JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Yann BUGEAUD, Florian LUCA, Maurice MIGNOTTE et Samir SIKSEK

Almost powers in the Lucas sequence

Tome 20, n° 3 (2008), p. 555-600.

<http://jtnb.cedram.org/item?id=JTNB_2008__20_3_555_0>

Journal de Théorie des Nombres
de Bordeaux **20** (2008), 555-600

Almost powers in the Lucas sequence

par Yann BUGEAUD, Florian LUCA, Maurice MIGNOTTE
et Samir SIKSEK

À Henri Cohen, à l'occasion de son soixantième anniversaire

Résumé. La liste complète des puissances pures qui apparaissent dans les suites de Fibonacci $(F_n)_{n\geq 0}$ et de Lucas $(L_n)_{n\geq 0}$ ne fut déterminée que tout récemment [10]. Les démonstrations combinent des techniques modulaires, issues de la preuve de Wiles du dernier théorème de Fermat, avec des méthodes classiques d'approximation diophantienne, dont la théorie de Baker. Dans le présent article, nous résolvons les équations diophantiennes $L_n = q^a y^p$, avec $a > 0$ et $p \geq 2$, pour tous les nombres premiers $q < 1087$, et en fait pour tous les nombres premiers $q < 10^6$ à l'exception de 13 d'entre eux. La stratégie suivie dans [10] s'avère inopérante en raison de la taille des bornes numériques données par les méthodes classiques et de la complexité des équations de Thue qui apparaissent dans notre étude. La nouveauté mise en avant dans le présent article est l'utilisation simultanée de deux courbes de Frey afin d'aboutir à des équations de Thue plus simples, et donc à de meilleures bornes numériques, qui contredisent les minorations que donne le crible modulaire.

Abstract. The famous problem of determining all perfect powers in the Fibonacci sequence $(F_n)_{n\geq 0}$ and in the Lucas sequence $(L_n)_{n\geq 0}$ has recently been resolved [10]. The proofs of those results combine modular techniques from Wiles' proof of Fermat's Last Theorem with classical techniques from Baker's theory and Diophantine approximation. In this paper, we solve the Diophantine equations $L_n = q^a y^p$, with $a > 0$ and $p \geq 2$, for all primes $q < 1087$ and indeed for all but 13 primes $q < 10^6$. Here the strategy of [10] is not sufficient due to the sizes of the bounds and complicated nature of the Thue equations involved. The novelty in the present paper is the use of the double-Frey approach to simplify the Thue equations and to cope with the large bounds obtained from Baker's theory.

Manuscrit reçu le 20 octobre 2007.
F. Luca is supported by grants SEP-CONACyT 79685 and PAPIIT 100508. S. Siksek is supported by a grant from the UK Engineering and Physical Sciences Research Council, and by a Marie–Curie International Reintegration Grant.

1. Introduction

We consider the Fibonacci sequence $(F_n)_{n\geq 0}$ and the Lucas sequence $(L_n)_{n\geq 0}$ which are both solutions to the linear recurrence $u_{n+2} = u_{n+1}+u_n$, with the initial conditions $F_0 = 0$, $F_1 = 1$ and $L_0 = 2$, $L_1 = 1$, respectively.

The problem of determining all perfect powers in the Fibonacci sequence and in the Lucas sequence was a famous open problem for over 40 years, and has been resolved only recently [10]; for a detailed history of the problem see [10, Section 10].

Theorem 1. *The only perfect powers among the Fibonacci numbers are* $F_0 = 0$, $F_1 = F_2 = 1$, $F_6 = 8$ *and* $F_{12} = 144$. *For the Lucas numbers, the only perfect powers are* $L_1 = 1$ *and* $L_3 = 4$.

Subsequent papers studied several multiplicative generalizations such as $F_n = q^a y^p$ with q prime (see [9]) and $F_{n_1} \cdots F_{n_r} = ay^p$ with $1 \leq r < p$ and a fixed integer a (see [7]).

Here, we consider the Diophantine equations $L_n = q^a y^p$, with $a > 0$, $p \geq 2$ and q prime. These equations appear to be much more difficult to solve than the equations $F_n = q^a y^p$. The reason for this is that the Lucas sequence $(L_n)_{n\geq 0}$ has weaker divisibility properties than the Fibonacci sequence. By combining Baker's theory of linear forms in logarithms and repeated use of an efficient sieve obtained via the double-Frey approach, we were able to solve it completely for all primes q less than 1087.

Theorem 2. *The only nonnegative integer solutions* (n, y, p) *of the equations*

$$L_n = q^a y^p, \quad \text{with } a > 0 \text{ , and } p \geq 2 \text{ ,} \tag{1}$$

with $q < 10^6$ *prime and*

$$q \neq 1087, 2207,\ 4481,\ 14503,\ 19207,\ 21503,\ 34303,\ 48767,\ 119809,\ 232049,\ 524287,\ 573569,\ 812167, \tag{2}$$

are

$$L_0 = 2,\ L_2 = 3,\ L_3 = 2^2,\ L_4 = 7,\ L_5 = 11,\ L_6 = 2 \times 3^2,\ L_7 = 29,$$
$$L_8 = 47,\ L_9 = 19 \times 2^2,\ L_{11} = 199,\ L_{13} = 521,\ L_{17} = 3571,\ L_{19} = 9349.$$

We note that equation (1) also has the solutions $L_{16} = 2207 \times 1$ and $L_{28} = 14503 \times 7^2$. We expect that the equation has no other solutions with $q < 10^6$, but for the moment are unable to prove this.

The traditional approach to Diophantine equations involving Fibonacci numbers combines clever tricks with various elementary identities connecting Fibonacci and Lucas numbers. Theorem 1 was proved by combining some of the deepest tools available in Number Theory: namely the modular approach (used in the proof of Fermat's Last Theorem) and a refined

version of Baker's theory of linear forms in logarithms. It also required substantial computations performed using the computer packages `PARI/GP` [1] and `MAGMA` [4]. The total running time for the various computational parts of the proof of Theorem 1 was about a week.

In [7] it is shown, among other things, how to deduce the solutions of the equation $F_n = ay^p$ from those of $F_n = y^p$ for any fixed a using the rich divisibility properties of the Fibonacci sequence. In contrast, the Lucas sequence has weaker divisibility properties, and the method of [7] is inapplicable. Moreover, a straightforward attempt to apply the method of [10] leads to very complicated Thue equations [1] and terrible bounds for the solutions that appear to be far too large for the modular sieve employed in [10]. In the current paper, we replace the standard modular approach with a double-Frey version (cf. [12]) which leads to a far more efficient sieve. Moreover, we use the information obtained by the double-Frey approach to simplify the Thue equations appearing along the way. This leads to substantially better bounds for the solutions and enables us to complete the proof of Theorem 2.

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 $|\alpha| \geq |\beta|$. If α/β is not a root of 1, then we define the Lucas sequence of the first kind $(U_n)_{n\geq 0}$ with parameters r, s to be the sequence of general term

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

This is also the sequence given by $U_0 = 0$, $U_1 = 1$ and $U_{n+2} = rU_{n+1} + sU_n$ for all $n \geq 0$. Its companion sequence $(V_n)_{n\geq 0}$ with parameters r, s is the sequence of general term

$$V_n = \alpha^n + \beta^n,$$

that is, the sequence given by $V_0 = 2$, $V_1 = r$ and $V_{n+2} = rV_{n+1} + sV_n$ for all $n \geq 0$ and it is usually referred to as a Lucas sequence of the second kind. In particular, the Lucas sequence $(L_n)_{n\geq 0}$ is the companion sequence of the Fibonacci sequence $(F_n)_{n\geq 0}$ and as such is a Lucas sequence of the second kind.

The general equation $U_n = ay^p$ is studied in [7], and our aim is to get similar results for the general equation $V_n = ay^p$. However, this is a more difficult problem, since the sequence $(V_n)_{n\geq 0}$ has weaker divisibility properties than the sequence $(U_n)_{n\geq 0}$. Nevertheless, we wish to point out that the method developed in the present paper is not specific only to the Lucas sequence $(L_n)_{n\geq 0}$ but can be, at least in principle, applied to solve any equation of the form $V_n = q^a y^p$.

[1] Recall that a Thue equation is an equation of the form $F(u, v) = c$ where F is an irreducible homogeneous polynomial of degree ≥ 3, with integral coefficients, and where c is a nonzero integer.

The present paper is organized as follows. We show, in Sections 2 and 3, that elementary arguments (and a little programming) establish Theorem 2 for any prime $2 \le q < 10^6$, except for $q = 3$, $q = 7$, $q = 47$, $q = 127$ and do not apply to the primes q in (2). The main part of the work is devoted to the complete resolution of the equation (1) for $q = 3$, 7 and 47. In Section 4, we show how to reduce to $L_{2r} = 3y^p$, $L_{4r} = 7y^p$ and $L_{8r} = 47y^p$, where r is odd and may be assumed to be prime when $r > 1$. These three equations have the trivial solutions $(r, y, p) = (1, 1, p), (1, 1, p)$ and $(1, 1, p)$, respectively, and it is precisely the existence of these trivial solutions that makes finding all their solutions quite difficult. In Sections 5–7, we deal with small values of y, r and p. Thus, we get lower bounds on y and r that help us to get a sharp upper bound on p by applying estimates for linear forms in three logarithms. This is the purpose of Section 8. The double–Frey approach is explained in Section 9. Its starting point are the two identities

$$5F_{2m}^2 + 4 = L_{2m}^2 \quad \text{and} \quad L_m^2 + 2(-1)^{m+1} = L_{2m}.$$

To each we associate a Frey curve. The first application of this is to construct a sieve, performed in Section 11, that yields that r (resp. $2r$, $4r$) is congruent to ± 1 (resp. ± 2, ± 4) modulo p when $q = 3$ (resp. $q = 7$, $q = 47$). This important auxiliary result allows us to apply in Section 12 estimates for linear forms in **two** logarithms in order to get much better upper bounds for the exponent p. Unfortunately, except for $q = 3$—for which we get $p < 1039$—these bounds remain too large [2] for completing the resolution of the equation. For $q = 7, 47$, we observe in Section 13 that, working in the quadratic field $\mathbb{Q}(\sqrt{2})$, we get the equations

$$L_{4r} \pm \sqrt{2} = (3 + \sqrt{2})(1 + \sqrt{2})^t (u + v\sqrt{2})^p$$

and

$$L_{8r} \pm \sqrt{2} = (7 + \sqrt{2})(1 + \sqrt{2})^t (u + v\sqrt{2})^p,$$

with $0 \le t \le p - 1$. Now a second application of the double–Frey sieve gives that $t = 0$. Using this information, we get another linear form in **two** logarithms, to which we apply Baker's theory to considerably improve upon the upper bound for p when $q = 7$, 47. In particular, we get at this stage that $p \le 1487$ for $q = 7$ and that $p \le 797$ for $q = 47$, provided that r is large enough. We stress that the particular shape of this linear form in two logarithms implies that the bound for p decreases when q increases. In Section 14, we derive from our equations Thue equations of degree p and, again by Baker's method, upper bounds for r. Finally, in Section 16, we perform again a modular sieve and conclude that $r = \pm 1$ for all three equations.

[2] For $q = 7$ we get $p < 2000$, and $p < 4000$ for $q = 47$.

In Section 10, we briefly indicate how we showed that (1) has no solutions for $q = 127$ using a modification of the double-Frey approach used for $q = 3, 7, 47$. In principle it should be possible to deal with the values of q in the list (2). We have however found that the necessary modular forms computations needed for these values are too demanding for the currently available hardware.

We warmly thank the referees for suggesting several improvements and corrections.

2. Elementary arguments

2.1. Some elementary facts. It is well-known—Binet's formulæ—that

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad L_n = \alpha^n + \beta^n \qquad \text{for all } n \geq 0, \tag{3}$$

where

$$\alpha = \frac{1+\sqrt{5}}{2} \quad \text{and} \quad \beta = \frac{1-\sqrt{5}}{2}.$$

This implies

$$5F_k^2 - L_k^2 = 4(-1)^{k+1}. \tag{4}$$

From this quadratic relation (4), one may deduce information on the divisors of Lucas numbers. For example, we see that 5 does not divide any Lucas number and also that, if k is even and q is an odd prime divisor of L_k, then $\left(\frac{5}{q}\right) = \left(\frac{-1}{q}\right)$. Here and in what follows, $(\frac{\bullet}{q})$ is the Jacobi symbol with respect to the odd integer q.

For a prime number q, we denote by $\mathrm{T}(q)$ the period of $(L_n)_{n\geq 0}$ modulo q. We also define $\mathrm{t}(q)$ by

$$\mathrm{t}(q) = \begin{cases} \text{the smallest } t > 0 \text{ such that } q \mid L_t, & \text{if such a } t \text{ exists;} \\ \infty, & \text{otherwise.} \end{cases}$$

We define the set

$$\mathcal{D} = \{q \,:\, q \text{ prime and } \mathrm{t}(q) < \infty\};$$

in other words, $\mathcal{D}$ is the set of primes dividing at least one Lucas number. For a prime number p and a nonzero integer m we write $\mathrm{v}_p(m)$ for the exact order at which p appears in the prime factorization of m; i.e., $\mathrm{v}_p(m) = a$, where $p^a \mid m$ but $p^{a+1} \nmid m$. We write $m \mid_2 n$ if $m \mid n$ and $\mathrm{v}_2(m) = \mathrm{v}_2(n)$.

The following lemma collects several well-known facts; a proof is included for convenience.

Lemma 2.1. *Let $q \neq 5$ be prime. Then*

$$\mathrm{T}(q) \mid \begin{cases} q-1, & \text{if } q \equiv \pm 1 \pmod 5; \\ 2(q+1), & \text{if } q \equiv \pm 2 \pmod 5. \end{cases} \tag{5}$$

Suppose from now on that q is odd. Then

$$\mathrm{T}(q) = \min\{n : \alpha^n \equiv \beta^n \equiv 1 \pmod q\}. \tag{6}$$

Suppose moreover that $q \in \mathcal{D}$ and put $t = \mathrm{t}(q)$. Then,

$$\mathrm{T}(q) = \begin{cases} 2t, & \text{if } t \text{ is odd;} \\ 4t, & \text{if } t \text{ is even} \end{cases} \tag{7}$$

and

$$q \mid L_n \iff n \equiv t \pmod{2t} \iff t \mid_2 n. \tag{8}$$

Proof. Suppose $q \neq 5$. Then 5 is a square modulo q if and only if $q \equiv \pm 1 \pmod 5$. If $q \equiv \pm 1 \pmod 5$, then (5) follows from Fermat's Little Theorem, so suppose that $q \equiv \pm 2 \pmod 5$. By the properties of the Frobenius automorphism, $\alpha^q \equiv \beta \pmod q$, so $\alpha^{q+1} \equiv \beta\alpha \equiv -1 \pmod q$, therefore $\alpha^{2(q+1)} \equiv 1 \pmod q$ and a similar argument applies to β. This proves (5).

Suppose now that q is odd. Using the definition of $\mathrm{T} = \mathrm{T}(q)$, we have that $\alpha^{\mathrm{T}} + \beta^{\mathrm{T}} \equiv L_0 \equiv 2 \pmod q$ and $\alpha^{\mathrm{T}+1} + \beta^{\mathrm{T}+1} \equiv L_1 \equiv 1 \pmod q$. Multiplying the first relation by β and subtracting it from the second we get $\alpha^{\mathrm{T}}(\alpha - \beta) \equiv 1 - 2\beta \pmod q$. Since $1 - 2\beta = (1-\beta) - \beta = \alpha - \beta$, is a number of norm 5 in $\mathbb{K} = \mathbb{Q}[\alpha]$, we get (as q is not 5) that $\alpha^{\mathrm{T}} \equiv 1 \pmod q$, and a similar argument works with α replaced by β. Since it is also clear that any positive n with $\alpha^n \equiv \beta^n \equiv 1 \pmod q$ must also satisfy $n \geq \mathrm{T}$, the desired formula (6) follows. Note that when $q = 5$, $\mathrm{T}(5) = 4$ but $\min\{n : \alpha^n \equiv \beta^n \equiv 1 \pmod 5\} = 20$.

