}$ be a fundamental system of units in $\mathbb{K}:=\mathbb{Q}(\alpha_1)$ given by Lemma 9.6, hence, satisfying

$$\prod_{1\le i\le p-1} \mathrm{h}(\varepsilon_{1,i}) \le \frac{\big((p-1)!\big)^2}{2^{p-2}p^{p-1}}\,R_{\mathbb{K}}, \tag{32}$$

where $R_{\mathbb{K}}$ denotes the regulator of the field $\mathbb{K}$. For $j=2,3$, denote by $\varepsilon_{2,1},\dots,\varepsilon_{2,p-1}$ and $\varepsilon_{3,1},\dots,\varepsilon_{3,p-1}$ the conjugates of $\varepsilon_{1,1},\dots,\varepsilon_{1,p-1}$ in $\mathbb{Q}(\alpha_2)$ and $\mathbb{Q}(\alpha_3)$, respectively. They all belong to the Galois closure $\mathbb{L}$ of $\mathbb{K}$.

The polynomial $P(X)$ is monic and the left-hand side of (28) is a unit. Thus $X-\alpha_1 Y$ is a unit. This simple observation appears to be crucial, since, roughly speaking, it allows us to gain a factor of size around $p^p R_{\mathbb{K}}$ (compare with the proofs in [10] and in [12]).

Since the only roots of unity in $\mathbb{K}$ are ±1, there exist integers $b_1,\dots,b_{p-1}$ such that $X-\alpha_1 Y=\pm\varepsilon_{1,1}^{b_1}\dots\varepsilon_{1,p-1}^{b_{p-1}}$; thus

$$\Lambda=\pm\left(\frac{\varepsilon_{3,1}}{\varepsilon_{2,1}}\right)^{b_1}\dots\left(\frac{\varepsilon_{3,p-1}}{\varepsilon_{2,p-1}}\right)^{b_{p-1}}\frac{\alpha_2-\alpha_1}{\alpha_3-\alpha_1}-1.$$

As in [10, 6.12], we infer from Lemma 9.6 that

$$\begin{aligned} B:=\max\{|b_1|,\dots,|b_{p-1}|\} &\le 2^{2-p}\,p\,(p!)^2\,(\log(3p))^3\,\mathrm{h}(X-\alpha_1 Y)\\ &\le p^{2(p+1)}\,\log|Y|, \end{aligned} \tag{33}$$

by (31).

Further, we notice that

$$\mathrm{h}\left(\frac{\alpha_2-\alpha_1}{\alpha_3-\alpha_1}\right)=\mathrm{h}\left(\frac{\alpha_2/2-\alpha_1/2}{\alpha_3/2-\alpha_1/2}\right)\le 4\,\mathrm{h}(\alpha_1/2)+\log 4\le\frac{6p+4}{p}\log 2,$$

since we have (here and below, $M(\cdot)$ denotes the Mahler measure and $\mathrm{H}(\cdot)$ stands for the naïve height)

$$\mathrm{h}(\alpha_1/2)\le\frac{\log M(Q)}{p}\le\frac{\log\big(\sqrt{p+1}\,\mathrm{H}(Q)\big)}{p}\le\frac{\log\big(2\sqrt{p+1}\binom{p}{[p/2]}\big)}{p}\le\frac{p+1}{p}\,\log 2.$$

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

$$\mathrm{h}'\left(\frac{\alpha_2-\alpha_1}{\alpha_3-\alpha_1}\right)\le 2(3p+2)(p-1)\log 2.$$

We may assume from Lemma 9.8 that the absolute value of the discriminant of $\mathbb{K}$ is $10^{p-1}p^p$, since the upper bound for n we aim to prove is an increasing function of $|D_{\mathbb{K}}|$. For $i = 1, \ldots, p-1$, we have $\mathrm{h}(\varepsilon_{1,i}) = \mathrm{h}(\varepsilon_{2,i}) = \mathrm{h}(\varepsilon_{3,i})$ and, by Lemma 9.5, the height of the real algebraic integer $\varepsilon_{1,i}$ satisfies $\mathrm{h}(\varepsilon_{1,i}) \geq (\log 10)/2$. Thus, we get

$$\mathrm{h}'\left(\frac{\varepsilon_{2,i}}{\varepsilon_{3,i}}\right) \leq 2p(p-1)\mathrm{h}(\varepsilon_{1,i}).$$

Consequently, using Theorem 9.4 in the real case with $n = p$ and $D = p(p-1)$, we get

$$\begin{aligned}(34)\quad \log|\Lambda| > &-1.4 \cdot 30^{p+3} p^{7/2} \big(p(p-1)\big)^{p+2} (3p+2)\big(1+\log(p(p-1))\big) \\ &\times (1+\log B)\,(2\log 2)\,2^{p-1} \prod_{1\leq i\leq p-1} \mathrm{h}(\varepsilon_{1,i}).\end{aligned}$$

Then, (32) gives us that

$$\begin{aligned}(35)\qquad \log|\Lambda| > &-3.9 \cdot 30^{p+3}\, p^{13/2}\,(p-1)^{p+2}\,(3p+2)\,\big((p-1)!\big)^2 \\ &\times \big(1+\log(p(p-1))\big)\,(1+\log B)\,R_{\mathbb{K}}.\end{aligned}$$

Furthermore, it follows from (31) that

$$(36)\qquad \log|\Lambda| < 5p^2 - (p-1)\log|Y|.$$

By (33), we have the upper bound

$$(37)\qquad (1+\log B) < 3p^2 + \log\log|Y|.$$

Finally, we observe that if F_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 (28) and $F_n^{2/p} = 4X^2 + Y^2$. Since $|X| \leq 1 + 4^p|Y|$ and $F_n \geq 0.4 \cdot 1.6^n$ (for $n \geq 7$), we derive from (30) that $n < 2.2\,p\log|Y|$. It then follows from (35), (36), and (37), together with Lemmas 9.1 and (9.8) that

$$n < 2.5\,p\,\Theta\log\Theta,$$

with

$$\Theta = 3.9{\cdot}30^{p+3}\,p^{13/2}\,(p{-}1)^{p+1}\,(3p{+}2)\,\big((p{-}1)!\big)^2\,\big(1{+}\log(p(p{-}1))\big)\,C_{\mathbb{K}}(10^{p-1}p^p).$$

This proves Proposition 9.2. □

9.3. *Proof of Proposition* 9.3. Suppose that (n, y, p) is a solution to the equation (18). In particular, we know

$$y^p = L_n = \omega^n + \tau^n,$$

where we recall that $\omega = (1+\sqrt{5})/2$ and τ is the conjugate of ω. We also know by Proposition 8.2 that n is congruent to ± 1 modulo p. This means that there exists an integer ν such that

$$y^p - \omega^{\pm 1}\,(\omega^\nu)^p = -\tau^n.$$

Thus, we are left with an equation of Thue type, namely

$$X^p - \omega^{\pm 1} Y^p = \text{unit in } \mathbb{Q}(\sqrt{5}). \tag{38}$$

We only deal with the + case, since the − case is very similar.

As in the statement of Proposition 9.3, denote by $\sqrt[p]{\omega}$ the real p-th root of ω and set $\mathbb{K} = \mathbb{Q}(\sqrt{5}, \sqrt[p]{\omega})$. Let ζ be a primitive p-th root of unity.

LEMMA 9.9. *The field $\mathbb{K}$ has degree $2p$ and $r_1 = 2$, $r_2 = p-1$ and $r = p$. The absolute value of the discriminant of $\mathbb{K}$ is at most equal to $5^p p^{2p}$. Its nontrivial subfields are $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt[p]{\omega} - (\sqrt[p]{\omega})^{-1})$, whose discriminant is, in absolute value, at most equal to $5^{(p-1)/2} p^p$. Furthermore, the Galois closure $\mathbb{L}$ of $\mathbb{K}$ is the field $\mathbb{K}(\zeta)$, of degree $2p(p-1)$.*

Proof. We observe that the minimal defining polynomial of $\sqrt[p]{\omega}$ over $\mathbb{Z}$ is $R(X) := X^{2p} - X^p - 1$. Thus

$$|D_{\mathbb{K}}| \le |\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(R'(\sqrt[p]{\omega}))| = |\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(p\sqrt{5}(\sqrt[p]{\omega})^{p-1})| = 5^p\, p^{2p}.$$

The fact that $\mathbb{K}$ has only two nontrivial subfields, one of degree two, and another of degree p, is clear. Furthermore, since $\mathbb{K}$ is obtained from the field $\mathbb{Q}(\sqrt[p]{\omega} - (\sqrt[p]{\omega})^{-1})$ by adjoining $\sqrt{5}$, we get from Lemma 9.7 that the absolute value of the discriminant of the field $\mathbb{Q}(\sqrt[p]{\omega} - (\sqrt[p]{\omega})^{-1})$ is not greater than $5^{(p-1)/2} p^p$. Since the roots of the polynomial $R(X)$ are the algebraic numbers $\sqrt[p]{\omega}$, $\zeta\sqrt[p]{\omega}, \ldots, \zeta^{p-1}\sqrt[p]{\omega}$, $\sqrt[p]{\tau}$, $\zeta\sqrt[p]{\tau}, \ldots, \zeta^{p-1}\sqrt[p]{\tau}$, we see that the Galois closure of $\mathbb{K}$ is the field $\mathbb{K}(\zeta)$. □

Let $\varepsilon_{1,1}, \ldots, \varepsilon_{1,p}$ be a fundamental system of units in $\mathbb{K}$ given by Lemma 9.6. There exist integers $b_1, \ldots, b_p$ such that

$$X - \sqrt[p]{\omega} Y = \pm \varepsilon_{1,1}^{b_1} \ldots \varepsilon_{1,p}^{b_p}.$$

Keep in mind that we are only interested in solutions (X, Y) of (38) with X an integer and Y an algebraic integer in the field $\mathbb{Q}(\sqrt{5})$. Thus, X/Y is real, $|X - \sqrt[p]{\omega} Y|$ is small, and $|X - \zeta^j \sqrt[p]{\omega} Y|$ is quite large for $j = 1, \ldots, p-1$ (consider the imaginary part). More precisely, for $Y > 2$,

$$|X - \sqrt[p]{\omega} Y| \le p^p\, Y^{-p+1}. \tag{39}$$

Furthermore, when $B = \max\{|b_1|, \ldots, |b_p|\}$, Lemma 9.6 yields

$$\begin{aligned} B &\le 2^{1-p}\, p (p!)^2 (\log 6p)^3\, \mathrm{h}(X - \sqrt[p]{\omega} Y) \\ &\le p^{2(p+1)}\, \log Y, \end{aligned} \tag{40}$$

by our assumptions on X and Y.

