Bennett et al. *Res. Number Theory* (2019)5:15
https://doi.org/10.1007/s40993-019-0153-2

Research in Number Theory

RESEARCH

Shifted powers in Lucas–Lehmer sequences

Michael A. Bennett[1*], Vandita Patel[2] and Samir Siksek[3]

*Correspondence: bennett@math.ubc.ca
[1]Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, Canada
Full list of author information is available at the end of the article

Abstract

We develop a general framework for finding all perfect powers in sequences derived via shifting non-degenerate quadratic Lucas–Lehmer binary recurrence sequences by a fixed integer. By combining this setup with bounds for linear forms in logarithms and results based upon the modularity of elliptic curves defined over totally real fields, we are able to answer a question of Bugeaud, Luca, Mignotte and the third author by explicitly finding all perfect powers of the shape $F_k \pm 2$ where F_k is the k-th term in the Fibonacci sequence.

Keywords: Exponential equation, Lucas sequence, shifted power, Galois representation, Frey curve, modularity, Level lowering, Baker's bounds, Hilbert modular forms, Thue equation

Mathematics Subject Classification: Primary 11D61, Secondary 11D41, 11F80, 11F41

1 Introduction

If $\{u_n\}$ is a non-degenerate integer binary linear recurrence sequence, then the sequence $\{u_n\}$ contains at most finitely many integer perfect powers, which may be effectively determined. This result was proved independently, using bounds for linear forms in Archimedean and non-Archimedean logarithms, by Pethő [19] and Shorey and Stewart [20]. The explicit determination of all such powers in a given sequence, however, has been achieved in only a few cases, principally in those where the problem may be reduced to a question of solving ternary Diophantine equations with integer coefficients. In such a situation, the possibility exists to combine the machinery of linear forms in logarithms with information derived from considering certain Frey–Hellegouarch curves corresponding to the ternary equations. A prototype for these problems may be found in the paper of Bugeaud, Mignotte and the third author [5], where all perfect powers in the Fibonacci sequence are determined; this amounts to finding the solutions to the equation

$$x^2 - 5y^{2p} = \pm 4,$$

in integers x, y and $p \geq 2$. Here, results from the theory of linear forms in logarithms provide a manageable upper bound upon the exponent p, but solving the remaining (hyperelliptic) equations is accomplished only through considering them as ternary equations of signature $(p, p, 2)$ and using arguments based upon the modularity of Galois representations to deduce arithmetic information guaranteeing that x is necessarily extraordinarily large (unless $x \in \{\pm 1, \pm 3\}$).

If we shift a given recurrence, considering, say, $u_n + c$ for a nonzero integer c, instead of just u_n, the situation becomes considerably more complicated. The resulting sequence need not possess much of the basic structure of a binary linear recurrence sequence, despite sharing a similar rate of growth. In particular, various divisibility statements may no longer hold, and questions of the existence of primitive divisors are significantly harder to address. Despite this, Shorey and Stewart [23] were able to show, under mild hypotheses, that, given fixed integers a and c, the equation

$$u_n + c = ay^p$$

has at most finitely many, effectively computable solutions. Only in very special cases, however, can such equations be made to correspond to Frey–Hellegouarch curves defined over $\mathbb{Q}$ (see e.g. the paper of Bugeaud, Luca, Mignotte and the third author [3] for a number of such examples).

In a previous paper [1], the first and third authors, with Dahmen and Mignotte, developed a method combining information derived from Frey–Hellegouarch curves defined over real quadratic fields with lower bounds for linear forms in logarithms to explicitly determine all shifted powers in certain binary recurrence sequences. The setup in [1] was as follows. Let K be a real quadratic number field, $\mathcal{O}_K$ its ring of integers and $\varepsilon \in \mathcal{O}_K$ a fundamental unit in K, with conjugate $\overline{\varepsilon}$. Define the Lucas sequences U_k and V_k, of the first and second kinds, respectively, via

$$U_k = \frac{\varepsilon^k - (\overline{\varepsilon})^k}{\varepsilon - \overline{\varepsilon}} \quad \text{and} \quad V_k = \varepsilon^k + (\overline{\varepsilon})^k, \quad \text{for} \quad k \in \mathbb{Z}.$$

Let $a, c \in \mathbb{Z}$ with $a \neq 0$, and consider the problem of determining the shifted powers $ay^p - c$ in one of these sequences, i.e. determining all integers k, y and p with $p \geq 2$ prime (say) such that we have

$$U_k + c = ay^p \tag{1}$$

or

$$V_k + c = ay^p. \tag{2}$$

In [1], techniques were introduced to potentially resolve such problems corresponding to either

- Eq. (1) with k odd and $\mathrm{Norm}(\varepsilon) = -1$, or
- Eq. (2) with either k even or $\mathrm{Norm}(\varepsilon) = 1$.

Let us now describe an approach to treat the remaining cases. For instance, a solution to (1) leads to the equation

$$\frac{\varepsilon^k - (\overline{\varepsilon})^k}{\varepsilon - \overline{\varepsilon}} = ay^p - c$$

and so we have

$$\varepsilon^{2k} + (\varepsilon - \overline{\varepsilon})c\varepsilon^k - \mathrm{Norm}(\varepsilon)^k = (\varepsilon - \overline{\varepsilon})a\varepsilon^k y^p.$$

It follows that

$$\left(2\varepsilon^k + (\varepsilon - \overline{\varepsilon})c\right)^2 - \left(4\,\mathrm{Norm}(\varepsilon)^k + (\varepsilon - \overline{\varepsilon})^2 c^2\right) = 4(\varepsilon - \overline{\varepsilon})a\varepsilon^k y^p. \tag{3}$$

Similarly, in the case of Eq. (2), we have

$$\varepsilon^k + (\overline{\varepsilon})^k = ay^p - c$$

whereby

$$\left(2\varepsilon^k + c\right)^2 + 4\,\mathrm{Norm}(\varepsilon)^k - c^2 = 4a\varepsilon^k y^p. \tag{4}$$

In either case (3) or (4), we can attach to a solution a Frey–Hellegouarch curve of signature $(p, p, 2)$, defined over the totally real (quadratic) field K.

2 Shifted powers in the Fibonacci sequence

We will now describe an open question from the literature which our techniques enable us answer. Let F_k be the *Fibonacci sequence* defined by

$$F_0 = 0, \quad F_1 = 1 \quad \text{and} \quad F_{k+2} = F_{k+1} + F_k.$$

Define further the *Lucas sequence* by

$$L_0 = 2, \quad L_1 = 1 \quad \text{and} \quad L_{k+2} = L_{k+1} + L_k.$$

For $K = \mathbb{Q}(\sqrt{5})$, writing

$$\varepsilon = \frac{1+\sqrt{5}}{2} \quad \text{and} \quad \overline{\varepsilon} = \frac{1-\sqrt{5}}{2},$$

it follows that ε is a fundamental unit of K and, by Binet's formula,

$$F_k = \frac{\varepsilon^k - \overline{\varepsilon}^k}{\sqrt{5}} \quad \text{and} \quad L_k = \varepsilon^k + \overline{\varepsilon}^k,$$

from which we obtain the well-known identity

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

In general, one has, for any integers a and b,

$$F_a L_b = F_{a+b} + (-1)^b F_{a-b}. \tag{6}$$

This identity is used with $|a-b| \in \{1, 2\}$ in [3] to solve the equations $F_k \pm 1 = y^p$ by reducing them to equations of the shape $F_k = \alpha y^p$, for fixed integers α (which may be treated by considering Frey–Hellegouarch curves defined over $\mathbb{Q}$). In this initial reduction, it is of importance that $F_{-1} = F_1 = F_2 = 1$ and $F_{-2} = -1$; more generally, analogous arguments allow one to treat equations of the form $F_n + c = y^p$, for $c = F_k$ where $k \equiv n \pmod 4$. In particular, such a reduction does not appear to be possible in general for the similar equation $F_k \pm 2 = y^p$ (which is posed an an open problem in [3]).

In this paper, we prove the following.

Theorem 1 *If k, y and $p \geq 2$ are integers, and*

$$F_k \pm 2 = y^p, \tag{7}$$

then $|k| \in \{1, 2, 3, 4, 9\}$.

Let us suppose that k, y and $p \geq 2$ are integers satisfying (7). In case k is odd, say $k = 2n + 1$, choosing $a = n + 2$ and $b = n - 1$ in (6),

$$F_k + (-1)^{n-1} 2 = F_{n+2} L_{n-1},$$

while $a = n - 1$ and $b = n + 2$ gives

$$F_k + (-1)^{n+2}2 = F_{n-1}L_{n+2},$$

and hence

$$F_{n+\delta_1}L_{n+\delta_2} = y^p \quad \text{where} \quad \{\delta_1, \delta_2\} = \{-1, 2\}. \tag{8}$$

We claim that

$$\gcd(F_{k\pm 3}, L_k) = \begin{cases} 4 & \text{if } k \equiv 3 \pmod 6, \\ 2 & \text{if } k \equiv 0 \pmod 6, \\ 1 & \text{otherwise.} \end{cases} \tag{9}$$

To see this, note the identities

$$3F_{k+3} = L_k + 4F_{k+2} \quad \text{and} \quad 3F_{k-3} = L_k - 4F_{k-2}$$

which imply, since $\gcd(F_{j+1}, F_j) = 1$ for each integer j, that $\gcd(F_{k\pm 3}, L_k) \mid 4$. The fact that

$$F_{k\pm 3} \equiv L_k \equiv 2 \pmod 4 \quad \text{if } k \equiv 0 \pmod 6$$

and

$$F_{k\pm 3} \equiv L_k \equiv 0 \pmod 4 \quad \text{if } k \equiv 3 \pmod 6,$$

while F_k and L_k are odd unless $3 \mid k$ completes the proof.

From (8) and (9), it thus follows that $L_{n+\delta_2} = 2^\alpha y_1^p$ for integers $\alpha \geq 0$ and y_1. Appealing to Theorem 2 of [4], and the identity $L_{-m} = (-1)^m L_m$, we thus have that

$$|n + \delta_2| \in \{0, 1, 3, 6\}.$$

We check that $F_{2n+1} \pm 2$ is a perfect power only for those n corresponding to

$$F_{-9} + 2 = F_9 + 2 = 6^2, \; F_{-9} - 2 = F_9 - 2 = 2^5, \; F_{-3} + 2 = F_3 + 2 = 2^2,$$
$$F_{-3} - 2 = F_3 - 2 = 0 \;\text{ and }\; F_{-1} - 2 = F_1 - 2 = -1.$$

We may thus suppose for the remainder of this paper that $k = 2n$ is even, so that $F_{-k} = -F_k$, and hence, without loss of generality, that $F_{2n} + 2 = \pm y^p$. The case $p = 2$ is easily dealt with by reducing the problem to the determination of integral points on elliptic curves; we will do this in Lemma 3.1. Assuming this result for the remainder of this section, we may therefore suppose, without loss of generality, that $p \geq 3$ is an odd prime and so, if necessary, absorb the minus sign into the y^p. We therefore consider the equation

$$F_{2n} + 2 = y^p. \tag{10}$$

This is of the shape (1) with $k = 2n$, $c = 2$ and $a = 1$. Writing $x = \varepsilon^{2n} + \sqrt{5}$, equation (3) implies that

$$x^2 - 6 = \sqrt{5}\varepsilon^{2n}y^p. \tag{11}$$

By thinking of the constant -6 as $-6 \cdot 1^p$, we may view this equation as a generalized Fermat equation of signature $(p, p, 2)$ over $\mathbb{Q}(\sqrt{5})$. To the solution (x, y, n, p) of (11) (and hence to the solution (n, y, p) to (10)) we associate the Frey–Hellegouarch curve

$$E_n \;:\; Y^2 = X^3 + 2xX^2 + 6X, \qquad x = \varepsilon^{2n} + \sqrt{5}. \tag{12}$$

This will prove much easier to deal with than the corresponding (p, p, p) equation defined over $\mathbb{Q}(\sqrt{5}, \sqrt{6})$ that we obtain from the arguments of [1]. We shall apply modularity and level-lowering to the mod p representation of E_n to deduce the following.

