New York Journal of Mathematics

New York J. Math. **26** (2020) 711–734.

Elliptic curves over finite fields with Fibonacci numbers of points

Yuri Bilu, Carlos A. Gómez, Jhonny C. Gómez and Florian Luca

Abstract. For a prime power q and an elliptic curve $\mathbf{E}$ over $\mathbb{F}_q$ having $q+1-a$ points, where $a \in [-2\sqrt{q}, 2\sqrt{q}]$ let $\{\#\mathbf{E}_m\}_{m\geq 1}$ be the sequence of numbers whose mth term is the number of points of $\mathbf{E}$ over $\mathbb{F}_{q^m}$. In this paper, we determine all instances when

$$\#(\{\#\mathbf{E}_m\}_{m\geq 1} \cap \{F_n\}_{n\geq 1}) \geq 2,$$

where $\{F_n\}_{n\geq 1}$ is the sequence of Fibonacci numbers. That is, we determine all six–tuples $(a, q, m_1, m_2, n_1, n_2)$ such that $\#\mathbf{E} = q+1-a$, $\#\mathbf{E}_{m_1} = F_{n_1}$ and $\#\mathbf{E}_{m_2} = F_{n_2}$.

Contents

1. The problem and the result

Let $\mathbf{E}$ be a curve of genus 1 over the finite field $\mathbb{F}_q$. It is known that its number of points $\#\mathbf{E}$ is of the form $q+1-a$, where $a \in [-2\sqrt{q}, 2\sqrt{q}]$. Knowing q and a it is easy to determine the number of points of $\mathbf{E}$ defined

Received December 24, 2019.

1991 *Mathematics Subject Classification.* 11D61; 11G20, 11J86, 11Y50, 11B39.

Key words and phrases. Fibonacci numbers; elliptic curves; linear forms in logarithms; Baker-Davenport reduction.

ISSN 1076-9803/2020

over the extension $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$. Namely, letting $\#\mathbf{E}_m$ denote this number, we have that $\#\mathbf{E}_m = q^m + 1 - (\alpha^m + \overline{\alpha}^m)$, where α, $\overline{\alpha}$ are the two roots of the quadratic equation $x^2 - ax + q = 0$. In particular, $\#\mathbf{E}_m = q^m + 1 - a_m$, where $a_m = \alpha^m + \overline{\alpha}^m$ satisfies $a_m \in [-2q^{m/2}, 2q^{m/2}]$. Thus, the parameters q and a determine entirely the sequence $\{\#\mathbf{E}_m\}_{m\geq 1}$. The details can be found in Silverman [10, Section V.2].

We let $\mathcal{F}$ be our sequence of favorite numbers and we ask what can we say about q and a such that the sequence $\{\#\mathbf{E}_m\}_{m\geq 1}$ contains members from $\mathcal{F}$. Formulated in this way, it is likely that there are infinitely many solutions to our problem if $\mathcal{F}$ contains arbitrarily large numbers. That is, take $m = 1$ and note that it suffices to find q and a with $|a| \leq 2\sqrt{q}$ such that $q + 1 - a = f \in \mathcal{F}$. This is equivalent to $q \in [(\sqrt{f} - 1)^2, (\sqrt{f} + 1)^2]$, a well known conjecture which however does not seem to follow from the Riemann Hypothesis. Goldston [4] deduced the validity of this conjecture assuming a strong form of Montgomery's pair correlation conjecture. See [2] for related results. So, to make our problem more interesting, we ask what about pairs (q, a) such that $\{\#\mathbf{E}_m\}_{m\geq 1}$ and $\mathcal{F}$ have at least two members in common?

Here, we completely answer this question for the case when $\mathcal{F} := \{F_n\}_{n\geq 1}$ is the sequence of Fibonacci numbers. To make the notation more precise, if $\#\mathbf{E} = q + 1 - a$, then we write $E_m(q, a) := \#\mathbf{E}_m$ for all $m \geq 1$. Our result is the following:

Theorem 1.1. *The only solutions (q, a) with q a prime power and a an integer in the interval $[-2\sqrt{q}, 2\sqrt{q}]$ of the system of Diophantine equations*

$$E_{m_1}(q, a) = F_{n_1}, \qquad E_{m_2}(q, a) = F_{n_2},$$

with $1 \leq m_1 < m_2$ are

$$\begin{array}{llll} E_1(2,1) = F_3, & E_2(2,1) = F_6; & & \\ E_1(2,2) = F_2, & E_2(2,2) = F_5, & E_3(2,2) = F_7; & \\ E_1(4,2) = F_4, & E_2(4,2) = F_8; & & \\ E_1(5,3) = F_4, & E_3(5,3) = F_{12}; & & \\ E_1(7,3) = F_5, & E_2(7,3) = F_{10}. & & \end{array} \tag{1}$$

Examples of actual curves with the above number of points are, respectively:

$$\begin{aligned} C_1 &:= \{(x,y) \in \mathbb{F}_2^2 : y^2 + xy = x^3 + x^2 + 1\} = \{\infty, (0,1)\};\\ C_2 &:= \{(x,y) \in \mathbb{F}_2^2 : y^2 + y = x^3 + x + 1\} = \{\infty\};\\ C_3 &:= \{(x,y) \in (\mathbb{F}_2[\theta]/(\theta^2 + \theta + 1))^2 : y^2 + y = x^3 + \theta x\}\\ &\quad = \{\infty, (0,0), (0,1)\};\\ C_4 &:= \{(x,y) \in \mathbb{F}_5^2 : y^2 = x^3 + 4x + 2\} = \{\infty, (3,1), (3,4)\};\\ C_5 &:= \{(x,y) \in \mathbb{F}_7^2 : y^2 = x^3 + x + 1\} = \{\infty, (0,1), (0,6), (2,3), (2,4)\}. \end{aligned}$$

2. The method

It is well–known that

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}} \quad \text{for all} \quad n \geq 0, \quad \text{where} \quad (\alpha, \beta) = \left(\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2} \right).$$

Since $F_n = \alpha^n/\sqrt{5}(1 + O(\alpha^{-2n}))$ and $E_m(q, a) = q^m(1 + O(q^{-m/2}))$, the equation $E_m(q, a) = F_n$ can be treated using linear forms in logarithms. That is, such equation implies easily that

$$|n \log \alpha - \log \sqrt{5} - m \log q| = O(\alpha^{-n/2}) = O(q^{-m/2}). \tag{2}$$

Using lower bounds for linear forms in logarithms, this gives

$$n = O((\log n)(\log q)).$$

The constant in O is not small (at least 10^{12}) since one works with linear forms in 3 logarithms. It remains to find some estimate independent of q. Writing down estimates (2) for $(m, n) = (m_i, n_i)$ for $i = 1, 2$, and eliminating the $\log q$ term one gets

$$|(n_1 m_2 - m_1 n_2) \log \alpha - (m_1 - m_2) \log \sqrt{5}| = O(m_2 \alpha^{-n_1/2}).$$

Now, using lower bounds for a linear form in 2 logs, one gets easily that $n_1 = O(\log n_2)$. Since also $\log q = O(n_1) = O(\log n_2)$ by going back to the linear form (2) for $(m, n) = (m_2, n_2)$, one gets

$$n_2 = O((\log n_2)(\log q)) = O((\log n_2)^2)$$

and one bounds n_2. In principle, this is all up to the computational details. As for the computational details, we first apply a linear form in 3 logs due to Matveev. This gives $m_2 < 4 \times 10^{12}$ and later that $q < 10^{55}$ and we need to lower these bounds. For this we apply a linear form in 3 logs due to Mignotte which lowers somewhat the bound on m_2 to $m_2 \leq 4 \times 10^9$. When lowering further the bounds, one can apply the Baker–Davenport procedure on the left–hand side of estimate (2) in order to find an actual numerical lower bound for that expression but one needs some good set of candidates for q. We win by showing that one of the three situations arises:

- (i) q is small; i.e., $q < 2 \times 10^{10}$;
- (ii) n_1 is small; i.e, $n_1 \leq 100$ and $q \in [(\sqrt{F_{n_1}} - 1)^2, (\sqrt{F_{n_1}} + 1)^2]$ is prime;
- (iii) m_2 is small; i.e, $m_2 < 4 \times 10^9$, $m_1 = 1$ and m_2 determines, up to a few choices, both parameters n_1 and a; hence, $q = F_{n_1} + (a - 1)$.

In each one of the above three cases, we get a certain list of possible values for q. For example, in case (i) there are 882206716 values of q and in case (ii), there are 7769416102. We applied the Baker–Davenport reductions for all the q's gathered from the above three cases and show that in all instances $n_2 \leq 1000$. Finally, we show how to cover the range $n_2 \leq 1000$.

3. Tools

3.1. Linear forms in logarithms. In order to prove our main result Theorem 1.1, we need to use several times a Baker–type lower bound for a nonzero linear form in logarithms of algebraic numbers. For us, they are in two or three logarithms. We start by recalling a result of Matveev [6, Theorem 2.1].

