PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 2, *Number* 1, *March* 2017, *pages* 21-30

Christophe Delaunay

Atypical averages of root numbers of families of elliptic curves

written by Fabio Caldarola

1 Introduction

An *elliptic curve* is a projective algebraic curve of genus one with a rational point. We recall that, if K is a number field and E is an elliptic curve defined over K, the Mordell-Weil theorem asserts that the (abelian) group $E(K)$ of K-rational points of E, is finitely generated; it means that $E(K) \simeq E(K)_{\text{tors}} \times \mathbb{Z}^r$, where the nonnegative integer $r = \text{rk}_K(E)$ is the *rank* of $E(K)$. Néron, in his thesis [8], generalized this theorem to abelian varieties defined over a field K finitely generated over its prime field and, subsequently, there were several other results of this type. Non-expert readers can find many texts and general references on the theory: we recommend, among others, [11] and [6].
In this paper we consider families of elliptic curves given by an equation of the kind

$$\mathcal{F}: \quad y^2 = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t), \tag{1}$$

where $a_i(t) \in \mathbb{Z}[t]$. In fact, for all but finitely many $t \in \mathbb{Z}$, the specialization $\mathcal{F}(t)$ of $\mathcal{F}$ is an elliptic curve over $\mathbb{Q}$ whose rank is denoted by $r(t)$. Moreover, we recall that the *global root number*

$\varepsilon(t) = \pm 1$ of $\mathcal{F}(t)$ is the sign of the functional equation for the L-series attached to $\mathcal{F}(t)$ (see, for example, [11, App. C.16] or [6, Chap. 16 §3]), and the Birch and Swinnerton-Dyer Conjecture implies $(-1)^{r(t)} = \varepsilon(t)$ (also called the *parity conjecture*; for a nice survey on the subject and for the relations with the Tate-Shafarevich group, see [4]).

We can also view (1) as a single elliptic curve over the rational function field $\mathbb{Q}(t)$: we denote its rank $\mathrm{rk}_{\mathbb{Q}(t)}(\mathcal{F})$ simply by r.

We define the *average root number* of the family (1) over $\mathbb{Z}$, as the following limit (if it exists)

$$\mathrm{Av}(\mathcal{F}) = \lim_{X\to\infty} \frac{1}{2X} \sum_{|t|<X} \varepsilon(t), \tag{2}$$

(where we have set $\varepsilon(t) := 0$ if $\mathcal{F}(t)$ is not an elliptic curve) and it is known that the average root number is zero and the average of $r(t)$ is r or $r+1$, for a large class of families of elliptic curves (see for example [5]); we are instead more interested to find families $\mathcal{F}$ such that $\mathrm{Av}(\mathcal{F}) \neq 0$ and $\mathrm{Av}(\mathcal{F}) \neq (-1)^r$, as better explained in Definition 1.1. Several problems are related with this issue: e.g., for the distribution of zeros of the L-functions $L(s, \mathcal{F}(t))$ and the underlying "symmetry type" of the family $\mathcal{F}$, see [3] and the references therein.

Definition 1.1 Let $\mathcal{F}$ be a non-isotrivial family of elliptic curves given by (1) with rank r over $\mathbb{Q}(t)$. We say that

(i) $\mathcal{F}$ is *potentially parity-biased* (or briefly *potentially biased*) *over* $\mathbb{Z}$ if there is no place of multiplicative reduction except possibly at ∞;

(ii) $\mathcal{F}$ is *parity-biased over* $\mathbb{Z}$ if $\mathrm{Av}(\mathcal{F})$ exists and is non-zero;

(iii) $\mathcal{F}$ has *excess rank over* $\mathbb{Z}$ if $\mathrm{Av}(\mathcal{F})$ exists and $\mathrm{Av}(\mathcal{F}) = -(-1)^r$.

