

NON-ISOTRIVIAL ELLIPTIC SURFACES WITH NON-ZERO AVERAGE ROOT NUMBER

SANDRO BETTIN, CHANTAL DAVID, AND CHRISTOPHE DELAUNAY

ABSTRACT. We consider the problem of finding non-isotrivial 1-parameter families of elliptic curves whose root number does not average to zero as the parameter varies in $\mathbb{Z}$. We classify all such families when the degree of the coefficients (in the parameter t) is less than or equal to 2 and we compute the rank over $\mathbb{Q}(t)$ of all these families. Also, we compute explicitly the average of the root numbers for some of these families highlighting some special cases. Finally, we prove some results on the possible values average root numbers can take, showing for example that all rational number in $[-1, 1]$ are average root numbers for some non-isotrivial 1-parameter family.

1. INTRODUCTION

This article is concerned with families of elliptic curves defined over $\mathbb{Q}$ such that the root number of the specializations does not behave, on average, as expected in the classical cases.

More precisely, by a family of elliptic curves, we mean an elliptic surface over $\mathbb{Q}$ or, equivalently, an elliptic curve defined over $\mathbb{Q}(t)$ given by a Weierstrass equation

$$(1.1) \quad \mathcal{F}: y^2 = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t)$$

where $a_2(t), a_4(t)$ and $a_6(t)$ are polynomials with coefficients in $\mathbb{Z}$. We denote by $r_{\mathcal{F}}$ the rank of $\mathcal{F}$ over $\mathbb{Q}(t)$.

For each $t \in \mathbb{Q}$, we denote by $\mathcal{F}(t)$ the associated curve over $\mathbb{Q}$ defined by the specialization at t of $\mathcal{F}$. Then, for all but finitely many values of t , $\mathcal{F}(t)$ is an elliptic curve defined over $\mathbb{Q}$ and we let $r_{\mathcal{F}}(t)$ and $\varepsilon_{\mathcal{F}}(t)$ denote its rank over $\mathbb{Q}$ and its root number respectively. The parity conjecture predicts that $(-1)^{r_{\mathcal{F}}(t)} = \varepsilon_{\mathcal{F}}(t)$ and Silverman's specialization theorem gives that $r_{\mathcal{F}}(t) \geq r_{\mathcal{F}}$ for all but finitely many values of t . One also conjectures that, up to a zero density subset of $\mathbb{Q}$, $r_{\mathcal{F}}$ is the smallest integer compatible with the parity conjecture and thus that $r_{\mathcal{F}}(t)$ is equal to either $r_{\mathcal{F}}$ or $r_{\mathcal{F}} + 1$ depending on the parity given by $\varepsilon_{\mathcal{F}}(t)$.

We define the average root number of $\mathcal{F}$ over $\mathbb{Z}$ as

$$(1.2) \quad \text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}}) := \lim_{T \rightarrow \infty} \frac{1}{2T} \sum_{|t| \leq T} \varepsilon_{\mathcal{F}}(t),$$

if the limit exists (and where we define $\varepsilon_{\mathcal{F}}(t) = 0$ if $\mathcal{F}(t)$ is not an elliptic curve).¹

The work of Helfgott ([Hel03, Hel09]) implies conjecturally (and unconditionally in some cases) that $\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}}) = 0$ as soon as there exists a place, other than $-\deg$, of multiplicative reduction of $\mathcal{F}$ over $\mathbb{Q}(t)$. Indeed, assuming the square-free sieve conjecture, one sees that in this case $\varepsilon_{\mathcal{F}}(t)$ behaves roughly like $\lambda(M(t))$ where λ is the Liouville's function and $M(t)$ is a certain non-constant square-free polynomial, so that Chowla's conjecture implies that $\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}}) = 0$. This is the typical case, which occurs for “most” families $\mathcal{F}$.

2010 *Mathematics Subject Classification.* 11G05, 11G40.

Key words and phrases. Rational elliptic surface, rank, root number, average root number.

¹Alternatively one could define $\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}})$ with the symmetric average $\frac{1}{2T} \sum_{|t| \leq T}$ replaced by $\frac{1}{T} \sum_{0 \leq t \leq T}$. All the same considerations we make in the paper works in this case as well mutatis mutandis.

