Bull. Aust. Math. Soc. **88** (2013), 509–519
doi:10.1017/S0004972713000166

L-FUNCTIONS OF ELLIPTIC CURVES AND BINARY RECURRENCES

FLORIAN LUCA ✉, ROGER OYONO and AYNUR YALCINER

(Received 22 December 2012; accepted 28 December 2012; first published online 22 March 2013)

Abstract

Let $L(s, E) = \sum_{n\geq 1} a_n n^{-s}$ be the L-series corresponding to an elliptic curve E defined over $\mathbb{Q}$ and $\mathbf{u} = \{u_m\}_{m\geq 0}$ be a nondegenerate binary recurrence sequence. We prove that if $\mathcal{M}_E$ is the set of n such that $a_n \neq 0$ and $\mathcal{N}_E$ is the subset of $n \in \mathcal{M}_E$ such that $|a_n| = |u_m|$ holds with some integer $m \geq 0$, then $\mathcal{N}_E$ is of density 0 as a subset of $\mathcal{M}_E$.

2010 *Mathematics subject classification*: primary 11G40; secondary 11B39, 11N36.
Keywords and phrases: *L*-functions of elliptic curves, linear recurrence sequences.

1. Introduction

Let E be an elliptic curve over the field of rational numbers $\mathbb{Q}$ given by the minimal *global Weierstrass equation*:

$$E \ : \ y^2 + A_1xy + A_3y = x^3 + A_2x^2 + A_4x + A_6 \tag{1.1}$$

and let Δ_E be its discriminant. For each prime p we put

$$a_p = p + 1 - \#E(\mathbb{F}_p),$$

where $E(\mathbb{F}_p)$ is the reduction of E modulo p. If $p \mid \Delta_E$, then $E(\mathbb{F}_p)$ has a singularity and one gets

$$a_p = \begin{cases} 0 & \text{for the case of a cusp,} \\ 1 & \text{for the case of a split node,} \\ -1 & \text{for the case of a nonsplit node.} \end{cases}$$

Work on this paper began during a visit of F.L. to Turkey supported by Tubitak, and continued during a visit of R.O. to the Centro de Ciencias Matemáticas of the UNAM in Morelia under Project PAPIIT IN104512. F.L. thanks Tubitak for financial support. F.L. was also supported in part by a Marcos Moshinsky Fellowship and projects CONACyT 163787 and 193539. The work of A.Y. was supported by Tubitak and the Scientific Research Office (BAP) of Selçuk University.

For all primes p we have $|a_p| \le 2\sqrt{p}$. The L-function associated to E is given by

$$L(s, E) = \prod_{p|\Delta_E} \frac{1}{1 - a_p p^{-s}} \prod_{p\nmid\Delta_E} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}.$$

The infinite product above is convergent for $\mathrm{Re}(s) > 3/2$ and therefore we can expand it into a series $L(s, E) = \sum_{n\ge1} a_n n^{-s}$.

Let $\mathbf{u} = \{u_m\}_{m\ge0}$ be a binary recurrent sequence of integers satisfying the recurrence

$$u_{m+2} = ru_{m+1} + su_m \quad \text{for all } m \ge 0,$$

where r and s are nonzero integers such that the quadratic equation

$$x^2 - rx - s = 0$$

has two distinct roots α and β. It is then well known that there exist two constants c and d in $\mathbb{K} = \mathbb{Q}(\alpha)$ such that the Binet formula

$$u_m = c\alpha^m + d\beta^m$$

holds for all $m \ge 0$. We assume that the sequence $\mathbf{u}$ is nondegenerate, meaning that $cd \ne 0$ and α/β is not a root of unity. We put $\Delta_{\mathbf{u}} = (\alpha - \beta)^2 = r^2 + 4s \ne 0$ for the discriminant of the sequence $\mathbf{u}$. The numbers $c\Delta_{\mathbf{u}}$ and $d\Delta_{\mathbf{u}}$ are algebraic integers.