Obviously (iii) implies (ii) and from a conjecture of Helfgott, (ii) would imply (i). In literature there are examples of parity-biased families with $\deg(a_i(t))$ quite large, but these families do not have excess rank over $\mathbb{Z}$. Hence it is clear that to obtain parity-biased families or with excess rank we need to control the rank r itself, the potentially parity-biased condition and the root numbers $\varepsilon(t)$ with their average. In this paper we show some results obtained in this sense by S. Bettin, C. David and C. Delaunay; for more details the reader can see the work-in-progress paper [1]. In particular, Theorems 3.1 and 3.2 classify potentially parity-biased families (1) with $\deg a_i(t) \leqslant 2$; then, considering a particular family $\mathcal{F}_a$ given in (5), Theorem 3.3 gives a formula for the root numbers in this family and Theorem 3.4 computes their average $\mathrm{Av}(\mathcal{F}_a)$. In the final part of the paper there are some applications of these results in order to have parity-biased families and families with excess rank.

We close the introductive section with the following well known

Example 1.2 For the Washington's family of elliptic curves, given by

$$\mathcal{F}_1 : \quad y^2 = x^3 + tx^2 - (t+3)x + 1, \tag{3}$$

the rank over $K(t)$ is one for every number field K (see [12, 2]). Moreover, in [9] Rizzo shows that $\varepsilon(t) = -1$ for every $t \in \mathbb{Z}$, and we conclude that this family is parity biased but it does not have excess rank over $\mathbb{Z}$. We notify, finally, that the constant value $\varepsilon(t) = -1\ \forall t \in \mathbb{Z}$ no longer holds out from $\mathbb{Z}$: for instance, $\varepsilon(t) = 1$ for many non integral $t \in \mathbb{Q}$.

2 The rank of a family of elliptic curves

Considering the elliptic curve $\mathcal{F}(t)$ from the family given in (1), we define the *trace of Frobenius* at p of $\mathcal{F}(t)$, denoted by $\mathrm{Tr}_t(p)$, as

$$\mathrm{Tr}_t(p) := \begin{cases} p + 1 - |E(\mathbb{F}_p)| & \text{if } \mathcal{F}(t) \text{ has good reduction at } p, \\ 0 & \text{otherwise}, \end{cases}$$

where $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ and $|E(\mathbb{F}_p)|$ is the number of points in the reduced curve, i.e. the cardinality of $\{(x, y) \in \mathbb{Z}^2 \mid y^2 \equiv x^3 + a_2(t)x^2 + a_4(t)x +$

$a_6(t) \mod p\}$ (see [11, V.2]). Denoting the average value of the trace by

$$A_p(\mathcal{F}) := \frac{1}{p}\sum_{t=0}^{p-1} \mathrm{Tr}_t(p),$$

we can enounce the following

Conjecture 2.1 (Nagao) $\lim_{X\to\infty} \sum_{p\leqslant X} -A_p(\mathcal{F}) \cdot \ln p = \mathrm{rk}_{\mathbb{Q}(t)}(\mathcal{F})$.

In [7] Nagao himself proved the conjecture for five family of elliptic curves, and, as an application of some main results, Rosen and Tate proved in [10] that Nagao Conjecture holds for rational surfaces, hence *a fortiori* when $\deg a_i(t) \leqslant 2$ in (1). Using this fact, for example, we can state the following

Proposition 2.2 *Let $b, e \in \mathbb{Z}$ such that $b^2 - 4e \neq 0$ and consider the following family*

$$\mathcal{F}\,' : y^2 = x^3 + tx^2 + (-bt - 3b^2 + 9e)x + et + b^3 - 3eb.$$

Then $r \leqslant 1$ and $r = 1$ if and only if $b^2 - 4e$ is ± a fourth power in $\mathbb{Z} - \{0\}$.

If $b^2 - 4e = 0$ then the curve $\mathcal{F}'(t)$ is singular. To give an idea of the proof we write $x^3+tx^2+(-bt-3b^2+9e)x+et+b^3-3eb$ as $B(x)\cdot t+C(x)$ where $B(x) = x^2 - bx + e$ and $C(x) = x^3 + (-3b^2 + 9e)x + b^3 - 3eb$. Then we have

$$r = \lim_{X\to\infty} \sum_{p\leqslant X} \frac{\ln p}{p} \sum_{x=0}^{p-1} \sum_{t=0}^{p-1} \left(\frac{B(x)t + C(x)}{p}\right), \tag{4}$$

where $\left(\frac{*}{*}\right)$ is the Legendre symbol. In the last sum in (4), the contribution will come from the zeros of B(x) modulo p. It has roots if and only if the discriminant of $B(x)$, i.e. $b^2 - 4e$, is a square modulo p. If $b^2 - 4e$ is not ± a fourth power, we obtain $r < 1$, so $r = 0$. If $b^2 - 4e$ is ± a fourth power, we obtain $r = 1$.

