PERFECT POWERS FROM PRODUCTS OF TERMS IN LUCAS SEQUENCES

YANN BUGEAUD, FLORIAN LUCA, MAURICE MIGNOTTE, SAMIR SIKSEK

Abstract. Suppose that $\{U_n\}_{n\geq 0}$ is a Lucas sequence, and suppose that $l_1, \ldots, l_t$ are primes. We show that the equation

$$U_{n_1} \cdots U_{n_m} = \pm l_1^{x_1} \cdots l_t^{x_t} y^p, \quad p \text{ prime}, \quad m < p,$$

has only finitely many solutions. Moreover, we explain a practical method of solving these equations. For example, if $\{F_n\}_{n\geq 0}$ is the Fibonacci sequence, then we solve the equation

$$F_{n_1} \cdots F_{n_m} = 2^{x_1} \cdot 3^{x_2} \cdot 5^{x_3} \cdots 541^{x_{100}} y^p$$

under the restrictions: p is prime and $m < p$.

1. Introduction and Results

The problem of proving that 0, 1, 8, 144 are the only perfect powers in the Fibonacci sequence was a classical problem that attracted much attention during the past 40 years. It was finally solved [8] in 2003 using a combination of tools from Wiles' proof of Fermat's Last Theorem and Baker's theory of linear forms in logarithms. In [3] it is explained that the method used in [8] can be applied to a wide range of Lucas sequences (defined below).

The last 40 years have also seen many ad hoc techniques applied to the problem of determining perfect powers in Lucas sequences, as well as several theoretical finiteness results. In this paper, we systematise, generalise and extend the many tricks and theorems appearing in the literature into a coherent theory. One novelty of this paper is that we deal systematically with the problem of determining the perfect powers arising as products of finitely many terms in a Lucas sequence. We prove a finiteness-type result (the Finiteness Theorem); moreover, we show that this problem—roughly speaking—reduces to the problem of determining the perfect powers in the Lucas sequence (the Reduction Theorem), which as we indicated above can be solved by the method of [8]. As an illustration, writing $\{F_n\}_{n\geq 0}$ for the Fibonacci sequence, we show that the only solutions of the equation $F_m F_n = y^p$ in integers $2 \leq m < n$ and $p \geq 2$ are given by $F_2 F_6 = 8$, $F_3 F_6 = 16$ and $F_2 F_{12} = 144$. This extends a result of Cohn [10], who solved this equation for the case $p = 2$.

We now state our results precisely. Let r, s be non-zero integers with $\Delta = r^2 + 4s \neq 0$. Let α, β be the roots of the equation $x^2 - rx - s = 0$ with the convention that $|\alpha| \geq |\beta|$. We define the Lucas sequence $\{U_n\}_{n\geq 0}$ with parameters

Date: July 18, 2006.

Y. Bugeaud is supported by the Austrian Science Fundation FWF, grant M822-N12. S. Siksek is supported by a grant from the UK Engineering and Physical Sciences Research Council.

r, s to be the sequence

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

This is also the sequence given by $U_0 = 0$, $U_1 = 1$ and $U_{n+2} = rU_{n+1} + sU_n$ for all $n \geq 0$. We say that the sequence $\{U_n\}_{n\geq 0}$ is non-degenerate if α/β is not a root of unity. Throughout we suppose, often implicitly, that the Lucas sequence under consideration is non-degenerate. The case $r = s = 1$ corresponds to the Fibonacci sequence $\{F_n\}_{n\geq 0}$.

In what follows, we repeatedly use the following notation. If $T = \{l_1, \ldots, l_t\}$ is a finite set of primes, we write $\overline{T}$ for the set of integers of the form

$$\pm l_1^{x_1} l_2^{x_2} \cdots l_t^{x_t}, \qquad x_i \geq 0.$$

Theorem 1. *(The Finiteness Theorem) Suppose that $\{U_n\}_{n\geq 0}$ is a non-degenerate Lucas sequence, and that T is a finite set of primes. There exists an effectively computable constant c depending only on the sequence $\{U_n\}_{n\geq 0}$ and the set T such that if*

$$\prod_{i=1}^{m} U_{n_i} = \mu y^p, \qquad \mu \in \overline{T}, \quad m,\ n_i,\ y \in \mathbb{Z}^+, \quad p \text{ prime}, \quad m < p, \tag{1}$$

then $n_i < c$ for $i = 1, \ldots, m$.

Our Finiteness Theorem does give an algorithm for solving equation (1), but it is by no means a practical one, since the computable constant c mentioned in the theorem is astronomical. We do however explain a method that should work in practice. Our method is based on the following result, which is also used in the proof of the Finiteness Theorem.

Theorem 2. *(The Reduction Theorem) Suppose that $\{U_n\}_{n\geq 0}$ is a non-degenerate Lucas sequence, and T is a finite set of primes. Suppose $n_1, \ldots, n_m$ satisfy (1), and let q be the* **greatest** *prime divisor of $n_1 \cdots n_m$. Then, there exists a computable positive integer A, and a finite computable set $\mathfrak{Q}$, both depending only on the sequence $\{U_n\}_{n\geq 0}$ and the set T, such that either $q \in \mathfrak{Q}$ or*

$$U_q = \pm A^{(q-1)/2} z^p \tag{2}$$

for some $z \in \mathbb{Z}^+$.

Later on we give a precise and practical recipe for writing down the integer A and set $\mathfrak{Q}$ appearing in the statement of the Reduction Theorem. Thus, applying the method of [8] and [3] to equation (2), we should be able to obtain an upper bound for the prime divisors of $n_1 \ldots n_m$ in equation (1). Once this is done, we explain a completely practical algorithm for solving (1): we call this the Distillation Algorithm. In essence the Reduction Theorem reduces (1) to (2); when r and s are coprime it turns out that $A = 1$ and so we reduce to the equation

$$U_q = z^p.$$

When applied to the Fibonacci sequence, our Distillation Algorithm gives the following results.

Theorem 3. *Let $\{F_n\}_{n\geq 0}$ be the Fibonacci sequence. If*

$$\prod_{i=1}^{m} F_{n_i} = y^p, \qquad n_i,\ m,\ y \in \mathbb{Z}^+, \quad p \text{ prime}, \quad m < p, \tag{3}$$

then the indices n_i belong to the set $\{1, 2, 3, 4, 6, 12\}$. Moreover, the solutions to the equation $F_m F_n = y^p$ with $1 \leq m \leq n$ and $p \geq 2$ are given by

- $m = n$,
- $m,\ n = 1,\ 2$,
- $n = 6,\ m = 1,\ 2,\ 3$,
- $n = 12,\ m = 1,\ 2$.

In fact, if we maintain the assumption $m < p$, then we can be far more ambitious as the following theorem shows.

Theorem 4. *Let $\{F_n\}_{n\geq 0}$ be the Fibonacci sequence. Let T be the set of primes l satisfying $2 \leq l < 541$; this is the set of the first hundred primes. If*

$$\prod_{i=1}^{m} F_{n_i} = \mu y^p, \qquad \mu \in \overline{T}, \quad n_i,\ m,\ y \in \mathbb{Z}^+, \quad p \text{ prime}, \quad m < p, \tag{4}$$

then the indices n_i belong to the set

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 18, 19, \\ 20, 21, 22, 24, 26, 27, 28, 30, 36, 42, 44\}.$$

Our last application is to unidigital numbers: we call a positive integer unidigital if all the digits of its base 10 representation are the same.