When the family $\mathcal{F}$ has no place of multiplicative reduction (other than possibly $-\deg$), the average root number could be non-zero. The case when the family is isotrivial², and more precisely the case of quadratic twist families, has been the subject of several studies in the literature (see e.g. [Roh93, Riz99, DD09, KMR13]). There are however very few examples of non-isotrivial families with $\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}}) \neq 0$. There is the Washington's family ([Was87]) for which Rizzo proved ([Riz03]) that $\varepsilon_{\mathcal{F}}(t) = -1$ for all $t \in \mathbb{Z}$. Rizzo ([Riz03]) also gave an example of a family $\mathcal{F}$ with j -invariant $j_{\mathcal{F}}(t) = t$ and $\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}}) \notin \{-1, 0, 1\}$ (however for this family the degree of the polynomials $a_i(t)$ of the model given in the form (1.1) are quite large: for example $\deg a_6(t) = 8$). Romano [Rom05] considered a slight generalization of Washington's family obtaining an infinite sequence of families $\mathcal{F}_s$ all with rational average root number and with $\lim_{s \rightarrow \infty} \text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}_s}) = \frac{3}{4}$. Finally, Helfgott ([Hel09]) gave an example of a non-isotrivial family with *average root numbers over $\mathbb{Q}$* not in $\{-1, 0, 1\}$ (the degree of the coefficients $a_i(t)$ are quite large in this case too).³

In this paper we study non-isotrivial families $\mathcal{F}$ of elliptic curves with non-zero $\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}})$ in a more systematic way, with particular attention to the case where we have control on the rank of $\mathcal{F}$ over $\mathbb{Q}(t)$. One of our first motivations was to illustrate several questions on elliptic curves and on their associated L -functions where $\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}})$ appears naturally as well as to be able to provide numerical experimentation. For example, in a forthcoming work we show under several conjectures that the one-level density function corresponding to a family $\mathcal{F}$ is

$$W_{\mathcal{F}}(t) = r_{\mathcal{F}} \delta_0(\tau) + \left(\frac{1 + (-1)^{r_{\mathcal{F}}} \text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}})}{2} \right) W_{\text{SO}(\text{even})}(\tau) + \left(\frac{1 - (-1)^{r_{\mathcal{F}}} \text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}})}{2} \right) W_{\text{SO}(\text{odd})}(\tau)$$

where δ_0 is the Dirac measure at 0 and $W_{\text{SO}(\text{even})}$ (resp. $W_{\text{SO}(\text{odd})}$) is the one-level density function of the classical orthogonal group of even size (resp. odd size). We can also rewrite $W_{\mathcal{F}}$ as

$$W_{\mathcal{F}}(t) = \left(r_{\mathcal{F}} + \frac{1 - (-1)^{r_{\mathcal{F}}} \text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}})}{2} \right) \delta_0(\tau) + 1 + (-1)^{r_{\mathcal{F}}} \text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}}) \frac{\sin 2\pi\tau}{2\pi\tau},$$

where $r_{\mathcal{F}} + \frac{1 - (-1)^{r_{\mathcal{F}}} \text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}})}{2}$ is (conjecturally) the average rank of the specialization. Notice that if $\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}}) \notin \{0, \pm 1\}$, then $W_{\mathcal{F}}(t)$ doesn't reduce to $W_{\text{SO}(\text{even})}$ or $W_{\text{SO}(\text{odd})}$ plus some multiple of $\delta_0(t)$, and so $W_{\mathcal{F}}(t)$ is not the 1-level density function of one of the classical compact groups (of course one can divide the family into two subfamilies according to the sign of $\varepsilon_{\mathcal{F}}(t)$ going back to $W_{\text{SO}(\text{even})}$ or $W_{\text{SO}(\text{odd})}$; see [Far05] and [Sar08] for two proposed definitions of "families of L -functions" where this division is requested, see also [Kow13] for a discussion on families). Another interesting case is that of "elevated rank", i.e. when $\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}}) = -(-1)^{r_{\mathcal{F}}}$ and so almost all specializations satisfy $r_{\mathcal{F}}(t) > r_{\mathcal{F}}$. Notice that when this happens then $W_{\mathcal{F}}(t)$ is, up to Dirac functions, equal to the 1-level density of the orthogonal group with size of parity opposite to that of $r_{\mathcal{F}}$.

