L-FUNCTIONS OF ELLIPTIC CURVES AND FIBONACCI NUMBERS

FLORIAN LUCA AND AYNUR YALÇINER

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 $\mathbb{Q}$. We prove that if E is non-CM and has non-trivial 2-torsion, then the set of positive integers n such that $|a_n|$ is a Fibonacci number has asymptotic density 0.

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 be its discriminant. For each prime p we let

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

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

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

If $p\nmid\Delta$, we have $|a_p|\leq 2\sqrt{p}$. The L-function associated to E is given by

$$L(s,E)=\prod_{p\mid\Delta}\frac{1}{1-a_pp^{-s}}\prod_{p\nmid\Delta}\frac{1}{1-a_pp^{-s}+p^{1-2s}}.$$

The infinite product above is convergent for $\mathrm{Re}(s)>3/2$ and therefore we can expand it into a series $L(s,E)=\sum_{n\geq 1}a_nn^{-s}$.

Here we study the set of positive integers n such that $|a_n|=F_m$ for some non-negative integer m. We address only the instance of non-CM curves E, which are those curves whose endomorphism ring over the field of complex numbers consists of the ring of integers; that is, their only endomorphisms are the maps n_E which send P to nP for all $P\in E(\mathbb{C})$ for an arbitrary integer n. Before we start, we remark that there could be many n such that a_n is a Fibonacci number simply because it may happen that $a_p=0$ for some prime p, in which case $n=p\ell$ with any positive integer ℓ coprime to p has the property that $a_n=0=F_0$. To discard this instance, let

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

It is known that if we let $\mathcal{M}_E(x)=\mathcal{M}_E\cap[1,x]$, then $\#\mathcal{M}_E(x)\gg x$ (see Théorème 16 in [7]). We let

$$\mathcal{N}_E=\{n\in\mathcal{M}_E: |a_n|=F_m\},$$

and for a positive real number x we let $\#\mathcal{N}_E(x)=\#\left(\mathcal{N}_E\cap[1,x]\right)$.

Research supported in part by Tubitak, grant PAPIIT IN104512, CONACyT 163787, CONACyT 193539 and a Marcos Moshinsky Fellowship.

Theorem 1.1. *Let E be a non-CM curve with non-trivial 2-torsion. The estimate*

$$\#\mathcal{N}_E(x) = O\left(\frac{x}{(\log x)^{0.0007}}\right) = O\left(\frac{\#\mathcal{M}_E(x)}{(\log \#\mathcal{M}_E(x))^{0.0007}}\right)$$

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

We recall that the study of distribution of values and the arithmetic properties of the sequence $(a_n)_{n\geq 1}$ is a mainstream topic of interest to many people. The reader is referred to [7] as well as to the survey [2].

A more general problem is studied in [5].

We use the usual notations. The letter p with or without subscripts stands for a prime number. We use $p^a \| n$ for $p^a \mid n$ but $p^{a+1} \nmid n$; i.e., a is the exact exponent of the prime p in the factorization of n. We use $\omega(n)$ and $\tau(n)$ for the number of distinct prime divisors of n and for the total number of divisors of n, respectively. We write $P(n)$ for the largest prime factor of n. We use α and β for positive absolute constants. For a subset $\mathcal{A}$ of positive integers and a real number x we use $\mathcal{A}(x)$ for $\mathcal{A} \cap [1, x]$. Finally, we use the Landau notation O and o as well as the Vinogradov notations $\ll$ and $\gg$ with their regular meanings. The constants implied by them might depend on E.