We now turn to the proof of (7). Note $\alpha^t + \beta^t \equiv 0 \pmod q$, which implies, via the fact that $\beta = -\alpha^{-1}$, that

$$\alpha^{2t} \equiv (-1)^{t+1} \pmod q. \tag{9}$$

The desired assertion (7) now follows easily from (6); it is now easy to deduce (8). □

Lemma 2.2. *Let X and Y be commuting variables. Put $S = X + Y$ and $P = XY$. Then for n odd,*

$$X^n + Y^n = S\, Q_n(S, P),$$

where $Q_n(S, P)$ is a polynomial with integer coefficients, which is even in S, and satisfies the relations $Q_n(0, 1) = (-1)^n n$ and $Q_n(0, -1) = n$.

Proof. If $n = 1$ this is trivial. If $n = 3$, then

$$X^3 + Y^3 = (X + Y)(X^2 - XY + Y^2) = S(S^2 - 3P),$$

as wanted. For $n \geq 5$ and odd,

$$X^n + Y^n = (X^2 + Y^2)(X^{n-2} + Y^{n-2}) - (XY)^2(X^{n-4} + Y^{n-4}),$$

so that

$$Q_n(S, P) = (S^2 - 2P)Q_{n-2}(S, P) - P^2 Q_{n-4}(S, P).$$

The desired result now follows easily by induction. □

The previous lemma implies at once:

Corollary 2.3. *If i, j and k are positive integers, with i odd and $k = ij$, then*

$$L_k = L_j L_{k,j},$$

where $L_{k,j}$ is an integer, and the greatest common divisor d of L_j and $L_{k,j}$ divides i. Furthermore, when i is an odd prime, then **either** $d = 1$, **or** $d = i$, *in which case $i^2 \nmid L_{k,j}$, and $\mathrm{v}_i(L_k) = 1 + \mathrm{v}_i(L_j)$.*

We also mention the following elementary result for further use.

Lemma 2.4. *The Lucas sequence satisfies the following divisibility properties:*

$2 \mid L_n \Leftrightarrow n \equiv 0 \pmod 3$*;*
$4 \mid L_n \Leftrightarrow n \equiv 3 \pmod 6$*;*
$3 \mid L_n \Leftrightarrow n \equiv 2 \pmod 4$*;*
$9 \mid L_n \Leftrightarrow n \equiv 6 \pmod{12}$.

From this result we derive the following lemma.

Lemma 2.5. *Suppose that $q \neq 2$, 3 is prime with $t = \infty$ or $\mathrm{v}_2(t) = 1$, where $t = \mathrm{t}(q)$. Then equation* (1) *has no solutions.*

Proof. By the definition of $\mathrm{t}(q)$, the conclusion is clear when $t = \infty$. Suppose instead that $\mathrm{v}_2(t) = 1$ and (n, y, p, a) is a solution to (1). Now $q \mid L_n$ implies that $t \mid_2 n$ by Lemma 2.1. From $\mathrm{v}_2(t) = 1$ we see that $\mathrm{v}_2(n) = 1$. By Lemma 2.4, $3 \mid L_n$. However, $q \neq 3$ and so from $L_n = q^a y^p$ and the fact that $p \geq 2$ we see that $9 \mid L_n$. By the Lemma 2.4 again, we obtain $n \equiv 6 \pmod{12}$. Finally, we see from the above divisibility properties that $2 \mid L_n$ but $4 \nmid L_n$ giving a contradiction. □

2.2. The avalanche. We introduce a lemma which enables us to solve, in a few steps, most equations of the form $L_n = q^a y^p$.

Lemma 2.6. *Let q be an odd prime and write $t_0 = \mathrm{t}(q)$. Suppose that there is a sequence of odd primes $q_1, q_2, \ldots, q_k$ (and write $t_i = \mathrm{t}(q_i)$) such that the following three conditions are satisfied:*

(i) *$t_i < \infty$ and $\mathrm{v}_2(t_i) = \mathrm{v}_2(t_0)$ for $i = 1, \ldots, k-1$,*
(ii) *$q_i \mid t_{i-1}$ for $i = 1, \ldots, k$,*
(iii) *either $t_k = \infty$ or $\mathrm{v}_2(t_k) \neq \mathrm{v}_2(t_0)$.*

Then

(a) *any solution to (1) satisfies*

$$n = \prod_{i=1}^{k} q_i^{r_i} \qquad \text{or} \qquad p = 2 \quad \text{and} \quad n = 3\prod_{i=1}^{k} q_i^{r_i}, \tag{10}$$

for some non-negative integers r_i.

(b) *If t_0 is not of the form $3^b q_1^{a_1} \cdots q_k^{a_k}$ for some non-negative integers a_i and for $b = 0$ or 1, then equation (1) has no solutions.*

(c) *Suppose there are positive integers $A_1, \ldots, A_k$ such that none of the Lucas numbers $L_{q_i^{A_i}}$ is of the form*

$$q^\alpha 3^\beta q_1^{\gamma_1} \ldots q_k^{\gamma_k} z^p, \qquad \alpha, \beta, \gamma_i, z \geq 0, \quad p \geq 2.$$

Then the exponents r_i in (10) satisfy $r_i < A_i$.

Proof. We prove (a) by contradiction. Let n be the smallest positive integer satisfying $L_n = q^a y^p$ for some $a \geq 1$, that is not of the form (10). By Lemma 2.1, $q \mid L_n$ implies that $t_0 \mid_2 n$. But $q_1 \mid t_0$ and so $q_1 \mid n$. Suppose first that $q_1 \nmid L_n$. Let $m = n/q_1$. By Corollary 2.3, we have that $L_m = q^b y_1^p$. If $b \geq 1$, then we quickly contradict minimality. Thus $L_m = y_1^p$. By Theorem 1, we see that $m = 1$ or $m = 3$, implying that $n = q_1$ or $3q_1$ which contradicts the fact that n is not of the form (10).

Hence we deduce that $q_1 \mid L_n$. We repeat the above argument to show that $q_i \mid L_n$ for $i = 1, \ldots, k-1$. Now as $q_{k-1} \mid L_n$ we obtain that $t_{k-1} \mid n$ and $q_k \mid n$. However the assumptions on t_k ensure that $q_k \nmid L_n$. This is trivially true if $t_k = \infty$. Suppose that $\mathrm{v}_2(t_k) \neq \mathrm{v}_2(t_0)$. We know that $t_0 \mid_2 n$. Hence $t_k \nmid_2 n$. Thus, either way, $q_k \nmid L_n$. Writing $m = n/q_k$ and arguing as above we obtain a contradiction. This completes the proof of (a).

Part (b) follows immediately from (a) since $t_0 \mid_2 n$ as stated above. Let us prove (c). Suppose that for some i, $r_i \geq A_i$. By Corollary 2.3, we have $L_n = L_{q_i^{A_i}} L'$ where the greatest common divisor of the two factors divides $n/q_i^{A_i}$. Part (c) follows at once as we are supposing that L_n is of the form $q^a y^p$ and n satisfies (10). □

3. Proof of Theorem 2 for most q

We programmed Lemmas 2.5 and 2.6 in `PARI/GP`, and used our program for all primes $3 \le q < 10^6$ (we return to the case $q = 2$ below). Our program took 1 hour and 21 minutes on a 2.8 GHz Opteron and succeeded in solving (1) for all primes q in this range except for the primes in (2) and for $q = 3$, 7, 47, 127. The remainder of this paper will be devoted to solving (1) for these four values $q = 3$, 7, 47, 127. Indeed, we shall show that there are no solutions for $q = 127$, and that the only solutions for $q = 3$, 7, 47 are respectively $n = 2$, 4, 8.

Before we solve (1), we illustrate the workings of our program by solving (1) for a few values of q.

- $q = 13$ and $q = 41$

Note that $\mathrm{t}(13) = \infty$ and $\mathrm{t}(41) = 10$. By Lemma 2.5, equation (1) has no solutions in these cases.

- $q = 29$

Note that $\mathrm{t}(29) = 7$ and $\mathrm{t}(7) = 2^2$. By Lemma 2.6 we know that n is of the form

$$n = 7^{r_1} \qquad \text{or} \qquad n = 3 \times 7^{r_1}.$$

However, $L_{7^2} = 29 \times 599786069$ as product of primes. By part (c) of Lemma 2.6 we have that $r_1 = 0$ or 1, so that $n = 1$, 3, 7, 21. We immediately obtain that $L_7 = 29 \times 1^p$ is the only solution to equation (1) with $q = 29$.

- $q = 709$

Note that $\mathrm{t}(709) = 59$, $\mathrm{t}(59) = 29$, $\mathrm{t}(29) = 7$, $\mathrm{t}(7) = 2^2$. By Lemma 2.6 we know that n is of the form

$$n = 59^{r_1} \times 29^{r_2} \times 7^{r_3} \qquad \text{or} \qquad n = 3 \times 59^{r_1} \times 29^{r_2} \times 7^{r_3}.$$

However,

$$L_{59} = 709 \times 8969 \times 336419, \quad L_{29} = 59 \times 19489, \quad L_{7^2} = 29 \times 599786069,$$

and so by part (c) of Lemma 2.6 we have that $r_1 = r_2 = 0$ and $r_3 = 0$ or 1. Thus $n = 1$, 3, 7, 21, and none of these give a solution to equation (1) with $q = 709$, which completes our proof in this case.

- $q = 812167$

Note that

$$\mathrm{t}(812167) = 2^2 \times 7 \times 14503, \qquad \mathrm{t}(14503) = 2^2 \times 7, \qquad \mathrm{t}(7) = 2^2.$$

Thus neither the conditions of Lemma 2.5 nor of Lemma 2.6 are satisfied, and we are unable to solve (1) in this case.

Finally we turn to the case $q = 2$ to which Lemma 2.5 and Lemma 2.6 are inapplicable, but which we can still solve.

- $q = 2$

Since 8 does not divide any Lucas number, there are two cases here, namely when $L_n = 2y^p$ and when $L_n = 4y^p$.

Consider first the case

$$L_n = 4y^p.$$

By Lemma 2.4, $n \equiv 3 \pmod 6$ and so $3 \nmid L_n$. Write $n = 3m$; by Corollary 2.3

$$L_m = \begin{cases} 4y_1^p, & \text{if } 3 \mid m; \\ y_1^p, & \text{if } 3 \nmid m. \end{cases}$$

If $L_m = 4y_1^p$ and $3 \mid m$ then we can continue in this way (eliminating a factor 3 at each step). We finally arrive at an equation for the form $L_k = z^p$ and by Theorem 1, the only solutions are $k = 1, 3$. Hence $n = 3^b$ for some $b > 0$. Since $L_9 = L_3(L_3^2 + 3) = 4 \times 19$ is not of the form $4y^p$, we get that the only solution to $L_n = 4y^p$ is $n = 3$ for which $L_3 = 4 \times 1^p$.

We now look at the equation

$$L_n = 2y^p.$$

Then $n \equiv 0 \pmod 6$. Suppose first that $n \equiv 0 \pmod{12}$. Then 3 does not divide L_n (because $\mathrm{t}(3) = 2$), and the previous process works again. At the end, we arrive at $m = 1$, which gives a contradiction. Thus, the equation $L_n = 2y^p$ has no positive solution with $4 \mid n$. Suppose next that $n \equiv 6 \pmod{12}$. Then 3 divides L_n. Put $b = \mathrm{v}_3(L_n)$. We then have that 3 divides $L_{n/3}$, and, by Corollary 2.3,

$$L_{n/3} = 2 \times 3^{b-1} y_1^p.$$

Similarly, $L_{n/3^2} = 2 \times 3^{b-2} y_2^p$, $L_{n/3^3} = 2 \times 3^{b-3} y_3^p$, ... etc. If $n = 3^\gamma m$, where 3 does not divide m, then at the end of the above process, we get $L_m = 3z^p$. We later show that the only solution to this latter equation is $m = 2$ and this completes the proof for $q = 2$.

4. A useful reduction

In this section, we simplify equation (1) for $q = 3, 7, 47$.

Lemma 4.1. *Let $n = 2^k m$, where $m > 1$ is odd. Let l be the smallest prime divisor of m and put $t = \mathrm{t}(l)$. Then l divides L_n if and only if $t = 2^k$.*

Proof. By Lemma 2.1, the number t divides either $(l-1)$ or $(l+1)$. Either way, all its odd prime divisors are $< l$. Suppose l divides L_n. Again by Lemma 2.1, $t \mid_2 n$. Since l is the smallest prime divisor of m, we see that t has no odd prime divisors and that $t = 2^k$. The converse is clear. □

Corollary 4.2. *Let $k \geq 1$ be such that $L_{2^k} = q$ is prime. Suppose that the equation*

$$L_n = q^a y^p, \quad a > 0, \ p \text{ prime},$$

admits a solution with $n > 2^k$ and let r be the largest odd prime factor of n that does not equal q. Then

$$L_{2^k r} = q z^p,$$

for some $z \mid y$.

Proof. Let $v = \mathrm{v}_q(n)$ and $n' = n/q^v$. By Corollary 2.3, we see that $L_{n'} = q^b y'^p$ for some $y' \mid y$. However, again by the same corollary, but considering the factorisation $L_{n'} = L_{2^k} L_{n',2^k}$ we see that $b = 1$.

If $n'/2^k$ is prime then we are finished. Otherwise let l be the smallest odd prime factor of $n'/2^k$. By Lemma 4.1 we see that $l \nmid L_n$. Let $n'' = n'/l$. By Corollary 2.3 we see that $L_{n''} = q y''^p$. We continue removing the smallest odd prime divisor of the index each time until we are left with $2^k r$ where r is the largest prime factor of n that does not equal q. □

Note that Corollary 4.2 applies to $q = 3, 7, 47$ with respective values of $k = 1, 2, 3$. Hence to complete the proof of Theorem 2 we require a proof that (1) has no solutions for $q = 127$ and we require a proof that the equation

$$L_{2m} = q y^p \tag{11}$$

has no solutions subject to the conditions

(12)
$$p \text{ prime}, \quad (q, m) = (3, r), \ (7, 2r), \ (47, 4r), \quad \text{where } r \text{ is an odd prime.}$$

Our choice of writing L_{2m} instead of L_n will allow us to introduce a slightly more uniform presentation in what follows. In Sections 5–16 we focus on $q = 3, 7, 47$. In the final section we explain briefly how the arguments used for these primes can be modified to show that (1) has no solutions for $q = 127$.

5. Auxiliary equations

In this section, we write down three auxiliary equations that will help us to solve (11). Note the following three identities which follow easily from Binet's formulæ:

$$\begin{aligned} 5F_{2m}^2 + 4 &= L_{2m}^2, \\ L_m^2 + 2(-1)^{m+1} &= L_{2m}, \\ 5F_m^2 + 2(-1)^m &= L_{2m}. \end{aligned}$$

From (11), we immediately deduce the following three equations:

$$5F_{2m}^2 + 4 = q^2 y^{2p}, \tag{13}$$

$$L_m^2 + 2(-1)^{m+1} = qy^p, \tag{14}$$

$$5F_m^2 + 2(-1)^m = qy^p. \tag{15}$$

5.1. Eliminating small exponents p. We will later use the modular approach to help us solve the equations $L_{2m} = qy^p$ by attaching Frey curves to one or more of the three auxiliary equations (13)–(15). In the modular approach, it is useful to avoid small exponents p where the Galois representation may be reducible. We thus first solve the equations $L_{2m} = qy^p$ for $2 \le p \le 11$ with the help of the computer algebra systems `PARI/GP` [1] and `MAGMA` [4].