Recall that ζ is a primitive p-th root of unity. We introduce the quantity

$$\Lambda := \frac{\zeta - \zeta^2}{\zeta^2 - 1} \cdot \frac{X - \sqrt[p]{\omega} Y}{X - \zeta \sqrt[p]{\omega} Y} = \frac{X - \zeta^2 \sqrt[p]{\omega} Y}{X - \zeta \sqrt[p]{\omega} Y} \cdot \frac{\zeta - 1}{\zeta^2 - 1} - 1, \tag{41}$$

hence, the linear form in logarithms

$$\Lambda = \left(\frac{\varepsilon_{3,1}}{\varepsilon_{2,1}}\right)^{b_1} \cdots \left(\frac{\varepsilon_{3,p}}{\varepsilon_{2,p}}\right)^{b_p} \frac{\zeta - 1}{\zeta^2 - 1} - 1.$$

Let h' denote the modified height related to the field $\mathbb{L}$. We have

$$\mathrm{h}'\left(\frac{\zeta - 1}{\zeta^2 - 1}\right) \le 2p(p-1)\log 4,$$

and $\mathrm{h}'(\varepsilon_{1,i}) = \mathrm{h}(\varepsilon_{1,i})$. To check this, we observe that any algebraic unit in $\mathbb{K}$ generates one of the subfields of $\mathbb{K}$, and we apply Lemma 9.9 (we may assume that the absolute value of the discriminant of $\mathbb{K}$ is $5^p p^{2p}$, since the upper bound for n (we aim to prove) is an increasing function of $|D_{\mathbb{K}}|$). Using Theorem 9.4 in the complex case with $n = p + 1$ and $D = 2p(p-1)$, we get

$$\begin{aligned}(42)\qquad \log|\Lambda| > {} & -3 \cdot 30^{p+5}(p+2)^{5.5}\big(2p(p-1)\big)^{p+3}\big(1 + \log(2p(p-1))\big) \\ & \times (1 + \log(p+1)B)\,(\log 4)\,2^p \prod_{1 \le i \le p} \mathrm{h}(\varepsilon_{1,i}).\end{aligned}$$

By (42) and Lemma 9.6, we get

$$\begin{aligned}(43)\qquad \log|\Lambda| > {} & -3 \cdot 30^{p+5}(p+2)^{5.5}\big(2p(p-1)\big)^{p+3}\big(1 + \log(2p(p-1))\big) \\ & \times \big(1 + \log((p+1)B)\big)\,(\log 4)\,2^{-p+1}\,p^{-p}\,(p!)^2\,R_{\mathbb{K}}.\end{aligned}$$

Furthermore, it follows from (39) and (41) that

$$(44)\qquad \log|\Lambda| < 5p^2 - (p-1)\log|Y|.$$

Observe now that if $L_n = y^p$ for some n, then equation (38) has a solution (X, Y) with $Y = \omega^{(n\pm1)/p}$, and we get that $-1 < L_n - \omega^{\pm 1} y^p < 0$; thus $n < 2.2\,p \log Y$. It then follows from (40), (42)–(44), together with Lemma 9.1 that

$$n < 2.5\,p\,\Theta \log \Theta,$$

with

$$\Theta = 67 \cdot 30^{p+5}(p-1)^{p+2}p^3\,(p+2)^{5.5}\,(p!)^2\,\big(1 + \log(2p(p-1))\big)\,C_{\mathbb{K}}(5^p p^{2p}).$$

This completes the proof of Proposition 9.3. □

10. The sieve

In this section we use Propositions 7.2 and 9.2 (for the Fibonacci case) and Propositions 8.1 and 9.3 (for the Lucas case) together with a substantial computation to prove the following.

PROPOSITION 10.1. *If (n, y, p) satisfies the equation and conditions* (17) *then*

$$p > 733, \qquad n \ge 1.033 \times 10^{8733}, \qquad \log y > 10^{8000}.$$

PROPOSITION 10.2. *If (n, y, p) satisfies the equation and conditions* (18) *then*

$$p > 283, \qquad n \geq 4.938 \times 10^{3383}, \qquad \log y > 10^{3000}.$$

We will focus on the Fibonacci case; the Lucas case is very similar. Throughout this section we will follow the notation of Section 7. In particular, H_n, E_n and E are given respectively by (20), (22), and (23).

LEMMA 10.3. *Suppose $l \equiv \pm 1 \pmod 5$ is prime and let*

$$K(l) = \operatorname{lcm}(l - 1, 6).$$

The trace of Frobenius $a_l(E_n)$ depends only on the residue class of n modulo $K(l)$.

Proof. By Lemma 3.3, the residue class of L_n modulo l depends only on the residue class of n modulo $l - 1$. From the definition of the integer H_n in (20) we see that H_n modulo l depends only on the residue class of n modulo $K(l)$. The lemma follows at once from the fact that the Frey curve E_n depends only on H_n. □

Suppose $l \equiv \pm 1 \pmod 5$; we see by Lemma 10.3 that for $n \in \mathbb{Z}/K(l)$ it makes sense to talk of $a_l(E_n)$. Suppose $q \geq 5$ is a fixed prime. Define $\mathcal{N}(l, q)$ to be the subset of all $n \in (\mathbb{Z}/K(l))^*$ such that

- either $H_n^2 + 4 \not\equiv 0 \pmod l$, and the integer $a_l(E_n) - a_l(E)$ is divisible by some prime $p > q$,
- or $H_n^2 + 4 \equiv 0 \pmod l$ and one of the two integers $l + 1 \pm a_l(E)$ is divisible by some prime $p > q$.

LEMMA 10.4. *Suppose that $q \geq 5$ is prime. Suppose l satisfies*

(45) $l \equiv \pm 1 \pmod 5$ *is prime and every prime factor of $l - 1$ is < 25000.*

If (n, p, y) satisfies the equation (17) *and $p > q$ then the reduction of n modulo $K(l)$ belongs to $\mathcal{N}(l, q)$.*

Proof. First observe, since n satisfies (17), that n is prime and $n \geq 25000$. However, every prime divisor of $l - 1$ is < 25000 and the same must be true of $K(l) = \operatorname{lcm}(l - 1, 6)$. Thus the reduction of n modulo $K(l)$ certainly belongs to $(\mathbb{Z}/K(l))^*$.

Next we recall (Lemma 7.1) that $H_n^2 + 4 = 5y^{2p}$ and so $l \mid y$ if and only if $H_n^2 + 4 \equiv 0 \pmod l$. The lemma now immediately follows from Proposition 7.2. □

Given two positive integers M_1, M_2, and two sets $T_1 \subset \mathbb{Z}/M_1$ and $T_2 \subset \mathbb{Z}/M_2$ recall that we have already defined their 'intersection' $T_1 \cap T_2$ to be the set of all elements of $\mathbb{Z}/\mathrm{lcm}(M_1, M_2)$ whose reduction modulo M_1 and M_2 is respectively in T_1 and T_2.

The following proposition will be our main tool in proving Proposition 10.1.

PROPOSITION 10.5. *Suppose $S = \{(l_1, q_1), \dots, (l_t, q_t)\}$ is a finite set of pairs of primes (l, q) where each l satisfies the condition* (45) *and each q is ≥ 5. Let $K(S) = \mathrm{lcm}(6, l_1 - 1, \dots, l_t - 1)$, and*

$$\mathcal{N}(S) = \cap_{(l,q)\in S} \mathcal{N}(l, q) \subset (\mathbb{Z}/K(S))^*.$$

Write

$$\mathcal{N}(S) = \left\{\overline{1}, \overline{a}, \overline{b}, \dots\right\} \quad \text{where} \quad 1 < a < b < \cdots < K(S).$$

If (n, y, p) is a solution to (17) *with $p > q_1, \dots, q_t$ then $n \geq a$.*

Proof. Suppose that (n, y, p) is a solution to the equation (17). It follows immediately from Lemma 10.4 and the definition of 'intersection' that the reduction of n modulo $K(S)$ belongs to $\mathcal{N}(S)$.

The reader can check that $\overline{1}$ is always in $\mathcal{N}(S)$. Moreover $n \neq 1$ since $n > 25000$. Hence $n \geq a$. □

The following lemma will provide a useful check for our later calculations.

LEMMA 10.6. *With the notation of the above proposition, suppose that $4 \mid K(S)$. Then the residue classes of 1, -1, $K(S)/2 + 1$, $K(S)/2 - 1$ modulo $K(S)$ all belong to the set $\mathcal{N}(S)$.*

Proof. We note that $H_1 = H_{-1} = 1$, and so $E_1 = E$. It follows from the definition of $\mathcal{N}(l, p)$ that the residue classes of 1 and -1 modulo $K(l)$ belong to $\mathcal{N}(l, q)$ for all pairs $(l, q) \in S$, and so residue classes of 1, -1 modulo $K(S)$ belong to $\mathcal{N}(S)$.

Let us prove the same for $n = K(S)/2 + 1$; we will leave the other case to the reader. Suppose that $(l, q) \in S$. We would like to prove that the residue class of n modulo $K(l)$ belongs to $\mathcal{N}(l, q)$. Write $v_2 : \mathbb{Z} \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ for the 2-adic valuation.

Clearly $(l - 1)$ divides $K(S)$. If $v_2(l - 1) < v_2(K(S))$ then $n \equiv 1 \pmod{K(l)}$ and we already know that $\overline{1} \in \mathcal{N}(l, q)$.