Here we study the set of positive integers n such that $|a_n| = |u_m|$ for some nonnegative integer m. Before we start, we remark that there could be many n such that a_n belongs to the sequence $\{u_m\}_{m\ge0}$ simply because it may happen that $a_p = 0 = u_k$ for some prime p and integer $k \ge 0$, in which case $n = p\ell$ with any positive integer ℓ coprime to p has the property that $a_n = 0 = u_k$. To discard this instance, let

$$\mathcal{M}_E = \{n : a_n \ne 0\}.$$

We put

$$\mathcal{N}_E = \{n \in \mathcal{M}_E : |a_n| = |u_m| \text{ for some } m \ge 0\},$$

and for a positive real number x and subset $\mathcal{A}$ of the positive integers we put $\#\mathcal{A}(x) = \#(\mathcal{A} \cap [1, x])$.

THEOREM 1.1. *Let E be an elliptic curve defined over $\mathbb{Q}$ and $\mathbf{u} = \{u_m\}_{m\ge0}$ be a nondegenerate binary recurrent sequence. There is a positive number $c = c(E, \mathbf{u})$ depending on E and $\mathbf{u}$ such that the estimate*

$$\#\mathcal{N}_E(x) = O\left(\frac{\#\mathcal{M}_E(x)}{(\log x)^c}\right)$$

holds for all $x \ge 2$. The implied constant depends on E.

https://doi.org/10.1017/S0004972713000166 Published online by Cambridge University Press

Our notation is standard. The letters p and q with or without subscripts stand for prime numbers. We use $\omega(n)$ and $\tau(n)$ for the number of distinct prime divisors of n and the total number of divisors of n, respectively. For a subset $\mathcal{P}$ of prime numbers we use $\omega_{\mathcal{P}}(n)$ for the number of prime factors $p \in \mathcal{P}$ of n. We write $P(n)$ for the largest prime factor of n. Finally, we use the Landau notation O and o as well as the Vinogradov notation $\ll$ and $\gg$ with their regular meanings. The constants implied by these might depend on E and $\mathbf{u}$. We use x_0 for a large positive real number not necessarily the same at each occurrence and $c, c_1, c_2, \ldots$ for positive constants depending on E and $\mathbf{u}$.

2. Weierstrass equations

With the standard birational transformation (see [9, Ch. III, Section 1]), replacing y in (1.1) by $(y - A_1x - A_3)/2$ gives an equation of the form

$$y^2 = 4x^3 + B_2x^2 + 2B_4x + B_6,$$

where

$$B_2 = A_1^2 + 4A_2, \quad B_4 = 2A_4 + A_1A_3, \quad B_6 = A_3^2 + 4A_6.$$

Further, defining the quantities

$$\begin{aligned} C_4 &= B_2^2 - 24B_4, \\ C_6 &= -B_2^3 + 36B_2B_4 - 216B_6, \end{aligned}$$

and then replacing (x, y) by $((x - 3B_2)/36, y/108)$ yields the simpler Weierstrass equation

$$E \ : \ y^2 = x^3 - 27C_4x - 54C_6.$$

We put $A = -27C_4$ and $B = -54C_6$. From now on, we assume that $p > 3$ is a prime so the above transformations are well defined modulo p and we work with the equation

$$E \ : \ y^2 = x^3 + Ax + B.$$

3. Some preparations

3.1. Removing n with a large square-full part. Recall that b is a square-full number if $p^2 \mid b$ whenever $p \mid b$. Put $y = (\log x)^2$. For each n we write

$$t(n) = \prod_{\substack{p \| n \\ p \nmid 6\Delta_E}} p \quad \text{and} \quad c(n) = \frac{n}{t(n)}.$$

Then $c(n) = ab$, where a is square-free and $a \mid 6\Delta_E$ and b is square-full. We put

$$\mathcal{N}_1(x) = \{n \le x : c(n) > y\}.$$

https://doi.org/10.1017/S0004972713000166 Published online by Cambridge University Press

If $n \in \mathcal{N}_1(x)$, then n is divisible by a number of the form ab, where $a \mid 6\Delta_E$ is square-free and $b > y/a \geq y/(6|\Delta_E|)$ is square-full. For fixed a and b, the number of such $n \leq x$ is $\lfloor x/ab \rfloor \leq x/ab \leq x/b$. Making a and b vary, we get that

$$\#\mathcal{N}_1(x) \leq \sum_{\substack{b>y/(6|\Delta_E|) \\ b \text{ square-full} \\ a|6\Delta_E}} \frac{x}{b} \leq x\tau(6|\Delta_E|) \sum_{\substack{b>y/(6|\Delta_E|) \\ b \text{ square-full}}} \frac{1}{b} \ll \frac{x}{y^{1/2}} = \frac{x}{\log x}, \tag{3.1}$$

where in the above calculation we use the Abel summation formula together with the fact that the counting function of the number of square-full numbers $b \leq t$ is $O(t^{1/2})$.