Theorem 3.1 (Matveev)**.** *Let $\gamma_1, \dots, \gamma_t$ be positive totally real multiplicatively independent algebraic numbers. Let $\mathbb{K} := \mathbb{Q}(\gamma_1, \dots, \gamma_t)$ and let $D := [\mathbb{K} : \mathbb{Q}]$. Let $b_1, \dots, b_t$ be nonzero integers, and put*

$$\Lambda := b_1 \log \gamma_1 + \cdots + b_t \log \gamma_t. \tag{3}$$

Let A_j $(1 \le j \le t)$ and E be defined by

$$A_j \ge \max\{Dh(\gamma_j), |\log \gamma_j|\},$$
$$E := \max\{1, \max\{|b_j| A_j / A_t : 1 \le j \le t\}\},$$

where $h(\gamma)$ is the Weil height of γ. Then

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

where

$$C(t) := \frac{8}{(t-1)!}(t+2)(2t+3)(4e(t+1))^{t+1};$$
$$C_0 := \log(e^{4.4t+7} t^{5.5} D^2 \log(eD));$$
$$W_0 := \log(1.5eED \log(eD));$$
$$\Omega := A_1 \cdots A_t.$$

The above linear form in logarithms gives us a huge bound on m_2. With a lot more work, we can save a factor of 10^3 by using the following result of Mignotte [7, Proposition 5.2]; see also [8].

Theorem 3.2. *Let $\Lambda := b_2 \log \gamma_2 - b_1 \log \gamma_1 - b_3 \log \gamma_3 \neq 0$ with b_1, b_2, b_3 positive integers with $\gcd(b_1, b_2, b_3) = 1$ and $\gamma_1, \gamma_2, \gamma_3$ positive real algebraic numbers > 1 in a field $\mathbb{K}$ of degree D. Let*

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

Let a_1, a_2, a_3 be real numbers such that

$$a_i \ge \max\{4, 4.296 \log \gamma_i + 2Dh(\gamma_i)\}, \quad i = 1, 2, 3, \quad \Omega := a_1 a_2 a_3 \ge 100.$$

Put

$$b' := \left(\frac{b_1'}{a_2} + \frac{b_2'}{a_1}\right)\left(\frac{b_3''}{a_2} + \frac{b_2''}{a_3}\right), \qquad \log \mathcal{B} := \max\{0.882 + \log b', 10/D\}.$$

Then one of the following holds:

(*i*)

$$\log |\Lambda| > \exp\left(-790.95 \Omega D^2 (\log \mathcal{B})^2\right);$$

(*ii*) *there exist nonzero integers* r_0, s_0 *with* $r_0 b_2 = s_0 b_1$ *satisfying the inequalities*

$$|r_0| < 5.61(D\log\mathcal{B})^{1/3}a_2 \quad \textit{and} \quad |s_0| < 5.61(D\log\mathcal{B})^{1/3}a_1;$$

(*iii*) *there exist integers* $r_1 \neq 0, s_1 \neq 0, t_1, t_2$ *satisfying*

$$\gcd(r_1, t_1) = \gcd(s_1, t_2) = 1, \qquad (t_1 b_1 + r_1 b_3)s_1 = r_1 b_2 t_2,$$

and also

$$|r_1 s_1| < 5.61\delta(D\log\mathcal{B})^{1/3}a_3,$$
$$|s_1 t_1| < 5.61\delta(D\log\mathcal{B})^{1/3}a_1,$$
$$|r_1 t_2| < 5.61\delta(D\log\mathcal{B})^{1/3}a_2,$$

where $\delta := \gcd(r_1, s_1)$. *If* $t_1 = 0$, *we can take* $r_1 = 1$ *and if* $t_2 = 0$ *we can take* $s_1 = 1$.

When $t = 2$ and γ_1, γ_2 are positive and multiplicatively independent, we can use a result of Laurent, Mignotte and Nesterenko [5]. Namely, let in this case $B_1,\ B_2$ be real numbers larger than 1 such that

$$\log B_i \geq \max\left\{h(\gamma_i), \frac{|\log\gamma_i|}{D}, \frac{1}{D}\right\}, \qquad \text{for} \quad i = 1, 2,$$

and put

$$b' := \frac{|b_1|}{D\log B_2} + \frac{|b_2|}{D\log B_1}.$$

Put

$$\Lambda := b_1\log\gamma_1 + b_2\log\gamma_2. \tag{4}$$

We note that $\Lambda \neq 0$ because γ_1 and γ_2 are multiplicatively independent. The following result is due to Laurent, Mignotte and Nesterenko ([5], Corollary 2, p. 288).

Theorem 3.3 (Laurent, Mignotte, Nesterenko)**.** *With the above notation, assuming that* γ_1, γ_2 *are positive and multiplicatively independent, then*

$$\log|\Lambda| > -24.34D^4\left(\max\left\{\log b' + 0.14, \frac{21}{D}, \frac{1}{2}\right\}\right)^2 \log B_1 \log B_2.$$

3.2. Continued fractions. During the course of our calculations, we get some upper bounds on our variables which are too large, thus we need to reduce them. To do so, we use some results from the theory of continued fractions. Specifically, for a nonhomogeneous linear form in two integer variables, we use a slight variation of a result due to Dujella and Pethő ([3], Lemma 5a, pp. 303–304), which itself is a generalization of a result of Baker and Davenport [1].

For a real number X, we write $||X|| := \min\{|X - n| : n \in \mathbb{Z}\}$ for the distance from X to the nearest integer.

Lemma 3.4 (Dujella, Pethő)**.** *Let M and Q be positive integers such that $Q > 6M$, and A, B, τ, μ be some real numbers with $A > 0$ and $B > 1$. Let further $\varepsilon := ||\mu Q|| - M||\tau Q||$. If $\varepsilon > 0$, then there is no solution to the inequality*

$$0 < |u\tau - v + \mu| < AB^{-w},$$

in positive integers u, v and w with

$$u \le M \quad \text{and} \quad w \ge \frac{\log(AQ/\varepsilon)}{\log B}.$$

In practical applications Q is always the denominator of a convergent of the continued fraction of τ, though this is not formally required for the statement.

The above lemma cannot be applied when $\mu = 0$ since then $\varepsilon < 0$. In this case, we use the following classical result in the theory of Diophantine approximation, which is the well–known Legendre criterion (see Theorem 8.2.4 in [9]).

Lemma 3.5 (Legendre)**.** (*i*) *Let τ be an irrational real number and x, y integers such that*

$$\left|\tau - \frac{x}{y}\right| < \frac{1}{2y^2}. \tag{5}$$

Then $x/y = P_k/Q_k$ is a convergent of τ. Furthermore,

$$\left|\tau - \frac{x}{y}\right| \ge \frac{1}{(a_{k+1} + 2)y^2}, \tag{6}$$

where $[a_0, \ldots, a_k, \ldots]$ is the continued fraction expansion of τ.

(*ii*) *If x, y are integers with $y \ge 1$ and*

$$|y\tau - x| < |Q_k\tau - P_k|,$$

then $y \ge Q_{k+1}$.

Recall that $P_k/Q_k = [a_0, \ldots, a_k]$ for all $k \ge 0$.

4. The final computations

We assume that we have shown that $n_2 \le 1000$ and we show how to finish off the problem.

4.1. The case of small q. We take $q \le 10000$. We generated a list $\mathcal{Q}$ of all prime powers $q \le 10000$. There are 1229 primes $p \le 10000$ but adjoining also the prime powers of exponent > 1 in this range we get a list of 1280 elements. For each $q \in \mathcal{Q}$ and each $a \in [-2\sqrt{q}, 2\sqrt{q}]$, we generated $E_m(q, a)$ for $m \ge 1$ as follows. First of all $\{E_m(q, a)\}_{m \ge 0}$ is linearly recurrent of order 4 whose initial values are

$$E_0(q, a) = 0, \qquad E_1(q, a) = q + 1 - a, \qquad E_2(q, a) = (q + 1)^2 - a^2,$$
$$E_3(q, a) = q^3 + 1 - a(a^2 - 3q).$$

Its characteristic polynomial is

$$(X-1)(X-q)(X^2-aX+q) = X^4-(q+a+1)X^3+(aq+a+2q)X^2 \\ -(qa+q^2+q)X+q^2.$$

Hence,

$$E_m(q,a) = (q+a+1)E_{m-1}(q,a)-(aq+a+2q)E_{m-2}(q,a) \\ +(qa+q^2+q)E_{m-3}(q,a)-q^2E_{m-4}(q,a) \qquad \text{for all} \quad m\ge 4.$$

We claim the following: if $E_m(q,a)=F_n$ with $q\le 10000$ and $n\le 1000$, then

$$m \le M_q := \left\lfloor \frac{\log((1-1/2^{25})^{-2}F_{1000})}{\log q} \right\rfloor. \tag{7}$$

Indeed, we may assume that $m\ge 50$, because $M_q\ge 50$ for $q\le 10000$. Hence,

$$F_{1000} \ge q^m+1-2\sqrt{q^m} = q^m\left(1-\frac{1}{q^{m/2}}\right)^2 \ge q^m\left(1-\frac{1}{2^{25}}\right)^2,$$

so

$$q^m < \left(1-\frac{1}{2^{25}}\right)^{-2} F_{1000}.$$

This proves (7).