Theorem 5. *Let $U_n = (10^n - 1)/(10 - 1)$. The only pairs of unidigital numbers whose products are perfect powers are as follows:*

- *$d\,U_n \times d\,U_n$ where $n \geq 1$ and $d = 1,\ 2,\ \ldots,\ 9$, or*
- *$U_n \times 4\,U_n$ where $n \geq 1$, or*
- *$U_n \times 9\,U_n$ where $n \geq 1$, or*
- *1×8 or 2×4 or 3×9 or 4×8.*

The present paper is organised as follows. In Section 2, we outline the links between the current paper and other papers appearing in the literature. Sections 3 and 5 are devoted to some preliminary results about Lucas sequences that are needed in the proofs of the Theorems. The Reduction Theorem is proved in three stages: A weak version is proved in Section 4, an intermediate version in Section 6, and a full-strength version in Section 7. In particular, the version of the Reduction Theorem in Section 7 gives completely explicit recipes for the set $\mathfrak{Q}$ and the integer A appearing in the statement of the theorem. The Finiteness Theorem is established in Section 8. The Distillation Algorithm, which concerns the practical resolution of equation (1) once equation (2) had been solved, is discussed in Section 9. The proofs of Theorems 3, 4 and 5 are given in Sections 10 and 11. Finally, the last section is devoted to a few concluding remarks. In particular, in the last section, we present a conjecture which if proven would allow us to remove the restriction $m < p$ in the above theorems.

We are grateful to Professor Paulo Ribenboim for suggesting to us to study the equation $F_nF_m = y^p$ which was the starting point of this work. We are also grateful to Mihai Cipu and the referee who suggested corrections to previous versions.

2. Links to Previous Works

In this section, we explain the link between this paper and previous works on Lucas sequences.

The Reduction Theorem is present behind the scenes in many papers concerning Lucas sequences. In a few of these papers, some explicit, though weak, version of the Reduction Theorem appears.

For example, Pethő [15] and Robbins [23], independently, established that if p is prime, $p \geq 3$ and $F_n = y^p$ for some integer y, then either $n = 0$, 1, 2, 6, or there exists a prime $q \mid n$ such that $F_q = y_1^p$ for some integer y_1. Clearly, this result can be regarded as a weak version of the Reduction Theorem for the Fibonacci sequence.

In [11] Inkeri solved the equation $a\frac{x^n-1}{x-1} = y^p$ for $1 < a < x \leq 10$. This was extended by Bugeaud [2] to $1 \leq a < x \leq 100$. Lemma 1 of Bugeaud's paper is again a weak version of the Reduction Theorem for the Lucas sequence $\frac{x^n-1}{x-1}$. That paper also features an argument similar in spirit to our Distillation Algorithm, and relies on the fact that the equation $\frac{x^n-1}{x-1} = y^p$ was solved previously by Bugeaud and Mignotte [5] for $x = z^t$ with $2 \leq z \leq 10^4$ and $t \geq 1$. The results of [2] can now be easily deduced using our Reduction Theorem and Distillation Algorithm.

In [19, 20], Ribenboim gave an algorithm for determining terms of the form Cx^h in Lucas sequences, under various restrictions: for example, for $h \geq 3$ he supposes that the discriminant Δ is positive, and the integers r, s appearing in the definition of the Lucas sequence are coprime. The algorithm is similar in spirit to ours but no version of the Reduction Theorem is made explicit. Even under these restrictions it is somewhat weaker than our algorithm. For example, if we want to solve the equation $F_n = q^m y^p$ for some prime q with the algorithm in [20], we must know the solutions to $F_n = 2^k y^p$. By contrast, our Reduction Theorem and Distillation Algorithm only demand knowledge of the solutions of $F_n = y^p$.

In many other papers one finds tortuous arguments that would have been circumvented using the Reduction Theorem and the Distillation Algorithm. To save other authors the embarrassment, we mention only one example of this which involves some of the authors of this paper. In [7], the equation $F_n = 2^k y^p$ is solved using the previous result on $F_n = y^p$. The ad hoc (one page) argument can now be replaced with a trivial (one line) calculation. The reader is invited to perform this calculation after reading this paper.

The equation $U_nU_m = y^2$ was studied—in various degrees of generality—by several authors: for example by Cohn in [10], by Ribenboim in [16, 17, 18], and by Ribenboim and McDaniel [21, 22]. Notice that this equation is not covered by our Theorems 1, 2, which however do cover the equation $U_nU_m = y^p$ for a prime $p \geq 3$. Thus, our results nicely complement those of Cohn, Ribenboim and McDaniel.

Very recently, Luca and Shorey [12] considered the equation

$$U_nU_{n+d}\cdots U_{n+(k-1)d} = y^p, \qquad \gcd(n, d) = 1,$$

which they showed has finitely many solutions. They also established that the product of consecutive Fibonacci numbers is never a positive perfect power except for the trivial case $F_1F_2 = 1$.

Moreover, independently, Pethő [14] and Shorey and Stewart [24] established that every binary recurrence sequence contains at most finitely many perfect powers. This is more general than our Finiteness Theorem for $m = 1$. However, we find in the literature no result comparable with our Finiteness Theorem for $m > 1$.

3. Preliminaries I

We keep the notation from the Introduction. Throughout, we denote by S the set of prime factors of 2Δ, by S_1 the set of prime factors of $\gcd(r, s)$, and by S_2 the set of prime factors of Δ not belonging to S_1. We write $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$; this is either $\mathbb{Q}$ or a quadratic extension of it. We write $\mathcal{O}$ for the ring of integers of K.

Notation. If $k \mid n$ are positive integers, we write

$$U_{n,k} = \frac{U_n}{U_k}.$$

Clearly, $U_{n,k}$ is a rational integer.

Lemma 1. *If m, n are positive integers, and $k = \gcd(m, n)$, then*

$$\gcd(U_m, U_n) = A\,U_k,$$

where $A \in \overline{S_1}$.

Proof. It is clear that U_k divides both U_m and U_n. Hence, $A = \gcd(U_m, U_n)/U_k$ is an integer. It remains to check that A is in $\overline{S_1}$.