Lemma 5.1. *The only solutions to the equation $L_{2m} = qy^p$ with $2 \le p \le 11$ and with $(q, m) = (3, r)$, $(7, 2r)$, $(47, 4r)$ and r odd, have $r = y = 1$.*

Proof. For $p = 2$, we work with equation (13). We make the substitution

$$Y = 25q^2 yF_{2m}, \qquad X = 5q^2 y^2,$$

and obtain the equation

$$Y^2 = X(X^2 - 100q^2).$$

This is an elliptic curve in standard Weierstrass form and we want its integral points. `MAGMA` quickly computes the integral points for $q = 3$, 7, 47. For example, for $q = 47$, we obtain

$$(X, Y) = (-470, 0),\ (0, 0),\ (470, 0),\ (-20, \pm 2100),\ (11045, \pm 1159725).$$

We instantly see that $5 \times 47^2 y^2 = X = 11045 = 5 \times 47^2$, giving $y = 1$ as required. The cases $q = 3$ and $q = 7$ with $p = 2$ are similar.

We now turn our attention to $3 \le p \le 11$. For the sake of uniformity, we work with equation (13) which is independent of the parity of m. Using the fact that the class number of $\mathbb{Q}(\sqrt{-5})$ is 2, equation (13) implies that formula

$$2 \pm F_{2m}\sqrt{-5} = \lambda(u + v\sqrt{-5})^p$$

holds, where $y^2 = u^2 + 5v^2$ and $\lambda = 2 + \sqrt{-5}$, $2 + 3\sqrt{-5}$, or $2 + 7\sqrt{-5}$, according to whether $q = 3$, 7, or 47, respectively. Identifying the coefficients of $\sqrt{-5}$, we obtain a Thue equation of the form $F(u, v) = 2$, where the leading coefficient of $F(u, 1)$ is 2. However, since y is odd, exactly one of u, v must be odd. An elementary examination of the coefficients of the Thue equation quickly shows that v is even and u is odd. Thus, we may write $v = 2v'$, and rewrite our equation in the form $F'(u, v') = 1$, where $F'(u, 1)$ is now monic. The best practical algorithms for solving Thue equations that we are aware of are those of Bilu and Hanrot [3], and of Hanrot [18]. Fortunately, these are implemented as part of the computer package `PARI/GP`, and using

these we have been able to solve the Thue equations for $3 \leq p \leq 11$ in under a day on a 2.4 GHz Xeon. □

6. Eliminating small values of y

We will apply several variants and refinements of Baker's method to solve equation (11) subject to conditions (12). In this section, we show that y is large. One sees at once that for large y, the equation $L_{2m} = qy^p$ implies that the linear form

$$\Lambda = 2m \log \alpha - \log q - p \log y$$

is very small (recall that $\alpha = (1 + \sqrt{5})/2$). Then a lower bound for linear forms in logarithms gives an upper bound on the exponent p. Applying directly Matveev's theorem [25] (see Theorem 3 of Section 8.2 for a precise statement) here gives $p < 4 \times 10^{14}$. We then apply the following version of the classical Baker–Davenport Lemma:

Proposition 6.1. *(*[16]*) Let A, B, θ, μ be positive real numbers and M a positive integer. Suppose that P/Q is a convergent of the continued fraction expansion of θ such that $Q > 6M$. Put $\varepsilon = \|\mu Q\| - M\|\theta Q\|$, where $\|\cdot\|$ denotes the distance from the nearest integer. If $\varepsilon > 0$, then there is no integer solution (j, k) to the inequality*

$$0 < j\theta - k + \mu < A \cdot B^{-j}$$

subject to the restriction that

$$\frac{\log(AQ/\varepsilon)}{\log B} \leq j \leq M.$$

Corollary 6.2. *Suppose that m, y and q satisfy equation* (11) *and conditions* (12)*. Then $y = 1$, or $y \geq 10^{10}$.*

Proof. One way of proving this result is to verify that

- if $q = 3$, then $y \equiv 1, 41, 281, 601 \pmod{840}$;
- if $q = 7$, then $y \equiv 1, 241 \pmod{480}$;
- if $q = 47$, then $y \equiv 1 \pmod{3360}$.

Using these congruences, we apply the Baker–Davenport Lemma for $\Lambda/\log\alpha$, choosing $M = 4 \times 10^{14}$ as an upper bound for j. After around 36 hours of computation we get that

$$1 < y < 10^{10} \implies p \leq 3.$$

However, we have already solved the cases $p = 2$, 3 in Lemma 5.1 and found that $y = 1$. We deduce that $y \geq 10^{10}$. An alternative proof of this result goes as follows. For every prime q let $\mathrm{z}(q)$ be the *order of apparition* of q in the Fibonacci sequence, namely the smallest positive integer k such

that $q \mid F_k$. It is known that $\mathrm{z}(q)$ always exists. It is even precisely when $\mathrm{t}(q)$ exists and in this case $z(q) = 2\,\mathrm{t}(q)$. D. D. Wall [35] conjectured that $q \,\|\, F_{z(q)}$ holds for all primes q. No counterexample to this conjecture (nor a proof of it either) has been found. Sun and Sun [33] deduced that the so-called first case of Fermat's Last Theorem is impossible under Wall's conjecture. However, recently McIntosh and Roettger [24] verified Wall's conjecture for all $p < 10^{14}$ and found it to be true. We now note that the computation of McIntosh and Roettger immediately implies that $y > 10^{14}$ if $y > 1$. Indeed, assume that $y \in [2, 10^{14}]$. Let s be any prime factor of y. Since $L_m = qy^p$, and $m = r$, $2r$ or $4r$, we get easily that $\mathrm{t}(s) = m$, therefore $z(s) = 2m$. However, since $\mathrm{v}_s(L_m) = p > 2$, it follows that Wall's conjecture is false for s. Hence, we must have $y \geq s > 10^{14}$ by the calculation from [24]. □

We next prove another elementary lower bound on y.

Lemma 6.3. *If $L_n = qy^p$ with $y > 1$ and n minimal, where $q = 3$, 7 or 47, then*

$$y > \frac{4}{\log \alpha}\, p \log y.$$

Proof. We first notice that since n is even and not divisible by 3, we have $L_n \equiv 3 \pmod 4$. Thus, the relation $L_n = qy^p$ implies $y \equiv 1 \pmod 4$ since $q \equiv 3 \pmod 4$.

Now let s be the minimal prime divisor of y. Then, with the notation of the second section, $\mathrm{t}(s) = n$ and the period of $(L_n)_{n\geq 0}$ modulo s is equal to $\mathrm{T}(s) = 4n$. Moreover, we also know that $\mathrm{T}(s)$ divides either $s-1$ or $2(s+1)$. We now distinguish two cases according to whether $y = s$ or $y \geq s^2$. In case $y = s$, then $2(y+1) = 2(s+1)$ is not a multiple of 8. Thus, $4n$ divides $s - 1$. Since $L_n = qy^p$ implies

$$n \log \alpha > p \log y,$$

we get the result. If $y \geq s^2$, it is clear that a much better lower bound holds. □

Remark. It may be interesting to notice that the proof of the previous lower bound on y does not involve any computer verification. As an example, it gives the following estimate:

$$p > 10^8 \implies y > 9.17 \times 10^{10}.$$

7. Eliminating small indices m

It will be useful to know that the index $2m$ (which is either $2r$, $4r$ or $8r$) is large. We prove this by using a simple sieve adapted from [10, Lemma 4.3].

Lemma 7.1. *Suppose that m, y, p, q and r satisfy equation* (11) *and conditions* (12). *Then $r > 2 \times 10^5$.*

Proof. By Lemma 5.1 and Corollary 6.2, we may suppose that $p \geq 13$ and $y \geq 10^{10}$. We can write $2m = 2^i r$, where $i = 1$, 2, 3 for $q = 3$, 7, and 47, respectively. Note that

$$q \cdot 10^{10p} \leq qy^p = L_{2m} = L_{2^i r} \leq L_{2^i}^r \leq q^r.$$

Thus,

$$13 \leq p \leq \frac{(r-1)\log q}{10 \log 10}.$$

It is sufficient to show that for each odd prime $r \leq 2 \times 10^5$ and each p in the corresponding range above, the number L_{2m} is not of the form qy^p. Of course, it is not practical to write down L_{2m} once m gets large, but we explain a quick way of testing that $L_{2m} \neq qy^p$.

Suppose $l \neq q$ is a prime satisfying $l \equiv 1 \pmod{p}$, and let $k = (l-1)/p$. We can write down L_{2m} modulo l very quickly using (3) since all that is involved is exponentiation modulo l. Now if $(L_{2m}/q)^k \not\equiv 0, 1 \pmod{l}$ then $L_{2m} \neq qy^p$ as desired.

We wrote a short `PARI/GP` [1] program to check for each odd prime $r \leq 2 \times 10^5$ and each p in the above range that there is some prime l proving that $L_{2m} \neq qy^p$. This took about 22 minutes for $q = 3$, about 35 minutes for $q = 7$, and about 40 minutes for $q = 47$, respectively, on a 3.2 GHz Pentium IV. □

8. A bound for p

We noted previously that Matveev's lower bound for linear forms in logarithms [25] gives $p < 4 \times 10^{14}$. This bound is far too large for our purposes. In this section, by applying certain results on linear forms in three logarithms, we shall deduce the following better bound.

Proposition 8.1. *Suppose that m, y, p, q and r satisfy equation* (11) *and conditions* (12). *Then*

$$p < \begin{cases} 1.05 \times 10^8, & \text{if } q = 3; \\ 1.92 \times 10^8, & \text{if } q = 7; \\ 3.94 \times 10^8, & \text{if } q = 47. \end{cases}$$

8.1. Preliminaries. From the equation

$$L_n = qy^p$$

and Binet's formula, we get at once that the linear form

$$\Lambda = n \log \alpha - p \log y - \log q$$

satisfies

$$0 < -\Lambda < \alpha^{-2n} < 1.001(qy^p)^{-2},$$

since $n > 10000$ (see Lemma 7.1).

We write

$$n = kp + r, \quad \text{with } |r| < p/2,$$

and rewrite the linear form Λ in the more convenient form

$$\Lambda = r \log \alpha - p \log(y\alpha^{-k}) - \log q.$$

We shall apply the result below to this expression. We have already mentioned Matveev's bound a few times. It is now time to state it explicitly.

8.2. Matveev's lower bound for linear forms in logarithms. Let $\mathbb{L}$ be a number field of degree D, let $\alpha_1, \ldots, \alpha_n$ be non-zero elements of $\mathbb{L}$ and $b_1, \ldots, b_n$ be rational integers. Set

$$B = \max\{|b_1|, \ldots, |b_n|\},$$
$$\Lambda = \alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1,$$

and

$$\Lambda' = b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n.$$

Let h denote the absolute logarithmic height [3] and let $A_1, \ldots, A_n$ be real numbers with

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

We call h' the modified height with respect to the field $\mathbb{L}$. With this notation, the main result of Matveev [25] implies the following estimate.

Theorem 3. *Assume that Λ' is non-zero. We then have*

$$\log|\Lambda| > -1.4 \cdot 30^{n+4} (n+1)^{5.5} D^2 (1 + \log D)(1 + \log nB) A_1 \cdots A_n.$$

Assume that Λ is non-zero. We then have

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

[3] Throughout this paper we use the following notation and definitions. The *measure* of a polynomial $P(X) = a \prod_{j=1}^{d} (X - z_j)$ with complex coefficients is equal to

$$\mathrm{M}(P) = |a| \prod_{j=1}^{d} \max\{1, |z_j|\}.$$

If α is an algebraic number of degree d whose minimal polynomial over the integers is equal to P then the *height* of α—or more precisely its *logarithmic absolute height*—is equal to

$$\mathrm{h}(\alpha) = \frac{\log \mathrm{M}(P)}{d}.$$

Additionally, if $\mathbb{L}$ *is real, we then have*

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

A better estimate for Λ' when $n = 2$ and $n = 3$ has been obtained in [22] and in [27], respectively.

8.3. A lower bound for the linear form. We use the following technical result proved in [27].

Theorem 4. *Let* α_1, α_2 *and* α_3 *be algebraic numbers, which are either all real and* > 1, *or all complex non-real of modulus one. Let* b_1, b_2 *and* b_3 *be positive integers with* $\gcd(b_1, b_2, b_3) = 1$. *Let*

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

where the determinations of the logarithms are arbitrary, but are either all real or all purely imaginary. We further assume that

$$0 < |\Lambda| < 2\pi/w,$$

where w *is the largest order of any root of unity belonging to the number field* $\mathbb{Q}[\alpha_1, \alpha_2, \alpha_3]$. *We assume that*

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

We put

$$d_1 = \gcd(b_1, b_2), \quad d_3 = \gcd(b_2, b_3), \quad b_2 = d_1 b_2' = d_3 b_2''.$$

We let K, L, R, R_1, R_2, R_3, S, S_1, S_2, S_3, T, T_1, T_2 *and* T_3 *be positive integers, with*

$$K \geq 3, \quad L \geq 5, \quad R > R_1+R_2+R_3, \quad S > S_1+S_2+S_3, \quad T > T_1+T_2+T_3.$$

Let $\rho \geq 2$ *be a real number. Assume further that*

(16)
$$\left(\frac{KL}{2} + \frac{L}{4} - 1 - \frac{2K}{3L}\right) \log \rho \;\geq (D+1) \log N + gL(a_1 R + a_2 S + a_3 T) + D(K-1)\, \log b - 2\log(e/2),$$

where $N = K^2 L$, $D = [\mathbb{Q}[\alpha_1, \alpha_2, \alpha_3] : \mathbb{Q}] \,/\, [\mathbb{R}[\alpha_1, \alpha_2, \alpha_3] : \mathbb{R}]$, $e = \exp(1)$,

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

where

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

and the numbers a_1, a_2 *and* a_3 *satisfy*

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

Put

$$\mathcal{V} = \sqrt{(R_1+1)(S_1+1)(T_1+1)}.$$

If, *for some positive real number* χ, *all the above inequalities*

(i) $(R_1+1)(S_1+1)(T_1+1) > K \cdot \max\Big\{R_1+S_1+1,\, S_1+T_1+1,\, R_1+T_1+1,\, \chi\mathcal{V}\Big\}$,

(ii) $\mathrm{Card}\{\alpha_1^r\alpha_2^s\alpha_3^t \,:\, 0 \le r \le R_1,\, 0 \le s \le S_1,\, 0 \le t \le T_1\} > L$,

(iii) $(R_2+1)(S_2+1)(T_2+1) > 2K^2$,

(iv) $\mathrm{Card}\{\alpha_1^r\alpha_2^s\alpha_3^t \,:\, 0 \le r \le R_2,\, 0 \le s \le S_2,\, 0 \le t \le T_2\} > 2KL$, *and*

(v) $(R_3+1)(S_3+1)(T_3+1) > 6K^2L$,

are satisfied, **then either**

$$\Lambda' > \rho^{-KL}, \quad \textit{where} \quad \Lambda' = |\Lambda| \cdot \frac{LSe^{LS|\Lambda|/(2b_2)}}{2|b_2|},$$

or—*degenerate case—at least one of the following three conditions* (**C1**), (**C2**), (**C3**) *holds:*

(**C1**) $$|b_1| \le R_1, \quad |b_2| \le S_1 \quad \textit{and} \quad |b_3| \le T_1;$$

(**C2**) $$|b_1| \le R_2, \quad |b_2| \le S_2 \quad \textit{and} \quad |b_3| \le T_2;$$

(**C3**) **either** *there exist two non-zero rational integers* r_0 *and* s_0 *such that*

$$r_0 b_2 = s_0 b_1$$

with

$$|r_0| \le \frac{(R_1+1)(T_1+1)}{\mathcal{M}-T_1} \quad \textit{and} \quad |s_0| \le \frac{(S_1+1)(T_1+1)}{\mathcal{M}-T_1},$$

where we put

$$\mathcal{M} = \max\Big\{R_1+S_1+1,\, S_1+T_1+1,\, R_1+T_1+1,\, \chi\mathcal{V}\Big\},$$

or *there exist rational integers* r_1, s_1, t_1 *and* t_2, *with* $r_1 s_1 \ne 0$, *such that*

$$(t_1b_1 + r_1b_3)s_1 = r_1b_2t_2, \qquad \gcd(r_1,t_1) = \gcd(s_1,t_2) = 1,$$

which also satisfy

$$|r_1s_1| \le \delta\,\frac{(R_1+1)(S_1+1)}{\mathcal{M}-\max\{R_1,S_1\}},\ |s_1t_1| \le \delta\,\frac{(S_1+1)(T_1+1)}{\mathcal{M}-\max\{S_1,T_1\}},$$
$$|r_1t_2| \le \delta\,\frac{(R_1+1)(T_1+1)}{\mathcal{M}-\max\{R_1,T_1\}},$$

where we take

$$\delta = \gcd(r_1,s_1).$$

Moreover, when $t_1 = 0$, we can take $r_1 = 1$, and when $t_2 = 0$ we can take $s_1 = 1$.