3 Potentially biased and parity-biased families

If $\mathcal{F}$ is the family of elliptic curves given by the equation (1) with $\deg a_i(t) \leqslant 2$, to be "potentially parity-biased" is equivalent to the condition

$$(\Delta(t) = 0) \Rightarrow (c_4(t) = 0),$$

where $\Delta(t)$ and $c_4(t)$ have the usual meaning for $\mathcal{F}(t)$ (see, for instance, [11, III.1] or [6, 3 §3]).

Theorem 3.1 *Let $\mathcal{F}$ be given by* (1) *a potentially biased family with* $\deg a_2(t) = 1$ *and* $\deg a_4(t), \deg a_6(t) \leq 2$. *Then $r \leqslant 1$ and up to a linear change of coordinates, $\mathcal{F}$ is one of the following*

(i) $\mathcal{F}' : \; y^2 = x^3 + tx^2 + (-at - 3a^2 + 9b)x + bt + a^3 - 3ab$ *with $a, b \in \mathbb{Z}$; in this case, $r = 1$ if and only if $a^2 - 4b$ is ± a fourth power in $\mathbb{Z}$.*

(ii) $\mathcal{G} : \; y^2 = x^3 + 3dtx^2 + 3d^2stx + d^3st^2$ *with $d, s \in \mathbb{Z}$; in this case,* $r = 1$ *if and only if $s \cdot d$ is a square in $\mathbb{Z}$ or -2 times a square.*

(iii) $\mathcal{H} : \; y^2 = x^3 + 3dtx^2 + 3d^2stx + d^3s^2t$ *with $d, s \in \mathbb{Z}$; in this case* $r = 0$.

And what does it happen if, in the statement of the previous theorem, we assume $\deg a_2(t) = 2$? In this case write $a_2(t) = ut^2 + vt + w$, where $u, v, w \in \mathbb{Z}$.

Theorem 3.2 *With such assumptions, up to a linear change of coordinates, $\mathcal{F}$ will be one of the following families*

(i) $\mathcal{F}'(ut^2 + vt + w)$, *and in this case $r \leqslant 3$.*

(ii) $\mathcal{H}(ut^2 + vt + w)$.

(iii) $y^2 = x^3 + 2vt(-4t + 1)x^2 + 4v^2t(2t + 1)x - v^3(4t^2 + 3t + 1)$*; in this case $r \leqslant 1$ and $r = 1$ if and only if v is -2 times a square.*

Now consider the equation of the family $\mathcal{F}'$ in Theorem 3.1 (i) with $b = 0$; more precisely, if $a^2 - 4b$ is a square, there exists a change of variables which transforms $\mathcal{F}'$ in the following

$$\mathcal{F}_a : \ y^2 = x^3 + tx^2 - a(3a + t)x + a^3 \tag{5}$$

(where $a \in \mathbb{Z}$ is not the same as before). For example, note that if we pose $f_a(t) := t^2 + 3at + 9a^2$, we easily find for $\mathcal{F}_a(t)$

$$c_4(t) = 16 f_a(t), \quad c_6(t) = -32(3a + 2t) f_a(t),$$
$$\Delta(t) = 16a^2(f_a(t))^2,$$

and, in the special case $a = 1$, we recover the Washington's family $\mathcal{F}_1$ given in (3).
As usual, we denote by $v_p(\cdot)$ the p-adic exponential valuation and by $(\cdot, \cdot)$ the gcd of two integers. Moreover, if $M \in \mathbb{Z}$, let M_0 be the odd part of M, i.e. $M = 2^{v_2(M)} M_0$.