We work with polynomials in a variable X. Using induction on $\max\{m, n\}$ as well as the formula

$$(X^m - 1) \ - X^{m-n}(X^n - 1) = X^{m-n} - 1 \qquad \text{whenever } m > n,$$

one proves the existence of polynomials $u(X)$ and $v(X)$ in $\mathbb{Z}[X]$ such that ([1])

$$u(X)(X^m - 1) + v(X)(X^n - 1) = X^k - 1.$$

Homogenising the above relation, it follows that there exists an integer $t \geq 1$ and homogeneous polynomials $u(X, Y)$ and $v(X, Y)$ with integer coefficients such that

$$u(X, Y)\,(X^m - Y^m) + v(X, Y)\,(X^n - Y^n) = Y^t\left(X^k - Y^k\right). \tag{5}$$

Specialising relation (5) in $(X, Y) = (\alpha, \beta)$, we get the relation

$$u(\alpha, \beta)\,U_{m,k} + v(\alpha, \beta)\,U_{n,k} = \beta^t, \qquad \text{where } \ u(\alpha, \beta),\ v(\alpha, \beta) \in \mathcal{O}.$$

Assume now that q is a prime dividing A. Let $\mathfrak{q}$ be a prime ideal of $\mathcal{O}$ dividing q. Then $\mathfrak{q}$ divides both $U_{n,k}$ and $U_{m,k}$ and by the above relation $\mathfrak{q} \mid \beta^t$. Since $\mathfrak{q}$ is prime, we get that $\mathfrak{q} \mid \beta$. Since α and β can be interchanged, we get that $\mathfrak{q}$ divides α as well, therefore it also divides $r = \alpha + \beta$ and $s = \alpha\beta$, which completes the proof of the lemma. □

Lemma 2. *Suppose that $n = kq$ where n, k and q are positive integers. Then $\gcd(U_k, U_{n,k})$ divides $q\epsilon$ for some $\epsilon \in \overline{S}$.*

[1] One knows from cyclotomy that $X^k - 1$ is the greatest common divisor of $X^m - 1$ and $X^n - 1$. Thus the existence of $u(X)$, $v(X) \in \mathbb{Q}[X]$ satisfying the given relation follows from Euclid's Algorithm. Here we need a stronger result, namely that we can take $u(X)$, $v(X) \in \mathbb{Z}[X]$.

Proof. We note that

$$U_k = \frac{\alpha^k - \beta^k}{\alpha - \beta},$$

and

$$U_{n,k} = \alpha^{k(q-1)} + \alpha^{k(q-2)}\beta^k + \cdots + \beta^{k(q-1)}.$$

Let $g = \gcd(U_k, U_{n,k})$. Since $g \mid U_k$, we see that

$$\alpha^k \equiv \beta^k \pmod{g\mathcal{O}}.$$

But $g \mid U_{n,k}$, so

$$0 \equiv \alpha^{k(q-1)} + \alpha^{k(q-2)}\beta^k + \cdots + \beta^{k(q-1)} \equiv q\alpha^{k(q-1)} \pmod{g\mathcal{O}}.$$

Thus, $g\mathcal{O}$ divides the ideal $q\alpha^{k(q-1)}\mathcal{O}$ and similarly the ideal $q\beta^{k(q-1)}\mathcal{O}$. The Lemma follows since the greatest common divisor of the ideals $\alpha\mathcal{O}$ and $\beta\mathcal{O}$ divides Δ. □

Lemma 3. *Suppose that $k \geq 1$ is an integer and $q \notin S$ is prime. If $q \mid U_k$, then $\gcd(k, q^2 - 1) > 1$.*

Proof. We may suppose that $k > 1$. Let $\mathfrak{q}$ be a prime ideal of $\mathcal{O}$ dividing q. Then

$$\alpha^k \equiv \beta^k \pmod{\mathfrak{q}}.$$

We see that if $\mathfrak{q}$ divides either α or β, then it divides both, and hence $q \mid \Delta$, which contradicts our assumption that $q \notin S$. We deduce that $\mathfrak{q}$ divides neither α, nor β. Moreover, again since $q \nmid \Delta$, we see that $\alpha - \beta$ is not divisible by $\mathfrak{q}$. We deduce that

$$\frac{\alpha}{\beta} \not\equiv 1, \qquad \left(\frac{\alpha}{\beta}\right)^k \equiv 1,$$

in the finite field $\mathcal{O}/\mathfrak{q}$. However, the group $(\mathcal{O}/\mathfrak{q})^*$ has order either $q - 1$ or $q^2 - 1$. Thus,

$$\gcd(k, q^2 - 1) > 1.$$

□

Lemma 4. *Suppose that k is odd and $q \notin S$ is prime. Suppose that for every prime $l \mid k$, we have $l \geq q$. Then $q \nmid U_k$.*

Proof. Suppose that k is odd, $q \notin S$ and $q \mid U_k$. By Lemma 3,

$$\gcd(k, q^2 - 1) > 1.$$

Since k is odd, there is some odd prime l satisfying $l \mid k$ and $l \mid (q^2 - 1)$. But all odd prime divisors of $q^2 - 1$ are strictly smaller than q. The Lemma follows. □

Lemma 5. *Suppose that n is an integer and let q be its* **smallest** *prime factor. Write $n = kq$. Then $\gcd(U_k, U_{n,k}) \in \overline{S}$.*

Proof. By Lemma 2, $\gcd(U_k, U_{n,k})$ divides $q\epsilon$, where $\epsilon \in \overline{S}$. If n is even, then $q = 2$ is in S and there is nothing more to prove. Likewise, there is nothing more to prove if $q \in S$.

Thus, suppose that n is odd and that $q \notin S$. Now Lemma 4 immediately gives $q \nmid U_k$, and this completes the proof. □

Lemma 6. *Let $n > 1$ be an integer and let q be its* **greatest** *prime factor. Then*

$$\gcd(U_q, U_{n,q}) \in \overline{S}.$$

Proof. Write $n = q_1 q_2 \cdots q_t$ with $q_1 \leq q_2 \leq \ldots \leq q_t = q$, all prime. Let $k_i = q_t q_{t-1} \cdots q_i$. We use induction to show, for $i = 2, \ldots, t$, that

$$\gcd(U_{k_i}, U_{n,k_i}) \in \overline{S}. \tag{6}$$

The lemma follows at once from this by observing that $k_t = q$.

For $i = 2$, we have $n = k_2 q_1$ and q_1 is the smallest prime factor of n. Thus, the case $i = 2$ follows from Lemma 5.

Now suppose $2 \leq i < t$ and that (6) holds. Observe that $U_{k_{i+1}} \mid U_{k_i}$, so we get

$$\gcd(U_{k_{i+1}}, U_{n,k_i}) \in \overline{S}.$$

Moreover, q_i is the smallest prime factor of k_i, and $k_i = k_{i+1} q_i$. Hence, by Lemma 5, we have

$$\gcd(U_{k_{i+1}}, U_{k_i,k_{i+1}}) \in \overline{S}.$$

From the last two inclusions and the fact that

$$U_{n,k_{i+1}} = U_{n,k_i} U_{k_i,k_{i+1}},$$

we deduce that

$$\gcd(U_{k_{i+1}}, U_{n,k_{i+1}}) \in \overline{S}.$$

This completes the proof. □

4. A Weak Version of the Reduction Theorem

We now prove the following weak version of the Reduction Theorem.

Lemma 7. *Suppose that $\{U_n\}_{n \geq 0}$ is a non-degenerate Lucas sequence and T is a finite set of primes. Suppose $n_1, \ldots, n_m$ satisfy (1). Let q be the* **greatest** *prime divisor of $n_1 \cdots n_m$. Then*

$$U_q = \eta z^p \tag{7}$$

for some $\eta \in \overline{S \cup T}$ and $z \in \mathbb{Z}^+$.