2. The Strategy of the Proof

In this section, we describe the strategy of the proof. This should make it easier for the reader to follow the details in the next section. Let $n \in \mathcal{N}_E(x)$. With few exceptions, positive integers $n \leq x$ have a "small" square-full part and about $\log\log x$ distinct prime factors. Further, again with few exceptions, such n have a "large" $P(n)$. In particular, such non-exceptional n can be written as $n = Pn_1$, where $P := P(n)$ is large and coprime to n_1. Fix n_1. Then the equation $a_n = \pm F_m$ gives $a_P = \pm F_m/a_{n_1}$. Now $P \leq x/n_1$, therefore $|a_P| \leq 2x^{1/2}$. In particular, $F_m \leq 2x^{1/2}$, so there are $O(\log x)$ possibilities for m. A result of Serre [7], which is also reproduced here as Lemma 3.1, asserts that for a fixed $a \neq 0$, the counting function of the set of primes $P \leq x$ such that $a_P = a$ is of order at most $x/(\log x)^{1+\delta+o(1)}$ as $x \to \infty$ for some $\delta > 0$ which is independent of a. The above result shows that the counting function of the number of pairs (P, m) when n_1 and m are fixed is of order at most $x/(n_1(\log x)^{1+\delta+o(1)})$ as $x \to \infty$. Summing up over all the possible values of $n_1 \leq x$ while keeping m fixed, we get a count of order $x/(\log x)^{\delta+o(1)}$ as $x \to \infty$. If $\delta > 1$, then we could also sum up over the $O(\log x)$ values for m getting a count of order $x/(\log x)^{\delta-1+o(1)}$ as $x \to \infty$, and we would be through since $\delta > 1$. However, Serre only proved that one can choose $\delta = 1/3$ if $a \neq \pm 2$ and $\delta = 1/4$ when $a = \pm 2$, so we need to cut down on the above count. The instance when $a = \pm 2$ is dealt with using a simple sieve, while for the instance when $a \neq \pm 2$, we use the fact that E has non-trivial 2 torsion to deduce that a_p is even for all odd p, and that n has about $\log\log x$ distinct prime factors, to deduce that a_{n_1} is divisible by a power of 2 of size about $2^{\log\log x} = (\log x)^{\log 2}$. This in turn implies that F_m is divisible by a power of 2 of size about $(\log x)^{\log 2}$, which via some well-known divisibility property of the Fibonacci numbers, implies that $m = O(\log x)$ is divisible by a power of 2 of the same size, namely, about $(\log x)^{\log 2}$. This cuts down on the number of possibilities for m from $O(\log x)$ to $O((\log x)^{1-\log 2})$. Since $1 - \log 2 < 1/3 = \delta$, the initial argument now yields a logarithmic saving. Introducing some parameters to quantify the statements that "the square-full part of n is small", or that "n is not too smooth", or that "n has enough distinct prime factors", getting effective logarithmic savings for the exceptional sets associated to the above conditions, and optimizing among these parameters, we get the conclusion of the theorem.

3. The Proof

3.1. **Weierstrass equations.** With the standard birational transformation (see Chapter III, Section 1 in [8]), 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

$$C_4 = B_2^2 - 24B_4;$$
$$C_6 = -B_2^3 + 36B_2B_4 - 216B_6,$$

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 let $A = -27C_4$ 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

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

3.2. **Removing n with a large square-full part.** Recall that s is a square-full number if $p^2 \mid s$ whenever $p \mid s$. Let $y = \log x$. For each n we write

$$t(n) = \prod_{\substack{p \| n \\ p \nmid 6\Delta}} p \qquad \text{and} \qquad s(n) = n/t(n).$$

Then $s(n) = ab$, where a is square-free and $a \mid 6\Delta$ and b is square-full. We let

$$\mathcal{N}_1(x) = \{n \le x : s(n) > y\}. \tag{3.1}$$

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

$$\begin{aligned}
\#\mathcal{N}_1(x) &\le \sum_{\substack{ab > y \\ b \text{ square-full} \\ a \mid 6\Delta}} \frac{x}{ab} \le x \sum_{\substack{b > y/(6|\Delta|) \\ b \text{ square-full} \\ a \mid 6\Delta}} \frac{1}{ab} \\
&\le x \sum_{\substack{b > y/(6|\Delta|) \\ b \text{ square-full} \\ a \mid 6\Delta}} \frac{1}{b} = x \sum_{\substack{b > y/(6|\Delta|) \\ b \text{ square-full}}} \frac{\tau(6|\Delta|)}{b} \\
&\ll x \sum_{\substack{b > y/(6|\Delta|) \\ b \text{ square-full}}} \frac{1}{b} \ll \frac{x}{y^{1/2}} = \frac{x}{(\log x)^{1/2}},
\end{aligned} \tag{3.2}$$

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 $s \le t$ is $O(t^{1/2})$ (see, for example, Theorem 14.4 in [4]).