Thus suppose that $v_2(l - 1) = v_2(K(S))$. Since 4 divides $K(S)$ we see that $l \equiv 1 \pmod 4$. Further we can write

$$n = \frac{K(S)}{2} + 1 = k\frac{(l-1)}{2} + 1$$

for some odd integer k. Note that

$$\omega^n \equiv (\omega^{\frac{l-1}{2}})^k \cdot \omega \equiv \pm\omega \pmod{l},$$

and so

$$H_n \equiv \pm L_n \equiv \pm(\omega^n - \omega^{-n}) \equiv \pm(\omega - \omega^{-1}) \equiv \pm 1 \pmod{l}.$$

A glance at the definition of $\mathcal{N}(l,q)$ shows that we must prove that $a_l(E_n) - a_l(E)$ is divisible by some prime greater than q. Actually we will prove that $a_l(E_n) = a_l(E)$. By comparing the equations for E and E_n we see that, modulo l, the two curves E and E_n are isomorphic when $H(n) \equiv 1 \pmod{l}$. If $H(n) \equiv -1 \pmod{l}$ then, modulo l, the curve E_n is the -1–twist of E. But $\left(\frac{-1}{l}\right) = 1$, and so again E and E_n are isomorphic modulo l. This proves that $a_l(E_n) = a_l(E)$ and completes the proof. □

10.1. *Proof of Proposition* 10.1. Suppose that (n, y, p) is a solution to (17). Notice that Proposition 10.5 provides us with a way of obtaining lower bounds for the index n, and Proposition 9.2 provides us with a way of obtaining an upper bound for n (dependent on p). This gives us hope, given a particular prime p, that we may be able to obtain a contradiction using these two propositions and so prove that there are no solutions for this particular p.

We wrote a `PARI/GP` program to carry out the above idea and derive the contradiction for the primes in the range $7 \le p \le 733$.

We would like to give the reader the flavour of this computation by providing more for the proof that $p > 7$.

A priori, all we know about the exponent p is that $p > 5$, so we take $q = 5$. We let $S = \{(11, 5)\}$. Then

$$\mathcal{N}(S) = \mathcal{N}(11,5) = \left\{\overline{1}, \overline{11}, \overline{19}, \overline{29}\right\} \subset \mathbb{Z}/30,$$

where we used our program to calculate $\mathcal{N}(11,5)$ from the definition of $\mathcal{N}(l,q)$. Next we look for primes l satisfying $l \equiv \pm 1 \pmod{5}$ and

$$(l-1) | M, \quad \text{where } M = 6983776800 = 2^5 \times 3^3 \times 5^2 \times 7 \times 11 \times \cdots \times 19$$

and for each such prime l we find we append $(l, 5)$ to the set S, thus redefining $\mathcal{N}$ to be $\mathcal{N}(S) \cap \mathcal{N}(l,5)$. We continue until $\mathcal{N} \subset \mathbb{Z}/M$ and $\mathcal{N}(S)$ has four elements (we do not expect less than four elements by Lemma 10.6). The reader will no doubt expect that since most of our $l - 1$ are highly composite and have lots of common factors, the set $\mathcal{N}(S)$ will be a small set of congruences modulo a large modulus. After a few seconds we found that

$$\mathcal{N}(S) = \left\{\overline{1}, \overline{3491888399}, \overline{3491888401}, \overline{6983776799}\right\} \subset \mathbb{Z}/M.$$

We then replaced the value of M by $M \times 23$ and continued until $\mathcal{N}(S)$ had exactly four elements and $\mathcal{N} \subset \mathbb{Z}/M$ with this new value of M, etc. The entire computation took 42 seconds and proved that the the reduction of n belongs to a set

$$\mathcal{N} = \left\{\overline{1}, \overline{a}, \overline{b}, \overline{c}\right\} \subset \mathbb{Z}/M$$

where

$$a = 1007045988544277770241794182739444114829990027 99,$$
$$b = 1007045988544277770241794182739444114829990028 01,$$
$$c = 2014091977088555540483588365478888229659980055 99,$$

and the value of M is now

$$M = 2^5 \times 3^3 \times 5^2 \times 7 \times 11 \times \cdots \times 109.$$

Note that $a \approx 1.007 \times 10^{47}$.

By Proposition 10.5, we know that $n \geq a$. However, if $p = 7$ then Proposition 9.2 implies that $n < 2.639 \times 10^{46}$. This proves that $p > 7$. As a check on our computations, we note that $a = M/2 - 1$, $b = M/2 + 1$ and $c = M - 1$, which is entirely consistent with Lemma 10.6.

The next step is to prove that $p > 11$. We continue as above but now take $q = 7$. We note that $\mathcal{N}(l, 7) \subseteq \mathcal{N}(l, 5)$ for any prime l, and that probably $\mathcal{N}(l, 7)$ is strictly smaller $\mathcal{N}(l, 5)$. Thus our sieve becomes more efficient.

The proof program took roughly 97 hours to run on a 1.7 GHz Intel Pentium 4. By the end of the proof the set S had 6262 pairs, and we have also shown that $p > 733$ and $n \geq 1.033 \times 10^{8733}$. To complete the proof we must show that $\log y \geq 10^{8000}$. However $y^p = F_n = (\omega^n - \tau^n)/\sqrt{5}$. Taking logarithms and using Pethő's result that $p < 5.1 \times 10^{17}$ (mentioned in Section 2) we deduce that $\log y \geq 10^{8000}$ with a huge margin.

10.2. *Proof of Proposition* 10.2. The proof of Proposition 10.2 is practically identical to the above proof of Proposition 10.1 and we omit almost all the details. We can take $K(l) = l - 1$ in this case, and we let E_n and E be given by equations (24) and (25) respectively. If $l \equiv \pm 1 \pmod 5$ and $q \geq 5$ are primes we define $\mathcal{N}(l, q)$ to be the subset of all $n \in (\mathbb{Z}/K(l))^*$ such that

- either $5F_n^2 - 4 \not\equiv 0 \pmod l$, and the integer $a_l(E_n) - a_l(E)$ is divisible by some prime $p > q$,
- or $5F_n^2 - 4 \equiv 0 \pmod l$ and one of the two integers $l + 1 \pm a_l(E)$ is divisible by some prime $p > q$.

The other details are practically identical to the Fibonacci case. Since the lower bound for p that we are trying to establish is much smaller in the Lucas case our program runs much faster, and completes the proof on the same machine in about six hours.

11. A refined bound on p using linear forms in two logarithms

In the previous section we showed that if (n, y, p) is a solution to equation (18) then $p > 283$. In this section we will use the results of the paper of

Laurent, Mignotte and Nesterenko [27] on linear forms in two logarithms to prove that $p \leq 283$, thus completing the proof of Theorem 2.

The Fibonacci case still needs more work, since it yields a linear form in three logarithms. However, for now we are able to show the following.

PROPOSITION 11.1. *If (n, y, p) is a solution to equation (17) then $p > 2 \times 10^8$.*

Proof. Suppose that (n, y, p) is a solution to (17). The most obvious approach to obtain an upper bound for p is to consider

$$F_n = \frac{\omega^n - \omega^{-n}}{\sqrt{5}} = y^p$$

and the linear form in logarithms

$$\Lambda = n \log \omega - \log \sqrt{5} - p \log y.$$

Then a standard argument shows that

$$\log |\Lambda| < -2p \log y + 1.$$

We note that Λ is a linear forms in three logarithms. In the remainder of this paper we will present a substantial improvement to the theory of linear forms in three logarithms, and apply our result to show that $p < 2 \times 10^8$.

For now, to prove the proposition, we argue by contradiction, assuming that $p < 2 \times 10^8$. We then know from Proposition 7.3 that $n \equiv \pm 1 \pmod{p}$ for primes p in this range. Write $n = sp + \epsilon$, where $\epsilon = \pm 1$. Note now that we can rewrite the expression Λ as

$$\Lambda = p \log (\omega^s / y) - \log (\sqrt{5} \omega^{-\epsilon}),$$

which is now a linear form in two logarithms! We can apply Théorème 1 of [27] with

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

where

$$b_1 = p, \quad \alpha_1 = \omega^s / y; \qquad b_2 = 1, \quad \alpha_2 = \sqrt{5}\, \omega^{-\epsilon}$$

and

$$\log \alpha_2 = \log \sqrt{5} - \epsilon \log \omega, \quad \log \alpha_1 \approx \frac{1}{p} \log \alpha_2,$$

and

$$\mathrm{h}(\alpha_2) = \frac{\log 10}{2}, \quad \mathrm{h}(\alpha_1) \leq \log y + \log 5.$$

Thus (with the notation of this result), we can take

$$a_1 = (\rho - 1) \log \alpha_1 + 4 (\log y + \log 5), \quad a_2 = (\rho - 1) \log \alpha_2 + 2 \log 10.$$

The case $\epsilon = -1$. In this case, we choose (again with the notation of [27]) $L = 8$, $\rho = 27.6$, $m = 0.209671121$ and get

$$p \leq 733.$$

The case $\epsilon = 1$. In this case, we choose $L = 7$, $\rho = 31.6$, $m = 0.218149476$ and get

$$p \leq 241.$$

In either case we have $p \leq 733$ which contradicts Proposition 10.1. This completes the proof of the proposition. □

As promised we also complete the resolution of the Lucas case by presenting the proof of Theorem 2.

Proof of Theorem 2. Suppose that (n, y, p) is a solution to equation (18). It is apparent, by Proposition 10.2, that all we have to do is to show that $p \leq 283$, and to do this we apply [27].