Proof. Suppose that $n_1, \ldots, n_m$ satisfy (1). Let q be the **greatest** prime divisor of $n_1 \cdots n_m$. Reorder the indices so that q divides $n_1, \ldots, n_{m'}$ and q does not divide the others. By Lemma 6, we can, for $i = 1, \ldots, m'$, write

$$U_{n_i} = U_q U_{n_i,q}$$

with $\gcd(U_q, U_{n_i,q}) \in \overline{S}$. Moreover, for $i > m'$, Lemma 1 gives $\gcd(U_q, U_{n_i}) \in \overline{S}$. It follows from (1) that there exists an integer G with

$$U_q^{m'} G = \mu y^p,$$

where the greatest common divisor of U_q and G is in $\overline{S}$. Hence,

$$U_q^{m'} = \eta' z'^p$$

for some $\eta' \in \overline{S \cup T}$ and $z' \in \mathbb{Z}^+$. Now recall the assumption $m < p$ made in (1). Thus, $m' \leq m < p$. So,

$$U_q = \eta z^p,$$

where $\eta \in \overline{S \cup T}$ and $z \in \mathbb{Z}^+$. This completes the proof of the Lemma. □

5. Preliminaries II

Let S_1 and S_2 be as in Section 3; namely S_1 is set of primes dividing $\gcd(r, s)$, and S_2 is the set of primes dividing Δ but not $\gcd(r, s)$.

Lemma 8. *Suppose that $l \notin S_1$ is a prime.*

(i) *If $l \mid s$ then $l \nmid U_n$ for all $n \geq 1$.*
(ii) *If $l \in S_2$ then $l \mid U_n$ if and only if $l \mid n$.*

Proof. For (i), suppose $l \mid s$. Then $l \nmid r$. It is straightforward to show that $U_n \equiv r^{n-1} \pmod{l}$ and so (i) follows.

For (ii), suppose $l \in S_2$. Let $\mathbb{Q}_l$ be the l-adic completion of $\mathbb{Q}$ and K_π be a completion of K with $\pi \mid l$. Write $\mathcal{O}_\pi$ for the π-adic integers. Since $l \in S_2$, we see that $\pi \nmid \alpha\beta$ but $\pi^t \mid\mid (\alpha - \beta)$ for some $t \geq 1$. Hence,

$$\frac{\alpha}{\beta} = 1 + \omega\pi^t$$

for some $\omega \in \mathcal{O}_\pi$ with $\pi \nmid \omega$. Then

$$\left(\frac{\alpha}{\beta}\right)^n \equiv 1 + n\omega\pi^t \pmod{\pi^{2t}},$$

which shows that

$$\alpha^n - \beta^n \equiv n\omega\beta^n\pi^t \pmod{\pi^{2t}}.$$

It follows that

$$U_n \equiv n\beta^{n-1} \pmod{\pi^t},$$

which proves (ii). □

Lemma 9. *Suppose that $l \nmid s\Delta$ is a prime. Then there exists an integer $m_l > 1$ such that $l^t \mid\mid U_{m_l}$ for some $t \geq 1$ and $l \nmid U_m$ for all $1 \leq m < m_l$. Moreover, for $n \geq 1$*

(i) *if $l \mid U_n$, then $m_l \mid n$;*
(ii) *$l^t \mid\mid U_n$ if and only if $m_l \mid n$ and $l \nmid n$;*
(iii) *$l^{t+1} \mid U_n$ if and only if $l\, m_l \mid n$.*

Remark. The integer m_l defined above is called *the rank of first appearance* of the prime l for the Lucas sequence $\{U_n\}$ (see [20]).

Proof. Suppose that $l \nmid s\Delta$ and let $\mathbb{Q}_l$, K_π and $\mathcal{O}_\pi$ be as in the proof of Lemma 8. Then $\pi \nmid \alpha\beta(\alpha - \beta)$ and

$$\alpha^{l^2-1} \equiv \beta^{l^2-1} \equiv 1 \pmod{\pi}.$$

It follows that $l \mid U_{l^2-1}$. Thus, there is certainly an $m > 1$ such that $l \mid U_m$, and we let m_l be the least such m, and $t \geq 1$ be such that $l^t \mid\mid U_{m_l}$.

For (i), suppose that $n > 1$ and $l \mid U_n$. By assumption, $l \nmid s$ and so $l \notin S_1$; it follows from Lemma 1 that $l \mid U_m$ where $m = \gcd(n, m_l)$. From the minimality of m_l, we deduce that $m = m_l$ and so $m_l \mid n$ as desired.

Let us now prove (ii) and (iii). Note that

$$\left(\frac{\alpha}{\beta}\right)^{m_l} = 1 + \omega\pi^t$$

for some $\omega \in \mathcal{O}_\pi$ and $\pi \nmid \omega$. Suppose now that $n = km_l$. Then

$$\left(\frac{\alpha}{\beta}\right)^n \equiv 1 + k\omega\pi^t \pmod{\pi^{2t}}.$$

The lemma follows immediately. □

Finally, for the proof of Theorem 1 we will need the following theorem, which is a restatement of Theorem 9.6 from [25].

Theorem 6. *Suppose that $\{U_n\}_{n\geq 0}$ is a non-degenerate Lucas sequence, and T is a finite set of primes. There is an effectively computable constant c depending only on the sequence $\{U_n\}_{n\geq 0}$ and the set T such that if*

$$U_n = \mu y^p, \qquad \mu \in \overline{T}, \quad n,\ y \in \mathbb{Z}^+, \quad p \geq 2,$$

then $n < c$.

6. An Intermediate Version of the Reduction Theorem

In Section 4 we proved a weak version of the Reduction Theorem. We now prove a stronger version of that result—though one which is still weaker than the Reduction Theorem itself. Later on we will deduce the Reduction Theorem from the version we prove here.

We introduce another Lucas sequence $\{U'_n\}$ associated to $\{U_n\}$ whose arithmetic is somewhat simpler. For $l \in S_1$ let

$$\xi_l = \min\left(\mathrm{ord}_l(r), \left\lfloor \frac{\mathrm{ord}_l(s)}{2} \right\rfloor\right), \tag{8}$$

and

$$g = \prod_{l \in S_1} l^{\xi_l}, \qquad r' = \frac{r}{g}, \qquad s' = \frac{s}{g^2}. \tag{9}$$

Clearly r' and s' are integers. We let $\{U'_n\}_{n\geq 0}$ be the Lucas sequence with parameters r' and s'. It is easy to see that

$$U_n = g^{n-1} U'_n \tag{10}$$

for positive integers n. We define Δ', S', S'_1, S'_2 for sequence $\{U'_n\}$ in exactly the same way as we defined the corresponding quantities for $\{U_n\}$. If l is prime, we write m'_l for the rank of first appearance of the prime l for the Lucas sequence $\{U'_n\}$.

Now we introduce some terminology and notation that will be helpful in this section and the rest of the paper. Suppose H is a finite set of primes and B is a non-zero integer. We say that B is a perfect power up to H if $B = \eta x^p$ for some $\eta \in \overline{H}$, positive integer x and prime p.