3.3. **Removing smooth n.** Recall that $P(n)$ is the largest prime factor of n. Let

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

We let

$$\mathcal{N}_2(x) = \{n \le x : P(n) \le z\}. \tag{3.3}$$

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

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

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

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

as $x \to \infty$, showing that

$$\#\mathcal{N}_2(x) = x\exp(-(1+o(1))\log\log x) = O\left(\frac{x}{(\log x)^{1/2}}\right). \tag{3.4}$$

3.4. **Removing n with too few prime factors.** Let $\alpha \in (0,1)$ to be found later and consider the set

$$\mathcal{N}_3(x) = \{n \le x : \omega(n) < (1-\alpha)\log\log x\}. \tag{3.5}$$

The results from Chapter 0 in [3] (see, for example, Problem 0.4 on Page 12 in [3]), show that

$$\#\mathcal{N}_3(x) \ll \frac{x}{(\log x)^{\beta}}, \tag{3.6}$$

where

$$\beta = 1 - (1-\alpha)\log\left(\frac{e}{1-\alpha}\right).$$

3.5. **A first application of Serre's Theorem.** For a nonzero integer a, let

$$\mathcal{P}_a = \{p : a_p = a\}.$$

The following statement is Théorème 20 in [7].

Lemma 3.1.

i) *If $a = \pm 2$, then*

$$\#\mathcal{P}_a(x) \ll \frac{x(\log\log x)^{1/2}(\log\log\log x)^{1/4}}{(\log x)^{5/4}}.$$

ii) *If $a \neq 0, \pm 2$, then*

$$\#\mathcal{P}_a(x) \ll \frac{x(\log\log x)^{2/3}(\log\log\log x)^{1/3}}{(\log x)^{4/3}}.$$

Let $\mathcal{N}_4(x) = \{n \le x : a_{P(n)} = \pm 2\} \setminus (\mathcal{N}_1(x) \cup \mathcal{N}_2(x) \cup \mathcal{N}_3(x))$. Assume that $n \in \mathcal{N}_4(x)$. Then $P \mid n$ for some prime $P \in \mathcal{P}_{\pm 2}(x)$. Fixing P, the number of such $n \le x$ is at most $\lfloor x/P \rfloor \le x/P$. Since $P > z$ (because $n \notin \mathcal{N}_2(x)$), we get that

$$\#\mathcal{N}_4(x) \le \sum_{\substack{z < P \le x \\ P \in \mathcal{P}_{\pm 2}}} \frac{x}{P} = x \sum_{\substack{z < P \le x \\ P \in \mathcal{P}_{\pm 2}}} \frac{1}{P}. \tag{3.7}$$

By the Abel summation formula and i) of Lemma 3.1, we get

$$\begin{aligned}\sum_{\substack{z<P\le x\\ P\in\mathcal{P}_{\pm 2}}}\frac{1}{P} &\ll \int_z^x \frac{d\#\mathcal{P}(t)}{t} = \left(\frac{\#\mathcal{P}(t)}{t}\Big|_{t=z}^{t=x}\right) + \int_z^x \frac{\#\mathcal{P}_{\pm 2}(t)}{t^2}dt\\ &\ll \frac{(\log\log x)^{1/2}(\log\log x)^{1/4}}{(\log x)^{5/4}} + \int_z^x \frac{(\log\log t)^{1/2}(\log\log\log t)^{1/4}}{t(\log t)^{5/4}}dt\\ &\ll \frac{1}{\log x} + \frac{(\log\log x)^{1/2}(\log\log\log x)^{1/4}}{(\log z)^{1/4}}\int_z^x \frac{dt}{t\log t}\\ &\le \frac{1}{\log x} + \frac{(\log\log x)^{3/2}(\log\log\log x)^{1/4}}{(\log z)^{1/4}} \ll \frac{1}{\log x} + \frac{(\log\log x)^{7/4}}{(\log x)^{1/4}}\\ &\ll \frac{1}{(\log x)^{1/5}}, \end{aligned} \tag{3.8}$$