Thus, for all $q\in\mathcal{Q}$ and all $a\in[-2\sqrt{q},2\sqrt{q}]$ we generated, using the above 4th order linear recurrence, the numbers $E_m(q,a)$ for $m\in[1,M_q]$ and we intersected this list with the list of Fibonacci numbers F_n for $n\in[1,1000]$. We asked Mathematica to tell us those pairs (q,a) such that this intersection has at least two elements. This calculation took about 10 minutes and gave the following 5 pairs:

$$(q,a)\in\{(2,1),\ (2,2),\ (4,2),\ (5,3),\ (7,3)\},$$

and the actual solutions are the ones from the statement of Theorem 1.1.

4.2. The case of large q. Here, we assume that $q>10000$. We have

$$F_n \ge (\sqrt{q^m}-1)^2 = q^m\left(1-\frac{1}{q^{m/2}}\right)^2 > q^m(0.99)^2.$$

We deduce two things. First, since $q>10000$, we get

$$m < \frac{\log(F_n(0.99)^{-2})}{\log q} < \frac{\log(F_{1000}(0.99)^{-2})}{\log 10000} < 52.2,$$

so $m\in[1,52]$. Next, if $m\ge 2$, since $\alpha^{n-1}>F_n$, we get

$$\alpha^{n-1} > F_n \ge q^m(0.99)^2 \ge (10000\times 0.99)^2 = 9900^2,$$

which gives

$$n > 1+\frac{\log(9900^2)}{\log\alpha} > 39,$$

so $n\in[40,1000]$. Thus, $n_2>n_1\ge 40$ if $m_1\ge 2$.

We next deduce that $m_1 = 1$. Assume for a contradiction that $m_1 \geq 2$. We return to

$$\frac{\alpha^n}{\sqrt{5}}(1+x) = q^m(1+y)^2, \quad |x| = \alpha^{-2n} < 10^{-16}, \quad |y| \leq q^{-m/2} < 10^{-2m_1}. \tag{8}$$

Taking logarithms and using the fact that $m_1 \geq 2$, we get

$$\begin{aligned} |n\log\alpha - \log\sqrt{5} - m\log q| &\leq |\log(1+x)| + 2|\log(1+y)| \\ &< 1.01|x| + 2.02|y| \\ &< \frac{2.03}{10^{\min\{8,2m_1\}}}. \end{aligned}$$

Apply the above with $(n,m) = (n_i, m_i)$ and $i = 1, 2$. Multiplying the above estimate for $i = 1$ with m_2 and the one for $i = 2$ with m_1 and subtracting them we get

$$|(n_2m_1 - m_2n_1)\log\alpha - (m_2 - m_1)\log(\sqrt{5})| < \frac{2.03(m_2+m_1)}{10^{\min\{8,2m_1\}}}.$$

The convergent p_3/q_3 of $\log\sqrt{5}/\log\alpha$ is $97/58$ and $m_2 - m_1 < 52 < 58$, while the convergent p_2/q_2 is $5/3$. Thus, from Lemma 3.5 (ii),

$$|(n_2m_1 - m_2n_1)\log\alpha - (m_2 - m_1)\log(\sqrt{5})| \geq |p_2\log\alpha - q_2\log\sqrt{5}| > 0.008,$$

which gives

$$0.008 < \frac{2.03(m_2+m_1)}{10^{\min\{8,2m_1\}}},$$

so

$$0.008 \times 10^{\min\{8,2m_1\}} < 2.03(m_2+m_1).$$

If $m_1 \geq 3$, the left–hand side is at least 8000, while the right–hand side is at most $2.03\times(52+51) < 210$, a contradiction. Thus, $m_1 = 2$, so the left–hand side is 80. Thus, $80 < 2.03(m_2+2)$, giving $m_2 \geq 38$. Thus,

$$F_{1000} \geq F_{n_2} \geq (0.99)^2 q^{m_2} \geq (0.99)^2 q^{38},$$

so $q < 3.1 \times 10^6$. Thus, $F_{n_1} \leq (1.01)^2 q^{m_1} \leq (1.01)^2(3.1\times 10^6)^2$, so $n_1 \leq 63$. This shows that $n_1 \in [40, 63]$. We checked that there is no solution to the equation $E_2(q,a) = F_n$ with $n \in [40,63]$. The way we did it, was to note that

$$F_n = E_2(q,a) = (q+1)^2 - a^2 = (q+1+a)(q+1-a).$$

Thus,

$$q+1+a = d_1, \quad q+1-a = d_2$$

for some divisors d_1, d_2 of F_n whose product is F_n. Thus, $d_2 = F_n/d_1$ and so

$$q = \frac{1}{2}\left(d_1 + \frac{F_n}{d_1}\right) - 1, \quad a = \frac{1}{2}\left(d_1 - \frac{F_n}{d_1}\right) \tag{9}$$

hold for some divisor d_1 of F_n. In a few seconds, Mathematica confirmed that there is no n_1 in $[40,63]$ such that for some divisor d_1 of F_{n_1}, the quantities q and a defined in (9) above are integers with $|a| \leq 2\sqrt{q}$.

Thus, $m_1 = 1$. Therefore, we have $F_{n_1} = E_1(q,a) = q+1-a$. Since $\mathbf{E}_1$ is a subgroup of $\mathbf{E}_{m_2}$, it follows that $E_1(q,a) \mid E_{m_2}(q,a)$ by Lagrange's theorem. Hence, $F_{n_1} \mid F_{n_2}$, which implies that $n_1 \mid n_2$. So, $n_2 = n_1\ell$. Assume first that $n_1 \geq 40$. Since $40 \leq n_1 < n_2 \leq 1000$, we get $\ell \in [2, 25]$. Also, since $n_1 = n_2/\ell \leq 1000/2$, it follows that $n_1 \leq 500$. Now we fix $n_1 \in [40, 500]$ and $\ell \in [2, 1000/n_1]$. Clearly, ℓ is at most 25 but it could be smaller if n_1 is large. We use the same battlehorse estimate (8), namely

$$|n \log \alpha - \log \sqrt{5} - m \log q| \leq |\log(1+x)| + 2|\log(1+y)|$$

with

$$|x| = \alpha^{-2n}, \quad |y| \leq q^{-\frac{m}{2}},$$

for $(m,n) = (m_i, n_i)$ and $i = 1, 2$. Since

$$(1.01)^2 q^m \geq q^m (1+y)^2 = F_n,$$

it follows that $q^{m/2} \leq 1.01/\sqrt{F_n}$. Thus,

$$|n \log \alpha - \log \sqrt{5} - m \log q| \leq 1.01|x| + 2(1.01)|y| \leq \frac{1.01}{\alpha^{2n}} + \frac{2(1.01)^2}{\sqrt{F_n}} < \frac{2.05}{\sqrt{F_n}}.$$

We apply the above inequality with (n,m) equal to $(n_1, 1)$ and $(n_1\ell, m_2)$, multiply the first one with m_2 and subtract it from the second to get

$$|(n_1 m_2 - n_1 \ell) \log \alpha + (m_2 - 1) \log \sqrt{5}| < \frac{2.05(m_2+1)}{\sqrt{F_{n_1}}}.$$

Since $m_2 \leq 52$, this implies that

$$\left| m_2 - \frac{n_1 \ell \log \alpha - \log \sqrt{5}}{n_1 \log \alpha - \log \sqrt{5}} \right| < \frac{110}{(n_1 \log \alpha - \log \sqrt{5})\sqrt{F_{n_1}}}.$$

In particular, m_2 is uniquely determined, that is

$$m_2 := \left\lfloor \frac{n_1 \ell \log \alpha - \log \sqrt{5}}{n_1 \log \alpha - \log \sqrt{5}} + \frac{110}{(n_1 \log \alpha - \log \sqrt{5})\sqrt{F_{n_1}}} \right\rfloor,$$

and

$$\left\{ \frac{n_1 \ell \log \alpha - \log \sqrt{5}}{n_1 \log \alpha - \log \sqrt{5}} + \frac{110}{(n_1 \log \alpha - \log \sqrt{5})\sqrt{F_{n_1}}} \right\} < \frac{220}{(n_1 \log \alpha - \log \sqrt{5})\sqrt{F_{n_1}}}.$$

The right–hand side above is very small (smaller than 0.0011 at $n_1 = 40$). We ran a computer code which checked for all $n_1 \in [40, 500]$ and all $\ell \in [2, \lfloor 1000/n_1 \rfloor]$, whether the above inequality is fulfilled. This took less than one second. No solution was found.