Put

$$\Lambda = p \log y - n \log \omega$$

where $\omega = (1 + \sqrt{5})/2$. By Proposition 10.2 we know that

$$\log y > 10^6,$$

and indeed much more. Then (because $L_n = \omega^n + (-1/\omega)^n$)

$$\log |\Lambda| < -2p \log y + 1.$$

Write $n = sp + r$ with $0 \leq r < p$ (notice that we do not use here the congruence $n \equiv \pm 1 \pmod{p}$ proved above). This allows us to rewrite Λ as

$$\Lambda = p \log(y/\omega^s) - r \log \omega.$$

We apply [27, Prop. 1] with the notation $D = 2$ and

$$\alpha_1 = y/\omega^s,\ \alpha_2 = \omega,\ b_1 = p,\ b_2 = r,\ a_1 = 2.00001\ \log(y\omega^s),\ a_2 = (\rho + 1) \log \omega.$$

Here

$$\tilde{b} = \frac{1}{\rho + 1} \left(\frac{p}{\log \omega} + \frac{r(1 + \rho)}{a_1} \right) \approx \frac{1}{\rho + 1} \frac{p}{\log \omega}.$$

We get either

$$p \leq \mu L (\rho + 1) \log \omega$$

or

$$\log |\Lambda| > -KL \log \rho - \log(KL)$$

provided that

$$2K \log \theta + 2 \log(2\pi K / e^{3/2}) - 3 \log(KL) - \frac{c + \log K}{3K} - \frac{a_1 L}{3} - \frac{a_2 L^2}{3} - \frac{2K}{\mu a_1} \geq 0$$

and

$$\mu\big((L-1)\log\rho + 2\log(2/\theta) - 2(1.5 - \log\mu + \log\tilde{b})\big) \geq \frac{L}{3}.$$

It is enough to take

$$\log\theta = \frac{1.01 \times a_1 L}{3 \times 2\mu^2 a_1 a_2 L} = \frac{1.01}{6\mu^2(\rho+1)\log\omega}.$$

For $\rho = 22.9$, taking $\mu = 2/(3\omega)$, working as above we first get $p < 326$ and then, after several iterations of the above argument,

$$p \leq 283.$$

Remark. Using the congruence $n \equiv \pm 1 \pmod{p}$ we could improve this estimate a little and get something like $p \leq 241$. □

12. An estimate on linear forms in three logarithms

12.1. *Preliminaries.*

LEMMA 12.1. *Let K, L, R, S, T be positive integers, put $N = K^2L$ and assume $N \leq RST$. Put also*

$$\ell_n = \left\lfloor \frac{n-1}{K^2} \right\rfloor, \quad 1 \leq n \leq N,$$

and $(r_1, \ldots, r_N) \in \{0, 1, \ldots, R-1\}^N$. Suppose that for each $r \in \{0, 1, \ldots, \ldots, R-1\}$ there are at most ST indices such that $r_j = r$. Then

$$\left| \sum_{n=1}^{N} \ell_n r_n - M \right| \leq G_R$$

where

$$M = \left(\frac{L-1}{2}\right) \sum_{n=1}^{N} r_n \qquad \text{and} \qquad G_R = \frac{NLR}{2}\left(\frac{1}{4} - \frac{N}{12RST}\right).$$

Proof. Apply [27, Lemme 4]. □

As in [3] or [52, p. 192], for $(k, m) \in \mathbb{N}^2$, we put $\|(k, m)\| = k + m$. And we put

$$\Theta(K_0, I) = \min\big\{\|(k_1, m_1)\| + \cdots + \|(k_I, m_I)\|\big\},$$

where the minimum is taken over if the I–tuples $(k_1, m_1), \ldots, (k_I, m_I) \in \mathbb{N}^2$ which are pairwise distinct and satisfy $m_1, \ldots, m_I \leq K_0$. Then, we have:

LEMMA 12.2. *Let K_0, L and I be positive integers with $K_0 \geq 3$, $L \geq 2$ and $I \geq K_0(K_0+1)/2$. Then*

$$\Theta(K_0, I) \geq \left(\frac{I^2}{2(K_0+1)}\right)\left(1 + \frac{(K_0-1)(K_0+1)}{I} - \frac{K_0(K_0+2)(K_0+1)^2}{12I^2}\right).$$

Proof. Except for some details, this is [3, Lemma 1.4]. We follow more or less the proof of this result. The argument is elementary: the smallest value for the sum $\|(k_1, m_1)\| + \cdots + \|(k_I, m_I)\|$ is reached when we choose successively, for each integer $n = 0, 1, \ldots$ all the points in the domain

$$D_n = \{(k, m) \in \mathbb{N}^2;\ m \leq K_0,\ k + m = n\},$$

and stop when the total number of points is I. Moreover,

$$\mathrm{Card}(D_n) = \begin{cases} n+1, & \text{if } n \leq K_0, \\ K_0 + 1, & \text{if } n \geq K_0. \end{cases}$$

With the notation of [3], the number I of points can be written as

$$I = \left(A - \frac{K_0}{2}\right)(K_0+1) + r, \quad \text{with } \ 0 \leq r \leq K_0,$$

provided that $I \geq K_0(K_0+1)/2$, which is a hypothesis of the lemma.

Then, the computation of [3] shows that

$$\Theta(K_0, I) \geq \tilde{\Theta}(K_0, I) := \frac{K_0+1}{2}\left(A(A-1) - \frac{K_0(K_0-1)}{3}\right) + rA.$$

In terms of I,

$$A = \frac{K_0}{2} + \frac{I-r}{K_0+1}.$$

We have,

$$\frac{\partial\tilde{\Theta}}{\partial r} = \frac{K_0+1}{2}(2A-1)\frac{\partial A}{\partial r} + A + r\frac{\partial A}{\partial r} = -\frac{2A-1}{2} + A - \frac{r}{K_0+1} = \frac{1}{2} - \frac{r}{K_0+1},$$

which shows that the minimum of $\tilde{\Theta}$ is reached either for $r = 0$ or $r = K_0$. It is easy to verify that $\tilde{\Theta}$ takes the same value for $r = 0$ and $r = K_0 + 1$ (which is indeed out of the range of r); this implies that the minimum is reached for $r = 0$. It follows that

$$\begin{aligned}
\frac{2\Theta(K_0, I)}{K_0+1} &\geq \left(\frac{K_0}{2} + \frac{I}{K_0+1}\right)\left(\frac{K_0}{2} + \frac{I}{K_0+1} - 1\right) - \frac{K_0(K_0-1)}{3} \\
&= \frac{K_0^2}{4} + \frac{I^2}{(K_0+1)^2} + \frac{K_0 I}{K_0+1} - \frac{K_0}{2} - \frac{I}{K_0+1} - \frac{K_0^2}{3} + \frac{K_0}{3} \\
&= \frac{I^2}{(K_0+1)^2} + \frac{(K_0-1)I}{K_0+1} - \frac{K_0^2}{12} - \frac{K_0}{6} \\
&= \left(\frac{I}{K_0+1}\right)^2\left(1 + \frac{(K_0-1)(K_0+1)}{I} - \frac{K_0(K_0+2)(K_0+1)^2}{12I^2}\right),
\end{aligned}$$

which proves the lemma. □

The version of Liouville inequality that we use is the same as in [27, pp. 298–99]:

LEMMA 12.3. *Let α_1, α_2, α_3 be nonzero algebraic numbers and $f \in \mathbb{Z}[X_1, X_2, X_3]$ such that $f(\alpha_1, \alpha_2, \alpha_3) \neq 0$. Then*

$$|f(\alpha_1, \alpha_2, \alpha_3)| \geq |f|^{-D+1}(\alpha_1^*)^{d_1}(\alpha_2^*)^{d_2}(\alpha_3^*)^{d_3} \times \exp\bigl\{-D\bigl(d_1\mathrm{h}(\alpha_1) + d_2\mathrm{h}(\alpha_2) + d_3\mathrm{h}(\alpha_3)\bigr)\bigr\}$$

where $D = [\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) : \mathbb{Q}] \,/\, [\mathbb{R}(\alpha_1, \alpha_2, \alpha_3) : \mathbb{R}]$,

$$d_i = \deg_{X_i} f, \quad i = 1, 2, 3, \qquad |f| = \max\bigl\{|f(z_1, z_2, z_3)|;\ |z_i| \leq 1,\ i = 1, 2, 3\bigr\},$$

and $\mathrm{h}(\alpha)$ *is the absolute logarithmic height of the algebraic number* α, *and* $\alpha^* = \max\{1, |\alpha|\}$.

LEMMA 12.4. *Let $K > 1$ be an integer; then*

$$\log\left(\prod_{k=1}^{K-1} k!\right)^{\frac{4}{K(K-1)}} \geq 2\log K - 3 + \frac{2\log(2\pi K/e^{3/2})}{K-1} - \frac{2 + 6\pi^{-2} + \log K}{3K(K-1)}.$$

Proof. This is a consequence of a variant of the proof of [27, Lemme 8]. □

Now we present the type of linear forms in three logarithms to be studied. For a while, we consider three nonzero algebraic numbers α_1, α_2 and α_3 and positive rational integers b_1, b_2, b_3 with $\gcd(b_1, b_2, b_3) = 1$, and the linear form

$$\Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1 - b_3 \log \alpha_3 \neq 0,$$

without any loss in generality.

We restrict our study to the following cases:

- the real case: α_1, α_2 and α_3 are real numbers > 1, and the logarithms of the α_i's are real (and > 0),
- the complex case: α_1, α_2 and α_3 are complex numbers of modulus one, and the logarithms of the α_i's are arbitrary determinations of the logarithm.

This does not cause inconvenience in practice since in the general case we obviously always have

$$|\Lambda| \geq \max\{|\Re(\Lambda)|, |\Im(\Lambda)|\}.$$

Without loss of generality, we may assume that

$$b_2|\log \alpha_2| = b_1|\log \alpha_1| + b_3|\log \alpha_3| \pm |\Lambda|.$$

Choosing rational positive integers K, L, R, S, T, with K, $L \geq 2$, we put $N = K^2L$ and assume $RST \geq N$. Let a_1, a_2, a_3 be positive real numbers.