where in the above calculation we used the fact that

$$\log z = \frac{\log x \log\log\log x}{\log\log x}.$$

Thus, by (3.7) and (3.8), we get

$$\#\mathcal{N}_4(x) \ll \frac{x}{(\log x)^{0.2}}. \tag{3.9}$$

3.6. **The final argument.** Assume $n \in \mathcal{N}_5(x) = \mathcal{N}_E(x)\setminus(\mathcal{N}_1(x)\cup\mathcal{N}_2(x)\cup\mathcal{N}_3(x)\cup\mathcal{N}_4(x))$. Since $n\notin\mathcal{N}_1(x)$, we may write

$$n = up_1\cdots p_\ell, \quad u\le y, \quad p_1<\cdots<p_\ell \quad\text{and}\quad \gcd(u, p_1\cdots p_\ell)=1.$$

Furthermore, $p_i \nmid 6\Delta$ for any $i=1,\dots,\ell$. Assume that x is large enough so that $z>y$. Then $P(n)=p_\ell$. Write

$$F_m = a_n = a_u a_{p_1}\cdots a_{p_\ell}. \tag{3.10}$$

Let $\varepsilon>0$ be arbitrary. Note that since

$$\omega(u) \ll \frac{\log u}{\log\log u} \ll \frac{\log y}{\log\log y} = o(\log\log x) \qquad \text{as} \qquad x\to\infty,$$

it follows that $\omega(u)<\varepsilon\log\log x$ holds whenever x is sufficiently large. For simplicity, we let $L := \lfloor(1-\alpha-\varepsilon)\log\log x\rfloor$. Note that $\ell=\omega(n/u)\ge L$ since $n\notin\mathcal{N}_3(x)$. Note also that since E has 2-torsion, it follows that $\#E(\mathbb{F}_p)$ is always even. Since $\#E(\mathbb{F}_p)=p-a_p+1$, it follows that a_p is even whenever p is odd. In particular, $2\mid a_{p_i}$ for all $i=1,\dots,\ell$. Since $\ell\ge L$, formula (3.10) implies that $2^L\mid a_n\mid F_m$. Since the inequality

$$|a_n|\le\tau(n)\sqrt{n}<x$$

holds for all sufficiently large x, it follows that $F_m<x$. Since

$$F_m = \frac{\gamma^m-\delta^m}{\gamma-\delta}, \qquad \text{where} \qquad (\gamma,\delta)=\left(\frac{1+\sqrt{5}}{2},\frac{1-\sqrt{5}}{2}\right),$$

it follows that $m<c_1\log x$ holds with some positive absolute constant c_1 which can be taken to be any constant larger than $1/\log\gamma$ provided that x is sufficiently large. We now exploit the condition $2^L\mid F_m$. It is known that for $L\ge 3$ (i.e., for x sufficiently large) this implies that