8.4. Application. The first step is to get an upper bound on p free of any condition. For this purpose, our previous Theorem 4 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, which leads to

$$p < 4 \times 10^{14},$$

as already mentioned at the beginning of Section 6.

In practice, it is important to notice that the larger y is, the smaller is the upper bound on p obtained via linear forms of logarithms is. Hence, the lower bounds on y proved at the end of Section 6 will be very useful.

Now we can apply Theorem 4. First, we may suppose that $p > 10^8$. To apply our result, we have to distinguish two cases according to whether $r \geq 0$, or $r < 0$. Since $n = d \times$ prime with $d \leq 8$ and $n > 8p$ by the proof of the above Lemma 6.3, we see that $r \neq 0$.

An application of a linear form in two logarithms shows that $|r| > 8$ for $p > 10^8$. [More precisely, if $|r| \leq 8$, we write $\Lambda = (r \log \alpha - \log q) - p \log(y\alpha^{-k})$ and we consider it as a linear form in **two** logarithms, to which we apply the main result of [22]; then we get $p < 10^8$: a contradiction.]

We thus have two cases, namely when $r > 8$ and when $r < -8$, respectively.

In the first case, following the notation of Theorem 4, we can take

$$\alpha_1 = y\alpha^{-k},\ \alpha_2 = \alpha,\ \alpha_3 = q, \quad b_1 = p,\ b_2 = r,\ b_3 = 1.$$

Then

$$\mathrm{h}(\alpha_1) = \tfrac{1}{2}\left(\log(y\alpha^{-k}) + \log(y\alpha^{k})\right) = \log y,$$

and

$$\log \alpha_1 = \tfrac{1}{p}(r \log \alpha - \log q - \Lambda) < \tfrac{1}{2} \log \alpha.$$

In the second case, we take

$$\alpha_1 = \alpha,\ \alpha_2 = \alpha^k/y,\ \alpha_3 = q, \quad b_1 = |r|,\ b_2 = p,\ b_3 = 1.$$

Then

$$\mathrm{h}(\alpha_2) = \mathrm{h}(y/\alpha^k) = \tfrac{1}{2} \log(y\alpha^{-k}) = \log y + \log(\alpha^k/y),$$

and

$$\log \alpha_2 = \log(\alpha^k/y) = \tfrac{1}{p}(\log q - r \log \alpha - \Lambda) < \tfrac{1}{2} \log \alpha + \tfrac{4}{p}.$$

Thus,

$$\mathrm{h}(\alpha_2) < \log y + \tfrac{1}{4} \log \alpha + \tfrac{2}{p}.$$

We also notice that we have to use linear forms in two logarithms in the degenerate case, in which case we apply the main result of [22]. In practice, it is important to optimize the choice of the parameter χ of Theorem 4.

Namely, we have to choose χ in such a way that the bounds obtained in the non-degenerate case and in the degenerate case are roughly the same.

Of course our results are obtained via a suitable program which chooses all the parameters in an optimal way. The details were given in several preceding papers ([10], [11]).

After several iterations of our program, we obtain Proposition 8.1.

9. Frey curves and level-lowering

In this section, we tackle equation (11) using the modular approach (by which we mean the approach to Diophantine equations via Frey curves and Galois representations). Before doing so, we make a choice concerning the value of m modulo 3. It follows from Lemma 2.1 and equation (4) that F_n and L_n are even precisely when n is divisible by 3. It follows, from (14) for example, that $3 \nmid m$. We note also that $L_{2m} = L_{-2m}$. Thus, by replacing m by $-m$, if necessary, we can suppose that $m \equiv 1 \pmod 3$. This assumption will bring some simplification in the application of the modular approach. However, the fact that we have allowed m to be negative means that we have to slightly change our conditions (12). Here, we rewrite our conditions to take into account both the possible change of sign for m as well as Lemmas 5.1 and 7.1 as:

$$p \geq 13 \text{ is prime}, \qquad r > 2 \times 10^5 \text{ is prime}, \tag{17}$$

$$(q, m) = (3, \pm r),\ (7, \pm 2r),\ (47, \pm 4r), \qquad m \equiv 1 \pmod 3. \tag{18}$$

We attach a Frey curve to each solution of equations (13), (14), (15) and use them to help solve our problem. Experience shows that the simultaneous use of more than one Frey curve gives far better information than the use of just one Frey curve. Such an approach is called the multi-Frey approach; see, for example, [12]. In the current paper, we use two Frey curves, one attached to equation (13) and the other to (14). Both these are equations of the form $Ax^p + By^p = Cz^2$. These equations are usually referred to as ternary Diophantine equations. For ternary Diophantine equations, suitable Frey curves have been specifically written down by Bennett and Skinner in [2]. The recipes of [2] are replicated in [13, Chapter 15], which is also a good introductory reference on the modular approach.

The reader will have noted that (15) is also of the same form $Ax^p + By^p = Cz^2$ and could also be used; alas, we have found that the relevant newforms that need to be computed for this equation are at too high a level to make such calculations useful.

Following the recipes in [2], we associate to solutions to equations (13) and (14) the Frey elliptic curves

$$\mathcal{G}_m \ : \quad Y^2 = X^3 + 5F_{2m}X^2 - 5X, \tag{19}$$

and

$$\mathcal{H}_m \ : \quad Y^2 = X^3 + 2L_m X^2 + 2(-1)^m X, \tag{20}$$

respectively.

Lemma 9.1. *The Galois representations on the 2-torsion of $\mathcal{G}_m$ and of $\mathcal{H}_m$ arise from normalized cuspidal newforms g and h of weight 2 and levels $100q$ and $128q$, respectively.*

The newforms have Fourier expansions around the cusp at infinity

$$g = w + \sum_{i\geq 2} g_i w^i, \qquad h = w + \sum_{i\geq 2} h_i w^i,$$

where the coefficients g_i, h_i are integers in certain number fields K_g, K_h. We denote the traces of the Frobenius of an elliptic curve E at a prime l by $a_l(E)$.

Lemma 9.2. *Suppose $l \neq 2, 5, q$, p is a prime. There exist primes $\mathfrak{P}_g$, $\mathfrak{P}_f$ of the fields K_g, K_h, both above p, such that*

(i) *if $l \nmid y$, then*

$$a_l(\mathcal{G}_m) \equiv g_l \pmod{\mathfrak{P}_g}, \qquad a_l(\mathcal{H}_m) \equiv h_l \pmod{\mathfrak{P}_h}.$$

(ii) *if $l \mid y$, then*

$$l + 1 \equiv \pm g_l \pmod{\mathfrak{P}_g}, \qquad l + 1 \equiv \pm h_l \pmod{\mathfrak{P}_h}.$$

For a prime $l \neq 5$ define

$$M_l = \begin{cases} l - 1, & \text{if } l \equiv \pm 1 \pmod 5, \\ 2(l + 1), & \text{if } l \equiv \pm 2 \pmod 5. \end{cases} \tag{21}$$

We will need the following lemma.

Lemma 9.3. *Suppose that $l \neq 5$ is a prime and $u \equiv v \pmod{M_l}$. Then*

$$F_u \equiv F_v \pmod l \qquad \text{and} \qquad L_u \equiv L_v \pmod l.$$

It follows that the traces of Frobenius $a_l(\mathcal{G}_m)$ and $a_l(\mathcal{H}_m)$ depend only on the value of m modulo M_l.

Proof. The first part follows from Lemma 2.1. The last part follows immediately from the first and the definitions of the Frey curves $\mathcal{G}_m$ and $\mathcal{H}_m$. □

Now let S_l be the set of integers $0 \leq m' \leq M_l - 1$ satisfying the following conditions:

(a) if $3 \mid M_l$, then $m' \equiv 1 \pmod 3$,
(b) $\gcd(m', M_l) = \gcd(2^\alpha, M_l)$, where $\alpha = 0, 1, 2$ according to whether $q = 3, 7$ or 47.

Let P_l be the largest prime factor of M_l.

Lemma 9.4. *Suppose that (m, y, p) is a solution to equation* (11) *satisfying conditions* (17), (18). *Let l be a prime satisfying*

$$l \neq 2,\ 5,\ q, \qquad P_l < 2 \times 10^5. \tag{22}$$

Then $m \equiv m' \pmod{M_l}$ for some $m' \in S_l$.

Proof. Let $0 \leq m' \leq M_l - 1$ be the unique integer satisfying $m \equiv m' \pmod{M_l}$. We would like to show that $m' \in S_l$. Suppose that r' is an odd prime dividing $\gcd(m', M_l)$. Then $r' \mid m$, and so from conditions (17) and (18) we deduce that $r' = r > 2 \times 10^5$. But $r' \mid M_l$, so $P_l > 2 \times 10^5$, giving a contradiction.

Hence, $\gcd(m', M_l) = 2^\alpha$. The fact that m', α satisfy (a) and (b.1–b.4) in the definition of S_l is quickly deduced from conditions (17) and (18). Thus, $m' \in S_l$ as required. □

The definition of S_l takes into account the information about m shown in (17) and (18). It does not take into account the information about m given by the Frey curves and the level-lowering. We will shortly introduce refinements of S_l that take into account this information also. Fix a pair of newforms (g, h) as above. Let $l \neq 2,\ 5,\ q$ be prime. For $m' \in S_l$ define

$$B_{g,h}(l, m') = \begin{cases} \gcd\left(\mathrm{Norm}(a_l(\mathcal{G}_{m'}) - g_l), \mathrm{Norm}(a_l(\mathcal{H}_{m'}) - h_l)\right), & \text{if } l \nmid L_{2m'}; \\ \gcd\left(\mathrm{Norm}((l+1)^2 - g_l^2), \mathrm{Norm}((l+1)^2 - h_l^2)\right), & \text{otherwise.} \end{cases}$$

Here, the norms are the absolute norms for the fields K_g and K_h, respectively. Let

$$B_{g,h}(l) = l \prod_{m' \in S_l} B_{g,h}(l, m'). \tag{23}$$

Lemma 9.5. *Suppose m, y, p and q satisfy equation* (11) *and conditions* (17) *and* (18). *Suppose that the Galois representations on $\mathcal{G}_m$, $\mathcal{H}_m$ arise from newforms g, h, respectively, and that l satisfies* (22). *Then*

$$p \mid B_{g,h}(l).$$

Proof. We note from the definition (23) that $l \mid B_{g,h}(l)$, and so the result follows trivially in the case $l = p$. We may therefore suppose that $l \neq p$.

By Lemma 9.4, we know that $m \equiv m' \pmod{M_l}$ for some $m' \in S_l$. Moreover, by Lemma 9.3, we observe that $l \mid L_{2m'}$ if and only if $l \mid L_{2m}$, which by equation (11) is equivalent to the condition $l \mid y$.

Lemma 9.3 also tells us that $a_l(\mathcal{G}_m) = a_l(\mathcal{G}_{m'})$ and $a_l(\mathcal{H}_m) = a_l(\mathcal{H}_{m'})$. It follows from Lemma 9.2 that p divides $B_{g,h}(l, m')$ and so it divides $B_{g,h}(l)$. □

9.1. Eliminating newforms. Lemma 9.1 gives too many possibilities for the newforms (g, h). For example, when $q = 47$, all we know is that g is a newform at level 4700 and h is a newform at level 6016. There are 27 newforms at level 4700 and 20 newforms at level 6016 (up to Galois equivalence). This gives us 540 possibilities for the pair (g, h). We would now like to eliminate all the possible pairs of newforms and keep just one pair for each of $q = 3$, $q = 7$ and $q = 47$, respectively. In each case the pair of newforms remaining will consist of two rational ones, and hence correspond to elliptic curves. We refer to these elliptic curves using their Cremona reference (as in Cremona's book [14], or his extended online tables [15]).

Proposition 9.6. *The Galois representations on the p-torsion of $\mathcal{G}_m$ and $\mathcal{H}_m$ arise from newforms corresponding to the elliptic curves $\mathcal{G}$ and $\mathcal{H}$ as follows:*

- *if $q = 3$, then $\mathcal{G} = 300D1$ and $\mathcal{H} = 384D1$;*
- *if $q = 7$, then $\mathcal{G} = 700H1$ and $\mathcal{H} = 896D1$;*
- *if $q = 47$, then $\mathcal{G} = 4700K1$ and $\mathcal{H} = 6016A1$.*

Proof. By Lemma 9.1, the Galois representation on the p-torsion of $\mathcal{G}_m$, and of $\mathcal{H}_m$ respectively arise from newforms at levels $100q$ and $128q$. `MAGMA` allows us to list all the newforms at these levels (the `MAGMA` program for doing this is based on algorithms explained in [32]). Suppose the Galois representation on the p-torsion of $\mathcal{G}_m$ and of $\mathcal{H}_m$ arise from a particular given pair of newforms g and h, respectively. By Lemma 9.5, we know that $p \mid B_{g,h}(l)$ for any prime l satisfying (22). We wrote a short `MAGMA` script which computes

$$C_{g,h} = \gcd\{B_{g,h}(l) \ : \ l < 100, \ l \neq 2, 5, q, \ l \text{ is prime}\}.$$

Now $p \geq 13$. If $C_{g,h}$ is divisible only by primes $2, 3, \ldots, 11$, then we have a contradiction, and we know that the pair (g, h) can be eliminated. For $q = 3$ and $q = 7$ we were able to eliminate all pairs except for the pair indicated in the proposition. For the indicated pair, all $B_{g,h}(l)$ computed were equal to 0. Let us explain why that is not surprising, taking for illustration the case $q = 7$. We note that the equation $L_{2m} = 7y^p$ has the solution $m = -2$ satisfying our condition $m \equiv 1 \pmod 3$. Now fix a prime l satisfying the above conditions. Let $m' = M_l - 2$. It is straightforward to check that $m' \in S_l$. By Lemma 9.3,

$$a_l(\mathcal{G}_{m'}) = a_l(\mathcal{G}_{-2}), \qquad a_l(\mathcal{G}_{m'}) = a_l(\mathcal{G}_{-2}).$$

But the elliptic curves $\mathcal{G}_{-2}$ and $\mathcal{H}_{-2}$ are isogeneous to the elliptic curves $\mathcal{G} = 700H1$ and $\mathcal{H} = 896D1$, respectively; let g and h be the newforms corresponding to this pair of elliptic curves. Thus,

$$g_l = a_l(\mathcal{G}) = a_l(\mathcal{G}_{-2}) = a_l(\mathcal{G}_{m'}), \quad h_l = a_l(\mathcal{H}) = a_l(\mathcal{H}_{-2}) = a_l(\mathcal{H}_{m'}).$$

It is easy to see that $B_{g,h}(l, m') = 0$ and so $B_{g,h}(l) = 0$.