The authors of [3] use Laurent's method, and they consider a suitable interpolation determinant Δ. Let i be an index such that (k_i, m_i, ℓ_i) runs through all triples of integers with $0 \le k_i \le K-1$, $0 \le m_i \le K-1$ and $0 \le \ell_i \le L-1$. Thus, each number $0, \dots, K-1$ occurs KL times as a k_i, and similarly as an m_i, and each number $0, \dots, L-1$ occurs K^2 times as an ℓ_i. With the above definitions, let

$$\Delta = \det \left\{ \binom{r_j b_2 + s_j b_1}{k_i} \binom{t_j b_2 + s_j b_3}{m_i} \alpha_1^{\ell_i r_j} \alpha_2^{\ell_i s_j} \alpha_3^{\ell_i t_j} \right\}$$

where r_j, s_j, t_j are nonnegative integers less than R, S, T, respectively, such that (r_j, s_j, t_j) runs over N distinct triples. Put $\beta_1 = b_1/b_2$, $\beta_3 = b_3/b_2$. Let

$$\lambda_i = \ell_i - \frac{L-1}{2}, \quad \eta_0 = \frac{R-1}{2} + \beta_1 \frac{S-1}{2}, \quad \zeta_0 = \frac{T-1}{2} + \beta_3 \frac{S-1}{2},$$

and

$$b = (b_2\eta_0)(b_2\zeta_0) \left(\prod_{k=1}^{K-1} k! \right)^{-\frac{4}{K(K-1)}}.$$

Notice that, by Lemma 12.4,

$$\begin{aligned} \log b \le & \log \frac{(R-1)b_2 + (S-1)b_1}{2} + \log \frac{(T-1)b_2 + (S-1)b_3}{2} \\ & -2\log K + 3 - \frac{2\log(2\pi K/e^{3/2})}{K-1} + \frac{2 + 6\pi^{-2} + \log K}{3K(K-1)}. \end{aligned}$$

Then $\sum_{i=0}^{N-1} \lambda_i = 0$ and ([3, formula (2.1)])

$$\alpha_1^{\ell_i r_j} \alpha_2^{\ell_i s_j} \alpha_3^{\ell_i t_j} = \alpha_1^{\lambda_i (r_j + s_j \beta_1)} \alpha_3^{\lambda_i (t_j + s_j \beta_3)} (1 + \theta_{ij} \Lambda'),$$

where

$$\Lambda' = |\Lambda| \cdot \max \left\{ \frac{LRe^{LR|\Lambda|/(2b_1)}}{2b_1}, \frac{LSe^{LS|\Lambda|/(2b_2)}}{2b_2}, \frac{LTe^{LT|\Lambda|/(2b_3)}}{2b_3} \right\}$$

and where all $|\theta_{ij}|$ are ≤ 1.

12.2. *An upper bound for* $|\Delta|$. It is proved in [3] (last formula of page 111) that

$$\Delta = \alpha_1^{M_1} \alpha_2^{M_2} \alpha_3^{M_3} \sum_{\mathcal{I} \subseteq \mathcal{N}} (\Lambda')^{N - |\mathcal{I}|} \Delta_{\mathcal{I}}$$

where

$$M_1 = \frac{L-1}{2} \sum_{j=1}^{N} r_j, \qquad M_2 = \frac{L-1}{2} \sum_{j=1}^{N} s_j, \qquad M_3 = \frac{L-1}{2} \sum_{j=1}^{N} t_j,$$

and where $\mathcal{N} = \{0, 1, \dots, N-1\}$ and $\Delta_{\mathcal{I}}$ is the determinant of a certain matrix $\mathcal{M}_{\mathcal{I}}$ defined below. Let

$$\phi_j(z,\zeta) = \frac{b_2^{k_i+m_i}}{k_i!\, m_i} z^{k_i} \zeta^{m_i} \alpha_1^{\lambda_i z} \alpha_3^{\lambda_i \zeta},$$

(where $\alpha_1^{\lambda_i z} = \exp(\lambda_i z \log \alpha_1)$ and similarly for $\alpha_3^{\lambda_i \zeta}$) and

$$\Phi_{\mathcal{I}}(x)_{ij} = \begin{cases} \phi_j(xz_j, x\zeta_j) & \text{if } i \in \mathcal{I}, \\ \theta_{ij}\phi_j(xz_j, x\zeta_j) & \text{if } i \notin \mathcal{I}. \end{cases}$$

Then, $\mathcal{M}_{\mathcal{I}} = \big(\Phi_{\mathcal{I}}(1)_{ij}\big)$ and when $\Psi_{\mathcal{I}}(x) = \det\big(\Phi_{\mathcal{I}}(x)\big)$,

$$|\Delta_{\mathcal{I}}| = \big|\det\big(\Phi_{\mathcal{I}}(1)\big)\big| = |\Psi_{\mathcal{I}}(1)|.$$

Now, when

$$J_{\mathcal{I}} = \operatorname{order}(\Psi, 0),$$

the maximum modulus principle implies

$$|\Psi_{\mathcal{I}}(1)| \le \rho^{-J_{\mathcal{I}}} \cdot \max_{|x|=\rho} |\Psi_{\mathcal{I}}(x)|.$$

Since $|z_j| \le \eta_0$ and $|\zeta_j| \le \zeta_0$,

$$\max_{|x|=\rho} \big|\Psi_{\mathcal{I}}(x)\big| \le N! \, \frac{{b_2}^{\sum k_i + \sum m_i}}{\prod k_i! \prod m_i!} \, (\rho\eta_0)^{\sum k_i} (\rho\zeta_0)^{\sum m_i} \times \max_{\sigma \in \mathfrak{S}(\mathcal{N})} \exp\Big\{\rho\Big(\big(\sum \lambda_i z_{\sigma(i)}\big)\log\alpha_1 + \big(\sum \lambda_i \zeta_{\sigma(i)}\big)\log\alpha_2\Big)\Big\}.$$

Put

$$g = \frac{1}{4} - \frac{N}{12RST}, \quad G_1 = \frac{NLR}{2}\, g, \quad G_2 = \frac{NLS}{2}\, g, \quad G_3 = \frac{NLT}{2}\, g,$$

then (see the proof of [3, p. 114] and use Lemma 12.1)

$$\sum_{i=0}^{N-1} \lambda_i z_{\sigma(i)} \le G_1 + \beta_1 G_2, \qquad \sum_{i=0}^{N-1} \lambda_i \zeta_{\sigma(i)} \le G_3 + \beta_3 G_2.$$

It follows that (recall that $b_2|\log\alpha_2| = b_1|\log\alpha_1| + b_3|\log\alpha_3| \pm |\Lambda|$)

$$\begin{aligned} &\exp\Big\{\rho\Big(\big(\sum \lambda_i z_{\sigma(i)}\big)|\log\alpha_1| + \big(\sum \lambda_i \zeta_{\sigma(i)}\big)|\log\alpha_3|\Big)\Big\} \\ &\le \exp\Big\{\rho\Big((G_1+\beta_1 G_2)|\log\alpha_1| + (G_3+\beta_3 G_2)|\log\alpha_3|\Big)\Big\} \\ &\le \exp\left\{\rho\left(G_1|\log\alpha_1| + G_2\Big(|\log\alpha_2| + \frac{|\Lambda|}{b_2}\Big) + G_3|\log\alpha_3|\right)\right\}. \end{aligned}$$

As in [3], we see that if

$$\Lambda' < \rho^{-KL} \tag{46}$$

then

$$\rho G_2 \frac{|\Lambda|}{b_2} \le \frac{\rho K^2 L}{4\rho^{KL}} \le \frac{eK^2 L}{4e^{KL}} \le \frac{K^2 L^2}{e^{KL}} < 10^{-4}$$

for $KL \ge 15$. Putting these estimates together, we see that condition (46) implies the upper bound

$$|\Delta| \le 1.0001\, {\alpha_1}^{M_1+\rho G_1}\, {\alpha_2}^{M_2+\rho G_2}\, {\alpha_3}^{M_3+\rho G_3}\, N! \times 2^N\, \rho^{\sum(k_i+m_i)} \times \frac{(b_2\eta_0)^{\sum k_i}}{\prod k_i!} \times \frac{(b_2\zeta_0)^{\sum m_i}}{\prod m_i!} \times \max_{\sigma\in\mathfrak{S}(\mathcal{N})} \frac{|\Lambda'|^{N-|\mathcal{I}|}}{\rho^{J_{\mathcal{I}}}}$$

where

$$J_{\mathcal{I}} = \operatorname{order}(\Psi_{\mathcal{I}}, 0).$$

Under condition (46), we have

$$\frac{|\Lambda'|^{N-|\mathcal{I}|}}{\rho^{J_{\mathcal{I}}}} \le \rho^{-KL(N-|\mathcal{I}|)-J_{\mathcal{I}}}.$$

If $|\mathcal{I}| \le 0.5\, N$ then

$$KL(N-|\mathcal{I}|) \ge 0.5\, KLN \ge \frac{NKL}{4}\left(1 + \frac{4}{L} + \frac{1}{2K-1}\right)$$

as soon as $K \ge 3$ and $L \ge 5$, conditions that we assume from now on.