The knowledge of $\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}})$ is also useful for the study of the average behavior of the Selmer and Tate-Shafarevich groups of $\mathcal{F}(t)$. There are several conjectures and heuristics for questions on this topic ([BKL⁺15], [PR12], [DJ14]). For example, let p be a prime number, one of the classical conjecture predicts the probability that the p -part of the Tate-Shafarevich group is trivial or not; this original prediction also depends on the rank $r_{\mathcal{F}}(t)$ (at least when $r_{\mathcal{F}} = 0$ and $\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}}) = 0$ and so when $r_{\mathcal{F}}(t) = 0$ or 1 almost always). Now, the p -Selmer group, denoted by $\text{Sel}_p(\mathcal{F}(t))$, and the Tate-Shafarevich group, denoted by $\text{III}(\mathcal{F}(t))$, are related by the following exact sequence

$$1 \rightarrow \mathcal{F}(t)(\mathbb{Q})/p\mathcal{F}(t)(\mathbb{Q}) \rightarrow \text{Sel}_p(\mathcal{F}(t)) \rightarrow \text{III}(\mathcal{F}(t))[p] \rightarrow 1$$

so that $|\text{Sel}_p(\mathcal{F}(t))| = p^{r_{\mathcal{F}}(t)} |\text{III}(\mathcal{F}(t))[p]|$ if $\mathcal{F}(t)(\mathbb{Q})$ has no p -torsion point (in general, $|\text{Sel}_p(\mathcal{F}(t))| = p^{r_{\mathcal{F}}(t)+d} |\text{III}(\mathcal{F}(t))[p]|$ where d is the dimension of $\mathcal{F}(t)(\mathbb{Q})[p]$ over $\mathbb{F}_p$). So, the p -divisibility of $|\text{Sel}_p(\mathcal{F}(t))|$

²Isotrivial means that the j -invariant of $\mathcal{F}$ is constant. For isotrivial families, one can take, for instance, the quadratic twist of a fixed elliptic curve $E/\mathbb{Q}$ by a polynomial $d(t) \in \mathbb{Z}[t]$, $E^{d(t)}: d(t)y^2 = y^2 = x^3 + a_2x^2 + a_4x + a_6$, where $a_i \in \mathbb{Z}$ for $i = 2, 5, 6$. In this case, it is easier to deal with the root number, for example if $d(t)$ is coprime with the conductor of E , then the root number is simply given by some congruence relations.

³See the end of the introduction for the precise definition of the average root number over $\mathbb{Q}$.

and $|\text{III}(\mathcal{F}(t))[p]|$ are correlated and depend on the rank, on the parity of the root number and so on the average root number. In the case where $r_{\mathcal{F}}(t) > 0$, the group $\text{Sel}_p(\mathcal{F}(t))$ is forced to be large because of the presence of $r_{\mathcal{F}}(t)$ generic points in $\mathcal{F}(t)(\mathbb{Q})$ and one can naturally wonder if those $r_{\mathcal{F}}(t)$ points do contribute in $\text{III}(\mathcal{F}(t))[p]$ or not (the answer seems to be no as discussed in a forthcoming study).

We are then led to define the following notions.

Definition 1. *Let $\mathcal{F}$ be a family of elliptic curves with rank $r_{\mathcal{F}}$ over $\mathbb{Q}(t)$. We say that*

- $\mathcal{F}$ is *potentially parity-biased* (or also *potentially biased*) over $\mathbb{Z}$ if it has no place of multiplicative reduction except possibly for the place corresponding to $-\deg$;
- $\mathcal{F}$ is *parity-biased* over $\mathbb{Z}$ if $\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}})$ exists and is non-zero;
- $\mathcal{F}$ has *elevated rank* over $\mathbb{Z}$ if $\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}})$ exists and $\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}}) = -(-1)^{r_{\mathcal{F}}}$.