We still need to cover the range $m_1 = 1,\ n_1 < 40$. Since $q > 10^4$ and $\alpha^{n_1 - 1} > F_{n_1} \geq q(0.99)^2$, we have that

$$n_1 > 1 + \frac{\log q(0.99)^2}{\log \alpha} > 20.09,$$

so $n_1 \geq 21$. We used the same method as the beginning of Subsection 4.1. Namely, for $n_1 \in [21, 39]$, we have $\sqrt{q} < \sqrt{F_{n_1}} + 1$. Hence, a is an integer in the interval $[-2(\sqrt{F_{n_1}} + 1), 2(\sqrt{F_{n_1}} + 1)]$. For each such value of a, we put $q := F_{n_1} - (a-1)$ and generated $E_m(q, a)$ for $m = 2, 3, \ldots, M_q$ (note that $E_1(q, a) = F_{n_1}$ by construction), where M_q is the maximal m such that $q^m(0.99)^2 \leq F_{1000}$. We took

$$M_q := \left\lfloor \frac{\log F_{1000}(0.99)^2}{\log q} \right\rfloor.$$

Then we intersected the list of $\{E_m(q, a) : 1 \leq m \leq M_q\}$ with the Fibonacci sequence and looked for values for which this intersection has at least two members. This computation took a few minutes and no solution was found. Thus, the only solutions for $n_2 \leq 1000$ are the ones appearing in (1).

For the rest of the paper, we assume that $n_2 > 1000$.

5. A linear form in 3 logs

Recall that we are studying

$$F_{n_1} = E_{m_1}(q, a), \qquad F_{n_2} = E_{m_2}(q, a),$$

where $n_1 < n_2$. We have the following lemma.

Lemma 5.1. *Assume $n_2 > 1000$. Then*

$$m_2 < 4 \times 10^{12}.$$

Proof. We write

$$(\sqrt{q^m} + 1)^2 \geq E_m(q, a) = F_n \geq (\sqrt{q^m} - 1)^2.$$

Thus,

$$q^{m_2/2} \geq \sqrt{F_{n_2}} - 1 \geq \sqrt{F_{1001}} - 1 > 10^{100}.$$

In particular,

$$1.001 q^{m_2} \geq F_{n_2} \geq 0.999 q^{m_2}. \tag{10}$$

We thus get that

$$\frac{\alpha^{n_2}}{\sqrt{5}}(1 + x) = q^{m_2}(1 + y)^2 \quad \text{with} \quad |x| = \alpha^{-2n_2},\ |y| \leq q^{-m_2/2}.$$

Thus,

$$\begin{aligned} |n_2 \log \alpha - \log \sqrt{5} - m_2 \log q| &\leq |\log(1 + x)| + 2|\log(1 + y)| \\ &\leq 1.01|x| + 2.02|y| \\ &< \frac{2.03}{\sqrt{F_{n_2}}}. \end{aligned} \tag{11}$$

Let $|\Lambda|$ be the expression in the left–hand side in (11). The fact that $\Lambda \neq 0$ is easy since $\Lambda = 0$ implies $\alpha^{2n_2} \in \mathbb{Q}$ which is false for any positive

integer n_2. We assume first that q is not a power of 5 and we apply Matveev's Theorem 3.1 with

$$t := 3,\ \gamma_1 := \alpha,\ \gamma_2 := \sqrt{5},\ \gamma_3 := q,\ b_1 := n_2,\ b_2 := -1,\ b_3 := -m_2. \quad (12)$$

The numbers $\gamma_1, \gamma_2, \gamma_3$ are totally real, positive and multiplicatively independent (because q is not a power of 5). We have $\mathbb{K} = \mathbb{Q}(\alpha)$ which has $D = 2$, so we can take $A_1 := \log\alpha,\ A_2 := \log 5,\ A_3 := 2\log q$. Then

$$\frac{|b_1|A_1}{A_3} = \frac{n_2\log\alpha}{2\log q}, \quad \frac{|b_2|A_2}{A_3} = \frac{\log 5}{2\log q}, \quad \frac{|b_3|A_3}{A_3} = m_2,$$

and by estimate (11), we have

$$m_2 \geq \frac{n_2\log\alpha}{\log q} - \frac{\log\sqrt{5}}{\log q} - \frac{2.03}{(\log q)\sqrt{F_{n_2}}} > \max\left\{\frac{n_2\log\alpha}{2\log q}, \frac{\log 5}{2\log q}\right\}$$

since $n_2 > 1000$. Thus, we can take $E = m_2$. We thus get that

$$\log|\Lambda| > -C(3)C_0W_0D^2\Omega,$$

where

$$\begin{aligned} C(3) &= \frac{8}{2!}(3+2)(2\cdot 3+3)(4e(3+1))^4 < 6.45\times 10^8;\\ C_0 &= \log(e^{4.4\cdot 3+7}3^{5.5}2^2\log(2e)) < 28.16;\\ W_0 &= \log(1.5em_2(2)\log(2e)) < \log m_2 + 2.63;\\ \Omega &= (\log\alpha)(\log 5)(2\log q) < 1.55\log q, \end{aligned}$$

so

$$\log|\Lambda| > -1.13\times 10^{11}(\log m_2 + 2.63)\log q. \quad (13)$$

Using (11) together with estimate (10), we get that

$$|\Lambda| < \frac{2.03}{\sqrt{F_{n_2}}} \leq \frac{2.03}{0.999q^{m_2/2}} < \frac{2.04}{q^{m_2/2}},$$

and taking logarithms and using (13), we get

$$(m_2/2)\log q < \log(2.04) + 1.127\times 10^{11}(\log m_2 + 2.63)\log q,$$

so

$$\begin{aligned} m_2 &< \frac{2\log(2.04)}{\log q} + 1.254\times 10^{10}(\log m_2 + 2.63)\\ &< 1.255\times 10^{11}(\log m_2 + 2.63), \end{aligned}$$

which gives $m_2 < 4\times 10^{12}$.

This was when q is not a power of 5. If q is a power of 5 then Theorem 3.1 does not apply with data (12) because γ_2 and γ_3 are multiplicatively dependent. However, in this case we can use Theorem 3.3 and obtain an even sharper result. If $q = 5^\lambda$ some positive integer λ, then (11) becomes

$$|2n_2\log\alpha - (2\lambda m_2 + 1)\log 5| < \frac{4.06}{\sqrt{F_{n_2}}}. \quad (14)$$

Next, we apply Theorem 3.3 with $t := 2$, $\gamma_1 := \alpha$, $\gamma_2 := 5, b_1 := 2n_2$ and $b_2 := -(2\lambda m_2 + 1)$. Again, since $\mathbb{K} = \mathbb{Q}(\sqrt{5})$, we have $D = 2$. Here, we take $\log B_1 := 1/2$, $\log B_2 := \log 5$,

$$b' = \frac{2n_2}{2\log B_2} + \frac{2\lambda m_2 + 1}{2\log B_1} = \frac{n_2}{\log 5} + \frac{2\lambda m_2 + 1}{\log \alpha} < \frac{3n_2}{\log 5} + 1,$$

where the last inequality follows by dividing both sides of (14) by the product $(\log \alpha)(\log 5)$ and using the fact that $4.06/\sqrt{F_{n_2}}$ is very small. We thus get that

$$\log |\Lambda| > -23.34 \times 2^3 (\log \alpha) \log 5 \max\{\log(3n_2/\log 5 + 1) + 0.14, 10.5\}^2.$$

Combining the above inequality with (14) and using $F_{n_2} > \alpha^{n_2 - 2}$, we get

$$\begin{aligned}(n_2 - 2)(\log \alpha)/2 &< \log(4.06) \\ &\quad + 23.34 \times 2^3 \log 5 \max\{\log(3n_2/\log 5 + 1) + 0.14, 10.5\}^2.\end{aligned}$$

If the maximum in the right above is 10.5, then

$$\log(3n_2/\log 5 + 1) + 0.14 \le 10.5,$$

which gives $n_2 \le 20,000$. If the maximum above is not 10.5, we then get $n_2 < 220,000$. Thus, $n_2 < 2.2 \times 10^5$. Using also (14), we have

$$m_2 < 2\lambda m_2 + 1 < \frac{2n_2 \log \alpha}{\log 5} + 1 < 1.4 \times 10^5,$$

which is much sharper than the desired inequality. □

6. The case (i) of Section 2

Here, we deal with $q \le 2 \times 10^{10}$. This is case (i) in Section 2. Recall that Lemma 5.1 gives $m_2 < 4 \times 10^{12}$, and next since $\alpha^{n_2 - 2} < F_{n_2} \le q^{m_2}(1.001)^2$, according to (10), we get

$$n_2 < 2 + \frac{m_2 \log q + 2\log(1.001)}{\log \alpha} < 2 \times 10^{14}.$$

We have to reduce this bound. We assume first that q is not a power of 5. We apply the Baker–Davenport reduction method explained in Lemma 3.4 to inequality (11) written under the form

$$\left| n_2 \frac{\log \alpha}{\log q} - m_2 - \frac{\log \sqrt{5}}{\log q} \right| < \frac{2.03\alpha}{(\log q)\alpha^{n_2/2}}. \tag{15}$$

If $q = p^\lambda$, we then get that

$$\left| n_2 \frac{\log \alpha}{\lambda \log p} - m_2 - \frac{\log \sqrt{5}}{\lambda \log p} \right| < \frac{2.03\alpha}{(\lambda \log p)\alpha^{n_2/2}},$$

and multiplying across by λ, we get inequality (15) with the same n_2 and with m_2 replaced by $m_2' := \lambda m_2$. Thus, we may assume that q is prime $\ne 5$

when applying the Baker–Davenport reduction to estimate (15). We take $A := 5 > (2.03\alpha/\log p)$ for any $p \geq 2$ and $B := \sqrt{\alpha}$.