Proposition 2.1 *Let (n, y, p) be a solution to (10) with $p \geq 5$. Let $\overline{\rho}_{E_n,p}$ be the mod p representation of E_n. Then $\overline{\rho}_{E_n,p}$ is irreducible. Moreover, $\overline{\rho}_{E_n,p} \sim \overline{\rho}_{\mathfrak{f},\pi}$ where $\mathfrak{f}$ is a Hilbert eigenform over $\mathbb{Q}(\sqrt{5})$ of weight $(2, 2)$ that is new of level*

$$\mathcal{N} = (2)^7 \cdot (3) \cdot (\sqrt{5}); \tag{13}$$

here $\pi \mid p$ is some prime of $\mathcal{O}_{\mathfrak{f}}$, the ring of integers of the number field generated by the Hecke eigenvalues of $\mathfrak{f}$.

The Hilbert newspace for weight $(2, 2)$ and level $\mathcal{N}$ has dimension 6144. It is not possible using current software and hardware capabilities to compute the eigenforms belonging to this space. One of the novelties of the current paper is a sieving argument that works with mod p eigensystems to eliminate all of the space except for three elliptic curves.

The resolution of (10) will require certain non-trivial computations. These are carried out in the computer algebra system `Magma` [2]. The reader can find our `Magma` scripts at https://www.math.ubc.ca/~bennett/BePaSi.

3 Dealing with small p and small $|y|$

We shall apply the methods of Galois representations and modularity to equation (10). Such techniques are somewhat harder to utilize with small exponent p, and so in this section we deal with the cases $p = 2$ and $p = 3$ separately. Later on, we will appeal to bounds for linear forms in logarithms to (10), and for this it is useful to know that y is not too small. We show below that if $n \neq -2, -1$ then $|y| \geq 19$.

Lemma 3.1 *The only solutions to the equation $F_{2n} + 2 = \pm y^2$ are $(n, y) = (-1, \pm 1)$ and $(-2, \pm 1)$.*

Proof Let $Y = 5yL_{2n}$ and $X = 5y^2$. It follows from identity (5) that (X, Y) is an integral point on one of the two elliptic curves

$$Y^2 = X(X^2 - 20X + 120) \quad \text{or} \quad Y^2 = X(X^2 + 20X + 120).$$

To determine the integral points on these two elliptic curves we used the computer package `Magma` [2] which utilizes a standard algorithm that employs lower bounds for linear forms in elliptic logarithms [22] (implemented in `Magma` as *IntegralPoints*). We find that the integral points on the first curve are given by

$$(X, Y) \in \left\{(0, 0), (5, \pm 15), (24, \pm 72)\right\},$$

and those on the second are

$$(X, Y) \in \left\{(0, 0), (5, \pm 35), (24, \pm 168)\right\}.$$

The lemma follows. □

Lemma 3.2 *If $p = 3$ then the only solutions to (10) are $(n, y) = (-1, 1)$ and $(n, y) = (-2, -1)$.*

Proof Write $2n = \alpha + 3m$ where $\alpha = 0, \pm 1$. Let

$$X = \sqrt{5}\varepsilon^{m+\alpha} y, \qquad Y = \sqrt{5}\varepsilon^{\alpha} x.$$

From (11), we deduce that (X, Y) is an $\mathcal{O}_K$-integral point on the elliptic curve

$$Y^2 = X^3 + 30\varepsilon^{2\alpha}.$$

These three elliptic curves (corresponding to $\alpha = 0, 1, -1$) all have rank 2 over K, and we are able to compute the $\mathcal{O}_K$-integral points via an algorithm of Smart and Stephens [23] implemented in `Magma`. These points are

$$(19, \pm 83), \qquad ((-3-\sqrt{5})/2, \pm(1-2\sqrt{5})), \qquad ((-3+\sqrt{5})/2, \pm(1+2\sqrt{5})),$$

for $\alpha = 0$, and

$$\begin{aligned} &((3-5\sqrt{5})/2, \pm(8-5\sqrt{5})), && (\sqrt{5}, \pm(5+2\sqrt{5})), \\ &((5+3\sqrt{5})/2, \pm(10+3\sqrt{5})), && ((55+15\sqrt{5})/2, \pm(165+58\sqrt{5})), \end{aligned}$$

for $\alpha = 1$, with conjugate points for $\alpha = -1$. The lemma easily follows. $\square$

Lemma 3.3 *Suppose (n, y, p) is a solution to (10). If $q \mid y$ is prime, then*

$$q \equiv 1, 5, 19, 23 \pmod{24}.$$

In particular, $2 \nmid y$ and $3 \nmid y$. Moreover,

$$n \equiv 2,\ 4,\ 7,\ 8,\ 10,\ 11 \pmod{12}.$$

Proof Suppose $2 \mid y$. From $F_{2n} + 2 = y^p$ we have $2 \,||\, F_{2n}$. However, $2 \mid F_{2n}$ implies that $3 \mid n$. Thus $F_6 \mid F_{2n}$. As $F_6 = 8$ we have a contradiction.

Now suppose $q \mid y$ is an odd prime. From (5) we obtain

$$L_{2n}^2 = 5y^{2p} - 20y^p + 24,$$

so $24 \equiv L_{2n}^2 \pmod{q^2}$. Thus $q \neq 3$, and 6 is a quadratic residue modulo q. It follows that $q \equiv 1, 5, 19, 23 \pmod{24}$.

The final part of the lemma follows from considering $F_{2n} + 2$ modulo 6. $\square$

Lemma 3.4 *The only solutions to the equation $F_{2n} + 2 = \pm 5^m$ are $F_{-4} + 2 = -1$, $F_{-2} + 2 = 1$, $F_4 + 2 = 5$.*

Proof As above we deduce that

$$L_{2n}^2 = 5 \cdot 5^{2m} \mp 20 \cdot 5^m + 24.$$

If m is even then write

$$X = 5^{m+1}, \qquad Y = 5^{(m+2)/2} \cdot L_{2n}.$$

Then (X, Y) satisfies

$$Y^2 = X^3 \mp 20X^2 + 120X;$$

we are interested in computing the integral points on these two elliptic curves. For this we again used the computer package `Magma` [2]. The integral points on the model $Y^2 = X^3 - 20X^2 + 120X$ are $(0, 0)$, $(5, \pm 15)$, $(24, \pm 72)$, and lead to the solution $F_{-2} + 2 = 1$. The integral points on the model $Y^2 = X^3 + 20X^2 + 120X$ are $(0, 0)$, $(5, \pm 35)$, $(24, \pm 168)$, and lead to the solution $F_{-4} + 2 = -1$.

If m is odd then write

$$X = 5^{m+2}, \qquad Y = 5^{(m+5)/2} \cdot L_{2n}.$$

Then (X, Y) satisfies

$$Y^2 = X^3 \mp 100X^2 + 3000X.$$

The integral points on the model $Y^2 = X^3 - 100X^2 + 3000X$ are $(0,0)$, $(24, \pm 168)$, $(125, \pm 875)$ and lead to the solution $F_4 + 2 = 5$. The integral points on the model $Y^2 = X^3 + 100X^2 + 3000X$ are $(0,0)$, $(2904, \pm 159192)$ and do not lead to any solutions to the original equation. □

Lemma 3.5 *Let (n, y, p) be a solution to (10) and suppose that $n \neq -2, -1$. Then $|y| \geq 19$.*

Proof As $n \neq -2, -1$ it follows that $|y| > 1$. Suppose $|y| < 19$. By Lemma 3.3, the only prime divisor of y is 5. This now contradicts Lemma 3.4. □

4 Irreducibility of the mod *p* representation

Henceforth (n, y, p) is a solution to (10) with prime exponent $p \geq 5$, and E_n is the Frey–Hellegouarch curve E_n given by (12). An easy application of Tate's algorithm (together with Lemma 3.3) yields the following.

Lemma 4.1 *The model in (12) is minimal with discriminant and conductor*

$$\Delta = 2^8 \cdot 3^2 \cdot \varepsilon^{2n} \cdot \sqrt{5} \cdot y^p, \qquad \mathfrak{N} = (2)^7 \cdot (3) \cdot (\sqrt{5}) \cdot \prod_{\mathfrak{q} \mid y,\ \mathfrak{q} \neq (\sqrt{5})} \mathfrak{q}.$$

We would like to apply level-lowering to the mod p representation $\overline{\rho}_{E_n,p}$, and for this we need to show that it is irreducible. We shall make use of the following result due to Freitas and the third author [12], which is based on the work of David [8] and Momose [18].

Proposition 4.2 *Let K be a totally real Galois number field of degree d, with ring of integers $\mathcal{O}_K$ and Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$. Let $S = \{0, 12\}^G$, which we view as the set of sequences of values 0, 12 indexed by $\tau \in G$. For $\mathbf{s} = (s_\tau) \in S$ and $\alpha \in K$, define the* ***twisted norm associated to*** $\mathbf{s}$ *by*

$$\mathcal{N}_{\mathbf{s}}(\alpha) = \prod_{\tau \in G} \tau(\alpha)^{s_\tau}.$$

Let $\varepsilon_1, \ldots, \varepsilon_{d-1}$ be a basis for the unit group of K, and define

$$A_{\mathbf{s}} := \mathrm{Norm}\left(\gcd((\mathcal{N}_{\mathbf{s}}(\varepsilon_1) - 1)\mathcal{O}_K, \ldots, (\mathcal{N}_{\mathbf{s}}(\varepsilon_{d-1}) - 1)\mathcal{O}_K)\right). \tag{14}$$

Let B be the least common multiple of the $A_{\mathbf{s}}$ taken over all $\mathbf{s} \neq (0)_{\tau \in G}, (12)_{\tau \in G}$. Let $p \nmid B$ be a rational prime, unramified in K, such that $p \geq 17$ or $p = 11$. Let E/K be an elliptic curve, and $\mathfrak{q} \nmid p$ be a prime of good reduction for E. Define

$$P_{\mathfrak{q}}(X) = X^2 - a_{\mathfrak{q}}(E)X + \mathrm{Norm}(\mathfrak{q})$$

to be the characteristic polynomial of Frobenius for E at $\mathfrak{q}$. Let $r \geq 1$ be an integer such that $\mathfrak{q}^r$ is principal. If E is semistable at all $\mathfrak{p} \mid p$ and $\overline{\rho}_{E,p}$ is reducible then

$$p \mid \mathrm{Res}(\, P_{\mathfrak{q}}(X),\ X^{12r} - 1\,) \tag{15}$$

where Res *denotes the resultant of the two polynomials.*

We observe in passing that since $P_{\mathfrak{q}}(X)$ has two complex roots of absolute value $\sqrt{\mathrm{Norm}(\mathfrak{q})}$, the resultant in (15) cannot be zero. We now arrive at the main result of this section.

Lemma 4.3 *Let (n, y, p) be a solution to (10) with $p \geq 5$ prime. Let E_n be the Frey curve given in (12). Then $\overline{\rho}_{E_n,p}$ is irreducible.*

Proof Let

$$M_0 = 2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7, \tag{16}$$

and

$$\mathcal{Q}' = \{\mathfrak{q} \text{ a prime ideal of } \mathcal{O}_K \ : \ \mathfrak{q} \nmid 2 \cdot 3 \cdot \sqrt{5} \text{ and } \mathrm{Norm}(\mathfrak{q}) < 300\}.$$

Let

$$\mathcal{Q} = \{\mathfrak{q} \in \mathcal{Q}' \ : \ \text{the multiplicative order of } \varepsilon^2 \text{ in } \mathbb{F}_{\mathfrak{q}} \text{ divides } M_0\}. \tag{17}$$

The set $\mathcal{Q}$ contains 25 prime ideals $\mathfrak{q}$. The Frey curve (12) modulo $\mathfrak{q}$ depends only on n modulo M_0. Let

$$\mathcal{M} = \{0 \leq m \leq M_0 \ : \ m \equiv 2, 4, 7, 8, 10, 11 \pmod{12}\}. \tag{18}$$

By Lemma 3.3, if (n, y, p) is a solution to (10) then $n \equiv m \pmod{M_0}$ for some unique $m \in \mathcal{M}$. In particular, $\varepsilon^{2n} \equiv \varepsilon^{2m} \pmod{\mathfrak{q}}$. Suppose $\mathfrak{q} \nmid ((\varepsilon^{2m} + \sqrt{5})^2 - 6)$ so that, from (11), we have $\mathfrak{q} \nmid y$. By Lemma 4.1 we see that E_n has good reduction modulo $\mathfrak{q}$. Moreover, $a_{\mathfrak{q}}(E_n) = a_{\mathfrak{q}}(E_m)$. In particular, if $t^2 - a_{\mathfrak{q}}(E_m)t + \mathrm{Norm}(\mathfrak{q})$ is irreducible modulo p, then $\overline{\rho}_{E_n,p}$ is irreducible.