For $q = 47$, there is a complication, which we now discuss. Let g and h be the newforms corresponding to the elliptic curves $\mathcal{G} = 4700K1$ and $\mathcal{H} = 6016A1$, respectively. At level 4700, there are 27 newforms (including g). One of these is

$$g' = w + \theta w^3 + \frac{1}{5}(-6\theta^8+23\theta^7+76\theta^6-304\theta^5-301\theta^4+1215\theta^3+383\theta^2-1390\theta-213)w^7+\dots,$$

with coefficients in $K = \mathbb{Q}(\theta)$ and θ is a root of

$$x^9 - x^8 - 22x^7 + 12x^6 + 169x^5 - 33x^4 - 508x^3 + 4x^2 + 503x + 71. \tag{24}$$

Our script eliminated all possible pairs of newforms except for (g, h) and (g', h). For (g, h), again all the $B_{g,h}(l)$ are zero for a similar reason to the above: $\mathcal{G}_4$ and $\mathcal{H}_4$ are isogeneous to the elliptic curves $\mathcal{G} = 4700K1$ and $\mathcal{H} = 6016A1$, respectively. However,

$$B_{g',h}(3) = 71,\ B_{g',h}(7) = 13^2 \times 71^2,\ B_{g',h}(11) = 2^{10} \times 7 \times 41 \times 47 \times 71, \dots$$

If $p \neq 71$, then we can eliminate the pair (g', h), and our proof is complete. For $p = 71$, we are unable to eliminate the pair (g', h) because all of the $B_{g',h}(l)$ are divisible by 71 as we shall prove shortly. Let $\mathfrak{P} = (\theta)$ be the principal ideal of K generated by θ. Note, by (24), that $\mathrm{Norm}_K(\theta) = -71$ and therefore $\mathfrak{P}$ is a prime ideal above 71. Write $g = \sum g_n w^n$ as before, and $g' = \sum g'_n w^n$. We would like to show that $g'_n \equiv g_n \pmod{\mathfrak{P}}$ for all $n \geq 1$. Proposition 9.7 below, applied to the modular form $g - g'$, says that it is sufficient for us to show that $g'_n \equiv g_n \pmod{\mathfrak{P}}$ for all $n \leq 1440$. We checked this again using a short `MAGMA` script. We deduce that $g'_n \equiv g_n \pmod{\mathfrak{P}}$ for all n. The reader can now use this to show that

$$71 \mid B_{g',h}(l, 4)$$

for all primes l. At first sight, eliminating the pair (g', h) when $p = 71$ appears hopeless, but there is a surprising twist coming up. Suppose the Galois representations on the p-torsion of $\mathcal{G}_m$ and $\mathcal{H}_m$ arise from g' and h. Then there is some prime ideal $\mathfrak{P}'$ of the field K, lying above 71, such that

$$a_l(\mathcal{G}_m) \equiv g'_l \pmod{\mathfrak{P}'},$$

for all $l \neq 2,\ 5,\ 47,\ l \nmid L_{2m}$. One checks that $M_3 = 8$ and $S_3 = \{4\}$. Moreover, $3 \nmid L_8 = 47$. Hence, $a_3(\mathcal{G}_m) = a_3(\mathcal{G}_4) = 0$. Thus, $\mathfrak{P}' \mid g'_3 = \theta$. It follows that $\mathfrak{P}' = \mathfrak{P}$. We deduce that

$$a_l(\mathcal{G}_m) \equiv g'_l \equiv g_l \pmod{\mathfrak{P}}.$$

But $a_l(\mathcal{G}_m)$ and g_l are in $\mathbb{Z}$. Hence,

$$a_l(\mathcal{G}_m) \equiv g_l \pmod{71},$$

for all but finitely many l. It now follows that the Galois representation on the p-torsion of $\mathcal{G}_m$, $\mathcal{H}_m$ also arises from the pair (g, h), as required! □

In the above proof, we used the following result of Kraus [19, Proposition 8.1] on congruences of modular forms.

Proposition 9.7. *(Kraus) Suppose that $\sum_{n\geq 0} a_n w^n$ is the Fourier expansion around infinity of a modular form of weight k and level N, with coefficients a_n belonging to the ring of integers $\mathcal{O}_K$ of a number field K. Suppose that $\mathcal{I}$ is a ideal of $\mathcal{O}_K$ dividing a_n for all*

$$n \leq \frac{kN}{12} \prod_{\substack{q \text{ prime,} \\ q|N}} \left(1 + \frac{1}{q}\right).$$

Then $\mathcal{I}$ divides a_n for all n.

10. Proof of Theorem 2 for $q = 127$

We now briefly turn our attention to equation (1) with $q = 127$ showing that it has no solutions. Note in this case, by Lemma 2.1, $2^6 = \mathrm{t}(127) \mid_2 n$. It is straightforward to adapt the first part of the proof of Corollary 2.3 to reduce to the case

$$L_{2m} = 127y^p,$$

where $p \geq 2$ is prime and $m = 2^5 r$. We are unable to show that r can be taken to be a prime, but merely observe that r must be odd. It is enough to show that this equation has no solutions.

Using a simple adaptation of the sieve used in the proof of Lemma 7.1, we can show that there are no solutions for prime exponent $2 \leq p \leq 11$. We now turn our attention to the $p \geq 13$. We may apply the double-Frey approach to $L_{2m} = 127y^p$ as in the previous section. We are forced to change the definition of S_l since $m = 2^5 r$ with r odd but not necessarily prime; we define S_l to be the set of integers $0 \leq m' \leq M_l - 1$ satisfying the following conditions:

(a) if $3 \mid M_l$, then $m' \equiv 1 \pmod 3$,
(b) $\gcd(2^5, M_l) \mid \gcd(m', M_l)$.

The arguments of the previous section now show that Galois representations on the p-torsion of $\mathcal{G}_m$ and of $\mathcal{H}_m$ arise from normalized cuspidal newforms g and h of weight 2 and levels 100×127 and 128×127, respectively. There are 26 newforms at the first level and 28 at the second level. Moreover, if l is any prime $\neq 2, 5, 127$, then $p \mid B_{g,h}(l)$ where $B_{g,h}(l)$ is as given in (23). We now apply the argument used in the proof of Proposition 9.6 which succeeds in eliminating **all** possible pairs of newforms g, h, giving a contradiction.

The computation of the relevant newforms took about 4.5 hours on a 2.8 GHz Opteron with 16 GB memory. The computation of newforms at high levels is a notoriously memory-intensive operation. In our case `MAGMA` used about 2 GB of memory. The same method can probably be used to solve equation (1) for the other values of q in (2), provided that the newforms at the relevant levels can be computed. This however is very much beyond the hardware that is currently available to us.

11. Congruences for m modulo p

In this section, we continue exploiting the modular approach. This time, our aim is to prove congruences for m modulo the exponent p. We continue with the notation of the previous section. In particular m, y, p, q and r are assumed to satisfy (11), (17), (18), $\mathcal{G}_m$ and $\mathcal{H}_m$ are the Frey curves given in (19) and (20), and $\mathcal{G}$ and $\mathcal{H}$ are as in Proposition 9.6.

Lemma 11.1. *Suppose $l \neq 2, 5$, q is a prime.*

(i) *If $l \nmid y$, then*

$$a_l(\mathcal{G}_m) \equiv a_l(\mathcal{G}) \pmod{p}, \quad a_l(\mathcal{H}_m) \equiv a_l(\mathcal{H}) \pmod{p}.$$

(ii) *If $l \mid y$, then*

$$l+1 \equiv a_l(\mathcal{G}) \left(\frac{-10F_{2m}}{l}\right) \pmod{p}, \quad l+1 \equiv a_l(\mathcal{H}) \left(\frac{-L_m}{l}\right) \pmod{p}.$$

Proof. The lemma follows from [20, Proposition 3]. If $l \nmid y$, then all the elliptic curves have good reduction at l. If $l \mid y$, then $\mathcal{G}$ and $\mathcal{H}$ have good reduction at l, and $\mathcal{G}_m$ and $\mathcal{H}_m$ have multiplicative reduction at l. Moreover, a quick calculation shows that $\mathcal{G}_m$, $\mathcal{H}_m$ have split reduction at l if and only if $-10F_{2m}$, $-L_m$ are squares modulo l, respectively. □

The above Lemma 11.1 includes a slight but very useful strengthening of Lemma 9.2, in that it allows the case $l = p$. This is very useful since p is not known and therefore awkward to avoid. We now fix a prime $p \geq 13$. Let $l \neq q$ be a prime with $l = kp + 1$, and $l \equiv \pm 1 \pmod{5}$. Let $A(p,k)$ be the set of $\zeta \in (\mathbb{F}_l^*)^p \backslash \{1\}$ satisfying

$$\left(\frac{q\zeta - 2}{l}\right) = \left(\frac{q\zeta + 2}{l}\right) = 1.$$

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

$$\delta_\zeta^2 \equiv q\zeta + 2(-1)^m.$$

Let

$$\mathcal{H}^\zeta \ : \quad Y^2 = X^3 + 2\delta_\zeta X^2 + 2(-1)^m X.$$

Lemma 11.2. *Suppose that $p \geq 13$ is prime. Suppose furthermore that there exists an integer k satisfying the following conditions:*

(a) *The integer $l = kp + 1$ is prime and $l \equiv \pm 1 \pmod 5$.*
(b) *The order of α modulo l is divisible p; equivalently, $\alpha^k \not\equiv 1 \pmod l$.*
(c) *For all $\zeta \in A(p, k)$,*
  (c.1) *if $l < p^2/4$ and $l \equiv 1 \pmod 4$ then $a_l(\mathcal{H}^\zeta) \neq a_l(\mathcal{H})$;*
  (c.2) *if $l < p^2/4$ and $l \equiv 3 \pmod 4$ then $a_l(\mathcal{H}^\zeta) \neq \pm a_l(\mathcal{H})$;*
  (c.3) *if $l > p^2/4$ and $l \equiv 1 \pmod 4$ then $a_l(\mathcal{H}^\zeta) \not\equiv a_l(\mathcal{H}) \pmod p$;*
  (c.4) *if $l > p^2/4$ and $l \equiv 3 \pmod 4$ then $a_l(\mathcal{H}^\zeta) \not\equiv \pm a_l(\mathcal{H}) \pmod p$.*

Then $m \equiv \pm 1, \pm 2, \pm 4 \pmod p$ according to whether $q = 3$, 7 and 47, respectively.

Proof. We first prove that $l \nmid y$. Suppose $l \mid y$. Then $y > 1$, and so by Corollary 6.2 we have that $y > 10^{10}$. However, from (11), we see that $l \mid L_{2m}$ or equivalently $\alpha^{2m} + \beta^{2m} \equiv 0 \pmod l$. Equation (9) leads to $\alpha^{8m} \equiv 1 \pmod l$. However, by assumption (b), we see that $p \mid m$, and from conditions (17) and (18) we deduce that $p = r$. We explain how to get a contradiction for $q = 47$; the other cases are almost identical. Since $m = 4r = 4p$, equation (11) can be rewritten as $L_{8p} = 47y^p$. Thus,

$$47y^p = \alpha^{8p} + \beta^{8p} < (\alpha^8 + \beta^8)^p = 47^p,$$

easily contradicting $y > 10^{10}$. Thus, $l \nmid y$. A similar reasoning shows that $l \nmid L_m$ and $l \nmid F_m$.

We next show that $y^p \equiv 1 \pmod l$. Suppose $y^p \not\equiv 1 \pmod l$. It is easy to see from equations (14) and (15) that there is some $\zeta \in A(k, p)$ such that $y^p \equiv \zeta \pmod l$; for this, we need our observation that $l \nmid F_m L_m$, and the fact that 5 is a quadratic residue modulo l because $l \equiv \pm 1 \pmod 5$. Further, from (14), $L_m \equiv \pm\delta_\zeta \pmod l$. Regarded as elliptic curves over $\mathbb{F}_l$, we note that $\mathcal{H}_m$ and $\mathcal{H}^\zeta$ are either identical, or quadratic twists by -1. If $l \equiv 1 \pmod 4$, then $a_l(\mathcal{H}_m) = a_l(\mathcal{H}^\zeta)$, and otherwise $a_l(\mathcal{H}_m) = \pm a_l(\mathcal{H}^\zeta)$. We complete the proof for $l \equiv 3 \pmod 4$; the proof for $l \equiv 1 \pmod 4$ is almost identical. By Lemma 11.1, we know that $a_l(\mathcal{H}_m) \equiv a_l(\mathcal{H}) \pmod p$. Hence,

$$a_l(\mathcal{H}^\zeta) \equiv \pm a_l(\mathcal{H}) \pmod p.$$

We have obtained a contradiction if $l > p^2/4$. Suppose now that $l < p^2/4$. The Hasse-Weil bounds tell us that both inequalities

$$|a_l(\mathcal{H}^\zeta)| \leq 2\sqrt{l}, \quad |a_l(\mathcal{H})| \leq 2\sqrt{l}$$

hold, so

$$|a_l(\mathcal{H}^\zeta) \mp a_l(\mathcal{H})| \leq 4\sqrt{l} < 2p.$$

But $a_l(\mathcal{H}^\zeta) \mp a_l(\mathcal{H})$ is divisible by p. Moreover, both curves $\mathcal{H}^\zeta$ and $\mathcal{H}$ have 2-torsion and so $a_l(\mathcal{H}^\zeta) \mp a_l(\mathcal{H})$ is divisible both by 2 and by p. It follows that $a_l(\mathcal{H}^\zeta) \mp a_l(\mathcal{H}) = 0$, giving a contradiction.

We have finally deduced that $y^p \equiv 1 \pmod{l}$. We complete the proof for the case $q = 47$, the other cases being similar. For $q = 47$, we have shown that

$$\alpha^{2m} + \beta^{2m} = L_{2m} = 47y^p \equiv 47 \pmod{l}.$$

Hence,

$$\alpha^{4m} - 47\alpha^{2m} + 1 \equiv 0 \pmod{l}.$$

The roots of the quadratic equation $X^2 - 47X + 1 = 0$ are α^8 and $\beta^8 = \alpha^{-8}$. Thus,

$$\alpha^{2m} \equiv \alpha^{\pm 8} \pmod{l}.$$

Since p divides the order of α modulo l, we obtain $m \equiv \pm 4 \pmod{p}$ as required. □

Proposition 11.3. *Suppose that m, y, p and q satisfy equation* (11) *and conditions* (17) *and* (18). *Then $m \equiv \pm 1, \pm 2, \pm 4 \pmod{p}$ according to whether $q = 3, 7, 47$, respectively.*

Proof. The result is true for $y = 1$, so we may suppose that $y > 1$. Proposition 8.1 says that $13 \le p < 1.05 \times 10^8$, $13 \le p < 1.92 \times 10^8$ and $13 \le p < 3.94 \times 10^8$ for $q = 3$, 7 and 47, respectively. Lemma 11.2 gives a criterion for showing that m satisfies the required congruence modulo p. We wrote a short `PARI/GP` program which, given a prime p in the indicated range, searches for suitable k satisfying the conditions of Lemma 11.2. For $q = 3$, 7 and 47, it took our program about 12 hours, 20 hours and 51 hours, respectively, to complete the proof of the proposition on a 3.2GHz Pentium IV. □

12. Linear forms in two logs I. A better upper bound for p

We now consider again the linear form studied previously, namely

$$\Lambda = n \log \alpha - \log q - p \log y,$$

with $n = 2r$, $4r$ or $8r$ with r prime for $q = 3$, 7 and 47, respectively. Let us put $n = dr$ to simplify the notation, where $d \in \{2, 4, 8\}$. We have seen that the modular method implies that

$$r \equiv \varepsilon \pmod{p}, \quad \text{when } \varepsilon = \pm 1.$$

We write $n = kdp + d\varepsilon$. Thus, Λ can be written as

$$\Lambda = p \log(\alpha^{kd}/y) - \log(q\alpha^{-d\varepsilon}).$$

Recall that

$$|\Lambda| < y^{-2p}.$$

We apply the main result of [22] to this linear form in **two** logarithms. The heights of the implied algebraic numbers satisfy

$$\mathrm{h}(\alpha^k/y) < \log(y) + 2/p, \quad \mathrm{h}(q\alpha^{-d\varepsilon}) = \log q.$$

In the case $\varepsilon = 1$, the logarithms which occur are very small and we get extremely good bounds:

- if $q = 3$, then $p \le 167$ (take $L = 8$ and $\rho = 32$ in the theorem of [22]);
- if $q = 7$, then $p \le 83$ (take again $L = 6$ but $\rho = 111$);
- if $q = 47$ then $p \le 113$ (choose now $L = 6$ and $\rho = 113.5$).