As for the notation, we define

$$\mathfrak{Q}' = S'_2 \cup \left\{m'_l \ :\ l \in S \cup T,\ l \nmid s'\Delta' \text{ and } m'_l \text{ is prime}\right\},$$

and

$$\mathfrak{Q} = \left\{q \in \mathfrak{Q}' \cup \{2\} \ :\ U_q \text{ is a perfect power up to } S \cup T\right\}. \tag{11}$$

Lemma 10. *Let $\mathfrak{Q}$ be as above. Suppose that the n_i satisfy (1), and let q be the largest prime divisor of $n_1 \cdots n_m$. Then either $q \in \mathfrak{Q}$ or q is odd and*

$$U'_q = \epsilon z^p \tag{12}$$

for some $\epsilon \in \overline{S'_1}$ and $z \in \mathbb{Z}^+$.

Proof. From the weak version of the Reduction Theorem (Lemma 7), we know that q satisfies (7) for some $\eta \in \overline{S \cup T}$ and $z \in \mathbb{Z}^+$. If $q = 2$ then we see that $q \in \mathfrak{Q}$ and we are finished. Suppose from now on that q is odd.

From the relation (10) and the fact that $g \in \overline{S_1} \subset \overline{S \cup T}$ we see that U'_q satisfies (12) for some $\epsilon \in \overline{S \cup T}$ and $z \in \mathbb{Z}^+$. To prove the lemma, it is clearly sufficient to show that if $\epsilon \notin \overline{S'_1}$ then $q \in \mathfrak{Q}$, or equivalently here that $q \in \mathfrak{Q}'$.

Suppose that $\epsilon \notin \overline{S'_1}$. Then ϵ is divisible by some prime $l \in S \cup T$ such that $l \notin S'_1$. But $\epsilon \mid U'_q$ and so $l \mid U'_q$. We now utilise Lemma 8 with the sequence $\{U'_n\}$ instead of $\{U_n\}$. First we see that $l \nmid s'$. If $l \in S'_2$ then $l \mid q$ and so $q = l \in S'_2 \subseteq \mathfrak{Q}'$ and we are finished.

From now on, we may suppose that $l \nmid s'$ and $l \notin S'_1 \cup S'_2$; in other words $l \nmid s'\Delta'$. Now part (i) of Lemma 9 gives that $m'_l \mid q$. But q is prime, and so $m'_l = q$. Hence, $q \in \mathfrak{Q}'$ as required. □

7. Proof of the Reduction Theorem

In this section we finally prove the Reduction Theorem in its full strength. We continue with the notation of the previous section; in particular ξ_l is given by (8). For $l \in S_1$ we define

$$\zeta_l = \begin{cases} 2\xi_l + 1 & \text{if } l \in S'_1, \\ 2\xi_l & \text{if } l \notin S'_1. \end{cases}$$

Let

$$A = \prod_{l \in S_1} l^{\zeta_l}.$$

We are now ready to state and prove the following totally explicit version of the Reduction Theorem.

Lemma 11. *Let $\mathfrak{Q}$ be as in* (11) *and A be as above. Suppose that the n_i satisfy (1), and let q be the largest prime divisor of $n_1 \cdots n_m$. Then either $q \in \mathfrak{Q}$ or q is odd and*

$$U_q = \pm A^{(q-1)/2} z^p \tag{13}$$

for some $z \in \mathbb{Z}^+$.

Proof. Suppose that $q \notin \mathfrak{Q}$. Lemma 10 tells us that q is odd and $U'_q = \epsilon z^p$ for some $\epsilon \in \overline{S'_1}$ and $z \in \mathbb{Z}^+$. Moreover, we know that $U_q = g^{q-1} U'_q$ with g given by (9). To prove the Lemma it is sufficient to show, for $l \in S_1$ that

$$\mathrm{ord}_l(U'_q) = \begin{cases} (q-1)/2, & \text{if } l \in S'_1. \\ 0, & \text{if } l \notin S'_1. \end{cases}$$

Suppose first that $l \in S'_1$; in other words $l \mid r'$ and $l \mid s'$. Pondering the definitions (8) and (9) we convince ourselves that $l \mid\mid s'$. A straightforward induction enables us to deduce that

$$\mathrm{ord}_l(U'_n) = \frac{n-1}{2} \quad \text{if } n \text{ is odd}, \qquad \mathrm{ord}_l(U'_n) \geq \frac{n}{2} \quad \text{if } n \text{ is even}.$$

This establishes the result we want if $l \in S_1'$.

Suppose finally that $l \notin S_1'$. We would like to show that $\mathrm{ord}_l(U_q') = 0$; to this end we suppose that $l \mid U_q'$ and deduce a contradiction. Now from $l \notin S'$ and $l \in S_1 \subset S \subset S \cup T$ it is easy to deduce, as in the proof of Lemma 10, that $q \in \mathfrak{Q}$. This gives the desired contradiction and completes the proof. □

8. Proof of the Finiteness Theorem

We now come to prove the Finiteness Theorem. Suppose that n_i satisfy (1). Using the Reduction Theorem and Theorem 6, we see that there exists a finite computable set R containing all of the prime divisors q of $n_1, \ldots, n_m$. Now the Finiteness Theorem follows immediately from Theorem 6 and the following lemma.

Lemma 12. *Let R be a set of primes containing all the prime divisors of $n_1, \ldots, n_m$. If $k \geq 1$ divides at least one of the n_i, then*

$$U_k = \zeta w^p$$

for some $\zeta \in \overline{R \cup S \cup T}$ and $w \in \mathbb{Z}^+$. In other words, U_k is a perfect power up to $R \cup S \cup T$.

Proof. We prove the lemma by contradiction. Suppose that $k > 1$ is the smallest positive integer dividing one of the n_i's for which the lemma fails. Thus, there is some prime $l \notin R \cup S \cup T$ such that $l^t \mid\mid U_k$ and $p \nmid t$.

As $l \notin S$, we see that $l \nmid \Delta$. From Lemma 8, we know that $l \nmid s$. Now part (i) of Lemma 9 tells us that $m_l \mid k$. Moreover, $l \nmid k$ since $l \notin R$ and all the prime divisors of k (which are among the prime divisors of some n_i) belong to R. Now parts (ii) and (iii) of Lemma 9 give $l^t \mid\mid U_{m_l}$.

There are two possibilities. The first is that $m_l < k$. By the minimality of k, we see that $p \mid t$ giving a contradiction.

The second possibility is that $m_l = k$. Rearrange the n_i so that m_l divides $n_1, \ldots, n_{m'}$ and does not divide the others. By Lemma 9 again, $l^t \mid\mid U_{n_i}$ for $i = 1, \ldots, m'$, and $l \nmid U_{n_i}$ for $i > m'$. From equation (1), we see that $p \mid tm'$, where we know that $1 \leq m' \leq m < p$. Hence $p \mid t$, again giving a contradiction. □

9. The Distillation Algorithm

In this section, we study the practical resolution of equation (1). The first step is to solve the equation

$$U_q = \pm A^{(q-1)/2} z^p, \qquad p \text{ prime}, \quad q \text{ odd prime}, \quad z \in \mathbb{Z}^+. \tag{14}$$

Until recently, solving such an equation has been a formidable task in most cases, but is now relatively practical (see [3] as well as [8], [9] and the remarks in Section 12). The method of [3] combines the classical approach via estimates for linear forms in two or three logarithms (to bound the exponent p), with the modular approach via Frey curves and Ribet's level-lowering theorem. This method is not an algorithm in the strict sense of the word, but is a practical and reliable strategy that should solve this equation.