We wrote a short `Magma` script which did the following. For each of the values $p = 5, 7, 13$, and for each $m \in \mathcal{M}$, it verified that there exists a $\mathfrak{q} \in \mathcal{Q}$ such that $\mathfrak{q} \nmid ((\varepsilon^{2m} + \sqrt{5})^2 - 6)$ and that $t^2 - a_{\mathfrak{q}}(E_m)t + \mathrm{Norm}(\mathfrak{q})$ is irreducible modulo p. This completes the proof for $p = 5, 7, 13$.

Thus we suppose that $p = 11$ or $p \geq 17$. We apply the above proposition. A fundamental unit for $K = \mathbb{Q}(\sqrt{5})$ is ε, and it follows that $B = 320$, where B is as in the statement of the proposition. Thus $p \nmid B$. Moreover, from Lemma 4.1, E_n is semistable at $\mathfrak{p} \mid p$. We suppose that $\overline{\rho}_{E_n,p}$ is reducible. Let

$$S = \{\mathfrak{q} \in \mathcal{Q} \ : \ \mathfrak{q} \text{ is above a rational prime } q \not\equiv 1, 5, 19, 23\}.$$

The set S has 15 elements. By Lemma 3.3, it follows that E_n has good reduction at all $\mathfrak{q} \in S$. Recall that $n \equiv m \pmod{M_0}$ for some unique $m \in \mathcal{M}$. Moreover, $a_{\mathfrak{q}}(E_n) = a_{\mathfrak{q}}(E_m)$ for $\mathfrak{q} \in S$. It follows from the above proposition that p divides

$$\gcd(\{\mathrm{Res}(t^2 - a_{\mathfrak{q}}(E_m)t + \mathrm{Norm}(\mathfrak{q}), t^{12} - 1) \ : \ \mathfrak{q} \in S\}).$$

We computed this greatest common divisor for each $m \in \mathcal{M}$ and verified that it is never divisible by 11 or any prime ≥ 17. The lemma follows. □

5 Level-lowering and consequences

We are now in a position to prove Proposition 2.1

Proof of Proposition 2.1 The elliptic curve E_n is modular by [10], and the mod p representation $\overline{\rho}_{E_n,p}$ is irreducible by Lemma 4.3. If $p > 5$, then the proposition immediately follows from the statement of Theorem 7 of [11] (which, we should note, is based on the work of Fujiwara, Jarvis and Rajaei). Now let $p = 5$. In this case the statement of theorem in [11] is inapplicable to our situation. Specifically condition (v) of that theorem is not satisfied in our setting as $5 \nmid \mathrm{ord}_{\sqrt{5}}(\Delta)$. However that condition is only needed to remove the primes above p from the level without increasing the weight. In our situation we content ourselves, when $p = 5$, with removing from the level the primes dividing y that do not also divide $2 \cdot 3 \cdot \sqrt{5}$. As in [11] this can be done whilst keeping the weight $(2, 2)$. □

Lemma 5.1 *With notation as in Proposition 2.1, let* $\mathfrak{q} \nmid p \cdot \mathcal{N}$ *be a prime of* $\mathcal{O}_K$. *Let* m *be an integer satisfying* $\varepsilon^{2m} \equiv \varepsilon^{2n} \pmod{\mathfrak{q}}$. *Write*

$$b_{\mathfrak{q}}(m) = \begin{cases} a_{\mathfrak{q}}(E_m) & \mathfrak{q} \nmid (F_{2m}+2) \\ \mathrm{Norm}(\mathfrak{q}) + 1 & \mathfrak{q} \mid (F_{2m}+2) \text{ and } -(\varepsilon^{2m}+\sqrt{5}) \\ & \text{is a square modulo } \mathfrak{q} \\ -\mathrm{Norm}(\mathfrak{q}) - 1 & \text{otherwise.} \end{cases} \tag{19}$$

Then $b_{\mathfrak{q}}(m) \equiv a_{\mathfrak{q}}(\mathfrak{f}) \pmod{\pi}$.

Proof Suppose $\mathfrak{q} \nmid p \cdot \mathcal{N}$. Since $F_{2n} + 2 = y^p$, we see from Lemma 4.1 that E_n has good reduction at $\mathfrak{q}$ if $\mathfrak{q} \nmid (F_{2n}+2)$ and multiplicative reduction at $\mathfrak{q}$ if $\mathfrak{q} \mid (F_{2n}+2)$. Suppose we are in the latter case. We know [21, Theorem V.5.3] that the reduction at $\mathfrak{q}$ is split if and only if $-c_6/c_4$ is a $\mathfrak{q}$-adic square, where c_4 and c_6 are the usual c-invariants of E_n. In our case

$$c_4 = 2^5(2x^2 - 9), \qquad c_6 = 2^7 x(-4x^2 + 27).$$

From (11) we have $x^2 \equiv 6 \pmod{\mathfrak{q}}$ and so $-c_6/c_4 \equiv -4x \pmod{\mathfrak{q}}$. As $x = \varepsilon^{2n} + \sqrt{5}$, the multiplicative reduction at $\mathfrak{q}$ is split if and only if $-(\varepsilon^{2n} + \sqrt{5})$ is a square modulo $\mathfrak{q}$.

By comparing the traces of the images of the Frobenius element at $\mathfrak{q}$ in $\overline{\rho}_{E_n,p} \sim \overline{\rho}_{\mathfrak{f},\pi}$ we obtain $b_{\mathfrak{q}}(n) \equiv a_{\mathfrak{q}}(\mathfrak{f}) \pmod{\pi}$ in all cases. Finally, as $\varepsilon^{2m} \equiv \varepsilon^{2n} \pmod{\mathfrak{q}}$, it follows that $F_{2m} \equiv F_{2n} \pmod{\mathfrak{q}}$, and so $b_{\mathfrak{q}}(m) = b_{\mathfrak{q}}(n)$ proving the lemma. □

Write $S = S^{\mathrm{new}}_{(2,2)}(\mathcal{N})$. Using `Magma` we find that S has dimension 6144. We let $\mathcal{F}$ be the set of eigenforms $\mathfrak{f}$ belonging to S (thus $\#\mathcal{F} = 6144$). Whilst it is not feasible to compute these newforms with current tools, it is, however, quite practical using `Magma` to compute the action of the Hecke operators $T_{\mathfrak{q}}$ on S for small primes $\mathfrak{q}$ of $\mathcal{O}_K$. For the theoretical details behind these algorithms, we recommend [9].

We used a `Magma` program written by Stephen Donnelly to search for elliptic curves over number fields with a given conductor. This program found 288 pairwise non-isogenous elliptic curves F/K with conductor $\mathcal{N}$. We know by [10] that these corresponds to 288 distinct $\mathfrak{f} \in \mathcal{F}$ with rational Hecke eigenvalues. We let $\mathcal{E}$ be this set of these 288 elliptic curves and we let $\mathcal{F}'$ be the subset of $\mathcal{F}$ coming from these 288 elliptic curves.

6 Reducing to elliptic curves

Proposition 6.1 *Let* (n, y, p) *be a solution to* (10) *with prime exponent* $p \geq 5$. *Then* $\overline{\rho}_{E_n,p} \sim \overline{\rho}_{E,p}$ *where* $E \in \mathcal{E}$.

We shall prove Proposition 6.1 by contradiction. Suppose $\overline{\rho}_{E_n,p} \nsim \overline{\rho}_{E,p}$ for any $E \in \mathcal{E}$. Then $\overline{\rho}_{E_n,p} \sim \overline{\rho}_{\mathfrak{g},\pi}$ for some $\mathfrak{g} \in \mathcal{F} - \mathcal{F}'$. Let $\mathcal{Q}$ and $\mathcal{M}$ be as in the proof of Lemma 4.3. Let m be the unique element of $\mathcal{M}$ such that $m \equiv n \pmod{M_0}$. In particular, we know that $\varepsilon^{2m} \equiv \varepsilon^{2n} \pmod{\mathfrak{q}}$ for all $\mathfrak{q} \in \mathcal{Q}$. From Lemma 5.1 we see that

$$b_{\mathfrak{q}}(m) \equiv a_{\mathfrak{q}}(\mathfrak{g}) \pmod{\pi} \tag{20}$$

for all $\mathfrak{q} \in \mathcal{Q}$ with $\mathfrak{q} \nmid p$.

Suppose for now that $\mathfrak{q} \in \mathcal{Q}$ and $\mathfrak{q} \nmid p$. Write $T_{\mathfrak{q}}$ for the Hecke operator corresponding to $\mathfrak{q}$ acting on the space $S = S^{\mathrm{new}}_{(2,2)}(\mathcal{N})$. Let $C_{\mathfrak{q}}(x) = \det(xI - T_{\mathfrak{q}}) \in \mathbb{Z}[x]$ be its characteristic polynomial; this has roots $a_{\mathfrak{q}}(\mathfrak{f})$ with $\mathfrak{f}$ running through $\mathfrak{f} \in \mathcal{F}$. Now let

$$C'_{\mathfrak{q}}(x) = \prod_{E \in \mathcal{E}} (x - a_{\mathfrak{q}}(E)) \in \mathbb{Z}[x].$$

Thus $C'_{\mathfrak{q}}(x)$ divides $C_{\mathfrak{q}}(x)$. Moreover, let

$$C''_{\mathfrak{q}}(x) = \frac{C_{\mathfrak{q}}(x)}{C'_{\mathfrak{q}}(x)} \in \mathbb{Z}[x].$$

The roots of $C''_{\mathfrak{q}}(x)$ are $a_{\mathfrak{q}}(\mathfrak{f})$ with $\mathfrak{f}$ running through $\mathfrak{f} \in \mathcal{F}'$. We see from (20) that $C''(b_{\mathfrak{q}}(m)) \equiv 0 \pmod{\pi}$. However as $C'' \in \mathbb{Z}[x]$ and $b_{\mathfrak{q}}(m) \in \mathbb{Z}$ it follows that

$$C''(b_{\mathfrak{q}}(m)) \equiv 0 \pmod{p}.$$

Now let

$$G_{m,\mathfrak{q}} = \mathrm{Norm}(\mathfrak{q}) \cdot C''(b_{\mathfrak{q}}(m)) \in \mathbb{Z}.$$

We see that $p \mid G_{m,\mathfrak{q}}$ for all $\mathfrak{q} \in \mathcal{Q}$ regardless of whether $\mathfrak{q}$ divides p or not. Thus p divides

$$H_m := \gcd\{G_{m,\mathfrak{q}} \ : \ \mathfrak{q} \in \mathcal{Q}\}.$$

We computed the integers H_m for all $m \in \mathcal{M}$ and factored them. It turns that all are non-zero, which means we have bounded p under the assumption that $\overline{\rho}_{E_n,p} \not\sim \overline{\rho}_{E,p}$ for all $E \in \mathcal{E}$. In particular, our computations reveal that $p \leq 109$. More precisely, we are left to consider precisely 9391 pairs (p, m) where $p \geq 5$ is a prime dividing H_m.