3.2. Removing smooth n. Put

$$z = \exp\left(\frac{\log x \log\log\log x}{2 \log\log x}\right).$$

We let

$$\mathcal{N}_2(x) = \{n \leq x : P(n) \leq z\}.$$

From known results from the distribution of smooth numbers (see [1]), in this range for z and x, it is known that

$$\#\mathcal{N}_2(x) = x \exp(-(1 + o(1))u \log u) \quad \text{as } x \to \infty,$$

where $u = \log x/\log z = 2 \log\log x/\log\log\log x$. Hence,

$$u \log u = (2 + o(1)) \log\log x,$$

as $x \to \infty$, showing that

$$\#\mathcal{N}_2(x) = x \exp(-(2 + o(1)) \log\log x) = O\left(\frac{x}{\log x}\right). \tag{3.2}$$

3.3. The size of m. Assume that $|a_n| = |u_m|$ holds for some positive integer $n \leq x$ with $u_m \neq 0$. Since $|a_n| \leq \tau(n)n^{1/2}$, it follows that $|a_n| \leq x$ if $x > x_0$. Since $u_m \neq 0$, it follows, by a result of Stewart (see [11, p. 33]), that the inequality $|u_m| \geq |\alpha|^{m-c_1 \log(m+1)}$ holds with some positive constant c_1 depending on $\mathbf{u}$. Thus,

$$x \geq |a_n| = |u_m| \geq |\alpha|^{m-c_1 \log(m+1)}.$$

Since $|\alpha| \geq (1 + \sqrt{5})/2$, it follows that $m \leq 5 \log x$ for $x > x_0$.

4. The proof in the CM case

Here, we treat the case when E has complex multiplication (CM). In this section, we will need the set $\mathcal{N}_2(x)$. We put $\mathbb{L} = \mathbb{Q}(\sqrt{-D})$ for the CM field of E,

https://doi.org/10.1017/S0004972713000166 Published online by Cambridge University Press

where $D \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$. Recall that if $a_p = 0$, then p is called *supersingular*. A result of Deuring [3] asserts that if we put

$$\mathcal{P}_E = \{p : p \text{ supersingular}\},$$

then up to finitely many exceptions, $p \in \mathcal{P}_E$ if and only if $(-D \mid p) = -1$, where the above symbol is the Legendre symbol of $-D$ with respect to p. This implies immediately, via a result of Wirsing (see [12, Satz 1]; [8, Proposition 18]), that the asymptotic

$$\#\mathcal{M}_E(x) \sim \frac{c_E x}{(\log x)^{1/2}} \quad \text{as } x \to \infty, \tag{4.1}$$

holds with some positive constant c_E.

Put

$$\mathcal{N}_3(x) = \mathcal{N}_E(x) \backslash (\mathcal{N}_1(x) \cup \mathcal{N}_2(x)).$$

Assume that $n \in \mathcal{N}_3(x)$. Write $|a_n| = |u_m|$ for some $m \geq 0$. Recall $m \leq 5 \log x$ by the argument from Section 3.3. Fix m. Now write $n = Pn_1$, where $P = P(n)$. Since $P > z$ (because $n \notin \mathcal{N}_2(x)$) and $z > y$ for $x > x_0$, it follows that $P(n_1) < P$ once x is sufficiently large because $n \notin \mathcal{N}_1(x)$. Then, by the multiplicativity of a_n,

$$|a_{n_1}||a_P| = |u_m|.$$

We fix n_1 such that $|a_{n_1}|$ is a divisor of $|u_m|$. Then $a_P = \pm|u_m|/|a_{n_1}|$ takes on one of two fixed values. By [2, Theorem 9], the number of possibilities for $P \leq x/n_1$ is of order at most

$$\frac{\sqrt{x/n_1}}{\log(x/n_1)} \ll \frac{\sqrt{x} \log\log x}{\sqrt{n_1} \log x}.$$