We suppose equation (14) has been solved. We now explain an algorithm—which we call the Distillation Algorithm—that enables us to write down a finite set containing all the possibilities for the indices n_i appearing in equation (1). For readability we will not write up the algorithm in a very formal way.

Step 1: Let

$$\mathcal{Q} = \{q \ : \ q \text{ is a solution to (14)}\} \cup \mathfrak{Q},$$

where $\mathfrak{Q}$ is as in Section 6. By Lemma 11, the greatest prime divisor of $n_1 \cdots n_m$ belongs to $\mathcal{Q}$. Let $q^* = \max(\mathcal{Q})$ and

$$R = \{q \ : \ q \text{ is prime and } q \le q^*\}.$$

Thus, all the prime divisors of $n_1, \ldots, n_m$ belong to R.

Step 2: Our second step is to refine R using Lemma 12; our objective is to replace R by a subset that still contains all the possible prime divisors of the n_i. We loop through the primes $q \in R$ and eliminate all those such that U_q is not a perfect power up to $R \cup S \cup T$. We repeat this until we have looped through all of the elements of R without eliminating a single element. Now write

$$R = \{q_1, \ldots, q_t\}.$$

Step 3: Our third step is to determine, for each $q_j \in R$, an upper bound for the power of q_j dividing the n_i. Fix q in R and let $a \ge 1$ be the smallest value such that U_{q^a} is not a power up to $R \cup S \cup T$. By Lemma 12, we know that q^a does not divide any of the n_i. Write a_j for the a that corresponds to q_j, and let $b_j = a_j - 1$. Thus, the exponents of q_j in the factorisations of the n_i are at most b_j.

Step 4: We now let N be the set of integers n such that

- n is of the form $\prod q_j^{x_j}$ with $0 \le x_j \le b_j$.
- U_k is a perfect power up to $R \cup S \cup T$ for all positive divisors k of n.

It follows from the above and Lemma 12 again that the n_i belong to this finite set N.

Step 5: We refine N in a way that it will still contain all of the possible n_i. We loop through $n \in N$. Suppose there is some prime $l \in R \cup S \backslash T$ such that $l \mid\mid U_n$, but $l \nmid U_{n'}$ for all $n' \ne n$ in N. We deduce from (1) that $n_i \ne n$ for all i (here we need again the hypothesis $m < p$), and so n can be eliminated from the set of possible indices N. We repeat this until we have looped through all of the elements of N once without eliminating any elements.

The set N produced by Step 5 is algorithm's output.

10. Powers from Products of Unidigital Numbers

In this section, we prove Theorem 5 concerning unidigital numbers. We leave the proofs of Theorems 3 and 4 until the next section.

Proof of Theorem 5. Let $U_n = (10^n - 1)/(10 - 1)$. A unidigital number is a positive integer of the form dU_n for some $n \ge 1$ and $d = 1, 2, \ldots, 9$. Thus, we want to solve the equation

$$d_1 d_2 U_n U_m = x^p, \qquad d_1,\ d_2 = 1,\ 2,\ \ldots,\ 9, \quad p \text{ is prime.}$$

We will show that $m = n = 1$ if $p > 2$ and $m = n$ if $p = 2$, which immediately gives the theorem.

It is clear that

$$U_n U_m = 2^a 3^b 5^c 7^d y^p.$$

Now 2, 5 cannot divide the product $U_n U_m$. Hence, we reduce to

$$U_n U_m = 3^b 7^d y^p.$$

Suppose first that $p > 2$. We note here that the two sequences $\{U_n\}$ and $\{U'_n\}$ are identical. In the usual notation, $r = 11$, $s = -10$, $\Delta = 81$, $S = \{2, 3\}$, $S_1 = \emptyset$, $S_2 = \{3\}$ and $T = \{3, 7\}$. Write q for the greatest prime dividing mn. From Lemma 11, we have that $q \in \mathfrak{Q}$ or $U_q = z^p$. But the equation $U_q = z^p$ has no solutions (see [4]). Hence, $q \in \mathfrak{Q}$. Now we apply the recipes in Section 6 to compute $\mathfrak{Q}'$ and $\mathfrak{Q}$. We find that $\mathfrak{Q}' = \{3\}$; for this, we need $m_7 = 6$ which is not a prime. Furthermore, $U_2 = 11$ and $U_3 = 3 \times 37$ which are not perfect powers up to $S \cup T$, and hence $\mathfrak{Q} = \emptyset$. We deduce that the largest prime divisor of mn does not exist. In other words, $m = n = 1$ as required.

We now turn our attention to the case $p = 2$. In this case,

$$U_m U_n = 3^b 7^d y^2. \tag{15}$$

We assume that b, $d \in \{0, 1\}$.

We first treat the case $b = d = 0$ and show that $m = n$. Writing $D = \gcd(m, n)$, we get that both U_m/U_D and U_n/U_D are squares. With $x = 10^D$, these equations show that $(x^{m/D} - 1)/(x - 1)$ and $(x^{n/D} - 1)/(x - 1)$ are perfect squares. The equation

$$\frac{x^t - 1}{x - 1} = y^2$$

was solved by Ljunggren (see [13]); its only solutions with $x > 1$ and $t > 2$ are given by $(x, t) = (3, 5)$, $(7, 4)$. Hence, m/D and n/D are 1 or 2, which shows that $m = n$ or $m = 2n$. In the latter case, we get that $U_{2n}/U_n = 10^n + 1$ is a perfect square, which is impossible modulo 3. Hence, $m = n$ as desired.

We now assume that $b, d \in \{0, 1\}$ are not both zero, and deduce a contradiction. Consider equation (15) modulo 5. Clearly, $U_m U_n \equiv 1 \pmod 5$ and $y^2 \equiv \pm 1 \pmod 5$. We deduce that $b = d = 1$. Furthermore, U_n is 1, 3, and -1 modulo 8 according to whether $n = 1$, $n = 2$, and $n \geq 3$, respectively. But $3^b 7^d y^2 = 21y^2 \equiv 5 \pmod 8$. Assuming without loss of generality that $m \leq n$, we see that $m = 2$ and $n \geq 3$. Since $U_2 = 11$, we can rewrite equation (15) as

$$U_n = 3 \times 7 \times 11 \times y_1^2. \tag{16}$$

Let q be the largest prime factor of n. We may now apply Lemma 11 with S, S_1, S_2 as before, and $T = \{3, 7, 11\}$. We deduce that $U_q = z^2$ or $q \in \mathfrak{Q}$. Again $U_q = z^2$ has no solutions by Ljunggren's result. Moreover, $\mathfrak{Q}' = \{2, 3\}$ (for this we need $m_{11} = 2$) and $\mathfrak{Q} = \{2\}$. Hence, the only possible prime divisor of n is 2. Moreover, $U_4 = 11 \times 101$, so Lemma 12 implies that $4 \nmid n$. Hence, $n = 1$ or 2. This contradicts (16). □

11. Powers from Products of Fibonacci Numbers

We now come to the proofs of Theorems 3 and 4. We give the proof of Theorem 3 first because it is simpler and the reader will be able to verify all the calculations without the need for any programming.