We shall describe in Section 2 the relation between potentially parity-biased and parity-biased families.

In this article we focus on potentially parity-biased families of elliptic curves. In particular, we classify all non-isotrivial potentially parity-biased families with $\deg a_i(t) \leq 2$ for $i = 2, 4, 6$. We prove that there are essentially 6 different classes of such families⁴ (cf. Theorem 7 and Theorem 8):

$$\begin{aligned}
 (1.3) \quad & \mathcal{F}_s: y^2 = x^3 + 3tx^2 + 3sx + st, \text{ with } s \in \mathbb{Z}_{\neq 0}; \\
 & \mathcal{G}_w: wy^2 = x^3 + 3tx^2 + 3tx + t^2, \text{ with } w \in \mathbb{Z}_{\neq 0}; \\
 & \mathcal{H}_w: wy^2 = x^3 + (8t^2 - 7t + 3)x^2 - 3(2t - 1)x + (t + 1), \text{ with } w \in \mathbb{Z}_{\neq 0}; \\
 & \mathcal{I}_w: wy^2 = x^3 + t(t - 7)x^2 - 6t(t - 6)x + 2t(5t - 27), \text{ with } w \in \mathbb{Z}_{\neq 0}; \\
 & \mathcal{J}_{m,w}: wy^2 = x^3 + 3t^2x^2 - 3mtx + m^2, \text{ with } m, w \in \mathbb{Z}_{\neq 0}; \\
 & \mathcal{L}_{w,s,v}: wy^2 = x^3 + 3(t^2 + v)x^2 + 3sx + s(t^2 + v), \text{ with } v \in \mathbb{Z}, s, w \in \mathbb{Z}_{\neq 0};
 \end{aligned}$$

In Section 3 we will compute the ranks and give generic points for all of families given in (1.3). We will see that the rank over $\mathbb{Q}(t)$ of all these families is either 0 or 1 (depending on the parameters) except for the family $\mathcal{L}_{w,s,v}$ for which the rank can also be 0, 1, 2, or 3. We remark that both $\mathcal{L}_{w,s,v}(t)$ and $\mathcal{G}_w(t)$ could be expressed in terms of $\mathcal{F}_s$. Indeed, we have that $\mathcal{L}_{w,s,v}(t)$ and $\mathcal{G}_w(t)$ are isomorphic to $\mathcal{F}_{sw^2}(w(t^2 + v))$ and $\mathcal{F}_{tw^2}(wt)$ respectively.

We can also compute the root number for all the specializations of the above families (the results are quite long to express, so we only give the ones for $\mathcal{F}_s$ in Appendix A). We use these results to compute their average root numbers in some representative cases, pin-pointing the cases of parity-biased families and of families with elevated rank over $\mathbb{Z}$ (we are able to provide families of elliptic curves of these types with rank equal to 0, 1, 2 and 3). We postpone the precise statements of our results to Section 2, 3 and 4. We state here only some examples.

For $a \in \mathbb{Z}_{\neq 0}$ we define

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

Notice that the family $\mathcal{W}_a$ is a particular case of the family $\mathcal{F}_s$. Indeed, one has that $\mathcal{W}_a(t)$ is isomorphic to $\mathcal{F}_{-3a^2/4}(t/3 + a/2)$ or, equivalently, to $\mathcal{F}_{-3^5 4a^2}(12t + 18a)$ if one wants a model defined over $\mathbb{Z}$. In Section 3 we shall see that all the families $\mathcal{F}_s$ which have rank 1 are all of type $\mathcal{W}_a$. We will study the root number and the average root number of $\mathcal{W}_a$ in full generality and extract from them several consequences.

In the following the letter p will always denote a prime number. Also, if $n \in \mathbb{Z}_{\neq 0}$ then we let n_p be such that $n = p^{v_p(n)} n_p$ where $v_p(n)$ is the p -adic valuation of n .

⁴By the work of Helfgott one also has that, under the square-free sieve and Chowla's conjectures for homogeneous polynomials in two variables, the only non-isotrivial families with $\deg a_i(t) \leq 2$ for $i = 2, 4, 6$ which can have non-zero average root number over $\mathbb{Q}$ are $\mathcal{F}_s$ and $\mathcal{G}_w$. See Corollary 4 for the precise statement.