Theorem 3.3 *Let $\varepsilon_a(t)$ be the root number of $\mathcal{F}_a(t)$, then*

$$\begin{aligned}\varepsilon_a(t) = &\ - s_a(t)\,(a_0, t)\\ &\cdot \prod_{p \left| \frac{a_0}{(a_0,t)} \right.} (-1)^{1+v_p(t)} \left(\frac{p^{-v_p(t)} t}{p} \right)^{1+v_p(t)} \qquad \bmod 4,\end{aligned}$$

where $s_a(t) \in \{-1, 1\}$ is explicit and depends only on a_0 $\bmod 8$, $v_2(a)$ $\bmod 2$, t_0 or $2^{v_2(a)}t$ $\bmod 8$.

If q, a are two integers such that $q|a$, we define $\mathrm{Av}_2(q, a)$ as the average of $s_a(qt)$ when t varies with $(t, q) = 1$. Then, using Theorem 3.3, we get

Theorem 3.4 *The following formula holds*

$$\mathrm{Av}(\mathcal{F}_a) = -\frac{1}{|a|} \sum_{\substack{q \mid |a| \\ p \left| \frac{a_0}{q_0} \right. \Rightarrow v_p(q) \text{ odd}}} \varphi(|a/q|)\, \chi_4(q_0)\, \mathrm{Av}_2(a, q),$$

where $\chi_4(q_0) \in \{-1, 1\}$ *is congruent to* $q_0 \bmod 4$ *and* $\mathrm{Av}_2(a, q) \in \{0, 1/2, 1\}$.

Note that, in particular, if a is square-free, then $q = a$ is the only divisor appearing in the previous sum, hence

$$\mathrm{Av}(\mathcal{F}_a) = \begin{cases} \pm 1/a & \text{if } a \equiv \mp 1 \mod 8 \\ \pm 1/(2a) & \text{if } a \equiv \pm 3 \mod 8 \\ 0 & \text{if } a \equiv \pm 2 \mod 8 \end{cases}.$$

The first consequence of Theorem 3.4 is the following corollary which gives necessary and sufficient conditions for the family $\mathcal{F}_a$ to be parity-biased.

Corollary 3.5 *The family* $\mathcal{F}_a$ *is parity-biased if and only if* $v_2(a) \neq 1$.

4 Families with excess rank

In this section we preserve the above notations and we continue the study to give some results and examples of families with excess rank. First of all, from Theorem 3.3, if $(a, b) = 1$ we have

$$e_a(at + b) = -\prod_{p|a} - \left(\frac{b}{p}\right),$$

and this means that

- if $p \equiv \pm 1 \bmod 8$ and b is not a square mod p, then $\mathcal{F}_p(pt + b)$ has excess rank over Z, with $r = 0$;
- if p is an odd prime and $p \nmid b$, then $\mathcal{F}_{p^2}(pt + b^2)$ has excess rank with $r = 1$.

To obtain families with higher rank we have to consider families of the form $F_{a^2}(ut^2 + vt + w)$: in this case, the rank is $\leqslant 3$.

Definition 4.1 We set

$$\mathcal{H}_{a^2,k}(t) := \mathcal{F}_{a^2}(t^2 - 2at - a^2 + k - a^2(t^2 + u^2)/k).$$

The first thing to do for working with this family, is to write its equation in the form

$$\mathcal{H}_{a^2,k}(t) : \; y^2 = A(x)t^2 + B(x)t + C(x)$$

for suitable polynomials $A(x), B(x), C(x) \in \mathbb{Z}[x]$ (recall (5)). For example, for the first two of them we find

$$A(x) = -\frac{a^2 - k}{k} x(x - a^2), \quad B(x) = -2ax(x - a^2).$$

Going further with computations and working on the characteristics of this family, we get results as the following

(a) We can take $k \in \mathbb{Z}$ such that $-\frac{a^8}{k}$ and $-\frac{ka^8}{(a^2 - k)^3}$ are not squares; in this case $r = 2$.

(b) We can take $k \in \mathbb{Z}$ such that $-\frac{a^8}{k}$ or $-\frac{ka^8}{(a^2 - k)^3}$ is a square; then $r = 3$.