Proof of Theorem 3. Here, $r = s = 1$, $\Delta = 5$, $S = \{2, 5\}$, $S_1 = \emptyset$, $S_2 = \{5\}$ and $T = \emptyset$.

Now note that we have $m_2 = 3$. In the notation of Section 6, we see that $\mathfrak{Q}' = \{3, 5\}$ and $\mathfrak{Q} = \{2, 3, 5\}$. As indicated in the introduction, the only solutions

to $F_n = y^p$ and given by $n = 0,\ 1,\ 2,\ 6,\ 12$. We now go through the steps of the Distillation Algorithm.

Step 1: This step tells us the greatest prime divisor q of the n_i belongs to the set $\mathcal{Q} = \{2, 3, 5\}$, and so all the divisors of the n_i belong to the set $R = \{2, 3, 5\}$.

Step 2: This step does not change R which is not surprising as R is already very small.

Step 3: Now note the prime factorisations

$$F_8 = 3 \times 7, \quad F_9 = 2 \times 17, \quad F_{25} = 5 \times 3001.$$

Thus, the exponents of 2, 3, 5 in the factorisations of the n_i are bounded respectively by 2, 1, 1.

Step 4: We deduce that the n_i belong to the set

$$\{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}.$$

We eliminate from this set all the elements n such that there is some $k \mid n$ for which F_k is not a perfect power up to $R \cup S \cup T = \{2, 3, 5\}$. Thus, since $F_{10} = 55$ and $F_{15} = 610$, we can eliminate 10, 15, 20, 30, 60. It turns out that we cannot eliminate any other n in this step. Hence, the n_i belong to $N = \{1, 2, 3, 4, 5, 6, 12\}$.

Step 5 Applying the last step of the algorithm eliminates 5 from N. This is because $F_5 = 5$ and $5 \nmid F_n$ for $n \neq 5$ in the set N. Thus the n_i belong to $N = \{1, 2, 3, 4, 6, 12\}$ as required in the first part of the theorem.

To prove the last assertion of the theorem, it only remains to solve the equation $F_m F_n = y^2$. This has been done by Cohn in [10], and independently but much later by Ribenboim in [16, Proposition 2]. They showed that either $m,\ n \in \{1, 2, 3, 6, 12\}$, or $m = n$. □

We point out that the set of possible indices $\{1, 2, 3, 4, 6, 12\}$ in Theorem 3 cannot be reduced further. Indeed, $F_1 = F_2 = 1$. Thus, equation (3) reduces to

$$F_3{}^a \cdot F_4{}^b \cdot F_6{}^c \cdot F_{12}{}^d = y^p \tag{17}$$

where $a,\ b,\ c,\ d \geq 0$ satisfy $a+b+c+d < p$ because of the condition $m < p$. We want to show that there is, for large enough p, a solution with $a,\ b,\ c,\ d > 0$; this certainly shows that the set of possible indices cannot be reduced further. By considering the prime-power factorisation, we deduce that equation (17) is equivalent to

$$a + 3c + 4d \equiv b + 2d \equiv 0 \pmod{p}. \tag{18}$$

Thus, a quadruple of integers (a, b, c, d) is a solution to equation (17) if and only if it belongs to the lattice (18). The conditions $a + b + c + d < p$ and $a,\ b,\ c,\ d > 0$ are equivalent to saying that the quadruple belongs to the convex set

$$\left\{(\delta_1, \ldots, \delta_4) \in \mathbb{R}^4 \ : \quad \delta_1, \ldots, \delta_4 > 0,\ \delta_1 + \cdots + \delta_4 < p\right\}. \tag{19}$$

The convex set has volume $p^4/24$, whilst the lattice has determinant p^2. Hence, the expected number of solutions is roughly $p^2/24$.

We finally turn to the proof of Theorem 4.

Proof of Theorem 4. We programmed our Distillation Algorithm using `pari/gp`. The theorem follows from applying our algorithm to the Fibonacci sequence with T being the set of the first hundred primes: $T = \{2, 3, 5, \ldots, 541\}$. We give only the output at each stage of the algorithm. Before applying the algorithm we have

$$\mathfrak{Q}' = \{3, 5, 7, 11, 13, 19, 37, 59, 67, 79, 97, 139, 157, 199, 229\},$$

and

$$\mathfrak{Q} = \{2, 3, 5, 7, 11, 13, 19\}.$$

Step 1: $\mathcal{Q} = \{2, 3, 5, 7, 11, 13, 19\}$ and $R = \{2, 3, 5, 7, 11, 13, 17, 19\}$.

Step 2: $R = \{2, 3, 5, 7, 11, 13, 19\}$.

Step 3: The bounds for the exponents of the primes in the prime factorisations of the n_i are all 1 except for the exponents of 2 and 3 where these bounds are 4 and 3, respectively.

Steps 4 and 5: These steps both give

$$N = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 18, \\ 19, 20, 21, 22, 24, 26, 27, 28, 30, 36, 42, 44\},$$

as required in the statement of the theorem. □

12. Concluding Remarks

The essence of this paper is the Reduction Theorem. To be able to apply the Reduction Theorem one needs to solve equations of the form (2). The papers [3], [8] are primarily concerned with the equation $U_n = y^p$. The purpose in this section is to convince the reader who is familiar with [3], [8] that the techniques of those papers are applicable to (2).

An equation of the form (2) yields a linear form in logarithms and this can be used to bound the exponent p. With current bounds for linear forms in logarithms we know the following:

- If the linear form involves 4 or more logarithms then the bound obtained for p will be hopelessly large and of no practical use in solving (2).
- If the linear form involves 3 logarithms then the bound for p will be quite reasonable—say around 10^9.
- If the linear form involves 2 logarithms then the bound for p will be small—say around 1000.

Since we want to bound p we may assume that p is odd. Equation (2) can be rewritten as

$$\frac{\alpha^q - \beta^q}{\alpha - \beta} = A^{(q-1)/2} z^p; \tag{20}$$

here we absorbed the $\pm$ into the z^p. Let us assume that α and β are real numbers. We deduce that

$$\frac{\alpha}{\alpha - \beta} \left(\frac{\alpha^2}{A} \right)^{(q-1)/2} z^{-p} - 1 = O(|z|^{-p}). \tag{21}$$

This clearly results in a linear form in 3 logarithms, and so yields a reasonable bound for p.

Now the modular approach should be used. In particular 'the method of predicting exponents' [26] should, for large enough p, predict q modulo p. At this stage we need the bound for p obtained from the linear form in 3 logarithms. This method of predicting exponents should show that $q \equiv q_1, \ldots, q_t \pmod{p}$ for some finite list of congruence classes $q_1, \ldots, q_t$ that does not depend on p. Assuming that $q \equiv q_i \pmod{p}$ we can rewrite (21) as

$$B_i \left(\frac{C_i^{k_i}}{z} \right)^p - 1 = O(|z|^{-p})$$

for a suitable algebraic constants B_i, C_i and integer k_i. This now results in a linear form in 2 logarithms which gives a very good bound for p.

Once these two steps are over and we have a very good bound for p the rest of the techniques in [3], [8] should enable us to complete the resolution of (2).