In the case $\varepsilon = -1$, the logarithms which occur are not small and we only get:

- if $q = 3$, then $p \le 1249$ (take $L = 8$ and $\rho = 23$ in the theorem of [22]);
- if $q = 7$, then $p \le 1949$, (take again $L = 8$ and $\rho = 23$);
- if $q = 47$, then $p \le 3863$, (choose now $L = 8$ and $\rho = 22$).

It may be useful to notice that in the case $q = 3$ and $\varepsilon = -1$, we get

$$p \le 1039 \quad \text{if } n > 2 \cdot 10^6$$

and that, in the case $\varepsilon = 1$, we get

$$p \le 127,\ 67,\ 107$$

for $q = 3$, 7 and 47, respectively, provided that $n > 1.1 \times 10^6$.

13. Simplifying the Thue equations

Later on, we will write down some Thue equations and use them to obtain an upper bound for n in terms of p.

Solving a Thue equation usually requires knowledge of the class group and units of the number field defined by the polynomial $F(u, 1)$ (see [3]); obtaining this information is a major difficulty once the degree of F is large. However, in case our Thue equation is of the form $F(u, v) = \pm 1$, where $F(u, 1)$ is monic, then all that is needed to solve the Thue equation is a subgroup of the unit group of full rank (see [18]). Likewise, the usual approach to bounding the size of the solutions of a Thue equation gives much better bounds if our Thue equation is of this desirable form.

Of the three auxiliary equations (13)–(15) in $\mathbb{Z}[\sqrt{-2}]$, the simplest one is (14). For $q = 3$, factoring the left-hand side of it we deduce that

$$L_m \pm \sqrt{-2} = (1 + \sqrt{-2})(u + v\sqrt{-2})^p. \tag{25}$$

Identifying imaginary parts, we obtain a Thue equation of the form $F(u, v) = \pm 1$, where $F(u, 1)$ is a monic polynomial.

For $q = 7$ and 47, we obtain instead

$$L_m \pm \sqrt{2} = \lambda(1+\sqrt{2})^r(u+v\sqrt{2})^p, \tag{26}$$

where $0 \le r \le p-1$, and $\lambda = 3+\sqrt{2}$ or $7+\sqrt{2}$ according to whether $q = 7$ or 47, respectively. Thus, we obtain p different Thue equations of the form $F(u,v) = \pm 1$, with unpleasant coefficients. Moreover, for $r \neq 0$, these Thue equations will not have the desirable property that $F(u,1)$ is monic. In this section, we use the modular approach to prove that for $q = 7$ and 47, the only possible value for r is $r = 0$. Thus, instead of having to solve p Thue equations, we only need to solve one which furthermore has the desirable property that $F(u,1)$ is monic. More importantly, as we will show in the next section, having $r = 0$ allows us also to derive that another linear form in two logarithms is small which improves our upper bounds on p for $q = 7$ and 47.

We establish that $r = 0$ by using a similar sieving technique to the one used in Section 11.

We assume that m, y, p, q and r satisfy equation (11) and conditions (17) and (18), where q is one of 7 or 47. Fix a prime $p \ge 13$. Let $l \neq q$ be a prime with $l = kp+1$ and $l \equiv \pm 1 \pmod 8$. Let $B(l,p)$ be the set of $\zeta \in (\mathbb{F}_l^*)^p$ satisfying

$$\left(\frac{5(q\zeta-2)}{l}\right) = \left(\frac{q\zeta+2}{l}\right) = 1.$$

Let $C(l,p)$ be the set of $\delta \in \mathbb{F}_l$ such that $\delta^2 = q\zeta+2$ for some $\zeta \in B(l,p)$. Let

$$\mathcal{H}^\delta \ : \quad Y^2 = X^3 + 2\delta X^2 + 2X.$$

Let $D(l,p)$ be the set of $\delta \in C(l,p)$ such that $a_l(\mathcal{H}^\delta) \equiv a_l(\mathcal{H}) \pmod p$. A straightforward modification of the first half of the proof of Lemma 11.2 proves that $L_m \equiv \delta \pmod l$ for some $\delta \in D(l,p)$.

Since $l \equiv 1 \pmod 8$, we may choose a square-root of 2 in $\mathbb{F}_l$ which we denote by $\sqrt{2}$. We also fix a primitive root of $\mathbb{F}_l^*$, and let

$$\theta_l \ : \quad \mathbb{F}_l^* \to \mathbb{Z}/(l-1)\mathbb{Z}$$

denote the discrete logarithm with respect to our fixed root. As $p \mid (l-1)$, we may compose this with the natural map $\mathbb{Z}/(l-1)\mathbb{Z} \to \mathbb{F}_p$ to obtain

$$\phi_l \ : \quad \mathbb{F}_l^* \to \mathbb{F}_p.$$

Using the fact that $L_m \equiv \delta \pmod l$ for some $\delta \in D(l,p)$, and applying ϕ_l to (26), we obtain

$$\phi_l(\delta \pm \sqrt{2}) - \phi_l(\lambda) \equiv r\phi_l(1+\sqrt{2}) \pmod p,$$

for some $\delta \in D(p,k)$.

Lemma 13.1. *Under the above conditions and notation, suppose moreover that* $\phi_l(1+\sqrt{2}) \not\equiv 0 \pmod{p}$. *Let*

$$\mathcal{E}(l,p) = \left\{ \frac{\phi_l(\delta+\sqrt{2}) - \phi_l(\lambda)}{\phi_l(1+\sqrt{2})},\ \frac{\phi_l(\delta-\sqrt{2}) - \phi_l(\lambda)}{\phi_l(1+\sqrt{2})} \quad : \quad \delta \in D(p,k) \right\}.$$

Then $r \bmod p \in \mathcal{E}(l,p)$.

Proposition 13.2. *We assume that* m, y, p, q *and* r *satisfy equation* (11) *and conditions* (17) *and* (18), *where* q *is one of* 7 *or* 47. *Then* $r = 0$ *in equation* (26).

Proof. We know that $0 \le r \le p-1$. To show that $r = 0$, all we have to show is that $r \equiv 0 \pmod{p}$. We wrote a short `PARI/GP` program which for a given p computes $\mathcal{E}(l_i,p)$ for suitable primes l_i satisfying the above conditions. If

$$\cap_i \mathcal{E}(l_i,p) = \{0 \bmod p\},$$

then our proof is complete for the particular prime p. It took about 2 minutes for our program to complete the proof for primes of the range $13 \le p \le 10^4$. But we have already shown in Section 12 that p is less than 4000. This completes the proof. □

14. Linear forms in two logs II. An even better upper bound for p

We previously witnessed in Section 12 the dramatic improvement in the upper bound for p after we were able to rewrite our linear form in 3 logarithms as a linear form in 2 logarithms. The bounds for p thus obtained are still somewhat large for the next step. However, for $q = 7$ and $q = 47$, there is another way of deriving a small linear form in two logarithms which can be used to yield better bounds for p. In this section, we prove the following result.

Proposition 14.1. *Suppose that* (m,y,p) *is a solution to equation* (11) *satisfying conditions* (17) *and* (18). *Suppose furthermore that* $m \ge 10^9$. *Then*

(1) *if* $q = 3$, *then* $p \le 1039$;
(2) *if* $q = 7$, *then* $p \le 1487$;
(3) *if* $q = 47$, *then* $p \le 797$.

The bound for the case $q = 3$ is the same one from Section 12; the method of this section is inapplicable here.

We continue with the previous notation and put $n = 2m$. Proposition 13.2 allows to write

$$L_m \pm \sqrt{2} = \lambda\gamma^p,$$

where γ is some algebraic number of norm y and $\lambda = 3+\sqrt{2}$ or $7+\sqrt{2}$ according to whether $q = 7$ or 47, respectively. Applying the algebraic conjugation (denoted by $z \mapsto z'$) and dividing we get

$$1 < (\lambda/\lambda')^{\pm 1}(\gamma/\gamma')^{\pm p} < 1 + 3L_m^{-1} < 1 + 2y^{-p/2}.$$

Thus, we consider the new linear form in **two** logarithms

$$\Lambda = \log(\lambda/\lambda') - p\,\log(\gamma'/\gamma),$$

which satisfies

$$|\Lambda| < 2y^{-p/2}.$$

We apply again the main result of [22] to this linear form in two logarithms. To estimate the heights of the implied algebraic numbers, the following elementary lemma is useful.

Lemma 14.2. *Let $aX^2 + bX + c$ be a quadratic polynomial with integer coefficients and with complex roots ξ and ξ'. Then the quotients ξ/ξ' and ξ'/ξ are the roots of the polynomial*

$$Q = acX^2 - (b^2 - ac)X + ac$$

whose Mahler measure is equal to $|ac|\max\{|\xi/\xi'|, |\xi'/\xi|\}$.

In particular, if ξ and ξ' are real, then

$$\mathrm{M}(Q) = |b^2 - ac| + (b^4 - 4acb^2)^{1/2}.$$

Otherwise,

$$\mathrm{M}(Q) = |ac|.$$

We now apply this Lemma 14.2. For $q = 7$, we have $\lambda = 3+\sqrt{2}$, which is a root of the polynomial X^2-6X+7. Thus, λ'/λ is a root of the polynomial $7X^2 - 22X + 7$, therefore

$$\mathrm{h}\left(\frac{3+\sqrt{2}}{3-\sqrt{2}}\right) = \tfrac{1}{2}\,\log(11+6\sqrt{2}).$$

To estimate the height of γ'/γ, we may assume that $\gamma' > \gamma$ without loss of generality. Then

$$\gamma > \left(\frac{L_m - \sqrt{2}}{3+\sqrt{2}}\right)^{1/p} \quad \text{and} \quad \gamma' < \left(\frac{L_m + \sqrt{2}}{3-\sqrt{2}}\right)^{1/p}.$$

We then get easily using the fact that $L_m - \sqrt{2} > 2^p - \sqrt{2} > 4p^2$ that

$$1 < \frac{\gamma}{\gamma'} < \left(\frac{(3+\sqrt{2})(L_m+\sqrt{2})}{(3-\sqrt{2})(L_m-\sqrt{2})}\right)^{1/p} < \left(\frac{3+\sqrt{2}}{3-\sqrt{2}}\right)^{1/p} e^{\frac{2\sqrt{2}}{p(L_m-\sqrt{2})}} < \left(\frac{3+\sqrt{2}}{3-\sqrt{2}}\right)^{1/(p-1)}$$

and

$$\mathrm{M}(\gamma/\gamma') < y \times \left(\frac{3+\sqrt{2}}{3-\sqrt{2}}\right)^{1/(p-1)}, \quad \mathrm{h}(\gamma/\gamma') < \frac{1}{2}\log y + \frac{1}{2(p-1)}\log\frac{3+\sqrt{2}}{3-\sqrt{2}}.$$

For $q = 47$ we have $\lambda = 7 + \sqrt{2}$, which is a root of the polynomial $X^2 - 14X + 47$. Then λ'/λ is a root of the polynomial $47X^2 - 102X + 47$. Thus,

$$\mathrm{h}\left(\frac{7+\sqrt{2}}{7-\sqrt{2}}\right) = \tfrac{1}{2}\log(51 + 14\sqrt{2}).$$

In this case,

$$\mathrm{M}(\gamma/\gamma') < y \times \left(\frac{7+\sqrt{2}}{7-\sqrt{2}}\right)^{1/(p-1)}, \quad \mathrm{h}(\gamma/\gamma') < \frac{1}{2}\log y + \frac{1}{2(p-1)}\log\frac{3+\sqrt{2}}{3-\sqrt{2}}.$$

Applying now the main theorem of [22], we deduce Proposition 14.1 in the following way; for $q = 7$, we take $L = 8$ and $\rho = 33.5$ in the main theorem of [22], while for $q = 47$, we take $L = 9$ and $\rho = 42$ in that theorem.

15. A bound for n in terms of p

Our objective in this section is to obtain bounds for n in terms of p for solutions to the equation $L_n = qy^p$ for the cases $q = 3$, 7 and 47, respectively.

15.1. Preliminaries. It follows from Baker's theory of linear forms in logarithms (see for example Chapter 9 from the book of Shorey and Tijdeman [30]), 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. But to solve our problem, we have just to consider the solutions which are Lucas numbers and then we can find all of them.

To get upper bounds for the solutions of the Thue equation involved here we might apply the results of Bugeaud and Győry [6] (see also Győry and Yu [17]). However, it is of much interest to rework the proof of Bugeaud and Győry in our particular context. On the one hand, our particular equations

have some nice properties not taken into account in the general result of [6], and, on the other hand, there has been an important improvement, due to Matveev, in the theory of linear forms in logarithms (see Theorem 3 of Section 8.2 for a precise statement) since [6] has appeared. Altogether, we actually compute a much better upper bound than the one obtained by applying the main result of [6] 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, [23] and [31]. We have however found it best to use a result of Landau.

Lemma 15.1. *Let $\mathbb{K}$ be a number field of degree $d = r_1+2r_2$, where r_1 and r_2 are the number of its real and complex embeddings, respectively. Denote its discriminant by $D_{\mathbb{K}}$, its regulator by $R_{\mathbb{K}}$, and the number of roots of unity in $\mathbb{K}$ by w. Let L be a real number such that $D_{\mathbb{K}} \le L$. 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

$$R_{\mathbb{K}} < C_{\mathbb{K}}(L).$$

We next apply again Matveev's lower bound for linear forms in logarithms (but now in the general case), given in Theorem 3 of Section 8.2.

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

Now we prove a lemma which gives a lower bound on the height of some algebraic numbers.

Lemma 15.2. *Let η be a real algebraic integer of degree d with r real conjugates and let M be the Mahler measure of η. Then*

$$r^2 \le 16d\log(2dM),$$

or, equivalently,

$$M \ge \frac{1}{2d}\,e^{r^2/(16d)}.$$

Proof. Without any loss of generality, we may suppose that η is positive. Let H be a positive integer and $D \geq d$ to be chosen later. Consider the set

$$E = \{P \in \mathbb{Z}[X] \,:\, P = \sum_{i=0}^{D} a_i X^i,\ 0 \leq a_i \leq H\},$$

and the map $P \mapsto P(\eta)$ from E to the real interval $I = [0, H(D+1)(\eta^*)^D]$, where we use $z^* = \max\{1, |z|\}$. If we partition the interval I into $H(H+1)^D$ subintervals of equal length, then, since E contains $(H+1)^{D+1}$ elements, there exist two different polynomials P_1 and P_2 in E such that $P_1(\eta)$ and $P_2(\eta)$ belong to the same subinterval. Putting $P = P_2 - P_1$, we then have

$$|P(\eta)| \leq (D+1)(H+1)^{-D}(\eta^*)^D,$$

and

$$|P(\eta_j)| \leq (D+1)H(\eta_j^*)^D$$

for each conjugate η_j of η. If now follows that

$$|\mathrm{Norm}\, P(\eta)| < (D+1)^d (H+1)^{d-1-D} M^D.$$

Thus, taking

$$H = \left\lfloor \left(M^D (D+1)^d \right)^{\frac{1}{D+1-d}} \right\rfloor,$$

we see that $|\mathrm{Norm}\, P(\eta)| < 1$. Hence, $P(\eta) = 0$. To conclude, we apply a theorem of Schur [29] to the polynomial P:

$$r^2 \leq 4D \log(\mathrm{L}(P)),$$

where $\mathrm{L}(P)$ is the length of P; *i.e.*, the sum of the absolute values of the coefficients of this polynomial. The result follows easily choosing $D = 2d - 1$. □

We next need some standard estimates on the roots of polynomials.