$3 \times 2^{L-2} \mid m$ (see the Theorem on Page 210 in Lucas' seminal paper [6]). Thus, $m = 3 \times 2^{L-2}k$ for some positive integer k satisfying the bound

$$k \leq \frac{c_1 \log x}{3 \times 2^{L-2}} \leq c_2 (\log x)^{1-(1-\alpha-\varepsilon)\log 2},$$

where $c_2 = 8c_1/3$. Let M be the above upper bound. Fix $k \leq M$. Also fix $v = n/p_\ell$. Put $P = p_\ell$. We then have

$$\pm F_m = a_n = a_v a_P.$$

Since v and m are fixed with $a_v \neq 0,\ F_m \neq 0$, it follows that $a_P = \pm F_m/a_v$ takes one of two fixed values. Thus, $P \in \mathcal{P}_{\pm F_m/a_v}$. Further, since $n \notin \mathcal{N}_4(x)$, it follows that $F_m/a_v \notin \{\pm 2\}$. Since also $P \leq x/v$, it follows, ii) of Lemma 3.1 shows that the number of possibilities for P is of order at most

$$\#\mathcal{P}_{\pm F_m/a_v}(x/v) \ll \frac{x(\log\log(x/v))^{2/3}(\log\log\log(x/v))^{1/3}}{v(\log(x/v))^{4/3}}. \tag{3.11}$$

Using the fact that $x/v \geq P > z$, so

$$\log(x/v) > \log z = \frac{(\log x)(\log\log\log x)}{\log\log x},$$

we get that the expression shown in the right-hand side of the inequality (3.11) above is bounded above by

$$\frac{x(\log\log x)^2}{v(\log x)^{4/3}}$$

whenever x is large enough. Summing over all possibilities for $v \leq x/z$ and k, we get that

$$\#\mathcal{N}_5(x) \ll \frac{x(\log\log x)^2 M}{(\log x)^{4/3}} \sum_{v<x/z} \frac{1}{v} \ll \frac{x(\log\log x)^2}{(\log x)^{(1-\alpha-\varepsilon)\log 2 - 2/3}}. \tag{3.12}$$

Comparing (3.2), (3.4), (3.6), (3.9) and (3.12), we get that

$$\#\mathcal{N}_E(x) \leq \sum_{i=1}^{5} \#\mathcal{N}_i(x) \ll \frac{x}{(\log x)^{1/2}} + \frac{x}{(\log x)^{1/2}} + \frac{x}{(\log x)^{0.2}} + \frac{x}{(\log x)^{\beta}} + \frac{x(\log\log x)^2}{(\log x)^{(1-\alpha-\varepsilon)\log 2 - 2/3}}. \tag{3.13}$$

The above bound suggests that we should choose α such that

$$1 - (1-\alpha)\log\left(\frac{e}{1-\alpha}\right) = \beta = (1-\alpha)\log 2 - 2/3. \tag{3.14}$$

Solving equation (3.14) we get $\alpha = 0.0371929$ with corresponding value of the expression (3.14) equal to 0.00070394 which is smaller than 0.2. Taking ε sufficiently small (say $\varepsilon < 10^{-6}$), we get the desired estimate from inequality (3.13).

Acknowledgement

We thank the referee for a careful reading of the manuscript and for suggestions which improved the quality of this paper.

References

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

[2] A. C. Cojocaru, *Questions about the reductions modulo primes of an elliptic curve*, Number Theory, 6179, CRM Proc. Lecture Notes, **36**, Amer. Math. Soc., Providence, RI, 2004.

[3] R. R. Hall and G. Tenenbaum, *Divisors*, Cambridge Univ. Press, 1988.

[4] A. Ivić, *The Riemann-Zeta Function, Theory and Applications*, Dover Publications, Mineola, New York, 2003.

[5] F. Luca, R. Oyono, and A. Yalçiner, *L-functions of elliptic curves and binary recurrences*, Bull. Australian Math. Soc., (to appear).

[6] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math., **1** (1878), 184–240, 289–321.

[7] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math., **54** (1981), 123–201.

[8] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, Berlin, 1995.

MSC2010: 11G40, 11B39, 11N36

Fundación Marcos Moshinsky, Instituto de Ciencias Nucleares UNAM, Circuito Exterior, C.U., Apdo. Postal 70-543, Mexico D. F. 04510, Mexico

E-mail address: fluca@matmor.unam.mx

Department of Mathematics, Faculty of Science, Selçuk University Campus 42075 Konya, Turkey

E-mail address: aynuryalciner@gmail.com