Theorem 1. *Let $a \in \mathbb{Z}_{\neq 0}$. Then $\mathcal{W}_a$ has rank 1 over $\mathbb{Q}(t)$ if and only if $a = \pm k^2$ for some $k \in \mathbb{Z}_{\neq 0}$, and rank 0 otherwise. Also, $\varepsilon_{\mathcal{W}_a}(t)$ is periodic modulo $4|a|$ and one has*

$$(1.4) \quad \varepsilon_{\mathcal{W}_a}(t) \equiv -s_a(t) \gcd(a_2, t) \prod_{p \mid \frac{a_2}{\gcd(a_2, t)}} (-1)^{1+v_p(t)} \left(\frac{t_p}{p}\right)^{1+v_p(t)} \pmod{4},$$

where $s_a(t)$ is defined in Proposition 15, and is a periodic function modulo $2^{v_2(a)+2}$. The average root number of the family $\mathcal{W}_a$ is

$$\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{W}_a}) = - \prod_{p \mid 2a} E_{\mathcal{W}_a}(p),$$

where $E_{\mathcal{W}_a}(p)$ is defined in Proposition 17. In particular, $\mathcal{W}_a$ is a parity-biased family if and only if $v_2(a) \neq 1$. Furthermore, if a is odd and square-free then the average root number of $\mathcal{W}_a$ is

$$(1.5) \quad \text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{W}_a}) = \begin{cases} -1/a & \text{if } a \equiv 1 \pmod{8}, \\ 1/(2a) & \text{if } a \equiv 3 \pmod{8}, \\ -1/(2a) & \text{if } a \equiv 5 \pmod{8}, \\ 1/a & \text{if } a \equiv 7 \pmod{8}. \end{cases}$$

The family $\mathcal{W}_a$ can be seen as a generalization of the well-known Washington's family associated to simplest cubic field and defined by

$$\mathcal{W}_1 : y^2 = x^3 + tx^2 - (t+3)x + 1.$$

One can see that $\mathcal{W}_1$ has rank one over $\mathbb{Q}(t)$ (the point $(0, 1)$ is a point of infinite order) and Rizzo proved that for all $t \in \mathbb{Z}$ one has $\varepsilon_1(t) = -1$ ([Riz03]), whence $\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{W}_1}) = -1$. As a consequence of Theorem 1, one can see that $|\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{W}_a})| = 1$ if and only if $a = \pm 1$ and in that case $\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{W}_a}) = -1$ and the rank of $\mathcal{W}_a$ over $\mathbb{Q}(t)$ is 1. So, $\mathcal{W}_a$ can not directly provide families with elevated rank over $\mathbb{Z}$. However, one can obtain examples of families with elevated rank using subfamilies of $\mathcal{W}_a$; indeed, in Section 4.1.3 we shall prove the following result.

Corollary 2. *Let p be a prime with $p \equiv \pm 1 \pmod{8}$, and let $a, b \in \mathbb{Z}$ be (non zero) quadratic residue and quadratic non-residue modulo p respectively. Then, the families*

$$\begin{aligned} \mathcal{W}_{p,a}^* &: y^2 = x^3 + (pt+a)x^2 - (p^3t+ap^2+3p^4)+p^6 \\ \mathcal{W}_{p,b}^{**} &: y^2 = x^3 + (pt+b)x^2 - (p^2t+3p^2+pb)x + p^3 \end{aligned}$$

are both families with elevated rank over $\mathbb{Z}$. More precisely, $\mathcal{W}_{p,a}^*$ has rank 1 over $\mathbb{Q}(t)$ with $\varepsilon_{\mathcal{W}_{p,a}^*}(t) = 1$ for all $t \in \mathbb{Z}$, and $\mathcal{W}_{p,b}^{**}$ has rank 0 over $\mathbb{Q}(t)$ and $\varepsilon_{\mathcal{W}_{p,b}^{**}}(t) = -1$ for all $t \in \mathbb{Z}$.