We took $M := 2.3 \times 10^{15}$. Since $F_{79} > 1.4 \times 10^{16} > 6M$, it follows that if P_k/Q_k denotes the kth convergent of $\tau := \log\alpha/\log q$, then $Q_{79} > 6M$. For each prime $q < 2 \times 10^{10}$ which is not 5, we computed $w := \|Q_{79}\mu\|$, where $\mu := \log(\sqrt{5})/\log q$. Since $M\|Q_{79}\tau\| = M|Q_{79}\tau - P_{79}| < M/Q_{79}$, we checked at each step that $wQ_{79} > 2M$. This ensures that at each step $\|Q_{79}\mu\| - M\|Q_{79}\tau\| > w/2$, so one can take $\varepsilon := w/2$. In order not to have to keep track of w, Q_{79}, we simply checked that $Q_{79}/w < 10^{80}$ at each step. In few days, a Mathematica code went through all the 882206715 primes $q \neq 5$ smaller than 2×10^{10} and confirmed that indeed in each case all the above conditions were fulfilled. Thus,

$$n_2 < \frac{\log(AQ\varepsilon^{-1})}{\log\sqrt{\alpha}} < \frac{\log(2A(Q/w))}{\log\sqrt{\alpha}} < \frac{\log(2\times 5\times 10^{80})}{\log\sqrt{\alpha}} < 800,$$

which is what we wanted. Assume next that $q = 5^\lambda$. Inequality (15) gives

$$\left|2n_2\frac{\log\alpha}{\log 5} - (2\lambda m_2 + 1)\right| < \frac{4.06\alpha}{(\log 5)\alpha^{n_2/2}} < \frac{5}{\alpha^{n_2/2}}.$$

Thus,

$$\left|\frac{\log\alpha}{\log 5} - \frac{2\lambda m_2+1}{2n_2}\right| < \frac{5}{(2n_2)\alpha^{n_2/2}} < \frac{1}{2(2n_2)^2} \qquad \text{for} \qquad n_2 > 30,$$

where the last inequality is implied by $\alpha^{n_2/2} > 20n_2$, which holds for $n_2 > 30$. Thus, by Lemma 3.5 (i), if $n_2 > 30$, the fraction $(2\lambda m_2 + 1)/(2n_2)$ is a convergent of $\log\alpha/\log 5$ with denominator at most $2n_2 < 4\times 10^{14}$. This shows that $(2\lambda m_2 + 1)/(2n_2) = P_k/Q_k$ for some $k < 29$ since $Q_{29} > 10^{16} > 2n_2$. We also have $\max\{a_k : 0 \leq k \leq 29\} = 59$. Thus, again by Lemma 3.5 (i),

$$\left|\frac{\log\alpha}{\log 5} - \frac{2\lambda m_2+1}{2n_2}\right| \geq \frac{1}{(59+2)(2n_2)^2} = \frac{1}{244n_2^2}.$$

We thus get that for $n_2 \geq 30$,

$$\frac{1}{244n_2^2} < \left|\frac{\log\alpha}{\log 5} - \frac{2\lambda m_2+1}{2n_2}\right| < \frac{5}{(2n_2)\alpha^{n_2/2}},$$

so $\alpha^{n_2/2} < 610n_2$, therefore $n_2 \leq 42$. This shows that $n_2 \leq 42$ in case q is a power of 5.

From now on, we may assume that $n_2 > 1000$ and that $q > 2 \times 10^{10}$. In particular, $F_{n_1} \geq q(0.999)^2 \geq 2 \times 10^{10}(0.999)^2$, so $n_1 > 50$.

7. Another linear form in 3 logs

Recall that we are studying

$$F_{n_1} = E_{m_1}(q, a), \qquad F_{n_2} = E_{m_2}(q, a),$$

where $n_1 < n_2$. We have the following lemma.

Lemma 7.1. *Assume $n_2 > 1000$. Put $\log \mathcal{B} := 0.8882 + \log(m_2^2 \log q)$. Then one of the following holds:*

(*i*)
$$m_2 < 1.5 \times 10^6 (\log \mathcal{B})^2;$$

(*ii*) *There exist integers a, b, c with $an_2 + b + cm_2 = 0$, where*

$$|a| < 29(\log \mathcal{B})^{1/3}, \qquad |b| < 48(\log \mathcal{B})^{1/3}, \qquad |c| < 59 \log q (\log \mathcal{B})^{1/3}.$$

Proof. As the proof of Lemma 5.1, we can write

$$\begin{aligned} |n_2 \log \alpha - \log \sqrt{5} - m_2 \log q| &\le \frac{2.03}{\sqrt{F_{n_2}}} \\ &\le \frac{2.03}{\sqrt{0.999} q^{m_2/2}} \\ &< \frac{2.04}{q^{m_2/2}}. \end{aligned} \tag{16}$$

Here, we apply Mignotte's Theorem 3.2 with

$$\gamma_1 := \sqrt{5},\ \gamma_2 := \alpha,\ \gamma_3 := q,\ b_1 := 1,\ b_2 := n_2,\ b_3 := m_2.$$

The numbers b_1, b_2, b_3 are positive and have $\gcd(b_1, b_2, b_3) = 1$ since $b_1 = 1$. Further, $d_1 = 1$, so $b_1' = b_1,\ b_2' = b_2$. We also have $D = 2$, and

$$h(\gamma_1) = (1/2) \log 5,\ h(\gamma_2) = (1/2) \log \alpha,\ h(\gamma_3) = \log q,$$

so we can take

$$\begin{aligned} a_1 &:= 6.68 > (4.296 + 4) \log \sqrt{5}; \\ a_2 &:= 4 = \max\{4, (4.296 + 2) \log \alpha\}; \\ a_3 &:= 8.296 \log q. \end{aligned}$$

Then $\Omega := a_1 a_2 a_3 > 221 \log q \ge 221 \log 2 > 100$. Then we can take

$$b' = \left(\frac{1}{4} + \frac{n_2}{6.68} \right) \left(\frac{m_2}{4} + \frac{n_2}{\log q} \right).$$

Since

$$\alpha^{n_2 - 2} < F_{n_2} < 1.001 q^{m_2},$$

we have that

$$n_2 < 2 + \frac{\log(1.001 q^{m_2})}{\log \alpha} < 2.003 + 2.07 m_2 \log q.$$

Thus,

$$\begin{aligned} b' &< (0.55 + 0.31 m_2 \log q)(2.22 m_2 + 2.003/\log q) \\ &< m_2^2 (\log q) \left(\left(\frac{0.55}{m_2 \log q} + 0.31 \right) \left(2.22 + \frac{2.003}{m_2 \log q} \right) \right) \\ &< m_2^2 \log q, \end{aligned}$$

where we used the fact that $n_2 > 1000$, so

$$q^{m_2} > F_{n_2}(0.999)^{-1} > F_{1000}(0.999)^{-1},$$

so $m_2 \log q > \log(F_{1000}(0.999)^{-1}) > 480$. Thus, we can take

$$\log \mathcal{B} := \max\{0.882 + \log(m_2^2 \log q), 5\}.$$

In case the maximum is at 5, we get $m_2 \log q \leq \exp(5 - 0.882) < 62$, which contradicts the fact that $m_2 \log q > 480$. Thus, we take

$$\log \mathcal{B} = 0.882 + \log(m_2^2 \log q).$$

We now go through the possibilities (i)–(iii) of Theorem 3.2.

7.1. The instance (i). In this case, we have

$$\begin{aligned} |\Lambda| &> \exp(-790.95 \times (222 \log q) \times 4 \times (0.882 + \log(m_2^2 \log q))^2 \\ &= \exp\left(-702364(0.882 + \log(m_2^2 \log q))^2 \log q\right). \end{aligned}$$

Comparing the above inequality with (16), we get

$$\begin{aligned} (m_2/2) \log q &< \log(2.04) + 702364(0.882 + \log(m_2^2 \log q))^2 \log q \\ &< 702365(0.882 + \log(m_2^2 \log q)) \log q, \end{aligned}$$

which gives

$$m_2 < 1.5 \times 10^6 (0.882 + \log(m_2^2 \log q))^2. \tag{17}$$

7.2. The instance (ii). We may assume that r_0 and s_0 are coprime, if not we simplify their greatest common divisor. Since $b_1 = 1$, we get that $r_0 = 1,\ s_0 = b_2$. Thus,

$$n_2 = b_2 < 5.61 \times 4(2(0.882 + \log(m_2^2 \log q)))^{1/3} < 29(0.882 + \log(m_2^2 \log q))^{1/3}.$$

However, since $q^{m_2} < F_{n_2} 0.999^{-1} < \alpha^{n_2 - 1} 0.999^{-1}$, we have that

$$m_2^2 \log q \leq \frac{(m_2 \log q)^2}{\log 2} < \frac{((n_2 - 1) \log \alpha - \log(0.999))^2}{\log 2},$$

which implies that

$$n_2 < 29 \left(0.882 + \log\left(\frac{((n_2 - 1) \log \alpha - \log(0.999))^2}{\log 2}\right)\right)^{1/3},$$

which gives $n_2 < 58$, a contradiction.