Summing the above bound over all $n_1 \leq x/z$ and $m \leq 5 \log x$, we get that

$$\begin{aligned} \#\mathcal{N}_3(x) &\ll \sum_{\substack{n_1 \leq x/z \\ m \leq 5 \log x}} \frac{\sqrt{x}(\log\log x)}{\sqrt{n_1} \log x} \ll \sqrt{x}(\log\log x) \sum_{n_1 \leq x/z} \frac{1}{\sqrt{n_1}} \\ &\ll \sqrt{x} \log\log x \int_1^{x/z} \frac{dt}{t^{1/2}} \ll \frac{x \log\log x}{\sqrt{z}} \ll \frac{x}{\log x}. \end{aligned} \tag{4.2}$$

Since $\mathcal{N}_E(x) \subseteq \mathcal{N}_1(x) \cup \mathcal{N}_2(x) \cup \mathcal{N}_3(x)$, we get, by (3.1), (3.2), (4.2) and (4.1), that

$$\#\mathcal{N}_E(x) \leq \sum_{i=1}^{3} \#\mathcal{N}_i(x) \ll \frac{x}{\log x} \ll \frac{\#\mathcal{M}_E(x)}{(\log x)^{1/2}},$$

which is what we wanted to prove with $c = 1/2$.

https://doi.org/10.1017/S0004972713000166 Published online by Cambridge University Press

5. Some more preparations for the non-CM case

5.1. Primes p with $a_p \equiv 0 \pmod q$. Let q_0 be a constant depending on E and $\mathbf{u}$ to be made more precise later. For the moment, we assume that $q_0 \geq P(6|\Delta_E|)$. Let

$$[q]E = \{P = (x_P, y_P) \in E : qP = O \text{ in } E\} \cup \{O\}.$$

Then $[q]E$ is isomorphic to $\mathbb{Z}/q\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z}$. Let $\mathbb{L}_q = \mathbb{Q}(x_P, y_P : P \in [q]E)$. By a Theorem of Serre [8], there exists a positive integer M_E depending on E such that if $q \nmid M_E$, then $\mathrm{Gal}(\mathbb{L}_q/\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$. So, let us assume that $q_0 \geq P(6|\Delta_E|M_E)$ and $q > q_0$. It follows, by a known application of the Chebotarev density theorem, that if we put

$$\mathcal{P}_q = \{p : a_p \equiv 0 \pmod q\},$$

then

$$\frac{\#\mathcal{P}_q(x)}{\pi(x)} = (1 + o(1))\frac{\#\{a \in \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z}) : \mathrm{tr}(a) = 0\}}{\#\,\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})} \quad \text{as } x \to \infty. \tag{5.1}$$

Put δ_q for the fraction appearing on the right-hand side of the above asymptotic. Since

$$\#\{a \in \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z}) : \mathrm{tr}(a) = 0\} = q^3 + O(q^2),$$
$$\#\,\mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z}) = q^4 + O(q^3),$$

it follows that $\delta_q \geq 1/(2q)$ if q is sufficiently large. We shall assume that q_0 is sufficiently large such that all inequalities $q_0 \geq P(6|\Delta_E|M_E)$ and $\delta_q \geq 1/(2q)$ hold for all $q > q_0$.

For reasons that will become clearer later, we shall also assume that

$$q_0 \geq P(N_{\mathbb{K}/\mathbb{Q}}(c\Delta_{\mathbf{u}})N_{\mathbb{K}/\mathbb{Q}}(d\Delta_{\mathbf{u}})s).$$

In particular, c, d, α, β, as well as their inverses are all defined modulo q.

Let $q_1 < q_2 < \cdots$ be all the prime numbers exceeding q_0. Let $\mathcal{Q}_{\mathbf{u}}$ be the following subset of primes:

$$\mathcal{Q}_{\mathbf{u}} = \{q > q_0 : u_n \equiv 0 \pmod q \text{ does not have an integer solution } n\}.$$

If $\mathcal{Q}_{\mathbf{u}}$ is nonempty, let q_L be the smallest prime in $\mathcal{Q}_{\mathbf{u}}$ and let $K \geq L$ be minimal such that

$$\sum_{i=1}^{K} \frac{\log q_i}{q_i} > 12. \tag{5.2}$$

If $\mathcal{Q}_{\mathbf{u}}$ is empty, we only choose K minimal such that (5.2) holds.