Lemma 15.3. *Let $P = \sum_{i=0}^{d} a_i X^{d-i}$ be a polynomial with complex coefficients, and let z be one of its roots. Then*

$$|a_0 z| \leq 2 \max_{1 \leq i \leq d} \{|a_i|^{1/i}\},$$

and the measure of P satisfies

$$\mathrm{M}(P) \leq \left(\sum_{i=0}^{d} |a_i|^2 \right)^{1/2}.$$

Moreover, if $\mathrm{sep}(P)$ is the minimal distance between different roots of P, then

$$\mathrm{sep}(P) > d^{-(d+2)/2} \mathrm{M}(P)^{1-d}.$$

Proof. The first inequality is a weaker version of an estimate proved by Lagrange. The bound on the measure is a corollary of a result of Landau of 1905 and the lower bound on $\mathrm{sep}(P)$ is due to Mahler. □

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

Lemma 15.4. *There exists a fundamental system $\{\varepsilon_1, \dots, \varepsilon_r\}$ of units in $\mathbb{K}$ 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 $(\log|\varepsilon_i^{(j)}|)_{i,j=1\dots r}$ do not exceed $(r!)^2\,2^{-r}\,(\log(3d))^3$. Here, $\alpha \to \alpha^{(j)}$ for $j = 1, \dots, r$ are the r complex embeddings of $\mathbb{K}$.

Proof. This is Lemma 1 of [5] combined with a result of Voutier [34] (see [6]) giving a lower bound for the height of any non-zero algebraic number which is not a root of unity. □

We also need sharp bounds for discriminants of number fields in a relative extension.

Lemma 15.5. *Let $\mathbb{K}_1 \subseteq \mathbb{K}_2$ be number fields 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 [28]. □

15.2. Statement of the results. In the case $q = 3$, we prove:

Proposition 15.6. *Suppose that $q = 3$ and that $p \ge 13$ is prime. Let γ be any root of the polynomial*

$$P(X) = \sum_{k=0}^{p} (-2)^{\lfloor k/2 \rfloor} \binom{p}{k} X^k, \tag{27}$$

and let $\mathbb{K} = \mathbb{Q}[\gamma]$. Let $C_{\mathbb{K}}(\cdot)$ be as in Lemma 15.1 and

$$\Theta = 11.7\cdot 30^{p+3}\,p^{15/2}\,(p-1)^{p+1}\,\left((p-1)!\right)^2\,(1+\log(p(p-1)))\,C_{\mathbb{K}}((6\sqrt{2})^{p-1}p^p).$$

Let $\mathcal{C}_{p,q} = 2.5p\,\Theta\log\Theta$. If (m, y, p) satisfies the equation (11) and conditions (17) and (18), then $m < \mathcal{C}_{p,q}$.

In the cases $q = 7$ and $q = 47$, we prove:

Proposition 15.7. *Suppose that $q = 7$ or 47 and that $p \ge 13$ is prime. Let again $\alpha = (1+\sqrt{5})/2$. For $q = 7$, put $e = 4$ and for $q = 47$, put $e = 8$.*

Denote the real p-th root of $q\alpha^e$ by ξ, set $\mathbb{K} = \mathbb{Q}[\sqrt{5}, \xi]$, and let $C_{\mathbb{K}}(\cdot)$ be as in Lemma 15.1. Let also

$$\Theta = 67 \cdot 30^{p+5}(p-1)^{p+2}p^3\,(p+2)^{5.5}\,(p!)^2\,(1+\log(2p(p-1))) \\ \times C_{\mathbb{K}}(p^{2p}\,(q^2-4)^p\,q^{2(p-1)})$$

and $\mathcal{C}_{p,q} = 1.25p\,\Theta\log\Theta$. If (m, y, p) satisfies the equation (11) *and conditions* (17) *and* (18)*, then $m < \mathcal{C}_{p,q}$.*

The method used to get Proposition 15.7 can also be applied for $q = 3$, but it then gives a larger upper bound for m than that obtained in Proposition 15.6.

15.3. Proof of Proposition 15.6. Let $n = 2m$ with m being an odd prime. From the relation $L_n = L_m^2 + 2$, we reduce the problem to solving the superelliptic equation $x^2 + 2 = 3y^p$. Put $\omega = \sqrt{-2}$. Factoring the left-hand side of it over $\mathbb{Z}[\omega]$, we deduce the existence of integers a and b with $a^2 + 2b^2 = y^2$ and

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

Consequently, we get

$$\pm 2\omega = (1+\omega)(a+b\omega)^p - (1-\omega)(a-b\omega)^p. \tag{28}$$

Dividing by 2ω, we get the Thue equation

$$\sum_{k=0}^{p} (-2)^{\lfloor k/2\rfloor} \binom{p}{k} X^k\,Y^{p-k} = \pm 1. \tag{29}$$

To bound the size of the solutions of (29) we follow the general scheme of [6], which was also used in [8]. Let $P(X)$ and γ and $\mathbb{K}$ be as in Proposition 15.6. We note that $P(X)$ is the polynomial naturally associated to the Thue equation (29). We first need information on the number field $\mathbb{K}$ and its Galois closure. We use the following lemma, a variant of which was proved in [10]:

Lemma 15.8. *The field $\mathbb{K} = \mathbb{Q}[\gamma]$ is totally real and its Galois closure $\mathbb{L}$ has degree $p(p-1)$ over $\mathbb{Q}$. Furthermore, the discriminant of $\mathbb{K}$ divides $3^{p-1}2^{(p-1)/2}(2p)^p$.*

Proof. Observe that any root of the polynomial

$$P(X) = \frac{1}{2\omega}\big((1+\omega)(X+\omega)^p - (1-\omega)(X-\omega)^p\big)$$

satisfies $|X+\omega| = |X-\omega|$, and so must be real. Hence, $\mathbb{K}$ is a totally real field. Furthermore, $\mathbb{L}[\omega]/\mathbb{Q}[\omega]$ is a Kummer extension obtained by adjoining the p-th roots of unity and the p-th roots of $(1+\omega)/(1-\omega)$. Hence, this extension has degree $p(p-1)$, and this is also true for $\mathbb{L}/\mathbb{Q}$.

Observe now that $\mathbb{K}[\omega]$ is generated over $\mathbb{Q}[\omega]$ by any root of either one of the following two monic polynomials with coefficients in $\mathbb{Z}[\omega]$, $Y^p - (1+\omega)(1-\omega)^{p-1}$, or $Y^p - (1-\omega)(1+\omega)^{p-1}$. Since the discriminant D_1 of the extension $\mathbb{K}[\omega]/\mathbb{Q}[\omega]$ divides the discriminant of each of these polynomials, we get that D_1 divides $p^p 3^{p-1}(1-\omega)^{(p-1)(p-2)}$ and $p^p 3^{p-1}(1+\omega)^{(p-1)(p-2)}$. However, $1+\omega$ and $1-\omega$ are relatively prime, thus D_1 divides $3^{p-1}p^p$. Furthermore, estimating the discriminant of $\mathbb{K}[\omega]/\mathbb{Q}$ in two different ways thanks to Lemma 15.5, gives

$$|D_{\mathbb{K}[\omega]}| = 8^p D_1^2 = |D_{\mathbb{K}}|^2 |\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(D_{\mathbb{K}[\omega]/\mathbb{K}})|. \tag{30}$$

Consequently, $|D_{\mathbb{K}}|$ divides $3^{p-1}2^{(p-1)/2}(2p)^p$. □

Let $\gamma_1, \ldots, \gamma_p$ be the roots of $P(X)$ and let (X, Y) be a solution of (29). Without any loss of generality, we assume that $\gamma = \gamma_1$ and $|X - \gamma_1 Y| = \min_{1\le j\le p} |X - \gamma_j Y|$. We will make repeated use of the fact that $|\gamma_1|, \ldots, |\gamma_p|$ are not larger than $2p$ by the first assertion of Lemma 15.3. Moreover, the Mahler measure of P is at most $(1+\sqrt{2})^p$ by an easy application of Landau's inequality given in Lemma 15.3. Assuming that Y is large enough, namely that

$$\log |Y| \ge (30p)^p, \tag{31}$$

we get (using the lower bound for $\mathrm{sep}(P)$ of Lemma 15.3)

$$|Y| \ge p \max_{2\le j\le p} \{|\gamma_1 - \gamma_j|^{-1}\},$$

which implies

$$|X - \gamma_j Y| \ge |\gamma_1 - \gamma_j||Y| - |X - \gamma_1 Y| \ge \left(1 - \frac{1}{p}\right) |\gamma_1 - \gamma_j||Y|.$$

Hence,

$$|X - \gamma_1 Y| \le 3 \left(\prod_{2\le j\le p} |\gamma_1 - \gamma_j| \right) |Y|^{-p+1} \le (4p)^p |Y|^{-p+1}, \tag{32}$$

since $\prod_{2\le j\le p} |\gamma_1 - \gamma_j| = P'(\gamma_1) \le p\,(1 + \sqrt{2}\,|\gamma_1|)^{p-1} < p\,(3p+1)^{p-1}$.

From the 'Siegel identity'

$$(X - \gamma_1 Y)(\gamma_2 - \gamma_3) + (X - \gamma_2 Y)(\gamma_3 - \gamma_1) + (X - \gamma_3 Y)(\gamma_1 - \gamma_2) = 0,$$

we have

$$\Lambda = \frac{\gamma_2 - \gamma_3}{\gamma_3 - \gamma_1} \cdot \frac{X - \gamma_1 Y}{X - \gamma_2 Y} = \frac{X - \gamma_3 Y}{X - \gamma_2 Y} \cdot \frac{\gamma_2 - \gamma_1}{\gamma_3 - \gamma_1} - 1.$$

Observe that the unit rank of $\mathbb{K}$ is $p-1$ since $\mathbb{K}$ is totally real. Let $\varepsilon_{1,1}$, $\ldots$, $\varepsilon_{1,p-1}$ be a fundamental system of units in $\mathbb{K}=\mathbb{Q}[\gamma_1]$ satisfying

$$\prod_{1\le i\le p-1} \mathrm{h}(\varepsilon_{1,i}) \le \frac{\big((p-1)!\big)^2}{2^{p-2}p^{p-1}}\, R_{\mathbb{K}}. \tag{33}$$

The fact that this exists is a consequence of by Lemma 15.4. Denote the conjugates of $\varepsilon_{1,1}$, $\ldots$, $\varepsilon_{1,p-1}$ in $\mathbb{Q}[\gamma_2]$ and $\mathbb{Q}[\gamma_3]$, by $\varepsilon_{2,1}$, $\ldots$, $\varepsilon_{2,p-1}$ and $\varepsilon_{3,1},\ldots,\varepsilon_{3,p-1}$, 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 equation (29) is a unit. Thus $X-\gamma_1 Y$ is a unit. This simple observation appears to be crucial, since, roughly speaking, it allows us to gain a factor of size around $p^pR_{\mathbb{K}}$ (compare with the proofs in [6] and in [8]).

Since the only roots of unity in $\mathbb{K}$ are ±1, there exist integers b_1, $\ldots$, b_{p-1} such that $X-\gamma_1 Y=\pm\varepsilon_{1,1}^{b_1}\cdots\varepsilon_{1,p-1}^{b_{p-1}}$. We thus have

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

As in [6, 6.12], we infer from Lemma 15.4 that

$$\begin{aligned} B=\max\{|b_1|,\ldots,|b_{p-1}|\} &\le 2^{2-p}\,p\,(p!)^2\,(\log(3p))^3\,\mathrm{h}(X-\gamma_1Y)\\ &\le p^{2(p+1)}\,\log|Y|, \end{aligned} \tag{34}$$

by (32).

Further, we notice that

$$\mathrm{h}\left(\frac{\gamma_2-\gamma_1}{\gamma_3-\gamma_1}\right)\le 4\,\mathrm{h}(\gamma_1)+\log 4\le 4\log(1+\sqrt{2})+\log 4,$$

since we have

$$\mathrm{h}(\gamma_1)\le\frac{\log \mathrm{M}(P)}{p}\le\log(1+\sqrt{2}).$$

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

$$\mathrm{h}'\left(\frac{\gamma_2-\gamma_1}{\gamma_3-\gamma_1}\right)\le 2(2\log(1+\sqrt{2})+\log 2)p(p-1).$$

By Lemma 15.8, we may replace the absolute value of the discriminant of $\mathbb{K}$ by $(6\sqrt{2})^{p-1}p^p$, since for the upper bound on n we only aim to find an increasing function of p. 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 15.2, the height of the real algebraic integer $\varepsilon_{1,i}$ satisfies $\mathrm{h}(\varepsilon_{1,i})>1$. We thus get

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

Consequently, using Theorem 3 in the real case with $n = p$ and $D = p(p-1)$, we get

(35)
$$\log|\Lambda| > -2.8\cdot 30^{p+3}p^{9/2}(p(p-1))^{p+2}\,(2\log(1+\sqrt{2})+\log 2) \times (1+\log(p(p-1)))(1+\log B)\,(1+\log 2)\,2^{p-1}\prod_{1\le i\le p-1}\mathrm{h}(\varepsilon_{1,i}).$$

Now (33) gives us that

(36)
$$\log|\Lambda| > -2.8\cdot 30^{p+3}\,p^{15/2}\,(p-1)^{p+2}\,(2\log(1+\sqrt{2})+\log 2)\,((p-1)!)^2 \times\,(1+\log 2)(1+\log(p(p-1)))\,(1+\log B)\,R_{\mathbb{K}}.$$

Furthermore, it follows from (32) that

$$\log|\Lambda| < 2p\log(2p) - (p-1)\log|Y|. \tag{37}$$

By (34), we have the upper bound

$$(1+\log B) < 3p^2 + \log\log|Y|. \tag{38}$$

Finally, we observe that since $L_n = 3y^p$ for some even $n > 100$, then there are integers X and Y such that (X, Y) is a solution of the Thue equation (29) and $(L_n/3)^{1/p} = X^2 + 2Y^2$. Since $|X| \le 3p|Y|$ and $L_n \ge \alpha^n$ (since n is even), we derive from (31) that $n < 4.2\,p\log|Y|$. It then follows from (36), (37), and (38), together with Lemmas 15.1 and 15.8, that

$$n < 5\,p\,\Theta\log\Theta,$$

with

$$\Theta = 11.7\cdot 30^{p+3}\,p^{15/2}\,(p-1)^{p+1}\,((p-1)!)^2\,(1+\log(p(p-1)))\,C_{\mathbb{K}}((6\sqrt{2})^{p-1}p^p).$$

This proves Proposition 15.6.

15.4. Proof of Proposition 15.7. Recall that

$$qy^p = L_n = \alpha^n + \beta^n.$$

By Proposition 11.3, the index n is congruent to $\pm e$ modulo p, where $e = 4$ if $q = 7$, and $e = 8$ if $q = 47$. This means that there exists an integer ν such that

$$(\alpha^\nu)^p - q\alpha^{\mp e}y^p = -\alpha^{\mp e}\beta^n.$$

Thus, we are left with a Thue equation, namely

$$X^p - q\alpha^{\mp e}\,Y^p = \text{unit in } \mathbb{Q}[\sqrt{5}]. \tag{39}$$

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

As in the statement of Proposition 15.7, we denote the real p-th root of $q\alpha^e$ by ξ and set $\mathbb{K} = \mathbb{Q}[\sqrt{5}, \xi]$. Let ζ be a primitive p-th root of unity.