To proceed further we remark that the Hilbert Modular Forms package in `Magma` computes a matrix, which shall denote by $R_{\mathfrak{q}}$, giving the action of the operator $T_{\mathfrak{q}}$ (with $\mathfrak{q}$ not dividing the level $\mathcal{N}$) with respect to a $\mathbb{Z}$-basis of a lattice in $S^{\mathrm{new}}_{(2,2)}(\mathcal{N})$ that is Hecke-stable. Write $\overline{R}_{\mathfrak{q}}$ for the reduction of $R_{\mathfrak{q}}$ modulo p and $\overline{\mathfrak{g}}$ for the mod p eigensystem corresponding to $\mathfrak{g}$. It follows from the above that the intersection

$$\bigcap_{\substack{\mathfrak{q} \in \mathcal{Q} \\ \mathfrak{q} \nmid p}} \mathrm{Ker}\left(\overline{R}_{\mathfrak{q}} - \overline{b_{\mathfrak{q}}(m)} \cdot I\right) \tag{21}$$

contains an $\mathbb{F}_p$-line corresponding to $\overline{\mathfrak{g}}$. We computed the intersection (21) for all the 9391 remaining pairs (p, m). This is merely $\mathbb{F}_p$-linear algebra once the matrices $R_{\mathfrak{q}}$ representing the Hecke operators were computed. We found that for all but 21 of the 9391 pairs (p, m) the space (21) is 0-dimensional giving us a contradiction. For the proof of Proposition 6.1 we need now only consider the following 21 remaining pairs (p, m):

$$\begin{array}{llllll}
(5, 2), & (5, 2518), & (5, 2519), & (7, 2), & (7, 2518), & (7, 2519), \\
(11, 2), & (11, 2518), & (11, 2519), & (13, 2), & (13, 2518), & (13, 2519), \\
(17, 2), & (17, 2519), & (19, 2), & (19, 2519), & (23, 2518), & (29, 2518), \\
(29, 2519), & (41, 2), & (43, 2518). & & &
\end{array}$$

Observe that $m \equiv 2, -2, -1 \pmod{M_0}$ in every one of these 21 cases. The presence of the possibilities $-2, -1$ is hardly surprising in view of the solutions $(n, y, p) = (-2, -1, p)$ and $(-1, 1, p)$ to (10); for an explanation of the value 2 see the next section. In all these

21 cases we found that the intersection (21) is 1-dimensional. We let E be E_2 if $m = 2$, E_{-2} if $m = 2518 \equiv -2 \pmod{M_0}$ and E_{-1} if $m = 2519 \equiv -1 \pmod{M_0}$. These all have conductors $\mathcal{N}$. Let $\mathfrak{f} \in \mathcal{F}$ be the Hilbert eigenform corresponding to E. Then $b_{\mathfrak{q}}(m) \equiv a_{\mathfrak{q}}(E) = a_{\mathfrak{q}}(\mathfrak{f}) \pmod{p}$. It follows that the reduction of the line corresponding to $\mathfrak{f}$ belongs to the 1-dimensional intersection (21), which also contains the reduction of the line corresponding to $\mathfrak{g}$. Thus the mod p eigensystems $\overline{\mathfrak{f}}$ and $\overline{\mathfrak{g}}$ are equal. It follows that $\overline{\rho}_{\mathfrak{f},p} \sim \overline{\rho}_{\mathfrak{g},\pi}$. Thus $\overline{\rho}_{E_n,p} \sim \overline{\rho}_{E,p}$. But $E_2, E_{-2}, E_{-1} \in \mathcal{E}$; this completes the proof of Proposition 6.1.

7 Reducing to only three elliptic curves

We know from Proposition 6.1 that $\overline{\rho}_{E_n,p} \sim \overline{\rho}_{E,p}$ where E is one of the 288 elliptic curves belonging to $\mathcal{E}$. In this section we eliminate all but three of the elliptic curves belonging to $\mathcal{E}$.

Proposition 7.1 *Let (n, y, p) be a solution to (10) with $p \geq 5$. Then $n \equiv m \pmod{M_0}$ and $\overline{\rho}_{E_n,p} \sim \overline{\rho}_{E,p}$ where*

(i) $m = 2$ and $E = E_2$;
(ii) $m = M_0 - 2$ and $E = E_{-2}$;
(iii) $m = M_0 - 1$ and $E = E_{-1}$.

We shall need the following slight strengthening of Lemma 5.1.

Lemma 7.2 *Let (n, y, p) be a solution to (10) with $p \geq 5$ and $E \in \mathcal{E}$ satisfy $\overline{\rho}_{E_n,p} \sim \overline{\rho}_{E,p}$. Further, let $\mathfrak{q} \nmid \mathcal{N}$ be a prime of $\mathcal{O}_K$ and suppose that m is an integer satisfying $\varepsilon^{2m} \equiv \varepsilon^{2n} \pmod{\mathfrak{q}}$. Then $b_{\mathfrak{q}}(m) \equiv a_{\mathfrak{q}}(E) \pmod{p}$, where $b_{\mathfrak{q}}(n)$ is given by (19).*

Proof If $\mathfrak{q} \nmid p$ then this is a special case of Lemma 5.1. If $\mathfrak{q} \mid p$ then this follows from the proof of Lemma 5.1 together with [13]. □

Now let $\mathcal{Q}$ be as in the proof of Lemma 4.3. The following is immediate.

Lemma 7.3 *Let (n, y, p) be a solution to (10) with $p \geq 5$ prime. Let $E \in \mathcal{E}$ such that $\overline{\rho}_{E_n,p} \sim \overline{\rho}_{E,p}$. Let $n \equiv m \pmod{M_0}$ with $m \in \mathcal{M}$. Then p divides*

$$B_m(E) = \gcd(\{b_{\mathfrak{q}}(m) - a_{\mathfrak{q}}(E) \ : \ \mathfrak{q} \in \mathcal{Q}\}).$$

We computed $B_m(E)$ for all of the 288 elliptic curves $E \in \mathcal{E}$ and $m \in \mathcal{M}$. We found that $B_m(E)$ is not divisible by any primes $p \geq 5$ except in three cases where $B_m(E) = 0$:

(i) $m = 2$ and $E = E_2$;
(ii) $m = M_0 - 2$ and $E = E_{-2}$;
(iii) $m = M_0 - 1$ and $E = E_{-1}$.

The possibilities (ii) and (iii) are natural, and they correspond to the solutions $(n, y, p) = (-2, -1, p)$ and $(-1, 1, p)$ respectively. The possibility (i) is a result of the identity $F_4 + 2 = 5$ from which it is easy to deduce that E_2 has conductor $\mathcal{N}$ and so it is natural (though annoying) that our sieve cannot eliminate this possibility. This proves Proposition 7.1.

8 Enlarging M_0

We let

$$M_1 = M_0 \times \prod_{\substack{\ell \text{ prime} \\ 11 \le \ell < 10^4}} \ell, \tag{22}$$

where, as before, $M_0 = 2520$. In this section we prove the following.

Lemma 8.1 *Let (n, y, p) be a solution to (10) with $p \geq 5$ prime. Then $\overline{\rho}_{E_n,p} \sim \overline{\rho}_{E,p}$ and $n \equiv m_0 \pmod{M_1}$ where*

(i) either $m_0 = 2$ and $E = E_2$;
(ii) or $m_0 = -2$ and $E = E_{-2}$;
(iii) or $m_0 = -1$ and $E = E_{-1}$.

Proof Fix $m_0 \in \{-2, -1, 2\}$, let $E = E_{m_0}$ and suppose $\overline{\rho}_{E_n,p} \sim \overline{\rho}_{E,p}$. We would like to show that $n \equiv m_0 \pmod{M_1}$.

There are 164 primes in the interval [11, 10000]; we denote them by

$$\ell_1 = 11, \ \ell_2 = 13, \ \ldots, \ \ell_{164} = 9973.$$

We let $L_0 = M_0$, and $L_i = \ell_i \cdot L_{i-1}$ for $1 \leq i \leq 164$. Then $L_{164} = M_1$. We shall show inductively that $n \equiv m_0 \pmod{L_i}$ for $0 \leq i \leq 164$ which gives the lemma. We know by the previous section that $n \equiv m_0 \pmod{L_0}$. For the inductive step, suppose $n \equiv m_0 \pmod{L_{i-1}}$. We want to show that $n \equiv m_0 \pmod{L_i}$. Let $\mathcal{Q}_i$ be a set of prime ideals $\mathfrak{q} \nmid \mathcal{N}$ satisfying the following

(i) $\text{Norm}(\mathfrak{q}) = q$ is a rational prime $\equiv 1 \pmod 5$;
(ii) $\ell_i \mid (q-1)$ and $(q-1) \mid L_i$.

Let

$$\mathcal{M}_i = \{0 \leq m \leq L_i - 1 \ : \ m \equiv m_0 \pmod{L_{i-1}}\}.$$

Thus $n \equiv m \pmod{L_i}$ for some unique $m \in \mathcal{M}_i$. Moreover, it follows from (i) and (ii) that $\varepsilon^{2n} \equiv \varepsilon^{2m} \pmod{\mathfrak{q}}$ for all $\mathfrak{q} \in \mathcal{Q}_i$. Define

$$B_m(\mathcal{Q}_i) := \gcd\{b_{\mathfrak{q}}(m) - a_{\mathfrak{q}}(E) \ : \ \mathfrak{q} \in \mathcal{Q}_i\}.$$

By Lemma 7.2, $p \mid B_m(\mathcal{Q}_i)$. We wrote a simple `Magma` script which for each $1 \leq i \leq 164$ and for each $m_0 \in \{-2, -1, 2\}$ found a set $\mathcal{Q}_i$ satisfying (i), (ii), such that, for all $m \in \mathcal{M}_i$ with $m \not\equiv m_0 \pmod{L_i}$, the integer $B_m(\mathcal{Q}_i)$ is non-zero and divisible only by the primes 2 and 3. Our computation took a total of around 45 minutes. This proves the inductive step and completes the proof. □

9 Linear forms in three logs

For any algebraic number α of degree d over $\mathbb{Q}$, we define the *absolute logarithmic height* of α via the formula

$$h(\alpha) = \frac{1}{d}\left(\log|a_0| + \sum_{i=1}^{d} \log\max\left(1, |\alpha^{(i)}|\right)\right), \tag{23}$$

where a_0 is the leading coefficient of the minimal polynomial of α over $\mathbb{Z}$ and the $\alpha^{(i)}$ are the conjugates of α in $\mathbb{C}$. The following is the main result (Theorem 2.1) of Matveev [16].

Theorem 2 (Matveev) *Let $\mathbb{K}$ be an algebraic number field of degree D over $\mathbb{Q}$ and put $\chi = 1$ if $\mathbb{K}$ is real, $\chi = 2$ otherwise. Suppose that $\alpha_1, \alpha_2, \ldots, \alpha_{n_0} \in \mathbb{K}^*$ with absolute logarithmic heights $h(\alpha_i)$ for $1 \le i \le n_0$, and suppose that*

$$A_i \ge \max\{D\, h(\alpha_i), \left|\log \alpha_i\right|\}, \ 1 \le i \le n_0,$$

for some fixed choice of the logarithm. Define

$$\Lambda = b_1 \log \alpha_1 + \cdots + b_{n_0} \log \alpha_{n_0},$$

where the b_i are integers and set

$$B = \max\{1, \max\{|b_i| A_i/A_{n_0} \ : \ 1 \le i \le n_0\}\}.$$

Define, with $e := \exp(1)$, further,

$$\Omega = A_1 \cdots A_{n_0},$$
$$C(n_0) = C(n_0, \chi) = \frac{16}{n_0!\chi} e^{n_0} (2n_0 + 1 + 2\chi)(n_0+2)(4n_0+4)^{n_0+1} \left(en_0/2\right)^{\chi},$$
$$C_0 = \log\left(e^{4.4n_0+7} n_0^{5.5} D^2 \log(eD)\right) \quad \textit{and} \quad W_0 = \log\left(1.5eBD\log(eD)\right).$$

Then, if $\log \alpha_1, \ldots, \log \alpha_{n_0}$ are linearly independent over $\mathbb{Z}$ and $b_{n_0} \ne 0$, we have

$$\log|\Lambda| > -C(n_0)\, C_0\, W_0\, D^2\, \Omega.$$

From (10), we have that

$$\sqrt{5} y^p - \varepsilon^{2n} = 2\sqrt{5} - \overline{\varepsilon}^{2n}$$

and so

$$0 < \Lambda = p \log y + \log(\sqrt{5}) - 2n \log \varepsilon < \frac{2\sqrt{5}}{\varepsilon^{2n}} < \frac{2.1}{y^p}. \tag{24}$$

We apply Theorem 2 with

$$D = 2, \ \chi = 1, \ n_0 = 3, \ b_1 = 1, \ \alpha_1 = \sqrt{5}, \ b_2 = -2n, \ \alpha_2 = \varepsilon, \ b_3 = p, \ \alpha_3 = y,$$

where, from Lemma 3.5, we have $y \ge 19$. We may thus take

$$A_1 = \log 5, \ A_2 = \log \varepsilon, \ A_3 = 2 \log y \ \text{ and } \ B = \max\left\{\frac{n \log \varepsilon}{\log y}, p\right\} = p.$$

Since

$$C_0(3) = 2^{18} \cdot 3^2 \cdot 5 \cdot e^4 < 6.45 \times 10^8, \quad C_0 = \log\left(e^{20.2} \cdot 3^{5.5} \cdot 4 \log(4e)\right) < 28.5$$

and

$$W_0 = \log\left(3ep \log(2e)\right) < 2.63 + \log p$$

we may therefore conclude that

$$\log \Lambda > -1.139 \cdot 10^{11} \left(2.63 + \log p\right) \log y.$$

From (24), we thus have that

$$p \log y < 1.139 \cdot 10^{11} \left(2.63 + \log p\right) \log y + \log(2.1),$$

and hence

$$\frac{p}{2.63+\log p} < 1.139\cdot 10^{11} + \frac{\log(2.1)}{(2.63+\log p)\log y} < 1.14\cdot 10^{11},$$

whereby $p < 3.6\times 10^{12}$.