If $|\mathcal{I}| \ge 0.5\, N$, then using [3, Lemma 1.3], we obtain

$$J_{\mathcal{I}} \ge \Theta(K_0, |\mathcal{I}|), \qquad \text{for} \quad K_0 = 2(K-1)\,.$$

Now, $|\mathcal{I}| \ge 0.5\, K^2 L$ implies $|\mathcal{I}| \ge 2.5\, K^2$ and using Lemma 12.2 we get (with the notation $I = |\mathcal{I}|$)

$$KL(N-I) + J_{\mathcal{I}} \ge KL(N-I) + \left(\frac{I^2}{2(K_0+1)}\right)\left(1 + \frac{(K_0-1)(K_0+1)}{I} - \frac{K_0(K_0+2)(K_0+1)^2}{12I^2}\right).$$

It is easy to verify that the right-hand side is a decreasing function of I in the range $[N/2, N]$, since $L \ge 5$, and we get (recall that $N = K^2 L$ and $K_0 = 2K-2$)

$$\begin{aligned} KL(N-|\mathcal{I}|) + J_{\mathcal{I}} &\ge \frac{N^2}{2(K_0+1)}\left(1 + \frac{K_0^2-1}{N} - \frac{K_0(K_0+2)(K_0+1)^2}{12N^2}\right) \\ &= \frac{N^2}{4K}\left(\frac{2K}{K_0+1} + \frac{2K(K_0-1)}{N} - \frac{KK_0(K_0+1)(K_0+2)}{6N^2}\right) \\ &= \frac{N^2}{4K}\left(1 + \frac{1}{2K-1} + \frac{2(2K-3)}{KL} - \frac{2(K-1)(2K-1)}{3K^2L^2}\right) \\ &= \frac{N^2}{4K}\left(1 + \frac{4}{L} + \frac{1}{2K-1} - \frac{4}{3L^2} - \frac{6}{KL} + \frac{2}{KL^2} - \frac{2}{3K^2L^2}\right) \\ &\ge \frac{N^2}{4K}\left(1 + \frac{4}{L} + \frac{1}{2K-1} - \frac{4}{3L^2} - \frac{6}{KL}\right), \end{aligned}$$

because $L \geq 5$, and this implies, in all cases,

$$KL(N - |\mathcal{I}|) + J_{\mathcal{I}} \geq \frac{N^2}{4K}\left(1 + \frac{4}{L} + \frac{1}{2K-1} - \frac{6}{KL} - \frac{4}{3L^2}\right).$$

Thus, gathering all the previous estimates and using the relations

$$\sum_{i=0}^{N-1} k_i = \sum_{i=0}^{N-1} m_i = \frac{(K-1)K}{2}\,KL = \frac{N}{2}\,(K-1),$$

and the definition of b, we obtain the following result.

PROPOSITION 12.5. *With, the previous notation, if $K \geq 3$, $L \geq 5$ and $\Lambda' \leq \rho^{-KL}$, and with $\rho \geq e$,*

$$\log|\Delta| \leq \sum_{i=1}^{3} M_i \log|\alpha_i| + \rho \sum_{i=1}^{3} G_i |\log \alpha_i| + \log(N!) + N\log 2 + \frac{N}{2}\,(K-1)\log b$$
$$\left(\frac{NKL}{4} + \frac{NKL}{4(2K-1)} - \frac{NK}{3L} - \frac{N}{2}\right)\log\rho + 0.0001.$$

12.3. *A lower bound for $|\Delta|$.* Using our Liouville estimate (Lemma 12.3) and arguing as in [3], or [27, Lemme 6], we get the following.

PROPOSITION 12.6. *If $\Delta \neq 0$ then*

$$\log|\Delta| \geq -\frac{D-1}{2}\,N\log N$$
$$+ \sum_{i=1}^{3}(M_i + G_i)\log|\alpha_i| - 2D\sum_{i=1}^{3} G_i \mathrm{h}(\alpha_i) - \frac{D-1}{2}(K-1)\,N\log b.$$

Proof. We have $\Delta = P(\alpha_1, \alpha_2, \alpha_3)$ where $P \in \mathbb{Z}[X_1, X_2, X_3]$ is given by

$$P(X_1, X_2, X_3)$$
$$= \sum_{\sigma \in \mathfrak{S}_N} \mathrm{sg}(\sigma) \cdot \prod_{i=1}^{N} \binom{r_{\sigma(i)}b_2 + s_{\sigma(i)}b_1}{k_i} \binom{t_{\sigma(i)}b_2 + s_{\sigma(i)}b_3}{m_i} X_1^{n_{r\sigma}} X_2^{n_{s\sigma}} X_3^{n_{t\sigma}},$$

and where

$$n_{r\sigma} = \sum_{i=1}^{N} \ell_i r_{\sigma(i)}, \quad n_{s\sigma} = \sum_{i=1}^{N} \ell_i s_{\sigma(i)}, \quad n_{t\sigma} = \sum_{i=1}^{N} \ell_i t_{\sigma(i)}.$$

By Lemma 12.1,

$$\left|\deg_{X_i} P - M_i\right| \leq G_i, \quad i = 1, 2, 3.$$

When

$$V_i = \lfloor M_i + G_i \rfloor, \qquad U_i = \lceil M_i - G_i \rceil, \quad i = 1, 2, 3,$$

then

$$\Delta = {\alpha_1}^{V_1}{\alpha_2}^{V_2}{\alpha_3}^{V_3}\,\tilde{P}(\alpha_1^{-1},\alpha_2^{-1},\alpha_3^{-1}),$$

where

$$\deg_{X_i}\tilde{P} \le V_i - U_i, \quad i = 1,\,2,\,3.$$

By our Liouville estimate

$$\log\bigl|\tilde{P}(\alpha_1^{-1},\alpha_2^{-1},\alpha_3^{-1})\bigr| \ge -(D-1)\log|\tilde{P}| - D\sum_{i=1}^{3}(V_i-U_i)\,\mathrm{h}(\alpha_i).$$

Now we have to find an upper bound for $|\tilde{P}|$ (or for $|P|$ which is equal to $|\tilde{P}|$). By the multilinearity of the determinant, for all $\eta,\,\zeta\in\mathbb{C}$,

$$P(z_1,z_2,z_3) = \det\left(\frac{(r_jb_2+s_jb_1-\eta)^{k_i}}{k_i!}\,\frac{(t_jb_2+s_jb_3-\zeta)^{m_i}}{m_i!}\cdot {z_1}^{\ell_i r_j}\cdot {z_2}^{\ell_i s_j}\cdot {z_3}^{\ell_i t_j}\right).$$

Choose

$$\eta = \frac{(R-1)b_2+(S-1)b_1}{2}, \quad \zeta = \frac{(T-1)b_2+(S-1)b_3}{2}$$

and notice that, for $1\le j\le N$,

$$|r_jb_2+s_jb_1-\eta|^{k_i} \le \left(\frac{(R-1)b_2+(S-1)b_1}{2}\right)^{k_i},$$

$$|t_jb_2+s_jb_3-\zeta|^{k_i} \le \left(\frac{(T-1)b_2+(S-1)b_3}{2}\right)^{m_i}$$

and that

$$\sum_{i=0}^{N-1}k_i = \sum_{i=0}^{N-1}m_i = \frac{(K-1)K}{2}\,KL = \frac{N}{2}\,(K-1).$$

Then Hadamard's inequality implies

$$|P| \le N^{N/2}\left(\frac{(R-1)b_2+(S-1)b_1}{2}\right)^{\frac{(K-1)N}{2}}\left(\frac{(T-1)b_2+(S-1)b_3}{2}\right)^{\frac{(K-1)N}{2}} \times\left(\prod_{i=0}^{K-1}k_i!\right)^{-1}\left(\prod_{i=0}^{K-1}m_i!\right)^{-1}.$$

Recall that

$$b = (b_2\eta_0)(b_2\zeta_0)\left(\prod_{k=1}^{K-1}k!\right)^{-\frac{4}{K(K-1)}},$$

where

$$\eta_0 = \frac{R-1}{2}+\beta_1\frac{S-1}{2}, \qquad \zeta_0 = \frac{T-1}{2}+\beta_3\frac{S-1}{2}.$$

Thus we get,

$$|P| \le N^{N/2}\,b^{(K-1)N/2}.$$

Collecting all the above estimates, we find

$$\log|\Delta| \geq -(D-1)\ \left(\log\left(N^{N/2}\right) + \frac{(K-1)N}{2}\ \log b\right) \\ -D\sum_{i=1}^{3}(V_i-U_i)\mathrm{h}(\alpha_i) + \sum_{i=1}^{3} V_i \log|\alpha_i|.$$

The inequalities $D\mathrm{h}(\alpha_i) \geq \log|\alpha_i| \geq 0$ imply

$$V_i\log|\alpha_i| - D(V_i-U_i)\mathrm{h}(\alpha_i) \geq (M_i+G_i)\log|\alpha_i| - 2DG_i\mathrm{h}(\alpha_i)$$

and the result follows. □

12.4. *Synthesis.* Under the hypotheses of Propositions 12.5 and 12.6, we get

$$-\frac{D-1}{2}\,N\log N + \sum_{i=1}^{3}(M_i+G_i)\log|\alpha_i| \\ -2D\sum_{i=1}^{3}G_i\mathrm{h}(\alpha_i) - \frac{D-1}{2}(K-1)\,N\log b \\ \leq \sum_{i=1}^{3}M_i\log|\alpha_i| + \rho\sum_{i=1}^{3}G_i|\log\alpha_i| + \log(N!) + N\log 2 + \frac{N}{2}\,(K-1)\log b \\ -\left(\frac{NKL}{4} + \frac{NKL}{4(2K-1)} - \frac{NK}{3L} - \frac{N}{2}\right)\log\rho + 0.0001.$$

Or, after some simplification,

$$-\frac{D-1}{2}\,N\log N \leq \sum_{i=1}^{3}G_i\big(\rho|\log\alpha_i| - \log|\alpha_i| + 2D\mathrm{h}(\alpha_i)\big) + \log(N!) \\ +N\log 2 + \frac{K-1}{2}\,DN\log b - \left(\frac{NKL}{4} + \frac{NKL}{4(2K-1)} - \frac{KN}{3L} - \frac{N}{2}\right)\log\rho + 0.0001.$$

This result implies (divide by $N/2$ and use $N! < N(N/e)^N$, true for $N > 7$):

PROPOSITION 12.7. *With, the previous notation, if $K \geq 3$, $L \geq 5$, $\rho \geq e$, and if $\Delta \neq 0$ then*

$$\Lambda' > \rho^{-KL}$$

provided that

$$\left(\frac{KL}{2} + \frac{L}{4} - 1 - \frac{2K}{3L}\right)\log\rho \geq (D+1)\log N + gL(a_1R + a_2S + a_3T) \\ +D(K-1)\ \log b - 2\log(e/2),$$

where the a_i's satisfy

$$a_i \geq \rho|\log\alpha_i| - \log|\alpha_i| + 2D\mathrm{h}(\alpha_i), \qquad i = 1,\,2,\,3.$$

Remark. We notice that the statement of Proposition 12.7 is perfectly symmetric with respect to the b_i's or the α_i's, except for the choice of b. From now on we do not assume that b_1 and b_3 are positive, but we still suppose that $b_2 > 0$ and that

$$b_2|\log\alpha_2| = |b_1\ \log\alpha_1| + |b_3\ \log\alpha_3| \pm |\Lambda|.$$

12.5. *Row rank.* To conclude we need to find conditions under which one of our determinants Δ is nonzero, a so called *zero lemma*. We quote [3, Th. 3] with some minor technical changes.