Lemma 15.9. *The field $\mathbb{K}$ has degree $2p$ and we have $r_1 = 2$, $r_2 = p-1$ and $r = p$. The absolute value of the discriminant of $\mathbb{K}$ is at most $p^{2p}\,(q^2-4)^p\,q^{2(p-1)}$. Its non-trivial subfields are $\mathbb{Q}[\sqrt{5}]$ and $\mathbb{Q}[\xi-\xi^{-1}]$, whose discriminants are, in absolute value, at most $p^p\,3^p\,q'^p\,5^{p-1}\,q^{p-1}$, where $q' = 1$ if $q = 7$, and $q' = 7$ if $q = 47$. Furthermore, the Galois closure $\mathbb{L}$ of $\mathbb{K}$ is the field $\mathbb{K}[\zeta]$, of degree $2p(p-1)$.*

Proof. It is easy to verify that the minimal defining polynomial of ξ over $\mathbb{Z}$ is $R(X) = X^{2p} - q^2X^p + q^2$. We thus have

$$|D_{\mathbb{K}}| \le |\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(R'(\xi))| = |\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(pq(2\alpha^e - q)\xi^{p-1})| = p^{2p}\,(q^2-4)^p\,q^{2(p-1)}.$$

The fact that $\mathbb{K}$ has only two non-trivial subfields, one of degree two, and another of degree p, is clear. Furthermore, since $\mathbb{K}$ is obtained from the field $\mathbb{Q}[\xi-\xi^{-1}]$ by adjoining $\sqrt{5}$, we get from Lemma 15.5 that the absolute value of the discriminant of the field $\mathbb{Q}[\xi-\xi^{-1}]$ is not greater than $p^p\,3^p\,q'^p\;5^{p-1}q^{p-1}$, where $q' = 1$ if $q = 7$, and $q' = 7$ if $q = 47$ (here, we use the factorizations $7^2-4 = 3^2\cdot 5$ and $47^2-4 = 3^2\cdot 7^2\cdot 5$). Since the roots of the polynomial $R(X)$ are the algebraic numbers ξ, $\zeta\xi$, $\ldots$, $\zeta^{p-1}\,\xi$, $\sqrt[p]{q\alpha^{-e}}$, $\zeta\sqrt[p]{q\alpha^{-e}}$, $\ldots$, $\zeta^{p-1}\sqrt[p]{q\alpha^{-e}}$, 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 15.4. There exist integers $b_1, \ldots, b_p$ such that

$$X - \xi Y = \pm\varepsilon_{1,1}^{b_1}\cdots\varepsilon_{1,p}^{b_p}.$$

We recall that we are only interested in the solutions (X, Y) of (39) with X and Y algebraic integers in the field $\mathbb{Q}[\sqrt{5}]$. Thus, X/Y is real, $|X - \sqrt[p]{\omega}Y|$ is small, and $|X - \zeta^j\xi Y|$ is quite large for $j = 1, \ldots, p-1$ (look at its imaginary part, for example). More precisely, for $Y > 2$, we get

$$|X - \xi Y| \le p^p\,Y^{-p+1}. \tag{40}$$

Furthermore, setting $B = \max\{|b_1|, \ldots, |b_p|\}$, Lemma 15.4 yields that

$$B \le 2^{1-p}\,p(p!)^2(\log 6p)^3\,\mathrm{h}(X-\xi Y) \le p^{2(p+1)}\,\log Y, \tag{41}$$

by our assumptions on X and Y.

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

$$\Lambda = \frac{\zeta-\zeta^2}{\zeta^2-1}\cdot\frac{X-\xi Y}{X-\zeta\xi Y} = \frac{X-\zeta^2\xi Y}{X-\zeta\xi Y}\cdot\frac{\zeta-1}{\zeta^2-1} - 1; \tag{42}$$

hence, the linear form in logarithms

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

where $\varepsilon_{2,p}$ (resp. $\varepsilon_{3,p}$) is the image of $\varepsilon_{1,p}$ under the embedding sending ξ to $\zeta\xi$ (resp. to $\zeta^2\xi$). 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 15.9 (we may again replace the absolute value of the discriminant of $\mathbb{K}$ by $p^{2p}\,(q^2-4)^p\,q^{2(p-1)}$, since we merely aim only to find an increasing function of p as an upper bound for n). Using Theorem 3 in the complex case with $n = p+1$ and $D = 2p(p-1)$, we get

$$\begin{aligned}\log|\Lambda| > {} & -3\cdot 30^{p+5}(p+2)^{5.5}\big(2p(p-1)\big)^{p+3}\,\big(1+\log(2p(p-1))\big)\\ & \times (1+\log(p+1)B)\,(\log 4)\,2^p \prod_{1\le i\le p}\mathrm{h}(\varepsilon_{1,i}).\end{aligned} \tag{43}$$

By (43) and Lemma 15.4, we get

$$\begin{aligned}\log|\Lambda| > {} & -3\cdot 30^{p+5}(p+2)^{5.5}\big(2p(p-1)\big)^{p+3}\,\big(1+\log(2p(p-1))\big)\\ & \times \big(1+\log((p+1)B)\big)\,(\log 4)\,2^{-p+1}\,p^{-p}\,(p!)^2\,R_{\mathbb{K}}.\end{aligned} \tag{44}$$

Furthermore, it follows from (40) and (42), that

$$\log|\Lambda| < 5p^2 - (p-1)\log|Y|. \tag{45}$$

Since $L_n = qy^p$ for some $n > 1000$, equation (39) has a solution (X,Y) with $Y = \big(q\alpha^{(n\mp e)}\big)^{1/p}$. We get that $n < 2.2\,p\log Y$. It then follows from (41), (43)–(45) and Lemma 15.1, that

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

with

$$\begin{aligned}\Theta = {} & 67\cdot 30^{p+5}(p-1)^{p+2}p^3\,(p+2)^{5.5}\,(p!)^2\,\big(1+\log(2p(p-1))\big)\\ & \times C_{\mathbb{K}}(p^{2p}\,(q^2-4)^p\,q^{2(p-1)}).\end{aligned}$$

This completes the proof of Proposition 15.7.

16. The double–Frey sieve

We continue with the assumption that m, y, p, q and r satisfy (11), (17), (18). From Propositions 15.6 and 15.7, we have that $|m| \le \mathcal{C}_{p,q}$ for some huge bound depending of p and q. In this section, we show that $m \equiv m_0 \pmod M$ where $m_0 = 1, -2$ or 4, according to whether $q = 3$, 7 or 47, respectively and $M > \mathcal{C}_{p,q}$. It follows at once that $m = m_0$ completing the proof of Theorem 1.

Let l be a prime satisfying (22). Let M_l, S_l be as in Section 9. We know from Lemma 9.4 that $m \equiv m' \pmod{M_l}$ for some $m' \in S_l$. Now fix some prime $\mathcal{P} \geq 13$. Let $\mathcal{N}(l, \mathcal{P})$ be set of $m' \in S_l$ satisfying

- $L_{2m'} \not\equiv 0 \pmod{l}$ and
$$\gcd\left(a_l(\mathcal{G}_{m'}) - a_l(\mathcal{G}), a_l(\mathcal{H}_{m'}) - a_l(\mathcal{H})\right)$$
is divisible by some prime $\geq \mathcal{P}$, or
- $L_{2m'} \equiv 0 \pmod{l}$ and
$$\gcd\left(l + 1 - a_l(\mathcal{G})\left(\frac{-10F_{2m'}}{l}\right), l + 1 - a_l(\mathcal{H})\left(\frac{-L_{m'}}{l}\right)\right)$$
is divisible by some prime $\geq \mathcal{P}$.

We see from Lemma 11.1 that $m \equiv m' \pmod{M_l}$ for some $m' \in \mathcal{N}(l, \mathcal{P})$, provided $p \geq \mathcal{P}$. It is convenient to think of $\mathcal{N}(l, \mathcal{P})$ as a subset of $\mathbb{Z}/M_l\mathbb{Z}$.

Now given two sets $\mathcal{N} \subset \mathbb{Z}/M\mathbb{Z}$ and $\mathcal{N}' \subset \mathbb{Z}/M'\mathbb{Z}$ we define their 'intersection' $\mathcal{N} \cap \mathcal{N}'$ to the set of elements in $\mathbb{Z}/\operatorname{lcm}(M, M')\mathbb{Z}$ whose reduction modulo M, M' is in $\mathcal{N}$, $\mathcal{N}'$, respectively. If $\mathcal{L} = \{l_1, \ldots, l_u\}$ is a set of primes satisfying the conditions (22) on l, define

$$\mathcal{N}(\mathcal{L}, \mathcal{P}) = \bigcap_{i=1}^{u} \mathcal{N}(l_i, \mathcal{P}), \qquad M_{\mathcal{L}} = \operatorname{lcm}\left(M_{l_1}, \ldots, M_{l_u}\right).$$

We deduce the following lemma.

Lemma 16.1. *If $p \geq \mathcal{P}$, then the reduction of m modulo $M_{\mathcal{L}}$ is in $\mathcal{N}(\mathcal{L}, \mathcal{P})$. Let $\mathcal{C}_{p,q}$ be as in either of Propositions 15.6 and 15.7. Suppose that the following two conditions are satisfied:*

- *$M_{\mathcal{L}} > \mathcal{C}_{p,q}$.*
- *$\mathcal{N}(\mathcal{L}, \mathcal{P}) = \{\overline{m_0} \in \mathbb{Z}/M_{\mathcal{L}}\mathbb{Z}\}$, where $m_0 = 1$ if $q = 3$, $m_0 = -2$ if $q = 7$ and $m_0 = 4$ if $q = 47$.*

Then the only solutions to equation $L_{2m} = qy^p$ have $m = \pm m_0$.

This is a far stronger sieve than the one used in [10, Section 10] and [7, Section 7] due to the simultaneous use of congruence conditions on the index m derived from two Frey curves.

16.1. Completion of the proof of Theorem 2. The rest of the proof is very much like [10, Section 10] and [7, Section 7]. We give some details for $q = 3$. We have reduced to solving the equation (11) and we would like to show that $m = \pm 1$. Let

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

Let $\mathcal{P} = 13$. Start with $\mathcal{L} = \{7\}$. We go through the primes $l \geq 11$ in order and we pick out those that satisfy $M_l \mid M$. If such a prime is found then

we append it to $\mathcal{L}$ and compute $\mathcal{N}(\mathcal{L}, \mathcal{P})$. Using 36 primes l, we find that

$$\mathcal{N}(\mathcal{L}, \mathcal{P}) = \{1 \bmod M\}.$$

We know so far, thanks to Lemma 16.1, that $m \equiv 1 \pmod{M}$. Hence, if $m \neq \pm 1$, then certainly $|m| \geq 10^{10}$. From Proposition 14.1, we know that $p \leq 1039$.

Now replace M by $M \times 23$, and continue to search for primes l such that $23 \mid M_l$ and $M_l \mid M$; append these to $\mathcal{L}$ and compute $\mathcal{N}(\mathcal{L}, \mathcal{P})$ until it is $\{1 \bmod M\}$, etc. After a few seconds we have that

$$M = 2^5 \times 3^3 \times 5^2 \times 7 \times 11 \times \cdots \times 193 \approx 1.4 \times 10^{80}$$

and $\mathcal{N}(\mathcal{L}, \mathcal{P}) = \{1 \bmod M\}$ with $\mathcal{L}$ having 104 elements. But $\mathcal{C}_{13,3} \approx 2.3 \times 10^{79}$. By Lemma 16.1 our proof is complete for $p = 13$. So, we let $\mathcal{P} = 17$ and suppose that $p \geq \mathcal{P}$. The reader will note that increasing $\mathcal{P}$ imposes a more stringent condition on the elements of $\mathcal{N}(l, \mathcal{P})$ making the sieve more efficient.

The entire computation for $13 \leq p \leq 1039$ took about 12 hours on a 2.2 GHz Intel Pentium IV. The approximates times for $q = 7$ and $q = 47$ were 74 hours, and 23 hours respectively.

References

[1] C. Batut, K. Belabas, D. Bernardi, H. Cohen, M. Olivier, *User's guide to PARI-GP*, version 2.3.2. (See also `http://pari.math.u-bordeaux.fr/`)

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

[3] Yu. Bilu, G. Hanrot, *Solving Thue equations of high degree*. J. Number Theory **60** (1996), 373–392.

[4] W. Bosma, J. Cannon, C. Playoust: *The Magma Algebra System I: The User Language*. J. Symb. Comp. **24** (1997), 235–265.
(See also `http://www.maths.usyd.edu.au:8000/u/magma/`)

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

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

[7] Y. Bugeaud, F. Luca, M. Mignotte, S. Siksek, *Perfect Powers from Products of Terms in Lucas Sequences*, J. reine angew. Math. **611** (2007), 109–129.

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

[9] Y. Bugeaud, M. Mignotte, 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.

[10] Y. Bugeaud, M. Mignotte, 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.

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

[12] Y. Bugeaud, M. Mignotte, S. Siksek, *A multi-Frey approach to some multi-parameter families of Diophantine equations*. Can. J. Math., **60** (2008), 491–519.

[13] H. Cohen, *Number Theory II. Analytic and Modern Methods*. GTM, Springer-Verlag, 2007.

[14] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd edition, Cambridge University Press, 1996.
[15] J. E. Cremona, *Elliptic curve data*, `http://www.maths.nott.ac.uk/personal/jec/`
[16] A. Dujella, A. Pethő, *A generalization of a theorem of Baker and Davenport*. Quart. J. Math. Oxford Ser. (2) **49**(1998), 291–306.
[17] K. Győry, K. Yu, *Bounds for the solutions of S-unit equations and decomposable form equations*. Acta Arith. **123** (2006), 9–41.
[18] G. Hanrot, *Solving Thue equations without the full unit group*. Math. Comp. **69** (2000), 395–405.
[19] A. Kraus, *Majorations effectives pour l'équation de Fermat généralisée*. Can. J. Math. **49** (1997), 1139–1161.
[20] A. Kraus, J. Oesterlé, *Sur une question de B. Mazur*. Math. Ann. **293** (1992), 259–275.
[21] E. Landau, *Verallgemeinerung eines Pólyaschen Satzes auf algebraische Zahlkörper*. Nachr. Kgl. Ges. Wiss. Göttingen, Math.-Phys. Kl. (1918), 478–488.
[22] M. Laurent, M. Mignotte, Y. Nesterenko, *Formes linéares en deux logarithmes et déterminants d'interpolation*. J. Number Theory **55** (1995), 255–265.
[23] H. W. Lenstra, Jr., *Algorithms in algebraic number theory*. Bull. Amer. Math. Soc. **26** (1992), 211–244.
[24] R. J. McIntosh, E. L. Roettger, *A search for Fibonacci-Wiefrich and Wolstenholme primes*. Math. Comp. **76** (2007), 2087–2094.
[25] 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.
[26] 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.
[27] M. Mignotte, *A kit on linear forms in three logarithms*, `http://www-irma.u-strasbg.fr/~bugeaud/travaux/kit.pdf`
[28] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*. Springer-Verlag, Berlin, 1990.
[29] I. Schur, *Untersuchungen über algebraische Gleichungen. I: Bemerkungen zu einem Satz von E. Schmidt*. Preuss. Akad. Sitzungsber. (1933), 403–428.
[30] T. N. Shorey, R. Tijdeman, *Exponential Diophantine equations*. Cambridge Tracts in Mathematics 87, Cambridge University Press, Cambridge, 1986.
[31] C. L. Siegel, *Abschätzung von Einheiten*. Nachr. Akad. Wiss. Göttingen II, Math.-Phys. Kl., Nr. 9, (1969), 71–86.
[32] W. A. Stein, *Modular Forms: A Computational Approach*. American Mathematical Society, Graduate Studies in Mathematics 79, 2007.
[33] Z. H. Sun, Z. W. Sun, *Fibonacci numbers and Fermat's last theorem*. Acta Arith. **60** (1992), 371–388.
[34] P. M. Voutier, *An effective lower bound for the height of algebraic numbers*. Acta Arith. **74** (1996), 81–95.
[35] D. D. Wall, *Fibonacci series modulo m*. Amer. Math. Monthly **67** (1960), 525–532.

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

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

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

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