7.3. The instance (*iii*). In case $t_1 = 0$, we may take $r_1 = 1$ and we get $s_1 m_2 = t_2 n_2$, where r_1, t_2 are positive, coprime,

$$\begin{aligned} s_1 &< 5.61 \times 8.296 \log q (2 \log \mathcal{B})^{1/3} \\ &< 59 \log q (\log \mathcal{B})^{1/3}; \\ t_2 &< 5.61 \times 4 (2 \log \mathcal{B})^{1/3} \\ &< 29 (\log \mathcal{B})^{1/3}. \end{aligned}$$

In case $t_1 \neq 0$, reducing the equation in (*iii*) modulo r_1, we get the divisibility $r_1 \mid t_1 s_1 b_1$ and since $b_1 = 1$ and r_1 and s_1 are coprime, we get that $r_1 \mid s_1$. Thus, $r_1 = \delta,\ s_1 = \delta s_1'$, and the equality in (*iii*) lead to $t_1 s_1' + \delta s_1' m_2 = t_2 n_2$, where

$$\begin{aligned} |\delta s_1'| &< 5.61 \times 8.296 \log q (2 \log \mathcal{B})^{1/3} \\ &< 59 \log q (\log \mathcal{B})^{1/3}; \\ |t_1 s_1'| &< 5.61 \times 6.68 (2 \log \mathcal{B})^{1/3} \\ &< 48 (\log \mathcal{B})^{1/3}; \\ |t_2| &< 5.61 \times 4 (2 \log \mathcal{B})^{1/3} \\ &< 29 (\log \mathcal{B})^{1/3}. \end{aligned}$$

This is situation (*ii*) described in the statement of the lemma with the coefficients $(a, b, c) := (t_2, -t_1 s_1', -\delta s_1')$. □

8. Bounding q

We start again with the equation

$$\frac{\alpha^n - \beta^n}{\sqrt{5}} = q^m + 1 - a_m,$$

where now $q \geq 2 \times 10^{10}$. As in previous arguments, this implies

$$|n \log \alpha - \log \sqrt{5} - m \log q| < \frac{2.03}{\sqrt{F_n}} < \frac{2.03}{\sqrt{0.999} q^{m/2}} < \frac{2.04}{q^{m/2}}.$$

We write the above inequality for (m_i, n_i) for $i = 1, 2$, we multiply the one for $i = 1$ by m_2 and the one for $i = 2$ by m_1, subtract them and use the absolute value inequality to get that

$$|(m_2 n_1 - m_1 n_2) \log \alpha - (m_2 - m_1) \log \sqrt{5}| < \frac{2.04(m_2 + m_1)}{q^{m_1/2}}. \tag{18}$$

This implies

$$\left| \frac{m_2 n_1 - m_1 n_2}{m_2 - m_1} - \frac{\log \sqrt{5}}{\log \alpha} \right| < \frac{2.04(m_2 + m_1)}{(m_2 - m_1)(\log \alpha) q^{m_1/2}}. \tag{19}$$

The 30th convergent of the continued fraction of $\log\sqrt{5}/\log\alpha$ is

$$\frac{P_{29}}{Q_{29}} = [1,1,2,19,2,9,1,1,3,1,9,1,2,6,1,1,1,5,1,14,29,1,2,1,4,2,1,2,9,18],$$

with the denominator $Q_{29} > 4\times 10^{12}$. Since $a_k \le 29$ for $k = 0,\ldots,29$, the left–hand side of (19) exceeds $1/(31(m_2-m_1)^2)$, which implies that

$$q^{m_1/2} < \frac{2.04\times 31(m_2^2-m_1^2)}{\log\alpha}. \tag{20}$$

In particular, since $m_2 < 4\times 10^{12}$ and $q > 2\times 10^{10}$, we get that $q^{m_1} < 5\times 10^{54}$ and $m_1 \in \{1,2,3,4,5\}$. Further,

$$F_{n_1} < q^{m_1}(1.001) < 10^{55}, \qquad \text{so} \qquad n_1 < 265.$$

8.1. A better bound on m_2. Here, we prove the following lemma.

Lemma 8.1. *We have $m_2 < 4\times 10^9$.*

Proof. We call upon Lemma 7.1. In situation (i), we get, using (20), that

$$m_2 < 1.5\times 10^6\left(0.882+\log(2m_2^2\log(2.04\times 31m_2^2/\log\alpha))\right)^2,$$

so $m_2 < 4\times 10^9$. This is the saving by a factor of 10^3. Let us look at possibility (ii). There,

$$\log\mathcal{B} = 0.882+\log(m_2^2\log q) < 0.882+\log((4\times 10^{12})^2\log 10^{55}) < 64,$$

so $(\log\mathcal{B})^{1/3} < 4$. We thus have

$$an_2+b+cm_2 = 0,$$

where $|a|<116,\ |b|<200,\ |c|<240\log q$. We write again

$$|n_2\log\alpha - \log\sqrt{5} - m_2\log q| < \frac{2.03}{\sqrt{F_{n_2}}}.$$

We multiply both sides with a and get

$$|(-b-cm_2)\log\alpha - a\log\sqrt{5} - am_2\log q| < \frac{240}{\sqrt{F_{n_2}}}.$$

Thus,

$$|m_2(a\log q + c\log\alpha) + a\log\sqrt{5} + b\log\alpha| < \frac{240}{\sqrt{F_{n_2}}}.$$

Multiplying by m_1 (less than or equal to 5), we get

$$\left|m_2(a\log(q^{m_1}) + cm_1\log\alpha) + am_1\log\sqrt{5} + bm_1\log\alpha\right| < \frac{240m_1}{\sqrt{F_{n_2}}} \le \frac{1200}{\sqrt{F_{n_2}}}.$$

Now

$$q^{m_1} = F_{n_1} - (1-a_{m_1}) = F_{n_1}(1+x),$$

where $x = -(1-a_{m_1})/F_{n_1}$. Then

$$\log(q^{m_1}) = \log F_{n_1} + \log(1+x).$$

Now

$$|x| \le \frac{2q^{m_1/2}+1}{F_{n_1}} < \frac{2q^{m_1/2}+1}{0.999q^{m_1}} < \frac{2.01}{q^{m_1/2}} < \frac{2.01}{10^5}.$$

Thus,

$$\log(1+x) = y, \qquad \text{where} \qquad |y| = |x - x^2/2 + x^3/3 + \cdots| < \frac{2.02}{10^5}.$$

Hence,

$$|m_2(a\log F_{n_1} + cm_1\log\alpha + ay) + am_1\log\sqrt{5} + bm_1\log\alpha| < \frac{1200}{\sqrt{F_{n_2}}}. \quad (21)$$

We have

$$|ay| < \frac{120\cdot 2.02}{10^5} < \frac{2.43}{10^3}.$$

We checked numerically that $|a\log F_{n_1} + cm_1\log\alpha| > 2.5/10^3$. This is equivalent to the inequality

$$\|a(\log F_{n_1}/\log\alpha)\| > \frac{2.5}{10^3(\log\alpha)}$$

with $a \in [1,116]$ and $n_1 \in [50,265]$, which we checked numerically (interesting enough this inequality fails for $a = 119$). This shows that

$$|a\log F_{n_1} + cm_1\log\alpha + ay| > \frac{0.07}{10^3} = \frac{7}{10^5}.$$

So, we get that

$$|m_2(a\log(q^{m_1}) + (cm_1)\log\alpha) + (am_1)\log\sqrt{5} + (bm_1)\log\alpha|$$
$$> \frac{7m_2}{10^5} - m_1(|a|\log\sqrt{5} + |b|\log\alpha).$$