When α and β are complex non-real numbers, we use estimates for linear forms in 3 non-Archimedean logarithms to derive from (20) a reasonable upper bound for p. Then, applying as above 'the method of predicting exponents' enables us to use estimates for linear forms in 2 non-Archimedean logarithms, thus to get a very good bound for p.

We finally make a remark about the condition $m < p$ in Theorems 1 and 2. The situation is much more complicated without this condition, since otherwise equation (1) has obviously infinitely many solutions (recall that the indices n_i are not assumed to be distinct). We present a conjecture that allows us to predict that apart from finitely many solutions, the solutions are essentially diagonal.

If n is a positive integer then a *primitive divisor* of U_n is a prime l dividing U_n but not dividing U_m for all $1 \leq m < n$. A celebrated theorem of Bilu, Hanrot and Voutier [1] states that if U_n is a non-degenerate Lucas sequence and $n > 30$ then U_n has a primitive divisor (under the additional assumption that associated parameters r, s are coprime). We shall call l a *primary divisor* of U_n if it is a primitive divisor and $l \,||\, U_n$.

Conjecture 7. *Suppose that $\{U_n\}_{n \geq 0}$ is a non-degenerate Lucas sequence. There exists a constant C such that for all $n \geq C$ the Lucas term U_n has a primary divisor.*

The above conjecture is based on extensive computational experience with Lucas sequences. It appears to be hopelessly out-of-reach, but it does allow us to deduce the following.

Theorem 8. *Assume that Conjecture 7 holds. Suppose that $\{U_n\}_{n \geq 0}$ is a non-degenerate Lucas sequence and T is a finite set of primes. Let C be the constant appearing in the conjecture above, and let*

$$C' = \max(C, \max_{q \in T}(m_q + 1)),$$

where as usual m_q denotes the rank of the first appearance of the prime q for the sequence $\{U_n\}$. Suppose that

$$\prod_{i=1}^{m} U_{n_i} = \mu y^p, \qquad \mu \in \overline{T}, \quad m,\ y \in \mathbb{Z}^+, \quad p \text{ prime}, \quad n_1 \geq n_2 \geq \cdots \geq n_m \geq 1.$$

Then there is an integer $k \geq 0$ such that

$$n_{kp+1}, \ldots, n_m < C'$$

and

$$n_1 = n_2 = \ldots = n_p, \quad n_{p+1} = \ldots = n_{2p}, \quad \ldots \quad n_{(k-1)p+1} = \ldots = n_{kp}.$$

Proof. If $n_1 < C'$ then there is nothing to prove. Thus suppose that $n_1 \geq C'$. By the conjecture above, there is a prime l that is a primitive divisor of U_{n_1} and $l \,||\, U_{n_1}$. Moreover, since $n_1 > m_q$ for $q \in T$ we see that $l \notin T$. Thus the exponent to which l divides the term μy^p is at least p. Since $l \,||\, U_{n_1}$ and $l \nmid U_n$ for $n < n_1$ we see that $n_1 = n_2 = \ldots = n_p$. We now divide both sides of the equation $\prod_{n_i} U_{n_i} = \mu y^p$ with $U_{n_1}^p$ and repeat the argument. □

References

[1] Yu. Bilu, G. Hanrot and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. reine angew. Math. **539** (2001), 75–122.

[2] Y. Bugeaud, *On the Diophantine equation* $a\frac{x^n-1}{x-1} = y^q$, Proceedings of the Number Theory Conference held in Turku, ed. M. Jutila and T. Metsänkylä, 19–24, De Gruyter, 2001.

[3] Y. Bugeaud, F. Luca, M. Mignotte and S. Siksek, *On perfect powers in Lucas sequences*, International Journal of Number Theory **1** (2005), no. 3, 309–332.

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

[5] Y. Bugeaud and M. Mignotte, *Sur l'équation diophantienne* $\frac{x^n-1}{x-1} = y^q$, *II*, C. R. Acad. Sci. Paris, Ser. I **328** (1999), 741–744.

[6] Y. Bugeaud and M. Mignotte, *L'Équation de Nagell-Ljunggren* $\frac{x^n-1}{x-1} = y^q$, Enseign. Math. **48** (2002), 147–168.

[7] Y. Bugeaud, M. Mignotte and S. Siksek, *Sur les nombres de Fibonacci de la forme* $q^k y^p$, C. R. Acad. Sci. Paris, Ser. I **339** (2004), 327–330.

[8] Y. Bugeaud, M. Mignotte and S. Siksek, *Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers*, Ann. of Math. **163** (2006), no. 3, 969–1018.

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

[10] J. H. E. Cohn, *Squares in some recurrent sequences*, Pacific J. Math. **41** (1972), 631–646.

[11] K. Inkeri, *On the diophantine equation* $a(x^n - 1)/(x - 1) = y^m$, Acta Arith. **21** (1972), 299–311.

[12] F. Luca and T. N. Shorey, *Diophantine equations with products of consecutive terms in Lucas sequences*, J. Number Theory **114** (2005), no. 2, 298–311.

[13] W. Ljunggren, *Some theorems on indeterminate equations of the form* $(x^n-1)/(x-1) = y^q$. (Norwegian) Norsk Mat. Tidsskr. **25**, (1943). 17–20.

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

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

[16] P. Ribenboim, *Square classes of Fibonacci and Lucas numbers*, Portugal. Math. **46** (1989), Fasc. 2, 159–175.

[17] P. Ribenboim, *Square classes of* $(a^n - 1)/(a - 1)$ *and* $a^n + 1$, Sichuan Daxue Xuebao **26** (1989), Special Issue, 196–199.

[18] P. Ribenboim, *Pell numbers, squares and cubes*, Publ. Math. Debrecen **54/1-2** (1999), 131–152.

[19] P. Ribenboim, *An algorithm to determine points with integral coordinates on certain elliptic curves*, J. Number Theory **74** (1999), 19–38.

[20] P. Ribenboim, The terms Cx^h $(h \geq 3)$ in Lucas sequences: an algorithm and applications to Diophantine equations, Acta Arith. **106.2** (2003), 105–114.

[21] P. Ribenboim and W. L. McDaniel, *Square classes of Lucas sequences*, Portugal. Math. **48** (1991), no. 4, 469–473.
[22] P. Ribenboim and W. L. McDaniel, *The square classes in Lucas sequences with odd parameters*, C. R. Math. Rep. Acad. Sci. Canada **XVIII** (1996), no. 5, 223–227.
[23] N. Robbins, *On Fibonacci numbers which are powers. II.* Fibonacci Quart. **21** (1983), no. 3, 215–218.
[24] T. N. Shorey and C. L. Stewart, *On the Diophantine equation* $ax^{2t} + bx^t y + cy^2 = d$ *and pure powers in second order linear recurrences*, Math. Scand. **52** (1983), 24–36.
[25] T. N. Shorey and R. Tijdeman, *Exponential Diophantine equations*, Cambridge University Press, 1986.
[26] S. Siksek *Level lowering and Diophantine equations*, in *Explicit Methods in Number Theory*, Ed. K. Belabas, Panoramas et Synthèses, Société Mathématique De France, to appear.

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

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

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

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