We make one additional comment about the case when $\mathcal{Q}_{\mathbf{u}}$ is empty. It follows from a result of Somer [10] that $\mathbf{u}$ is a scalar multiple of a shift of the Lucas sequence of the first kind with roots α and β. Namely, let $\mathbf{v} = \{v_m\}_{m\in\mathbb{Z}}$ be the sequence given by

$$v_m = \frac{\alpha^m - \beta^m}{\alpha - \beta} \quad \text{for all } m \in \mathbb{Z}.$$

Then there exist $\lambda \in \mathbb{Q}$ and $m_0 \in \mathbb{Z}$ such that $u_m = \lambda v_{m+m_0}$. We shall use this fact later.

https://doi.org/10.1017/S0004972713000166 Published online by Cambridge University Press

5.2. Sieving away numbers n with few prime factors in $\mathcal{P}_{q_i}$ for $i = 1, \dots, K$. Let $\rho \in (0, 1)$ be fixed and assume that $\mathcal{P}$ is a subset of primes such that

$$\sum_{\substack{p \le t \\ p \in \mathcal{P}}} \frac{1}{p} = (\rho + o(1)) \log\log t \quad \text{as } t \to \infty. \tag{5.3}$$

Then 'most' positive integers n have $\omega_{\mathcal{P}}(n)/\log\log n \ge \rho - \varepsilon$ for any $\varepsilon > 0$. To make this statement quantitative, assume that $\gamma \in (0, \rho)$ and let

$$\mathcal{M}_{-,\gamma,\mathcal{P}}(x) = \{n \le x : \omega_{\mathcal{P}}(n) < (\rho - \gamma)\log\log x\}.$$

Then

$$\#\mathcal{M}_{-,\gamma,\mathcal{P}}(x) \ll \frac{x}{(\log x)^{\eta + o(1)}} \quad (x \to \infty), \tag{5.4}$$

where

$$\eta = \rho - (\rho - \gamma)\log\left(\frac{e\rho}{\rho - \gamma}\right).$$

This can be found in [5, Ch. 0]. Now observe that by (5.1) and Abel's summation formula, (5.3) holds with $\mathcal{P} = \mathcal{P}_q$ and with $\delta = \delta_q$. We thus let $\rho = \delta_{q_i}$ and let $\gamma = 1/(4q_i)$ for $i = 1, \dots, K$ and consider the set

$$\mathcal{N}_4(x) = \{n \le x : \omega_{\mathcal{P}_{q_i}}(n) < (\delta_{q_i} - 1/(4q_i))\log\log x \text{ for some } i = 1, \dots, K\}.$$

Then, by (5.4),

$$\#\mathcal{N}_4(x) \ll \frac{x}{(\log x)^{c_2}} \tag{5.5}$$

for some constant $c_2 > 0$, which can be computed as

$$c_2 = \min\{\eta_i : i = 1, \dots, K\},$$

where

$$\eta_i = \delta_{q_i} - (\delta_{q_i} - 1/(4q_i))\log\left(\frac{e\delta_{q_i}}{\delta_{q_i} - 1/(4q_i)}\right) \quad \text{for } i = 1, \dots, K.$$

6. The proof in the non-CM case

Throughout this proof, we will not use the set $\mathcal{N}_2(x)$. Let again

$$\mathcal{P}_E = \{p : p \text{ supersingular}\}.$$

A result of Elkies [4] says that $\mathcal{P}_E$ is infinite. It follows from a result of Serre [8] that

$$\#\mathcal{P}_E(x) \ll \frac{x(\log\log x)(\log\log\log x)^{1/2}}{(\log x)^{3/2}}.$$

https://doi.org/10.1017/S0004972713000166 Published online by Cambridge University Press

In particular, by Abel's summation formula,

$$\sum_{p\in\mathcal{P}_E}\frac{1}{p}=O(1),$$

which implies, via the principle of inclusion and exclusion (or [8, Théorème 14]), that the asymptotic

$$\#\mathcal{M}_E(x)\sim c_E x \quad \text{as } x\to\infty, \tag{6.1}$$

holds with some positive constant c_E.