PROPOSITION 12.8. *Let K, L, R, R_1, R_2, S, S_1, S_2, T, T_1, T_2 be rational integers all ≥ 3, with $K \geq 2L$, $R > R_1 + R_2$, $S > S_1 + S_2$, $T > T_1 + T_2$ and $T_1 \geq R_1$. Let b_1, b_2, b_3 and α_1, α_2, α_3 be as above and moreover assume that α_1, α_2, α_3 are multiplicatively independent. If*

(i) $$4(R_1+1)(S_1+1) \geq T_1+1,$$

(ii) $$4(R_1+1)(T_1+1) \geq S_1+1,$$

(iii) $$(R_2+1)(S_2+1)(T_2+1) \geq 12(K-1)^2(L-1),$$

and

(iv) $$(R_1+1)(S_1+1)(T_1+1) \geq 8(2K+L-2)^2$$

then **either** *there exists a choice of Δ which is nonzero* **or** *at least one of the following conditions holds:*

(C1)
$\exists r,\ s \in \mathbb{Z}, \quad rb_2 = sb_1$ *with* $0 < r \leq R_i$ *and* $0 < s \leq S_i$ *for some* $i = 1, 2,$

(C2)
$\exists t,\ s \in \mathbb{Z}, \quad tb_2 = sb_3$ *with* $0 < t \leq T_i$ *and* $0 < s \leq S_i$ *for some* $i = 1, 2,$

(C3)*: there exist r', s', t', $t'' \in \mathbb{Z}$, such that*

$$s't'b_1 + r't''b_2 + r's'b_3 = 0,$$

which satisfy

$$0 < |r'| < \min\left\{R_1+1, \left(\frac{(R_1+1)(S_1+1)}{T_1+1}\right)^{1/2}\right\},$$

$$0 < |s'| < \min\left\{S_1+1, \left(\frac{(R_1+1)(S_1+1)}{T_1+1}\right)^{1/2}\right\}$$

and

$$0 < |t'| < \min\left\{T_1+1, \left(\frac{(S_1+1)(T_1+1)}{R_1+1}\right)^{1/2}\right\},$$

$$|t''| < \min\left\{T_1+1, \left(\frac{(R_1+1)(T_1+1)}{S_1+1}\right)^{1/2}\right\},$$

which implies a nontrivial relation of the form

$$d_1b_1+d_2b_2+d_3b_3=0 \qquad \text{with } |d_1|\le S_1,\ |d_2|\le R_1,\ |d_3|\le \frac{(R_1+1)(S_1+1)}{T_1+1}.$$

12.6. *A lower bound for the linear form.* Now we have all the tools to conclude and we get at once the following result.

THEOREM 12.9. *Consider three nonzero algebraic numbers α_1, α_2 and α_3 which are multiplicatively independent and positive rational integers b_1, b_2, b_3 with $\gcd(b_1,b_2,b_3)=1$, and the linear form*

$$\Lambda = b_2\log\alpha_2 - b_1\log\alpha_1 - b_3\log\alpha_3 \neq 0.$$

Suppose that **either** *α_1, α_2 and α_3 are real numbers >1, and the logarithms of the α_i's are real (and >0),* **or** *α_1, α_2 and α_3 are complex numbers of modulus one, and the logarithms of the α_i's are arbitrary determinations of the logarithm. Without loss of generality, one may assume that*

$$b_2|\log\alpha_2| = b_1|\log\alpha_1| + b_3|\log\alpha_3| \pm |\Lambda|.$$

Let K, L, R, R_1, R_2, S, S_1, S_2, T, T_1, T_2 be rational integers all ≥ 3, with $K\ge 2L$, $L\ge 5$, $R>R_1+R_2$, $S>S_1+S_2$, $T>T_1+T_2$ and $T_1\ge R_1$. Let $\rho\ge e$ be a real number. Assume first that

$$\text{(o)} \qquad \left(\frac{KL}{2}+\frac{L}{4}-1-\frac{2K}{3L}\right)\log\rho \ge (D+1)\log N + gL(a_1R+a_2S+a_3T) + D(K-1)\log b - 2\log(e/2),$$

where $N=K^2L$, $D=[\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3):\mathbb{Q}]\ /\ [\mathbb{R}(\alpha_1,\alpha_2,\alpha_3):\mathbb{R}]$,

$$g=\frac{1}{4}-\frac{N}{12RST}, \qquad b=(b_2\eta_0)(b_2\zeta_0)\left(\prod_{k=1}^{K-1}k!\right)^{-\frac{4}{K(K-1)}},$$

where

$$\eta_0=\frac{R-1}{2}+\frac{b_1}{b_2}\times\frac{S-1}{2}, \qquad \zeta_0=\frac{T-1}{2}+\frac{b_3}{b_2}\times\frac{S-1}{2},$$

and

$$a_i \ge \rho|\log\alpha_i| - \log|\alpha_i| + 2D\mathrm{h}(\alpha_i), \qquad i=1,2,3.$$

If

$$\text{(i)} \qquad 4(R_1+1)(S_1+1)\ge T_1+1,$$

$$\text{(ii)} \qquad 4(R_1+1)(T_1+1)\ge S_1+1,$$

$$\text{(iii)} \qquad (R_2+1)(S_2+1)(T_2+1)\ge 12(K-1)^2(L-1),$$

and

$$(R_1+1)(S_1+1)(T_1+1) \geq 8(2K+L-2)^2, \tag{iv}$$

then either

$$\Lambda' > \rho^{-KL}$$

where

$$\Lambda' = |\Lambda| \cdot \max\left\{ \frac{LRe^{LR|\Lambda|/(2b_1)}}{2b_1}, \frac{LSe^{LS|\Lambda|/(2b_2)}}{2b_2}, \frac{LTe^{LT|\Lambda|/(2b_3)}}{2b_3} \right\}$$

or *at least one of the conditions* (C1), (C2), (C3) *of Proposition* 12.8 *holds.*

13. Proof of Theorem 1

We are now ready to complete the proof of Theorem 1. We argue by contradiction. Suppose that there is a perfect power in the Fibonacci sequence other than those listed in Theorem 1. By Propositions 6.1 and 11.1 there is a solution (n, y, p) to (17) with $p > 2 \times 10^8$.

Recall that $F_n = (\omega^n - \omega^{-n})/\sqrt{5}$. Thus the linear form

$$\Lambda = n \log \omega - \log \sqrt{5} - p \log y$$

satisfies

$$\log |\Lambda| < -2p \log y + 1.$$

By Proposition 10.1

$$\log y > 10^{20}$$

(and indeed much more). It seems very difficult to get good lower bounds for $|\Lambda|$ when it is written in the previous form. We write

$$n = kp - q, \qquad \text{where } \ 0 \leq q < p.$$

(Notice that q is not necessarily a prime number, but we have some lack of letters!) Then

$$\Lambda = p \log(\omega^k / y) - q \log \omega - \log \sqrt{5}$$

and it is easy to see that it is now of the right form. We know that $p > 2 \times 10^8$ and we will obtain a contradiction by showing that $p < 2 \times 10^8$ using our Theorem 12.9.

The first step is to get an upper bound on p free of any condition. For this purpose our Theorem 12.9 is inconvenient to use; we have to deal with the conditions (C1), (C2) and (C3). This is the reason why we first apply Matveev's estimate (Corollary 2.3). Assume $\Lambda \neq 0$; if real numbers A_j satisfy

$$A_j \geq \max\{D\mathrm{h}(\alpha_j), |\log \alpha_j|, 0.16\}, \quad 1 \leq j \leq 3,$$

and if

$$B = \max\{|b_1|, |b_2|, |b_3|\}$$

then

$$\log|\Lambda| > \frac{3e}{2} 30^6 3^{3.5} D^2 A_1 A_2 A_3 \log(eD)\log(eB),$$

where $D = 2$ and $B = p$ in our case. This leads to

$$p < 2.4 \times 10^{13}.$$

We can now apply Theorem 12.9 with

$$\alpha_1 = \omega, \quad \alpha_2 = \omega^k/y, \quad \alpha_3 = \sqrt{5}, \quad D = 2$$

and

$$b_1 = q, \quad b_2 = p, \quad b_3 = 1.$$

We can take

$$a_1 = (\rho + 3)\log\sqrt{5}, \quad a_2 = (\rho + 2p)\log\omega + 4\log y > 4 \cdot 10^{20},$$
$$a_3 = (\rho + 1)\log\omega,$$

where $\rho > e$. To apply the theorem, we shall choose some rational integer

$$L \geq 100$$

and put

$$K = \lfloor mLa_1a_2a_3 \rfloor, \quad \text{with} \ \ 10 < m < 50,$$

and take

$$R_1 = \lfloor c_1 L^{2/3} a_2 a_3 \rfloor, \quad S_1 = \lfloor c_1 L^{2/3} a_1 a_3 \rfloor, \quad T_1 = \lfloor c_1 L^{2/3} a_1 a_2 \rfloor,$$

with $c_1 = (32.001\, m^2)^{1/3}$, and finally

$$R_2 = \lfloor c_2 L a_2 a_3 \rfloor, \ \ S_2 = \lfloor c_2 L a_1 a_3 \rfloor, \ \ T_2 = \lfloor c_2 L a_1 a_2 \rfloor, \ \ \text{with} \ \ c_2 = (12\, m^2)^{1/3}.$$

We use the notation

$$R = R_1 + R_2 + 1, \quad S = S_1 + S_2 + 1, \quad T = T_1 + T_2 + 1.$$

With such a choice it is easy to check that the four conditions (i), (ii), (iii), (iv) hold. And we get either

$$\log|\Lambda| > -KL\log\rho - \log(KL)$$

or at least one of the conditions (C1), (C2) and (C3) hold. First notice that, in our case (where $b_2 = p$ is prime),

$$\big((\text{C1}) \text{ or } (\text{C2})\big) \ \Rightarrow \ p \leq \max\{S_1, S_2\}.$$