For example, if we take $a = 2$ and $k = 1$, from (a) we obtain that the family $\mathcal{H}_{4,1}(t)$ has excess rank with $r = 2$. Instead, if we take $p \equiv \pm 1$ mod 8 and $l \in \mathbb{Z}$ with $p \nmid l$ we find that $\mathcal{H}_{p^2,-p^2}(pt + l)$ has excess rank with $r = 3$.

5 Twist of Washington family

We end the paper going back to the family in the Example 1.2: if $d \in \mathbb{Z} - 0$, the quadratic twist by d of Washington family (3) is

$$E_{d,t} : \; y^2 = x^3 + dtx^2 - (t + 3)d^2x + d^3, \tag{6}$$

which is in fact $\mathcal{F}_d(dt)$ (see (5)).

Theorem 5.1 *For $v_2(d)$ even the following hold*

(i) If $d_0 \equiv \pm 1 \mod 8$, then $\varepsilon(E_{d,t}) \equiv -|d_0| \mod 4$.

(ii) If $d_0 \equiv 3 \mod 8$, then $\varepsilon(E_{d,t}) = \operatorname{sgn}(d_0) \iff t \equiv 0, 1, 2 \mod 4$.

(iii) If $d_0 \equiv 5 \mod 8$, then $\varepsilon(E_{d,t}) = \operatorname{sgn}(d_0) \iff t \equiv 1 \mod 4$.

For $v_2(d)$ odd, $\varepsilon(E_{d,t}) = \operatorname{sgn}(d_0)$ if and only if $t \equiv 0, 3 \mod 4$.

The rank of $E_{d,t}$ is always zero, unless $d = \pm 1$. If we set $d = d_t(u)$, the generic point of $E_{d_t(u),t}$ is $(ud_t(u), d_t(u)^2)$ and $E_{d_t(u),t}$ has rank $\geqslant 1$ over $\mathbb{Q}(t)$.

Proposition 5.2

(i) If $u \equiv 1 \mod 4$, then $\varepsilon(E_{d_t(u),t}) = 1$ if and only if $d_t(u) > 0$.

(ii) If $u \equiv 0 \mod 4$, then $\varepsilon(E_{d_t(u),t}) = 1$ if and only if $d_t(u) < 0$.

References

[1] S. Bettin, C. David and C. Delaunay, *Families of elliptic curves with non-zero average root number*, preprint.

[2] B. Conrad, K. Conrad and H.A. Helfgott, *Root numbers and ranks in positive characteristic*, Adv. in Math. **198** (2005), pp. 684-731.

[3] C. David, D.K. Huynh and J. Parks, *One-level density of families of elliptic curves and the Ratios Conjecture*, J. Res. Number Theory (2015) 1: 6, 37 pages

[4] T. Dokchitser, *Notes on the Parity Conjectures*, in *Elliptic Curves, Hilbert Modular Forms and Galois Deformations*, Springer (2013), pp. 201-249.

[5] H.A. Helfgott, *On the behaviour of root numbers in families of elliptic curves*, arXiv:math/0408141 (2009).

[6] D. Husemöller, *Elliptic Curves, 2nd Ed.*, Springer, New York, Graduate Text in Math. **111** (2004).

[7] K.-I. Nagao, *$\mathbb{Q}(T)$-rank of elliptic curves and certain limit coming from the local points*, Manuscr. Math. **92**(1) (1997), pp. 13-32.

[8] A. Néron, *Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps*, Bull. Soc. Math. France **80** (1952), pp. 101-166.

[9] O. Rizzo, *Average root numbers for a non-constant family of elliptic curves*, Compositio Math. **136** (2003), pp. 1-23.

[10] M. Rosen and J.H. Silverman, *On the rank of an elliptic surface*, Invent. Math. **133**(1) (1998), pp. 43–67.

[11] J.H. Silverman, *The Arithmetic of Elliptic Curves, 2nd Ed.*, Springer, New York, Graduate Text in Math. **106** (2009).

[12] L. Washington, *Class numbers of the simplest cubic fields*, Math. Comp. **48** (1987), pp. 371-384.

Fabio Caldarola
Dep. of Mathematics and Computer Science
University of Calabria
Cubo 31/B, ponte Bucci
87036 Arcavacata di Rende, Italy.
email: `caldarola@mat.unical.it`