Combining the above inequality with estimate (21), we get

$$\frac{7m_2}{10^5} - m_1(|a|\log\sqrt{5} + |b|\log\alpha) < \frac{1200}{\sqrt{F_{n_2}}} < 1,$$

so

$$m_2 < \frac{10^5}{7}(5(120\log\sqrt{5} + 200\log\alpha) + 1) < 2\times 10^7,$$

which is better than the conclusion from situation (i). □

As a byproduct, let us show that $m_1 = 1$. Indeed, since $m_2 < 4\times 10^9$, inequality (20) now implies that $q^{m_1/2} < 2.2\times 10^{21}$, which shows that $m_1 \in \{1,2,3,4\}$ and that $F_{n_1} < (1.001)q^{m_1} < 5\times 10^{42}$, so $n_1 < 210$. We need to eliminate the cases $m_1 \in \{2,3,4\}$. We use the method described at (9). Say $m_1 = 2$. Then

$$F_{n_1} = (q+1)^2 - a^2 = (q+1+a)(q+1-a),$$

so there is a divisor d_1 of F_{n_1} such that with

$$q+1 = (d_1 + F_{n_1}/d_1)/2, \qquad a = (d_1 - F_{n_1}/d_1)/2,$$

we have that q and a are integers with $|a| < 2\sqrt{q}$. A Mathematica code checked in a few minutes that there is no $n_1 \in [50, 210]$ with F_{n_1} having such a divisor d_1. The argument applies to $m_1 = 4$ as well since in that case, with $a_2 := a^2 - 2q$, we have that $E_4(q, a) = E_2(q^2, a_2)$. For $m_1 = 3$, we have

$$F_{n_1} = E_3(q, a) = (q + 1 - a)((q + 1)^2 + a^2 + a(q + 1) - 3q).$$

Thus, putting $d_1 = q + 1 - a$, we have that d_1 is a divisor of F_{n_1} and

$$(q + 1)^2 + a^2 + a(q + 1) - 3q = F_{n_1}/d_1.$$

Substituting $q + 1 = d_1 + a$ in the above quadratic, we get

$$3a^2 + 3(d_1 - 1)a + ((d_1^2 - F_{n_1}/d_1) - 3(d_1 - 1)) = 0.$$

In particular, $z := (1/3)(d_1^2 - F_{n_1}/d_1)$ is an integer. Secondly, the above quadratic has integer roots so $\Delta := (d_1 - 1)^2 - 4(z - d_1 + 1)$ must be a perfect square. A Mathematica code checked in a few minutes that there is no $n_1 \in [50, 210]$ such that F_{n_1} has a divisor d_1 such that z is an integer and Δ is a perfect square. Thus, $m_1 = 1$. In particular, $n_1 \mid n_2$.

Finally, since $q < 5 \times 10^{42}$ (by 20) and $m_2 < 4 \times 10^9$, by (15), we have

$$n_2 < \frac{\log \sqrt{5} + m_2 \log q + 1}{\log \alpha} < 2 \times 10^{12}.$$

9. The case (ii) of Section 2

We start again with the equation

$$\frac{\alpha^n - \beta^n}{\sqrt{5}} = q^m + 1 - a_m,$$

where again $q \geq 2 \times 10^{10}$. As in previous arguments, this implies

$$\left| n_i \log \alpha - \log \sqrt{5} - m_i \log q \right| < \frac{2.03}{\sqrt{F_{n_i}}} < \frac{2.04}{q^{m_i/2}}.$$

We write the above inequality for (m_i, n_i) for $i = 1, 2$, we multiply the one for $i = 1$ by m_2 and the one for $i = 2$ by m_1, subtract them and use the absolute value inequality to get that

$$|(m_2 n_1 - m_1 n_2) \log \alpha - (m_2 - m_1) \log \sqrt{5}| < \frac{2.04(m_2 + m_1)}{q^{1/2}}. \tag{22}$$

Lemma 9.1. *If $n_2 > 1000$, then*

$$\frac{2.04(m_2 + m_1)}{q^{1/2}} < \log \alpha. \tag{23}$$

Proof. Assume inequality (23) fails. Then

$$q^{1/2} < 2.04(\log \alpha)^{-1}(m_2 + m_1) < 2 \times 10^{10}.$$

Thus,

$$F_{n_1} < 1.001q < 5 \times 10^{20},$$

so it follows that $n_1 \leq 100$. Let us compute a bound on n_2. Using (10), we have

$$\alpha^{n_2-2} \leq F_{n_2} \leq 1.001 q^{m_2},$$

so

$$n_2 \leq 2 + \frac{\log(1.001 q^{m_2})}{\log \alpha} \leq 2 + \frac{\log(1.001) + 4 \times 10^9 \times \log(4 \times 10^{20})}{\log \alpha},$$

therefore $n_2 < 4 \times 10^{11}$. In particular, the inequality $n_2 < 2 \times 10^{14}$ as at the beginning of Section 6 holds and together with it the inequality (15) holds as well. If q is not a prime, then $q = p^\lambda$ with $\lambda \geq 2$. Since $q < 4 \times 10^{20}$, it follows that $p < (4 \times 10^{20})^{1/2} < 2 \times 10^{10}$, and the calculations from Section 6, based on the Baker–Davenport reductions when $q = p^\lambda$ for some prime $p < 2 \times 10^{10}$ and $n_2 < 2 \times 10^{14}$, show that in fact $n_2 \leq 1000$. So, we may assume that q is prime. Now since also $m_1 = 1$, we have

$$(\sqrt{q} - 1)^2 \leq F_{n_1} \leq (\sqrt{q} + 1)^2,$$

so

$$q \in [(\sqrt{F_{n_1}} - 1)^2, (\sqrt{F_{n_1}} + 1)^2]. \tag{24}$$

These ones are the primes appearing in (ii) in Section 2. So, for each $n_1 \in [50, 100]$ we generated the primes in $[(\sqrt{F_{n_1}} - 1)^2, (\sqrt{F_{n_1}} + 1)^2]$ and for each one of those primes we applied the Baker–Davenport Lemma 3.4 to (15) with

$$\tau := \log \alpha / \log q, \quad \mu := \log \sqrt{5} / \log q, \quad A := 5, \quad B := \alpha^{1/2}$$

in order to lower n_2. There are

$$\sum_{n_1=50}^{100} \left(\pi \left((\sqrt{F_{n_1}} + 1)^2 \right) - \pi \left((\sqrt{F_{n_1}} - 1)^2 \right) \right) = 7769416102$$

primes q, where π denotes the prime counting function. We split the range of n_1 on various computers and we look for the prime numbers q in the interval indicated in (24) to apply the exactly same procedure as in Section 6 (using $Q := Q_{79}$). We checked that $Q/w < 10^{80}$ and also that $\varepsilon > w/2$. Hence, again

$$n_2 < \frac{\log(AQ\varepsilon^{-1})}{\log \sqrt{\alpha}} < \frac{\log(2A(Q/w))}{\log \sqrt{\alpha}} < \frac{\log(2 \times 5 \times 10^{80})}{\log \sqrt{\alpha}} < 800,$$

which is what we wanted and in fact gives a contradiction since we assumed that $n_2 > 1000$. The calculations were done with Mathematica and the running time was about two weeks on 25 computers. This takes care of the proof of the current lemma. □

10. The case (iii) of Section 2

We return to (22) and we suppose that (23) holds. Thus,

$$|(m_2n_1 - m_1n_2)\log\alpha - (m_2 - m_1)\log\sqrt{5}| < \frac{2.03\alpha(m_2+m_1)}{\alpha^{n_1/2}} < \log\alpha. \quad (25)$$

Thus,

$$\left|(m_2n_1 - m_1n_2) - (m_2 - m_1)\frac{\log\sqrt{5}}{\log\alpha}\right| < 1.$$

In particular, if m_2 and m_1 are given, then

$$m_2n_1 - m_1n_2 \in \{\lfloor x\rfloor, \lceil x\rceil\} \qquad \text{where} \qquad x := (m_2 - m_1)\frac{\log\sqrt{5}}{\log\alpha}. \quad (26)$$

We need to throw into the mix one more element. We start again with

$$F_n = q^m + 1 - a_m, \quad (n,m) = (n_i, m_i) \quad \text{for} \quad i = 1, 2.$$

At $i = 1$, we have $m_1 = 1$, $a_{m_1} = a$. So, we write $q = F_{n_1} + (a-1)$ and take logarithms to get

$$\begin{aligned}\log q = \log(F_{n_1} + (a-1)) &= \log F_{n_1} + \log\left(1 + \frac{a-1}{F_{n_1}}\right)\\ &= n_1\log\alpha - \log\sqrt{5} + \zeta_1 + \frac{a-1}{F_{n_1}} + \zeta_2,\end{aligned}$$

where

$$|\zeta_1| \le \frac{1.01}{\alpha^{2n_1}} \qquad \text{and} \qquad |\zeta_2| \le 1.01\left(\frac{a-1}{F_{n_1}}\right)^2.$$

We need a better bound for $|\zeta_2|$. Note that

$$|a-1| \le 2\sqrt{q} + 1 \le 2\sqrt{F_{n_1}} + 3 \le 2.001\sqrt{F_{n_1}},$$

therefore

$$|\zeta_2| \le 1.01\left(\frac{2.001}{\sqrt{F_{n_1}}}\right)^2 < \frac{4.05}{F_{n_1}}.$$

Thus,

$$|\zeta_1 + \zeta_2| \le |\zeta_1| + |\zeta_2| \le \frac{4.05}{F_{n_1}} + \frac{1.01}{\alpha^{2n_1}} < \frac{4.06}{F_{n_1}}.$$

We thus get that

$$\log q = n_1\log\alpha - \log\sqrt{5} + \frac{a-1}{F_{n_1}} + \zeta, \qquad |\zeta| \le \frac{4.06}{F_{n_1}}. \quad (27)$$

We do the same for $(n,m) = (n_2, m_2)$. Here, we get

$$\log q^{m_2} = n_2\log\alpha - \log\sqrt{5} + \frac{a_{m_2} - 1}{F_{n_2}} + \zeta_1', \qquad |\zeta_1'| \le \frac{4.06}{F_{n_2}}.$$