Thus, if $p > \max\{S_1, S_2\}$ then (C1) and (C2) do not hold and then (C3) holds. If (C3) holds then recall that

$$s't'b_1 + r't''b_2 + r's'b_3 = 0,$$

where the factors of the b_i's are bounded above as in Proposition 12.8. In the previous relation we may assume that

$$\gcd(s', t'') = \gcd(r', t') = 1.$$

Moreover, since $|s'| < p$, we see that s' and pt'' are coprime, so that the above relation implies that s' divides r', say $r' = r''s'$. Then this relation is simplified into

$$t'b_1 + r''t''b_2 + r''s'b_3 = 0.$$

Then, since r' and t'' are coprime, $\gcd(r'', t') = 1$ and r'' divides b_1. In the present case, we get

$$t'q' + t''p + s' = 0, \quad \text{with } \ q = r''q',$$

where

$$|t'| \le 1 + \left(\frac{(S_1+1)(T_1+1)}{R_1+1}\right)^{1/2} < 1 + 1.0001 \cdot \left(\frac{(S_1+1)a_1}{a_3}\right)^{1/2}$$

and

$$0 < r' < \left(\frac{(R_1+1)(S_1+1)}{T_1+1}\right)^{1/2} < 1.0001 \cdot \left(\frac{(S_1+1)a_3}{a_1}\right)^{1/2}.$$

Now, we rewrite $s'\Lambda$ as a linear form in two logarithms:

$$s'\Lambda = p\log\bigl(\alpha_2^{s'}{\alpha_3}^{t''}\bigr) - q'\log\bigl(\omega^{r'}{\alpha_3}^{-t'}\bigr),$$

where

$$\omega = \frac{1+\sqrt{5}}{2}, \qquad \alpha_2 = \frac{\omega^k}{y}, \qquad \alpha_3 = \sqrt{5}.$$

This ends our preliminary discussion.

Now, after a computer search we see that we can apply Theorem 12.9 with the choices

$$L = 250, \qquad \rho = 11, \qquad m = 21.8432676837,$$

and then, in the first case,

$$p < 426 \times 10^6.$$

With these choices,

$$\max\{S_1, S_2\} = \max\{64049, 290961\} < 10^8$$

so that neither condition (C1) nor condition (C2) holds. And, using the upper bounds obtained above thanks to Proposition 12.8, we get

$$|r'| \le 354, \qquad |t'| \le 182.$$

Moreover, the relation $t'q' + t''p + s' = 0$, combined with $0 \le q < p$, implies the inequality $|t''| \le |t'|$; hence we also have

$$|t''| \le 182.$$

Then we apply the main result (Théorème 1) of [27], with the choices (using the notation of this result)

$$L = 13, \quad R_1 = 1,\ S_1 = 13, \quad m = 0.138356081647,\ \rho = 22,\ \ldots$$

and we get

$$n < 295 \times 10^6.$$

Thus we have proved that $p < 426 \times 10^6$. From this upper bound, if we use this process once more (taking now $L = 180$ and $r = 11$ in the first case, and keeping the same values $L = 13$ and $\rho = 22$ in the application of [27]), we get:

$$p < 197 \times 10^6,$$

which certainly shows that $p < 2 \times 10^8$ and we have obtained our contradiction. This completes the proof of Theorem 1.

Université Louis Pasteur, Strasbourg, France
E-mail address: bugeaud@math.u-strasbg.fr

Université Louis Pasteur, Strasbourg, France
E-mail address: mignotte@math.u-strasbg.fr

University of Warwick, Coventry, United Kingdom
E-mail address: siksek@maths.warwick.ac.uk

References

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

[2] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier, User's guide to PARI-GP, version 2.1.1 (See also `http://pari.math.u-bordeaux.fr/`).

[3] C. D. Bennett, J. Blass, A. M. W. Glass, D. B. Meronk, and R. P. Steiner, Linear forms in the logarithms of three positive rational numbers, *J. Théor. Nombres Bordeaux* **9** (1997), 97–136.

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

[5] M. A. Bennett and C. M. Skinner, Ternary Diophantine equations via Galois representations and modular forms, *Canadian J. Math.* **56** (2004), 23–54.

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

[7] W. Bosma, J. Cannon, and C. Playoust, The magma algebra system I: The user language, *J. Symbolic Comput.* **24** (1997), 235–265.

[8] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises, *J. Amer. Math. Soc.* **14** (2001), 843–939.

[9] Y. Bugeaud and K. Győry, Bounds for the solutions of unit equations, *Acta Arith.* **74** (1996), 67–80.

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

[11] Y. Bugeaud and M. Mignotte, On integers with identical digits, *Mathematika* **46** (1999), 411–417.

[12] Y. Bugeaud, M. Mignotte, Y. Roy, and T. N. Shorey, The equation $(x^n-1)/(x-1) = y^q$ has no solutions with x square, *Math. Proc. Cambridge Philos. Soc.* **127** (1999), 353–372.

[13] Y. Bugeaud, M. Mignotte, and S. Siksek, Classical and modular approaches to exponential Diophantine equations II. The Lebesgue-Nagell equation, *Compositio Math.* **142** (2006), 31–62.

[14] J. H. E. Cohn, On square Fibonacci numbers, *J. London Math. Soc.* **39** (1964), 537–540.

[15] ———, Lucas and Fibonacci numbers and some Diophantine equations, *Proc. Glasgow Math. Assoc.* **7** (1965), 24–28.

[16] ———, Perfect Pell powers, *Glasgow Math. J.* **38** (1996), 19–20.

[17] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, 2nd edition, Cambridge Univ. Press, Cambridge, 1997.

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

[19] G. Frey, Links between stable elliptic curves and certain Diophantine equations, *Ann. Univ. Sarav. Ser. Math.* **1** (1986), 1–40.

[20] ———, Links between solutions of $A - B = C$ and elliptic curves, in *Number Theory* (Ulm 1987), *Lecture Notes in Math.* **1380**, Springer-Verlag, New York (1989), 31–62.

[21] E. Halberstadt and A. Kraus, Courbes de Fermat: résultats et problèmes, *J. Reine Angew. Math.* **548** (2002), 167–234.

[22] W. Ivorra, Sur les équations $x^p+2^\beta y^p = z^2$ et $x^p+2^\beta y^p = 2z^2$, *Acta Arith.* **108** (2003), 327–338.

[23] A. Kraus, Sur l'équation $a^3 + b^3 = c^p$, *Experiment. Math.* **7** (1998), 1–13.

[24] A. Kraus and J. Oesterlé, Sur une question de B. Mazur, *Math. Ann.* **293** (1992), 259–275.

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

[26] M. Laurent, Linear forms in two logarithms and the interpolation determinants, *Acta Arith.* **66** (1994), 181–199.

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

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

[29] W. Ljunggren, Über die unbestimmte Gleichung $Ax^2 - By^4 = C$, *Arch. f. Mat. og Naturvid.* **41** (1938), No. 10, 18 pp.

[30] ———, On the diophantine equation $x^2 + 4 = Ay^2$, *Norske Vid. Selsk. Forh.*, *Trondheim.* **24** (1951), 82–84.

[31] ———, On the diophantine equation $Ax^4 - By^2 = C$ $(C = 1, 4)$, *Math. Scand.* **21** (1967), 149–158.

[32] W. Ljunggren, *Collected Papers of Wilhelm Ljunggren*, *Vol.* 1, 2 (Paulo Ribenboim, ed.), *Queen's Papers in Pure and Applied Math.* **115**, Queen's University, Kingston, ON, 2003.

[33] H. London and R. Finkelstein, On Fibonacci and Lucas numbers which are perfect powers, *Fibonacci Quart.* **5** (1969), 476–481.

[34] J. McLaughlin, Small prime powers in the Fibonacci sequence, preprint.

[35] 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.

[36] B. Mazur, Rational isogenies of prime degree, *Invent. Math.* **44** (1978), 129–162.

[37] 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.

[38] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, second edition, Springer-Verlag, New York, 1990.

[39] A. Pethő, Perfect powers in second order linear recurrences, *J. Number Theory* **15** (1982), 5–13.

[40] ———, Full cubes in the Fibonacci sequence, *Publ. Math. Debrecen* **30** (1983), 117–127.

[41] ———, Perfect powers in second order recurrences, in *Topics in Classical Number Theory, Vol. I, II*, *Proc. of the Conference in Budapest* 1981, *Colloq. Math. Soc. János Bolyai* **34**, pp. 1217–1227, North-Holland, Amsterdam, 1984.

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

[43] K. Ribet, On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms, *Invent. Math.* **100** (1990), 431–476.

[44] N. Robbins, On Fibonacci numbers which are powers. II, *Fibonacci Quart.* **21** (1983), 215–218.

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

[46] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, *Cambridge Tracts in Math.* **87**, Cambridge University Press, Cambridge, 1986.

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

[48] S. Siksek and J. E. Cremona, On the Diophantine equation $x^2 + 7 = y^m$, *Acta Arith.* **109** (2003), 143–149.

[49] R. L. Taylor and A. Wiles, Ring theoretic properties of certain Hecke algebras, *Ann. of Math.* **141** (1995), 553–572.

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

[51] M. Waldschmidt, Minorations de combinaisons linéaires de logarithmes de nombres algébriques, *Canad. J. Math.* **45** (1993), 176–224.

[52] ———, *Diophantine Approximation on Linear Algebraic Groups*, Springer-Verlag, New York, 2000.

[53] A. Wiles, Modular elliptic curves and Fermat's last Theorem, *Ann. of Math.* **141** (1995), 443–551.

[54] O. Wyler and A. P. Rollett, Advanced problems and solutions: Solution: 5080, *Amer. Math. Monthly* **71** (1964), 220–222.

(Received November 24, 2003)