Our immediate goal is to sharpen this inequality by proving that $p < 10^{11}$. We will assume for the remainder of this section that

$$10^{11} \le p < 3.6\times 10^{12}. \tag{25}$$

We begin by appealing to a sharper but less convenient lower bound for linear forms in three complex logarithms, due to Mignotte (Proposition 5.1 of [17]).

Theorem 3 (Mignotte) *Consider three non-zero algebraic numbers α_1, α_2 and α_3, which are either all real and >1, or all complex of modulus one and all $\neq 1$. Further, assume that the three numbers α_1, α_2 and α_3 are either all multiplicatively independent, or that two of the numbers are multiplicatively independent and the third is a root of unity. We also consider three positive rational integers b_1, b_2, b_3 with $\gcd(b_1, b_2, b_3) = 1$, and the linear form*

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

where the logarithms of the α_i are arbitrary determinations of the logarithm, but which are all real or all purely imaginary. Suppose further that

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

and put

$$d_1 = \gcd(b_1, b_2) \ \ \text{and} \ \ d_3 = \gcd(b_3, b_2).$$

Let $\rho \ge e$ be a real number. Let a_1, a_2 and a_3 be real numbers such that

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

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

$$\Omega := a_1a_2a_3 \ge 2.5 \ \ \text{and} \ \ a := \min\{a_1,a_2,a_3\} \ge 0.62.$$

Let m and L be positive integers with $m\ge 3$, $L \ge D+4$ and set $K = [m\Omega L]$. Let χ be fixed with $0 < \chi \le 2$ and define

$$c_1 = \max\{(\chi mL)^{2/3}, \sqrt{2mL/a}\},\ c_2 = \max\{2^{1/3}\,(mL)^{2/3}, L\sqrt{m/a}\},\ c_3 = (6m^2)^{1/3}L,$$

$$R_i = [c_ia_2a_3],\ S_i = [c_ia_1a_3] \ \ \text{and}\ T_i = [c_ia_1a_2],$$

for $i\in\{1,2,3\}$, and set

$$R = R_1+R_2+R_3+1,\ S = S_1+S_2+S_3+1 \ \ \text{and} \ \ T = T_1+T_2+T_3+1.$$

Define

$$c = \max\left\{\frac{R}{La_2a_3}, \frac{S}{La_1a_3}, \frac{T}{La_1a_2}\right\}.$$

Finally, assume that the quantity

$$\left(\frac{KL}{2}+\frac{L}{4}-1-\frac{2K}{3L}\right)\log(\rho) - (D+1)\log L - 3gL^2c\,\Omega$$
$$-D(K-1)\log B - 2\log K + 2D\log 1.36$$

is positive, where

$$g = \frac{1}{4} - \frac{K^2L}{12RST} \quad \textit{and} \quad B = \frac{e^3c^2\Omega^2L^2}{4K^2d_1d_3}\left(\frac{b_1}{a_2} + \frac{b_2}{a_1}\right)\left(\frac{b_3}{a_2} + \frac{b_2}{a_3}\right).$$

Then either

$$\log \Lambda > -(KL + \log(3KL))\log(\rho), \tag{26}$$

or the following condition holds :

either *there exist non-zero rational integers r_0 and s_0 such that*

$$r_0b_2 = s_0b_1 \tag{27}$$

with

$$|r_0| \le \frac{(R_1+1)(T_1+1)}{M-T_1} \quad \textit{and} \quad |s_0| \le \frac{(S_1+1)(T_1+1)}{M-T_1}, \tag{28}$$

where

$$M = \max\left\{R_1 + S_1 + 1,\ S_1 + T_1 + 1,\ R_1 + T_1 + 1,\ \chi\ \tau_1^{1/2}\right\},$$
$$\tau_1 = (R_1+1)(S_1+1)(T_1+1),$$

or *there exist rational integers r_1, s_1, t_1 and t_2, with $r_1s_1 \neq 0$, such that*

$$(t_1b_1 + r_1b_3)s_1 = r_1b_2t_2, \qquad \gcd(r_1,t_1) = \gcd(s_1,t_2) = 1, \tag{29}$$

which also satisfy

$$|r_1s_1| \le \gcd(r_1,s_1)\cdot\frac{(R_1+1)(S_1+1)}{M-\max\{R_1,S_1\}},$$
$$|s_1t_1| \le \gcd(r_1,s_1)\cdot\frac{(S_1+1)(T_1+1)}{M-\max\{S_1,T_1\}}$$

and

$$|r_1t_2| \le \gcd(r_1,s_1)\cdot\frac{(R_1+1)(T_1+1)}{M-\max\{R_1,T_1\}}.$$

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

We apply this result with

$$b_2 = p,\ \alpha_2 = y,\ b_1 = 1,\ \alpha_1 = \sqrt{5},\ b_3 = 2n \ \text{ and } \ \alpha_3 = \varepsilon,$$

so that we may take

$$D = 2,\ d_1 = 1,\ d_3 \in \{1,p\},\ a_1 = \frac{\rho+3}{2}\log 5,\ a_2 = (\rho+3)\log y$$

and $a_3 = (\rho+1)\log(\varepsilon)$, whence $a = a_3$.

Notice that, in our situation, (27) becomes the equation $r_0p = s_0$ from which necessarily $|s_0| \ge p > 10^{11}$, whereby (28) implies that

$$\frac{(S_1+1)(T_1+1)}{M-T_1} \ge 10^{11}. \tag{30}$$

If instead we have (26), then inequality (24) implies that

$$p\log y < (KL + \log(3KL))\log(\rho) + \log(2.1). \tag{31}$$

We will choose L, m, ρ and χ to contradict both (30) and (31), whereby we necessarily have (29). Specifically, we set

$$L = 485,\ m = 20,\ \rho = 5.7 \ \text{ and } \ \chi = 2,$$

so that

$$K = \left[20 \cdot 485 \cdot 4.35 \log(5) \cdot 6.7 \log(\varepsilon) \cdot 8.7 \log y\right],$$

whereby

$$1904870 \log y < K \le 1904871 \log y.$$

We have

$$\begin{aligned}
c_1 &< 721.996,\ c_2 < 1207.96,\ c_3 < 6493.5,\\
R_1 &< 20252 \log y,\ R_2 < 33883 \log y,\ R_3 < 182142 \log y,\\
S_1 &= 16297,\ S_2 = 27266,\ S_3 = 146572,\\
T_1 &< 43977 \log y,\ T_2 < 73576 \log y,\ T_3 < 395514 \log y,
\end{aligned}$$

so that

$$R < 236277 \log y + 1,\ S = 190136,\ T < 513067 \log y + 1,$$

and

$$c < 17.37,\ g < 0.244 \ \text{ and } \ B < 0.3\, p^2.$$

We check that

$$\left(\frac{KL}{2} + \frac{L}{4}\right) \log(\rho) + 4 \log(1.36) > 8.03 \cdot 10^8 \log y,$$

while, using that $p < 3.6 \cdot 10^{12}$ and $y \ge 19$,

$$\left(1 + \frac{2K}{3L}\right) \log(\rho) + 3 \log L + 3gL^2 c\, \Omega + 2(K-1) \log B + 2 \log K < 8.021 \cdot 10^8 \log y.$$

It follows that the hypotheses of Theorem 3 are satisfied. Since we may check that $M > 7.6 \cdot 10^6 \log y$, we have that

$$\frac{(S_1 + 1)(T_1 + 1)}{M - T_1} < 95$$

contradicting (30). Also,

$$(KL + \log(3KL)) \log(\rho) + \log(2.1) < 5 \cdot 10^9,$$

contradicting (31).

We may thus conclude that there exist rational integers r_1, s_1, t_1 and t_2, with $r_1 s_1 \ne 0$, such that

$$(t_1 + 2nr_1)s_1 = r_1 t_2 p, \tag{32}$$

where, again using that $M > 7.6 \cdot 10^6 \log y$,

$$\left|\frac{r_1 s_1}{\gcd(r_1, s_1)}\right| \le 43 \ \text{ and } \ \left|\frac{s_1 t_1}{\gcd(r_1, s_1)}\right| \le 94.$$

Since, in all cases, we assume that $p > 10^{11}$, we thus have

$$\max\{|r_1|, |s_1|, |t_1|\} < p,$$

whence, from the fact that $\gcd(r_1, t_1) = \gcd(s_1, t_2) = 1$, we have $r_1 = \pm s_1$ and so $t_1 + 2r_1 n = \pm t_2 p$. Without loss of generality, we may thus write

$$u + 2r|n| = tp,$$

where $r = |r_1|$ and $t = |t_2|$ are positive integers, $u = \pm t_1$, $r \leq 43$ and $|u| \leq 94$.

We can thus rewrite the linear form

$$\Lambda = p \log y + \log(\sqrt{5}) - 2n \log \varepsilon$$

as a linear form in two logarithms

$$\Lambda = p \log\left(\frac{y}{\varepsilon^{t/r}}\right) + \log\left(5^{1/2}\varepsilon^{u/r}\right). \tag{33}$$

We are in position to apply the following sharp lower bound for linear forms in two complex logarithms of algebraic numbers, due to Laurent (Theorem 2 of [15]).

Theorem 4 (Laurent) *Let α_1 and α_2 be multiplicatively independent algebraic numbers, h, ρ and μ be real numbers with $\rho > 1$ and $1/3 \leq \mu \leq 1$. Set*

$$\sigma = \frac{1+2\mu-\mu^2}{2},\ \lambda = \sigma \log \rho,\ H = \frac{h}{\lambda} + \frac{1}{\sigma},$$
$$\omega = 2\left(1+\sqrt{1+\frac{1}{4H^2}}\right),\ \theta = \sqrt{1+\frac{1}{4H^2}} + \frac{1}{2H}.$$

Consider the linear form $\Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1$, where b_1 and b_2 are positive integers. Put

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

and assume that

$$h \geq \max\left\{D\left(\log\left(\frac{b_1}{a_2} + \frac{b_2}{a_1}\right) + \log \lambda + 1.75\right) + 0.06,\ \lambda,\ \frac{D \log 2}{2}\right\},$$
$$a_i \geq \max\left\{1, \rho|\log \alpha_i| - \log|\alpha_i| + 2Dh(\alpha_i)\right\} \qquad (i = 1, 2),$$

and

$$a_1 a_2 \geq \lambda^2.$$

Then

$$\log|\Lambda| \geq -C\left(h + \frac{\lambda}{\sigma}\right)^2 a_1 a_2 - \sqrt{\omega\theta}\left(h + \frac{\lambda}{\sigma}\right) - \log\left(C'\left(h + \frac{\lambda}{\sigma}\right)^2 a_1 a_2\right) \tag{34}$$

with

$$C = \frac{\mu}{\lambda^3 \sigma}\left(\frac{\omega}{6} + \frac{1}{2}\sqrt{\frac{\omega^2}{9} + \frac{8\lambda\omega^{5/4}\theta^{1/4}}{3\sqrt{a_1 a_2} H^{1/2}} + \frac{4}{3}\left(\frac{1}{a_1} + \frac{1}{a_2}\right)\frac{\lambda\omega}{H}}\right)^2$$

and

$$C' = \sqrt{\frac{C\sigma\omega\theta}{\lambda^3 \mu}}.$$

We apply this result with

$$b_1 = 1,\ b_2 = p,\ \alpha_1 = 5^{1/2}\varepsilon^{u/r},\ \alpha_2 = \frac{\varepsilon^{t/r}}{y},$$

so that $D = 2r$,

$$h(\alpha_1) \le \frac{\log 5}{2} + \frac{|u|}{2r}\log\varepsilon \quad\text{and}\quad h(\alpha_2) \le \log y + \frac{t}{2r}\log\varepsilon.$$