Clearly, we may assume that $n_2 = n_1\ell$ with $\ell \geq 5$, since otherwise $\ell \leq 4$ and since $n_1 \leq 210$, we would get $n_2 \leq 4 \times 210 < 1000$, which is what we wanted. Thus,

$$\left|\frac{a_{m_2}-1}{F_{n_2}}\right| \leq \frac{2\sqrt{F_{n_2}}+3}{F_{n_2}} \leq \frac{3}{\sqrt{F_{n_2}}} \leq \frac{3\alpha}{\alpha^{\ell n_1/2}} \leq \frac{3\alpha}{\alpha^{2.5n_1}} < \frac{0.01}{F_{n_1}}.$$

Similarly,

$$|\zeta_1'| \leq \frac{4.06}{F_{n_2}} \leq \frac{4.06\alpha^2}{\alpha^{n_2}} \leq \frac{4.06\alpha^2}{\alpha^{5n_1}} \leq \frac{0.01}{F_{n_1}}.$$

Hence,

$$\log(q^{m_2}) = n_2 \log\alpha - \log\sqrt{5} + \zeta', \qquad |\zeta'| \leq \frac{0.02}{F_{n_1}}. \tag{28}$$

Thus, multiplying (27) by m_2 and subtracting (28), we get

$$\begin{aligned}\left|(n_1m_2-n_2)\log\alpha - (m_2-1)\log\sqrt{5} + \frac{m_2(a-1)}{F_{n_1}}\right| &\leq m_2|\zeta| + |\zeta'| \\ &\leq \frac{4.06m_2+0.02}{F_{n_1}}.\end{aligned}$$

Dividing both sides by m_2 and multiplying by F_{n_1}, we get

$$\left|\frac{(n_1m_2-n_2)\log\alpha - (m_2-1)\log\sqrt{5}}{m_2}\cdot F_{n_1} - (a-1)\right| < 4.06 + \frac{0.02}{m_2} < 4.1.$$

This shows that, for $\kappa \in [-4,4]$,

$$a - 1 = \left\lfloor \frac{(n_1m_2-n_2)\log\alpha - (m_2-1)\log\sqrt{5}}{m_2}\cdot F_{n_1} \right\rceil + \kappa. \tag{29}$$

We are now ready to do some calculations. For each $m_2 \in [2, 4\times 10^9]$, we compute the integer in the right–hand side of equation (26) and its divisors $n_1 \in [50, 210]$. If there are no such divisors n_1, then m_2 is not convenient and we ignore it. If there are such n_1, then we also find n_2 via the formula (26) with $m_1 = 1$ which gives $n_2 = m_2n_1 - z$, where $z \in \{\lfloor x\rfloor, \lceil x\rceil\}$. Now for every such (n_1, n_2), we compute $a-1$ using (29). There are 9 possibilities for $a-1$ according to the value of the integer $\kappa \in [-4,4]$. Then we set $q := F_{n_1} + (a-1)$. These are the q's from item (iii) of Section 2. We ran the code by splitting the interval $[2, 4\times 10^9]$ for m_2 in various sub-intervals which were run independently on several computers. In each case, we selected the q's that are prime or prime powers. This was computationally challenging and we did not keep track of q's (in fact, it is quite likely that the same q could be obtained from various choices of m_2). Once such q was found prime or a prime power, we applied the Baker–Davenport reduction Lemma 3.4 to inequality (15), with such q and the remaining parameters as explained in

Section 6. It was again checked that in all cases $Q/w < 10^{80}$, so again

$$n_2 < \frac{\log(2AQ/w)}{\log\sqrt{\alpha}} < \frac{\log(2\times 5\times 10^{80})}{\log\sqrt{\alpha}} < 800.$$

Hence, again $n_2 < 1000$, which finishes the proof of the theorem.

All calculations were done with Mathematica. The total calculation time for the Mathematica software for this paper was 20 days on 25 parallel desktop computers (Intel Xeon E3-1240 v5, 3.5 GHz, 16 Gb of RAM).

Acknowledgements

The authors thank the Department of Mathematics at the Universidad del Valle for the Cluster time used to perform calculations, and especially the Computer Center Jurgen Tischer for their advice on parallelisation of the algorithm used. Yu. B. worked on this paper when he was visiting Universidad de Valparaíso, supported by the Project MEC 80160038, and Institute of Mathematical Sciences in Chennai, supported by SPARC Project P445. He thanks Instituto de Matemáticas UV and IMSc for excellent working conditions. C.A.G. was supported in part by Project 71228 (Universidad del Valle). J.C.G. worked on this project during a visit to the FLAME in Morelia, Mexico, in August 2019. This author also thanks the Universidad del Valle for support during his Ph.D. studies. F.L worked on this paper while he was visiting the Max Planck Institute for Mathematics in Fall 2019. He thanks this institution for hospitality and support. In addition, F. L. was also supported in part by grant CPRR160325161141 from the NRF of South Africa and the Focus Area Number Theory grant RTNUM19 from CoEMaSS Wits.

The authors thank Karim Belabas, Yann Bugeaud and Amalia Pizarro-Madariaga for stimulating discussions and helpful suggestions, and the referee for careful reading of the manuscript and useful comments.

References

[1] Baker, Alan; Davenport, Harold. The equations $3x^2-2=y^2$ and $8x^2-7=z^2$. *Quart. J. Math. Oxford Ser.* (2) **20** (1969), 129–137. MR0248079 (40 #1333), Zbl 0177.06802, doi: 10.1093/qmath/20.1.129. 715

[2] Bazzanella, Danilo. Primes between consecutive squares. *Arch. Math. (Basel)* **75** (2000), no. 1, 29–34. MR1764888 (2001e:11096), Zbl 1047.11087, doi: 10.1007/s000130050469. 712

[3] Dujella, Andrej; Pethő, Attila. A generalization of a theorem of Baker and Davenport. *Quart. J. Math. Oxford Ser.* (2) **49** (1998), no. 195, 291–306. MR1645552 (99g:11035), Zbl 0911.11018. 715

[4] Goldston, Daniel A. Linnik's theorem on Goldbach numbers in short intervals. *Glasgow Math. J.* **32** (1990), no. 3, 285–297. MR1073669 (91i:11134), Zbl 0719.11065, doi: 10.1017/S001708950000937X. 712

[5] Laurent, Michel; Mignotte, Maurice; Nesterenko, Yuri. Formes linéaires en deux logarithmes et déterminants d'interpolation. *J. Number Theory* **55** (1995), no.

2, 285–321. MR1366574 (96h:11073), Zbl 0843.11036, doi: 10.1006/jnth.1995.1141. 715

[6] Matveev, E. M. An explicit lower bound for a homogeneous rational linear form in the logarithms of algebraic numbers. II. *Izv. Ross. Akad. Nauk Ser. Mat.* **64** (2000), no. 6, 125–180; translation in *Izv. Math.* **64** (2000), no. 6, 1217–1269. MR1817252 (2002e:11091), Zbl 1013.11043, doi: 10.1070/IM2000v064n06ABEH000314. 714

[7] Mignotte, Maurice. A kit for linear forms in three logarithms. Preprint, 2008. `http://irma.math.unistra.fr/~bugeaud/travaux/kit.pdf`. 714

[8] Mignotte, Maurice. Linear forms in two and three logarithms and interpolation determinants. *Diophantine equations*, 151–166, Tata Inst. Fund. Res. Stud. Math., 20. *Tata Inst. Fund. Res., Mumbai*, 2008. MR1500224 (2010h:11119), Zbl 1198.11071. 714

[9] Murty, M. Ram; Esmonde, Jody. Problems in algebraic number theory. Second edition. Graduate Texts in Mathematics, 190. *Springer-Verlag, New York*, 2005. xvi+352 pp. ISBN: 0-387-22182-4. MR2090972 (2005c:11130), Zbl 1055.11001, doi: 10.1007/b138452. 716

[10] Silverman, Joseph H. The arithmetic of elliptic curves. Second edition. Graduate Texts in Mathematics, 106. *Springer, Dordrecht*, 2009. xx+513 pp. ISBN: 978-0-387-09493-9. MR2514094 (2010i:11005), Zbl 1194.11005, doi: 10.1007/978-0-387-09494-6. 712

(Yuri Bilu) IMB, Université de Bordeaux & CNRS, 351 cours de la Libération, 33405, Talence CEDEX, France
`yuri@math.u-bordeaux.fr`

(Carlos A. Gómez) Departamento de Matemáticas, Universidad del Valle, 25360 Cali, Calle 13 No 100-00, Colombia
`carlos.a.gomez@correounivalle.edu.co`

(Jhonny C. Gómez) Departamento de Matemáticas, Universidad del Valle, 25360 Cali, Calle 13 No 100-00, Colombia
`jhonny.gomez@correounivalle.edu.co`

(Florian Luca) School of Mathematics, Wits University, Johannesburg, South Africa; Research Group in Algebraic Structures and Applications, King Abdulaziz University, Jeddah, Saudi Arabia and Centro de Ciencias Matemáticas, UNAM, Morelia, Mexico
`florian.luca@wits.ac.za`

This paper is available via `http://nyjm.albany.edu/j/2020/26-32.html`.