Let

$$\mathcal{N}_5(x)=\mathcal{N}_E(x)\backslash(\mathcal{N}_1(x)\cup\mathcal{N}_2(x)\cup\mathcal{N}_4(x)).$$

We shall in fact show that $\mathcal{N}_5(x)$ is empty for $x>x_0$. This will imply that the containment $\mathcal{N}_E(x)\subseteq\mathcal{N}_1(x)\cup\mathcal{N}_2(x)\cup\mathcal{N}_4(x)$ holds, so that, by (3.1), (3.2) and (5.5),

$$\#\mathcal{N}_E(x)\le\#\mathcal{N}_1(x)+\#\mathcal{N}_2(x)+\#\mathcal{N}_4(x)\ll\frac{x}{(\log x)^{c_3}}$$

for some $c_3>0$, which together with (6.1) completes the proof of the theorem.

So, let us show that $\mathcal{N}_5(x)=\emptyset$ if $x>x_0$. Assume that this is not so and let $n\in\mathcal{N}_5(x)$.

Since $n\notin\mathcal{N}_1(x)$, we may write

$$n=n_2p_1\cdots p_\ell,\quad n_2\le y,\quad p_1<\cdots<p_\ell\quad\text{and}\quad\gcd(6\Delta_E n_2,p_1\cdots p_\ell)=1.$$

Let $T=T(x)$ be the maximal positive integer such that

$$\prod_{p\le T}p\le y.$$

By the prime number theorem, $T=(1+o(1))\log y=(2+o(1))\log\log x$. Therefore $\pi(T)=o(\log\log x)$ as $x\to\infty$.

Since $n\notin\mathcal{N}_4(x)$, it follows that for each $i=1,\dots,K$, n has at least

$$\left(\delta_{q_i}-\frac{1}{4q_i}\right)\log\log x\ge\frac{1}{4q_i}\log\log x$$

distinct primes in $\mathcal{P}_{q_i}$. Of these, at most $\pi(T)$ divide n_2. Thus, among $p_1,\dots,p_\ell$ there are at least

$$\frac{\log\log x}{4q_i}-\pi(T)\ge\frac{\log\log x}{5q_i}$$

of them which are in $\mathcal{P}_{q_i}$ for $i=1,\dots,K$ and $x>x_0$. Since a_n is divisible by $\prod_{i=1}^{\ell}a_{p_i}$, we conclude that if we write

$$a_n=q_1^{\gamma_1}\cdots q_K^{\gamma_K}b,$$

where b is coprime to $q_1\dots q_K$, then $\gamma_i\ge(\log\log x)/(5q_i)$ for $i=1,\dots,K$. In particular, $q_L\mid a_n\mid u_m$, which is impossible if $\mathcal{Q}_{\mathbf{u}}$ is nonempty. This shows that $\mathcal{N}_5(x)$

https://doi.org/10.1017/S0004972713000166 Published online by Cambridge University Press

is empty for $x > x_0$ unless $\mathcal{Q}_{\mathbf{u}}$ is empty. So, let us assume that $\mathcal{Q}_{\mathbf{u}}$ is empty. Then, by Somer's result [10], $u_m = \lambda v_{m+m_0}$ for some fixed $m_0 \in \mathbb{Z}$. For each $q \geq q_0$, let $z(q)$ be the index of appearance of q in $\mathbf{v}$ and let f_q be the exponent of q in the factorisation of $v_{z(q)}$. Recall that the index of appearance of q is the smallest positive integer k such that $q \mid v_k$. It is well known that if $q^k \mid v_\ell$ for some $k > f_q$, then $q^{k-f_q} \mid \ell$ (see, for example, the theorem in [7, p. 210]). So, assume that x is sufficiently large such that $(\log\log x)/(30q_i) > f_{q_i}$ for all $i = 1, \ldots, K$ once $x > x_0$. Since $q_i^{\gamma_i} \mid \lambda v_{m+m_0}$, $\lambda = c\alpha^{m_0}(\alpha - \beta)$ and q_0 exceeds the largest prime factor of $N_{\mathbb{K}/\mathbb{Q}}((c\Delta_{\mathbf{u}})(d\Delta_{\mathbf{u}})s)$; hence, the largest prime factor of the numerator and denominator of λ, we get that $q_i^{\gamma_i} \mid v_{m+m_0}$. Hence, $m + m_0$ is a multiple of

$$q_i^{\gamma_i - f_{q_i}} \geq q_i^{(\log\log x)/(5q_i) - f_{q_i}} \geq q_i^{(\log\log x)/(6q_i)} \quad \text{for all } i = 1, \ldots, K. \tag{6.2}$$