We take $\mu = 1$ and $\rho = e^4$, so that $\sigma = 1$ and $\lambda = 4$. From (33), inequality (24), $|u| \le 94$, $1 \le r \le 43$, and $p > 10^{11}$, we have that

$$\left|\log y - \frac{t}{r}\log\varepsilon\right| < \frac{1}{p}\left(\frac{2.1}{y^p} + \log\left(5^{1/2}\varepsilon^{94}\right)\right) < 10^{-9}$$

and hence may choose

$$a_1 = 2562 \quad\text{and}\quad a_2 = 6r\log y + 1.$$

We have

$$2r\left(\log\left(\frac{1}{6r\log y + 1} + \frac{p}{2562}\right) + \log 4 + 1.75\right) + 0.06 < 2r\log p$$

whence

$$h = 2r\log p$$

is a valid choice for h. A short computation reveals that

$$C < 0.029, \quad C' < 0.044,$$

and hence from (34), $y \ge 19$ and $p > 10^{11}$,

$$\frac{\log|\Lambda|}{\log y} > -1784\,(r\log p + 2)^2\, r - 1.39\,(r\log p + 2) - 3 - 0.7\log(r\log p + 2) - \frac{\log r}{\log y}.$$

From (24),

$$\frac{\log|\Lambda|}{\log y} < \frac{\log 2.1}{\log y} - p < 0.26 - p$$

whereby it follows that

$$p < 1784\,(r\log p + 2)^2\, r + 1.39\,(r\log p + 2) + 3.26 + 0.7\log(r\log p + 2) + \frac{\log r}{\log y}$$

and so, since $r \le 43$, we find that $p < 9.1 \cdot 10^{10}$, contradicting (25).

10 The method of Kraus

We let M_1 be given by (22). The aim of this section is to prove the following proposition, which improves on Lemma 8.1.

Proposition 10.1 *Let (n, y, p) be a solution to (10) with $p \ge 5$ prime. Then there is an $m_0 \in \{-2, -1\}$ such that*

(i) $\overline{\rho}_{E_n,p} \sim \overline{\rho}_{E,p}$ *where* $E = E_{m_0}$*;*
(ii) $n \equiv m_0 \pmod{M_1}$*;*
(iii) $n \equiv m_0 \pmod{p}$*.*

Observe that this proposition improves over Lemma 8.1 in two ways. First the elliptic curve E_2, corresponding to the 'pseudo-solution' $F_4 + 2 = 5$, is eliminated. But also we know that $n \equiv m_0 \pmod{p}$. This will allow us to rewrite our linear form in three logarithms as a linear form in two logarithms (Sect. 11) and deduce a much sharper bound for the exponent p.

In view of Section 9 we need only prove Proposition 10.1 for prime exponents $5 \le p < 10^{11}$. Fix $m_0 \in \{-2, -1, 2\}$ and suppose $n \equiv m_0 \pmod{M_1}$. Write $E = E_{m_0}$. By Lemma 8.1 we know that $\overline{\rho}_{E_n,p} \sim \overline{\rho}_{E,p}$. We shall give a computational criterion, modelled on ideas of Kraus [14] (see also [5, Lemma 7.4]) which allows us, for each $5 \le p < 10^{11}$, to deduce a contradiction when $m_0 = 2$, and to conclude that $n \equiv m_0 \pmod{p}$ when $m_0 = -2$ or $m_0 = -1$.

Let k be a positive integer satisfying the following:

(I) $q = kp + 1$ is a prime with $q \equiv \pm 1 \pmod 5$.

Let θ_i be the two square roots of 5 modulo q. Then $q\mathcal{O}_K = \mathfrak{q}_1\mathfrak{q}_2$ where the prime ideals $\mathfrak{q}_i$ are given by $\mathfrak{q}_i = (q, \sqrt{5} - \theta_i)$. Observe that

$$\mathcal{O}_K/\mathfrak{q}_1 = \mathbb{F}_q = \mathcal{O}_K/\mathfrak{q}_2.$$

Moreover,

$$\sqrt{5} \equiv \theta_i \pmod{\mathfrak{q}_i}.$$

If we write

$$\varepsilon_1 = (1 + \theta_1)/2,$$

then it follows that

$$\varepsilon \equiv \varepsilon_1 \pmod{\mathfrak{q}_1}.$$

As $\theta_2 = -\theta_1$, we know that

$$\varepsilon \equiv -1/\varepsilon_1 \pmod{\mathfrak{q}_2}.$$

If $q \mid y$ then E_n has multiplicative reduction at both $\mathfrak{q}_1$ and $\mathfrak{q}_2$. In this case by Lemma 7.2 we know that $a_{\mathfrak{q}_i}(E) \equiv \pm(q+1) \equiv \pm 2 \pmod{p}$. We impose the following condition:

(II) $a_{\mathfrak{q}_1}(E) \not\equiv \pm 2 \pmod{p}$ or $a_{\mathfrak{q}_2}(E) \not\equiv \pm 2 \pmod{p}$.

From condition (II) we have $q \nmid y$. Let ϱ be a primitive root (i.e. a cyclic generator) for $\mathbb{F}_q^*$, and let $\omega = \varrho^p$. Let

$$\mathcal{Y}_{q,p} = \{\omega^r \ : \ 0 \le r \le k-1\}.$$

Observe that the set $\mathcal{Y}_{q,p}$ has cardinality k and that $y^p \pmod{q} \in \mathcal{Y}_{q,p}$. In practice we choose k to be small so that (I) and (II) are satisfied. This is one of the key ideas underlying the method of Kraus.

Now fix $\varpi \in \mathcal{Y}_{q,p}$ and suppose $y^p \equiv \varpi \pmod{q}$. Note that $\sqrt{5} \equiv \theta_1 \pmod{\mathfrak{q}_i}$. By (11) we see that $\varepsilon^{2n} \pmod{\mathfrak{q}_1}$ is a root (in $\mathbb{F}_q$) of the quadratic polynomial

$$P_\varpi = T^2 + (2 - \varpi) \cdot \theta_1 \cdot T - 1.$$

We will write

$$\mathcal{T}_{q,p} = \{t \in \mathbb{F}_q \ : \ P_\varpi(t) = 0 \text{ for some } \varpi \in \mathcal{Y}_{q,p}, \text{ and } t \text{ is a square}\}.$$

Thus $\varepsilon^{2n} \pmod{\mathfrak{q}_1}$ belongs to $\mathcal{T}_{q,p}$. The set $\mathcal{T}_{q,p}$ has at most $2k$ elements. We will reduce its size using what we know about n. Recall that $n \equiv m_0 \pmod{M_1}$ and therefore $2n \equiv 2m_0 \pmod{2M_1}$. Let $\nu = (q-1)/\gcd(q-1, 2M_1)$. It follows that $(\varepsilon^{2n}/\varepsilon^{2m_0})^\nu \equiv 1 \pmod{q}$. We deduce that $\varepsilon^{2n} \pmod{\mathfrak{q}_1}$ belongs to

$$\mathcal{S}_{q,p}(m_0) = \{t \in \mathcal{T}_{q,p} \ : \ (t/\varepsilon_1^{2m_0})^\nu \equiv 1 \pmod{q}\}.$$

Lemma 10.2 *With notation and assumptions as above, let q be a prime satisfying conditions (I) and (II). Let*

$$\mathcal{R}_{q,p}(m_0) = \{t \in \mathcal{S}_{q,p} : a_q(G_t) \equiv a_{\mathfrak{q}_1}(E) \text{ and } a_q(H_t) \equiv a_{\mathfrak{q}_2}(E) \pmod{p}\},$$

where the elliptic curves $G_t/\mathbb{F}_q$ and $H_t/\mathbb{F}_q$ are given by

$$G_t \; : \; Y^2 = X^3 + 2(t+\theta_1)X^2 + X \quad \text{and} \quad H_t \; : \; Y^2 = X^3 + 2(t^{-1}+\theta_2)X^2 + X,$$

respectively. Then $\varepsilon^{2n} \pmod{\mathfrak{q}_1}$ belongs to $\mathcal{R}_{q,p}$.

Proof Let $t \in \mathcal{S}_{q,p}$ satisfy $t \equiv \varepsilon^{2n} \pmod{\mathfrak{q}_1}$. Then G_t is the reduction of E_n modulo $\mathfrak{q}_1$, and H_t is the reduction of E_n modulo $\mathfrak{q}_2$. In particular, $a_{\mathfrak{q}_1}(E_n) = a_q(G_t)$ and $a_{\mathfrak{q}_2}(E_n) = a_q(H_t)$. But by Lemma 7.2 we have $a_{\mathfrak{q}_i}(E_n) \equiv a_{\mathfrak{q}_i}(E)$ for $i = 1, 2$. It follows that $a_q(G_t) \equiv a_{\mathfrak{q}_1}(E) \pmod{p}$ and $a_q(H_t) \equiv a_{\mathfrak{q}_2}(E) \pmod{p}$. □

Finally we shall need one more assumption on q.

(III) $\varepsilon_1^{2k} \not\equiv 1 \pmod{q}$.

Lemma 10.3 *Let (n, y, p) be a solution to (10) with $p \geq 5$.*

(a) Let q be a prime satisfying (I), (II) and suppose that $\mathcal{R}_{q,p}(2) = \emptyset$. Then $n \not\equiv 2 \pmod{M_1}$.
(b) Let q be a prime satisfying (I), (II), (III). Suppose $n \equiv m_0 \pmod{M_1}$ where $m_0 = -2$ or -1. Suppose every $t \in \mathcal{R}_{q,p}(m_0)$ satisfies $(t/\varepsilon_1^{2m_0}) \equiv 1 \pmod{q}$. Then $n \equiv m_0 \pmod{p}$.

Proof Part (a) follows immediately from the above. For part (b), recall that $\varepsilon \equiv \varepsilon_1 \pmod{\mathfrak{q}_1}$ and also that the reduction of ε^{2n} modulo $\mathfrak{q}_1$ belongs to $\mathcal{R}_{q,p}(m_0)$. From the hypothesis in (b), we have $\varepsilon_1^{2(n-m_0)} \equiv 1 \pmod{q}$. However $q = 2kp + 1$ and by assumption (III), $\varepsilon_1^{2k} \not\equiv 1 \pmod{q}$. Thus $p \mid (n - m_0)$ as required. □

10.1 Proof of Proposition 10.1

In Section 9 we showed that if $n \neq -2, -1$, then $p < 10^{11}$. We may therefore assume this bound. We wrote a short `Magma` script which for each prime in the range $5 \leq p < 10^{11}$, searches for primes q satisfying (I), (II), (III) and applies the criteria in Lemma 10.3 to prove Proposition 10.1. The total processor time for the proof is roughly 1200 days, although the computation, running on a 2499MHz AMD Opterons, was spread over 50 processors, making the actual computation time about 24 days.

11 Linear forms in two logs

Lemma 11.1 *Let (n, y, p) be a solution to (10) with $n \neq -1, -2$. Then $p < 5000$.*

Let us assume that $p > 5000$. Note that $F_{-2n} = -F_{2n}$. Let $N = |n|$ and $Y = |y|$. Thus $F_{2N} \pm 2 = Y^p$. This can be rewritten as

$$\frac{\varepsilon^{2N}}{\sqrt{5}Y^p} - 1 = \frac{\varepsilon^{-2N} \mp 2\sqrt{5}}{\sqrt{5}Y^p}.$$

Let

$$\Delta = 2N \log \varepsilon - \log \sqrt{5} - p \log Y.$$

Using Lemma B.2 of [22], we have

$$|\Delta| < \frac{2.1}{Y^p},$$

and therefore

$$\log|\Delta| < \log 2.1 - p\log(Y). \tag{35}$$

By Proposition 10.1 we have $n \equiv -1, -2 \pmod{p}$. Thus we can write $N = kp + \delta$ where $\delta = \pm 1, \pm 2$. Therefore the linear form in three logarithms Δ may now be rewritten as a linear form in two logarithms,

$$\Delta = p\log(\varepsilon^{2k}/Y) - \log(\sqrt{5}/\varepsilon^{2\delta}).$$

From (35), $|\delta| \leq 2$, $Y \geq 19$ and $p > 5000$, we have that

$$\left|2k\log\varepsilon - \log Y\right| < \frac{16}{p} < 0.0032. \tag{36}$$

We will apply Theorem 4 with

$$b_1 = 1, \quad b_2 = p, \quad \alpha_1 = \sqrt{5}/\varepsilon^{2\delta}, \quad \alpha_2 = \varepsilon^{2k}/Y, \quad \text{and } D = 2.$$

We have that

$$h(\alpha_1) \leq \frac{1}{2}\log\left(\frac{15}{2} + \frac{7}{2}\sqrt{5}\right) < 1.365$$

and

$$h(\alpha_2) \leq \max\{\log Y, 2k\log\varepsilon\} < 1.01\log Y,$$

whereby we can choose, from (36),

$$a_1 = (\rho - 1)\log(\sqrt{5}\,\varepsilon^4) + 5.46$$

and

$$a_2 = 0.0032\,(\rho - 1) + 4.04\log Y.$$

Lemma 11.2 *Suppose $n \neq -1, -2$. Then α_1, α_2 are multiplicatively independent.*

Proof If α_1, α_2 are multiplicatively dependent then $y = \pm 5^r$ for some r. This contradicts Lemma 3.4. □

We now choose $\rho = 23$ and check that, in all cases, inequality (34) contradicts (35). This completes the proof of Lemma 11.1.

12 Deriving the unit equation

With a reasonably good upper bound upon p in hand, our objective now is to obtain a bound for n in terms of p (which we will obtain in the next section). Towards this goal we reduce (10) to a unit equation. We start with (11), where we recall that $x = \varepsilon^{2n} + \sqrt{5}$. Thus

$$(\varepsilon^{2n} + \sqrt{5} + \sqrt{6})(\varepsilon^{2n} + \sqrt{5} - \sqrt{6}) = \sqrt{5}\cdot\varepsilon^{2n}\cdot y^p. \tag{37}$$

Let $K = \mathbb{Q}(\sqrt{5})$ and $K' = K(\sqrt{6})$. Write $\mathcal{O}$ and $\mathcal{O}'$ for the rings of integers of K and K'; these both have class number 1. As $\gcd(6, y) = 1$ (Lemma 3.3), the two factors on the left-hand side of (37) are coprime in $\mathcal{O}'$. The prime ideal $\sqrt{5}\mathcal{O}$ splits as a product of two primes in $\mathcal{O}'$:

$$\sqrt{5}\mathcal{O}' = \varphi_1\mathcal{O}' \cdot \varphi_2\mathcal{O}'$$

where

$$\varphi_1 = -2 + \sqrt{5} + \left(\frac{1-\sqrt{5}}{2}\right)\sqrt{6} \quad \text{and} \quad \varphi_2 = -2 + \sqrt{5} - \left(\frac{1-\sqrt{5}}{2}\right)\sqrt{6}.$$

Let

$$\delta = \sqrt{5} + \sqrt{6} \quad \text{and} \quad \mu = 5 + 2\sqrt{6}.$$

Then ε, δ, μ is a system of fundamental units for $\mathcal{O}'$, and the torsion unit group is just $\{\pm 1\}$. It follows that

$$\varepsilon^{2n} + \sqrt{5} + \sqrt{6} = \varepsilon^a \cdot \delta^b \cdot \mu^c \cdot \varphi_i \cdot \alpha^p \tag{38}$$

for some $i \in \{1, 2\}$, $a, b, c \in \mathbb{Z}$ and $\alpha \in \mathcal{O}'$. The exponents a, b, c matter to us only modulo p, as we can absorb any p-th power into the term α^p.

We now write $M_2 = \text{lcm}(M_1, p)$, where M_1 is given by (22). By Proposition 10.1 we know that $n \equiv -2$ or $-1 \pmod{M_2}$.

Lemma 12.1 *Let* $m_0 \in \{-2, -1\}$. *Let* (n, y, p) *be a solution to* (10) *with* $p \geq 5$, *and* $n \equiv m_0 \pmod{M_2}$. *Then*

$$\varepsilon^{2n} + \sqrt{5} + \sqrt{6} = \left(\varepsilon^{2m_0} + \sqrt{5} + \sqrt{6}\right) \cdot \alpha^p \tag{39}$$

for some $\alpha \in \mathcal{O}_K$.

Proof The lemma certainly holds if $n = -2$ or -1. We may therefore suppose $n \neq -2$, -1, whence, by Lemma 11.1, that $p < 5000$. We observe that

$$\varepsilon^{-4} + \sqrt{5} + \sqrt{6} = -1 \cdot \varepsilon^{-2} \cdot \mu \cdot \varphi_1,$$

and

$$\varepsilon^{-2} + \sqrt{5} + \sqrt{6} = \varepsilon^{-1} \cdot \delta \cdot \varphi_2.$$

Thus, if $m_0 = -2$, then we want to show, in (38), that $i = 1$ and

$$(a, b, c) \equiv (-2, 0, 1) \pmod{p},$$

while, if $m_0 = -2$, we want to show that $i = 2$ and

$$(a, b, c) \equiv (-1, 1, 0) \pmod{p}.$$

Observe that

$$\text{Norm}_{K'/K}(\varepsilon) = \varepsilon^2, \quad \text{Norm}_{K'/K}(\delta) = -1 \quad \text{and} \quad \text{Norm}_{K'/K}(\mu) = 1.$$

Taking norms on both sides of (38) and comparing with (37) we deduce that $2a \equiv 2n \pmod{p}$ and so $a \equiv n \pmod{p}$. As $p \mid M_2$ we have derived the required congruences for a.

Now let $\mathfrak{q}$ be a prime ideal of K' satisfying the following conditions:

(i) $\mathfrak{q}$ has degree 1; we denote by q the rational prime below $\mathfrak{q}$, so $\text{Norm}(\mathfrak{q}) = q$.
(ii) $p \mid (q-1)$.
(iii) $(q-1) \mid M_2$.

Fix a choice of a primitive root ϖ for $\mathbb{F}_{\mathfrak{q}}^* = \mathbb{F}_q^*$ and let $\log_{\mathfrak{q}} : \mathbb{F}_{\mathfrak{q}}^* \to \mathbb{Z}/p\mathbb{Z}$ be the composition of the discrete logarithm $\mathbb{F}_{\mathfrak{q}}^* \to \mathbb{Z}/(q-1)\mathbb{Z}$ induced by ϖ with the quotient map

$\mathbb{Z}/(q-1)\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$; it is here that we make use of condition (ii). Now $n \equiv m_0 \pmod{M_2}$ where $m_0 = -2$ or -1. By assumption (iii) we have $\varepsilon^{2n} \equiv \varepsilon^{2m_0} \pmod{\mathfrak{q}}$. Applying $\log_{\mathfrak{q}}$ to (38) we obtain

$$b \log_{\mathfrak{q}}(\delta) + c \log_{\mathfrak{q}}(\mu) \equiv \log_{\mathfrak{q}}(\varepsilon^{2m_0} + \sqrt{5} + \sqrt{6}) - m_0 \log_{\mathfrak{q}}(\varepsilon) - \log_{\mathfrak{q}} \varphi_i \pmod{p}.$$

It follows that for each choice of $\mathfrak{q}$ satisfying conditions (i), (ii) and (iii), we obtain a linear congruence for b and c modulo p. We wrote a `Magma` script which did the following. For each prime $5 \le p < 5000$, each choice $m_0 \in \{-2, -1\}$ and $i \in \{1, 2\}$, the script found five prime ideals $\mathfrak{q}$ satisfying (i), (ii) and (iii), and solved the corresponding linear system of congruences for b and c. We found that for $m_0 = -2$ the system had precisely one solution when $i = 1$, and that solution is $(b, c) \equiv (0, 1) \pmod{p}$, and no solution when $i = 2$. Likewise we found that for $m_0 = -1$ the system had precisely one solution when $i = 2$, namely $(b, c) \equiv (1, 0) \pmod{p}$, and no solution when $i = 1$. This completes the proof. □

Next we let

$$\kappa = (\varepsilon^{2m_0} + \sqrt{5} + \sqrt{6}) \cdot (\sqrt{6} - \sqrt{5}).$$

Then we can rewrite (39) as

$$-(\sqrt{5} + \sqrt{6}) \cdot \varepsilon^{2n} = 1 - \kappa \cdot \alpha^p. \tag{40}$$

The left hand-side is a unit of K'. Let

$$\tau_j = 1 - \zeta^j \cdot \sqrt[p]{\kappa} \cdot \alpha, \qquad \zeta = \exp(2\pi i/p)$$

for $j = 0, \ldots, p-1$. It follows that τ_j is a unit in the ring of integers of $K_j = K'(\zeta^j \cdot \sqrt[p]{\kappa})$. Let

$$\nu_0 = \zeta^2 - \zeta, \qquad \nu_1 = 1 - \zeta^2, \qquad \nu_2 = \zeta - 1.$$

We obtain the unit equation

$$\nu_0 \tau_0 + \nu_1 \tau_1 + \nu_2 \tau_2 = 0. \tag{41}$$

13 A bound for *n*

In this section we derive a bound for the unknown index n in (10). This bound will follow from the bounds on the heights of the solutions to the unit equation (41). In order to obtain bounds for solutions to unit equations we closely follow [6]. For this we merely need some information about the number fields containing these solutions. Recall $K' = \mathbb{Q}(\sqrt{5}, \sqrt{6})$ and $K_j = K'(\zeta^j \cdot \sqrt[p]{\kappa})$. Let $L = K'(\sqrt[p]{\kappa}, \zeta) = K_0(\zeta)$.

Lemma 13.1

$$[K_j : \mathbb{Q}] = 4p, \qquad [L : \mathbb{Q}] = \begin{cases} 40 & \text{if } p = 5 \\ 4p(p-1) & \text{if } p > 5. \end{cases}$$

Moreover, the signature of K_j *is* $(4, 2p-2)$.

Proof The element $\kappa \in \mathcal{O}'$ generates a prime ideal of norm 5 or 19 depending on whether $m_0 = -2$ or -1. Thus $[K_j : K'] = p$, and so $[K_j : \mathbb{Q}] = 4p$ by the tower law. To deduce the signature we observe that for each of the four embeddings $\sigma : K' \to \mathbb{R}$, there is exactly one real choice for the p-th root of $\sigma(\kappa)$, and $(p-1)/2$ complex conjugate pairs of such choices.

Next we compute $\mathbb{Q}(\zeta) \cap K_j$. Since $\mathbb{Q}(\zeta)$ has degree $p-1$, which is not divisible by p, we see that $\mathbb{Q}(\zeta) \cap K_j = \mathbb{Q}(\zeta) \cap K'$. If $p > 5$ then the intersection is $\mathbb{Q}$, as the intersection is unramified at all primes. If $p = 5$ then the intersection in $\mathbb{Q}(\sqrt{5})$. The assertion regarding $[L : \mathbb{Q}]$ follows. □

We shall need a bound for the absolute discriminant of K_j; such a bound is furnished by the following lemma.