Since $m + m_0$ is a multiple of $\prod_{i=1}^{K} q_i^{\gamma_i - f_{q_i}}$ and since by (6.2) and the way we have chosen K (see (5.2)),

$$\prod_{i=1}^{K} q_i^{\gamma_i - f_{q_i}} \geq \exp\Bigl(\log\log x \sum_{i=1}^{K} \frac{\log q_i}{6q_i}\Bigr) > (\log x)^2 > |m + m_0|$$

for all $x > x_0$ (because $m \leq 5 \log x$ (see Section 3.3)), we get $m + m_0 = 0$, showing that $u_m = 0$, which is not allowed. Thus, $\mathcal{N}_5(x)$ is indeed empty for $x > x_0$, which completes the proof of the theorem.

7. Comments and heuristics

Better, or more explicit, results can be proved about the problem studied in this paper if one makes additional assumptions. For example, in [6], the first and third authors showed, by a different method, that in the conclusion of Theorem 1.1 one can take $c(E, \mathbf{u}) = 0.0007$ for the particular case when $\mathbf{u} = \mathbf{F}$ is the Fibonacci sequence, and the curve E is non-CM and has nontrivial 2-torsion. Further improvements can be obtained in the non-CM case if one assumes the generalised Riemann hypothesis for the Dedekind zeta function of the division fields of E. Let $\mathbf{u} = (u_m)_{m \geq 0}$ be any nondegenerate linearly recurrent sequence of order d, such that $|u_m|$ is neither constant nor a linear polynomial in m for all sufficiently large values of m. Assume that its characteristic polynomial is $f(X) \in \mathbb{Z}[X]$ and write $f(X) = (X - \alpha_1)^{\sigma_1} \cdots (X - \alpha_k)^{\sigma_k}$, where $\alpha_1, \ldots, \alpha_k$ are nonzero complex numbers and $\sigma_1, \ldots, \sigma_k$ are positive integers. Recall that the nondegeneracy condition means that α_i/α_j is not a root of 1 for all $i \neq j$ in $\{1, \ldots, k\}$. In this case,

$$u_m = \sum_{i=1}^{k} P_i(m)\alpha_i^m \quad \text{for all } m \geq 0,$$

where $P_i(X) \in \mathbb{C}[X]$ is of degree $\sigma_i - 1$ for $i = 1, \ldots, k$. We shall further assume that $|\alpha_1| \geq \cdots \geq |\alpha_k|$. If $|\alpha_1| > 1$, then it is known that, for all $\varepsilon > 0$, the inequality $|u_m| > |\alpha_1|^{(1-\varepsilon)m}$ holds for all $m \geq 0$ with finitely many exceptions. In particular, $|u_m| > |\alpha_1|^{m/2}$ holds for all but finitely many m.

https://doi.org/10.1017/S0004972713000166 Published online by Cambridge University Press

Define similarly $\mathcal{N}_E(x) = \{n \le x : |a_n| = |u_m| \text{ for some integer } m\}$. We conjecture that there exists $\eta > 0$ such that $\#\mathcal{N}_E(x) \ll x^{1-\eta}$ and give some heuristic support to this conjecture. Indeed, since $|a_n| \le \sqrt{n}\tau(n)$ for all $n \ge 1$, it follows that if $n \le x$, then $|a_n| \le x^{1/2+o(1)}$ for all $n \le x$ as $x \to \infty$. In particular, this suggests that perhaps the estimate

$$\#\{n \le x : |a_n| = a\} \ll x^{1/2+o(1)} \tag{7.1}$$

holds uniformly in a as $x \to \infty$. Assume that (7.1) holds. As we have seen, if $n \in \mathcal{N}_E(x)$, then $|a_n| = |u_m|$ for some m. Hence, if $|\alpha_1| > 1$, then with finitely many exceptions in m, we have that $|\alpha_1|^{m/2} < |u_m| = |a_n| \le x^{1/2+o(1)}$ as $x \to \infty$, so $m = O(\log x)$. If $|\alpha_1| = 1$, then by Kronecker's theorem, all roots of $f(X)$ are roots of unity. Since the ratio of any two of them cannot be a root of unity, it follows that $k = 1$ and $\alpha_1 \in \{\pm 1\}$. Thus, $|u_m| = |P_1(m)|$, where $P_1(X)$ is a polynomial of degree d with rational coefficients. Since $P_1(X)$ is neither constant nor a linear polynomial in X, it follows that $d \ge 2$. Then $|P_1(m)| \gg m^d$, showing that

$$m^d \ll |P_1(m)| = |u_m| = |a_n| \le x^{1/2+o(1)} \quad \text{as } x \to \infty.$$