Lemma 13.2 *Write Δ_{K_j} for the absolute discriminant of K_j. If $m_0 = -2$ then Δ_{K_j} divides $2^{6p} \cdot 3^{2p} \cdot 5^{3p-1} \cdot p^{4p}$. If $m_0 = -1$ then Δ_{K_j} divides $2^{6p} \cdot 3^{2p} \cdot 5^{2p} \cdot 19^{p-1} \cdot p^{4p}$.*

Proof The absolute discriminant of K' is $\Delta_{K'} = 14400 = 2^6 \times 3^2 \times 5^2$. The extension K_j/K' is generated by a root of the polynomial $x^p - \kappa$, and hence its relative discriminant ideal divides the discriminant of this polynomial which is $\pm p^p \kappa^{p-1}$. We now apply the following standard formula [7, Theorem 2.5.1] for the absolute discriminant

$$\Delta_{K_j} = \pm \operatorname{Norm}_{K'/\mathbb{Q}}(\Delta_{K_j/K'}) \cdot \Delta_{K'}^{[K_j:K']}.$$

The result follows as $\operatorname{Norm}_{K'/\mathbb{Q}}(\kappa) = -5$ or 19 depending on whether $m_0 = -2$ or -1. □

Recall that we are interested in bounding the heights of the solutions to the unit equation (41) for $m_0 = -2, -1$ and $5 \le p < 5000$ prime. For each possible choice of m_0 and p, Lemma 13.2 gives us an upper bound for the absolute value of the discriminant of K_j. Now [6, Section 5], based on a theorem of Landau, gives a computational method for deriving an upper bound for the regulators R_{K_j}. As an illustration, we mention that with $p = 4999$ (the largest prime in our range) the bounds we obtain for R_{K_j} are

$$R_{K_j} < 2.2 \times 10^{64529}, \qquad R_{K_j} < 1.4 \times 10^{66241}$$

for $m_0 = -2, -1$ respectively.

We now explain how to obtain a bound for n. Proposition 8.1 of [6] gives positive numbers A_1, A_2 (depending on the regulators and unit ranks of the K_j) such that

$$h(\nu_2\tau_2/\nu_0\tau_0) \le A_2 + A_1 \log(H + \max\{h(\nu_j\tau_j) \ : \ j = 0, 1, 2\}), \tag{42}$$

where H is an upper bound for the heights $h(\nu_j)$. We shall make repeated use of the following properties for absolute logarithmic heights (see for example [6, Lemma 4.1]):

(i) if r is an integer and β is a non-zero algebraic number then $h(\beta^r) = |r| \cdot h(\beta)$;
(ii) if $\beta_1, \ldots, \beta_m$ are algebraic numbers then

$$h(\beta_1 \cdots \beta_m) \le h(\beta_1) + \cdots + h(\beta_m) \ \text{ and } \ h(\beta_1 + \cdots + \beta_m) \le \log m + h(\beta_1) + \cdots + h(\beta_m).$$

As each ν_j is a sum of two roots of unity, (ii) implies that $h(\nu_j) \le \log 2$, so we can take $H = \log 2$. By the definition of logarithmic height

$$h(\tau_2/\tau_0) = h(\nu_2\tau_2/\nu_0\tau_0)$$

since $\nu_2/\nu_0 = \zeta^{-1}$ is a root of unity. We let $Y = h(\alpha \cdot \sqrt[p]{\kappa})$. Recall that $\tau_j = 1 - \zeta^j \cdot \alpha \cdot \sqrt[p]{\kappa}$. Thus

$$\alpha \cdot \sqrt[p]{\kappa} = 1 + \frac{\zeta^2 - 1}{\tau_2/\tau_0 - \zeta^2}$$

so

$$Y \leq 3\log 2 + h(\tau_2/\tau_0).$$

Observe that

$$h(\nu_j\tau_j) \leq 2\log 2 + h(\tau_j) = 2\log 2 + h(1 - \zeta^j \cdot \alpha \cdot \sqrt[p]{\kappa}) \leq Y + 3\log 2.$$

From (42) we deduce

$$Y \leq A_2 + 3\log 2 + A_1 \log(Y + 4\log 2). \tag{43}$$

By Lemma 9.1 of [6] we have

$$Y \leq 2A_1 \log A_1 + 2A_2 + 10\log 2.$$

Now that we have obtained a bound for $Y = h(\alpha \cdot \sqrt[p]{\kappa})$ we deduce a bound for n. From (40)

$$|n| \cdot \log(\varepsilon) \leq pY + \log 2 + \frac{1}{2}\log(\sqrt{5} + \sqrt{6}),$$

which yields a completely explicit bound for n. As an illustration with $p = 4999$, we obtain the bounds

$$|n| \leq 2.57 \times 10^{398775} \quad \text{and} \quad |n| \leq 1.01 \times 10^{402199},$$

respectively for $m_0 = -2$ and $m_0 = -1$. The corresponding upper bounds for smaller values of p are, in each case, rather less.

14 Completing the proof of Theorem 1

Lemma 14.1 *Suppose $p \leq 79$. Then $n = -2, -1$.*

Proof Proposition 10.1 tells us that $n \equiv m_0 \pmod{M_1}$ where M_1 is given by (22), and $m_0 = -2$ or -1. In fact

$$M_1 \approx 7.12 \times 10^{4298}.$$

We computed the upper bounds upon n for all $p < 5000$. We found that for $p \leq 79$ we have

$$|n| < 1.14 \times 10^{4196} \quad \text{and} \quad |n| < 2.75 \times 10^{4254},$$

respectively for $m_0 = -2$ or -1. Thus for $p \leq 79$, $n = -2$ or -1. □

The bounds for n we obtain as in the previous section are larger than M_1 for the remaining values $83 \leq p < 5000$. To complete the proof of Theorem 1, we will show, for $m_0 \in \{-2, -1\}$ and for each of the remaining p, the existence of some M' that is much larger than the corresponding bound for n, and such that $n \equiv m_0 \pmod{M'}$. For this we shall use a very simple sieve. Fix a prime $83 \leq p < 5000$ and a value $m_0 \in \{-2, -1\}$. Let $3 \leq \ell < 10^4$ be a prime, distinct from p. Suppose we know that $n \equiv m_0 \pmod{M'}$, where M' is a large smooth integer, certainly divisible by M_1. Let $r = \mathrm{ord}_\ell(M')$. We want to show that $n \equiv m_0 \pmod{\ell^{r+1}}$ and so $n \equiv m_0 \pmod{\ell M'}$. We look for primes $q \equiv \pm 1 \pmod 5$ of the form $q = kp\ell^{r+1} + 1$, such that $kp\ell^r \mid M'$ (recall that $M_1 \mid M$ is divisible by all primes $< 10^4$ and so certainly divisible by p). Let $\mathcal{Q}$ be a (small) set of such primes. Let

$$\mathcal{S} := \{m_0 + t \cdot \ell^r \ : \ 0 \leq t \leq \ell - 1\}.$$

Then $n \equiv m \pmod{\ell^{r+1}}$ for some unique value $m \in \mathcal{S}$. We would like to obtain a contradiction for each possible $m \in \mathcal{S}$ except for $m = m_0$. It would then follow that $n \equiv m_0 \pmod{\ell^{r+1}}$ and so $n \equiv m_0 \pmod{\ell M'}$ as required. Fix $m \in \mathcal{S}$, $m \neq m_0$. As $q = kp\ell^{r+1} + 1$ and $kp\ell^r \mid M'$, the assumptions $n \equiv m \pmod{\ell^r}$ and $n \equiv m_0 \pmod{M'}$ force $n \equiv n_q(m) \pmod{q-1}$ for some unique congruence class $n(m, q)$ (which depends on our choices of q and $m \in \mathcal{S}$). Now from Binet's formula, as $q \equiv \pm 1 \pmod 5$, we have $F_{2n} \equiv F_{2n(m,q)} \pmod q$. Since $F_{2n} + 2 = y^p$ we have

$$(F_{2n(m,q)} + 2)^{k\ell^{r+1}} \equiv 0 \quad \text{or} \quad 1 \pmod q. \tag{44}$$

If we find some prime $q \in \mathcal{Q}$ such that (44) fails, then we will have eliminated that particular value of m. Once we have eliminated all possibilities for all $m \in \mathcal{S}$, $m \neq m_0$, we will have deduced $n \equiv m_0 \pmod{\ell M'}$ and we can replace M' by $\ell M'$.

We wrote a simple `Magma` script which keeps increasing the exponents of the primes $3 \leq \ell < 10^4$, $\ell \neq p$ in M' until M' is sufficiently large to deduce that $n = m_0$. The total processor time for the proof is roughly 70 days, although the computation, running on a 2499MHz AMD Opterons, was spread over 50 processors, making the actual computation time about 1.4 days. This completes the proof of Theorem 1.

Author details
[1]Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, Canada,
[2]Department of Mathematics, University of Toronto, Toronto M5S 2E4, Canada,
[3]Mathematics Institute, University of Warwick, Coventry CV4 7AL, UK.

Acknowledgements
The first-named is supported by NSERC. The third-named author is supported by an EPSRC Leadership Fellowship EP/G007268/1, and EPSRC *LMF: L-Functions and Modular Forms* Programme Grant EP/K034383/1.

Received: 26 September 2018 Accepted: 18 January 2019
Published online: 30 January 2019

References

1. Bennett, M.A., Dahmen, S., Mignotte, M., Siksek, S.: Shifted powers in binary recurrence sequences. Math. Proc. Camb. Philos. Soc. **158**, 305–329 (2015)
2. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system I: the user language, *J. Symb. Comp.***24**, 235–265. (See also http://magma.maths.usyd.edu.au/magma/) (1997)
3. Bugeaud, Y., Luca, F., Mignotte, M., Siksek, S.: Fibonacci numbers at most one away from a perfect power. Elem. Math. **63**(2), 65–75 (2008)
4. Bugeaud, Y., Luca, F., Mignotte, M., Siksek, S.: Almost powers in the Lucas sequences. J. Théor. Nombres Bordeaux **20**, 555–600 (2008)
5. Bugeaud, Y., Mignotte, M., Siksek, S.: Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers. Ann. Math **163**, 969–1018 (2006)
6. Bugeaud, Y., Mignotte, M., Siksek, S., Stoll, M., Tengely, Sz: Integral points on hyperelliptic curves. Algebra Number Theory **2**, 859–885 (2008)
7. Cohen, H.: Advanced Topics in Computational Algebraic Number Theory, vol. 193. Springer–Verlag, Berlin (2000)
8. David, A.: Caractère d'isogénie et crittéres d'irréductibilité, arXiv:1103.3892v2 [math.NT]
9. Dembélé, L., Voight, J.: Explicit methods for Hilbert modular forms, In *Elliptic curves, Hilbert modular forms and Galois deformations*, Adv. Courses Math. CRM Barcelona, pp. 135–198. Birkhäuser/Springer, Basel (2013)
10. Freitas, N., Le Hung, B., Siksek, S.: Elliptic curves over real quadratic fields are modular. Invent. Math. **201**, 159–206 (2015)
11. Freitas, N., Siksek, S.: The asymptotic Fermat's last theorem for five-sixths of real quadratic fields. Compos. Math. **151**, 1395–1415 (2015)
12. Freitas, N., Siksek, S.: Criteria for the irreducibility of mod *p* representations of Frey curves. J. Théor. Nombres Bordeaux **27**, 67–76 (2015)
13. Kraus, A., Oesterlé, J.: Sur une question de B. Mazur. Math. Ann **293**, 259–275 (2002)
14. Kraus, A.: Sur l'équation $a^3 + b^3 = c^p$. Exp. Math. **7**, 1–13 (1998)
15. Laurent, M.: Linear forms in two logarithms and interpolation determinants. II. Acta Arith. **133**, 325–348 (2008)

16. Matveev, E.: An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II. Izv. Math **64**, 1217–1269 (2000)
17. Mignotte, M.: A kit on linear forms in three logarithms, p. 45. http://www-irma.u-strasbg.fr/~bugeaud/travaux/kit.ps
18. Momose, F.: Isogenies of prime degree over number fields. Compos. Math. **97**, 329–348 (1995)
19. Pethő, A.: Perfect powers in second order linear recurrences. J. Number Theory **15**, 5–13 (1982)
20. Shorey, T., Stewart, C.L.: On the Diophantine equation $ax^{2t} + bx^t y + cy^2 = d$ and pure powers in recurrence sequences. Math. Scand. **52**, 24–36 (1983)
21. Silverman, J.H.: Advanced topics in the arithmetic of elliptic curves, Graduate Texts in Mathematics 151. Springer-Verlag, New York (1994)
22. Smart, N.P.: The Algorithmic Resolution of Diophantine Equations. Cambridge University Press, Cambridge (1998)
23. Smart, N.P., Stephens, N.M.: Integral points on elliptic curves over number fields. Math. Proc. Camb. Philos. Soc. **122**, 9–16 (1997)