Therefore $m \le x^{1/(2d)+o(1)}$ as $x \to \infty$. By (7.1), for each possible m,

$$\#\{n \le x : |a_n| = |u_m|\} \le x^{1/2+o(1)} \quad \text{as } x \to \infty$$

independently in m. This heuristic argument suggests that

$$\#\mathcal{N}_E(x) \le x^{1/2+o(1)} \times \{m : |u_m| \le x^{1/2+o(1)}\} \le \begin{cases} x^{1/2+o(1)} & \text{if } |\alpha_1| > 1 \\ x^{1/2+1/(2d)+o(1)} & \text{if } |\alpha_1| = 1, \end{cases}$$

which indeed seems to suggest that the inequality $\#\mathcal{N}_E(x) \ll x^{1-\eta}$ holds for all $x \ge 1$ with some $\eta > 0$. Further, one may perhaps take any $\eta \in (0, 1/2)$ provided that $|u_m|$ is not a polynomial of degree $d \ge 2$ for all sufficiently large m.

Acknowledgements

We thank Christian Ballot, Graeme Cohen, Alina Cojocaru, Chantal David and the anonymous referee for useful suggestions.

References

[1] E. R. Canfield, P. Erdős and C. Pomerance, 'On a problem of Oppenheim concerning factorisatio numerorum', *J. Number Theory* **17** (1983), 1–28.

[2] A. C. Cojocaru, 'Questions about the reductions modulo primes of an elliptic curve', in: *Number Theory: Proceedings of the 7th Conference of the Canadian Number Theory Association (Montreal, 2002)*, CRM Proceedings and Lecture Notes, 36 (eds. H. Kisilevsky and E. Goren) (American Mathematical Society, Providence, RI, 2004), 61–79.

[3] M. Deuring, 'Die Typen der Multiplikatorenringe elliptischer Functionenkörper', *Abh. Math. Sem. Hansischen Univ.* **14** (1941), 197–272.

https://doi.org/10.1017/S0004972713000166 Published online by Cambridge University Press

[4] N. D. Elkies, 'The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$', *Invent. Math.* **89** (1987), 561–567.
[5] R. R. Hall and G. Tenenbaum, *Divisors* (Cambridge University Press, Cambridge, 1988).
[6] F. Luca and A. Yalçiner, '*L*-functions of elliptic curves and Fibonacci numbers', *Fibonacci Quart.* to appear.
[7] E. Lucas, 'Théorie des fonctions numériques simplement périodiques', *Amer. J. Math.* **1** (1878), 189–240; 289–321.
[8] J.-P. Serre, 'Quelques applications du théorème de densité de Chebotarev', *Publ. Math. Inst. Hautes Études Sci.* **54** (1981), 123–201.
[9] J. H. Silverman, *The Arithmetic of Elliptic Curves* (Springer-Verlag, Berlin, 1995).
[10] L. Somer, 'Which second-order linear integral recurrences have almost all primes as divisors?', *Fibonacci Quart.* **17** (1979), 111–116.
[11] C. L. Stewart, *Divisor Properties of Arithmetical Sequences*, PhD Thesis, University of Cambridge, 1976.
[12] E. Wirsing, 'Das asymptotische Verhalten von Summen über multiplikative Funktionen', *Math. Ann.* **143** (1961), 75–102.

FLORIAN LUCA, Fundación Marcos Moshinsky,
Instituto de Ciencias Nucleares UNAM, Circuito Exterior, C.U.,
Apdo. Postal 70-543, Mexico D.F. 04510, Mexico
e-mail: fluca@matmor.unam.mx

ROGER OYONO, Équipe GAATI, Université de la Polynésie Française,
BP 6570, 98702 Faa'a, Tahiti, French Polynesia
e-mail: roger.oyono@upf.pf

AYNUR YALCINER, Department of Mathematics,
Faculty of Science, Selçuk University, Campus 42075 Konya, Turkey
e-mail: aynuryalciner@gmail.com

https://doi.org/10.1017/S0004972713000166 Published online by Cambridge University Press