We in fact have $\mathcal{W}_{p,a}^*(t) = \mathcal{W}_{p^2}(pt+a)$ and $\mathcal{W}_{p,b}^{**}(t) = \mathcal{W}_p(pt+b)$. One can also use $\mathcal{W}_a(t)$ to construct families with elevated rank and with rank 2 or 3 over $\mathbb{Q}(t)$ (see Section 4.1.3).

We shall also focus on another subfamily of $\mathcal{F}_s$, namely the subfamily

$$\mathcal{V}_a : y^2 = x^3 + 3tx^2 + 3atx + a^2t.$$

Notice that $\mathcal{V}_a(t)$ is isomorphic to $\mathcal{F}_{4a^2}(4t-2a)$.

Theorem 2. *Let $a \in \mathbb{Z}_{\neq 0}$. Then,*

$$\begin{aligned} \varepsilon_{\mathcal{V}_a}(t) &= w_2(t) w_3(t) \prod_{\substack{p \geq 5 \\ 0 \leq v_p(a) \leq v_p(t)}} \begin{cases} \left(\frac{-3}{p}\right) \left(\frac{3}{p}\right)^{v_p(t)+v_p(t-a)+v_p(a)} & \text{if } 6 \nmid v_p(t-a) - v_p(t) + 3v_p(a), \\ 1 & \text{if } 6 \mid v_p(t-a) - v_p(t) + 3v_p(a), \end{cases} \\ &\times \prod_{\substack{p \geq 5 \\ 0 \leq v_p(t) < v_p(a)}} \begin{cases} -\left(\frac{3t_p}{p}\right) & \text{if } v_p(t) \text{ is even} \\ \left(\frac{-1}{p}\right) & \text{if } v_p(t) \text{ is odd,} \end{cases} \end{aligned}$$

where $w_2(t)$ and $w_3(t)$ are given by Proposition 43 and 42 of Appendix B. Also,

$$\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{V}_a}) = - \prod_{p \text{ prime}} E_{\mathcal{V}_a}(p),$$

where $E_{\mathcal{V}_a}(p)$ are defined in Proposition 24. In particular, $\mathcal{V}_a$ is a parity-biased family if and only if $v_2(a) \neq 1$. Finally, if $a = \pm 1$ we have

$$(1.6) \quad \text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{V}_a}) = -\frac{1}{21} \prod_{\substack{p \geq 5 \\ p \equiv 2 \pmod{3}}} \left(1 - \frac{4(p-1)(p^3+p)}{p^6-1} \right) \approx 0.038562 \dots$$

We remark that the same method used to prove (1.5) and (1.6) can also be used for computing the average root number for all the other families given in (1.3) (conditionally on the square-free sieve conjecture in the case of $\mathcal{L}_{w,s,v}$ and unconditionally in all other cases, cf. Remark 1).

We are also able to obtain new results on the possible numbers that can arise as average root numbers. Before stating them we need some more notation.

We let $\mathfrak{F}$ be the set of all families of elliptic curves over $\mathbb{Q}$, and $\mathfrak{F}_i$ and $\mathfrak{F}'$ be the subset of $\mathfrak{F}$ consisting of the isotrivial and of the non-isotrivial families respectively. Furthermore, we let $\mathfrak{F}_{\mathbb{Z}}$ be the subset of $\mathfrak{F}$ consisting of the families $\mathcal{F}$ such that $\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}})$ exists. Similarly, define $\mathfrak{F}_{i,\mathbb{Z}}$ and $\mathfrak{F}'_{\mathbb{Z}}$. By the work of Helfgott (see Theorem 6 below) we know, under Chowla's and the square-free sieve conjectures (see the next section for their statements), that $\mathfrak{F} = \mathfrak{F}_{\mathbb{Z}}$ and thus also $\mathfrak{F}_i = \mathfrak{F}_{i,\mathbb{Z}}$ and $\mathfrak{F}' = \mathfrak{F}'_{\mathbb{Z}}$. Furthermore, we indicate by $\mathfrak{F}_p$ the set of families $\mathcal{F}$ such that $\varepsilon_{\mathcal{F}}(t)$ is a periodic function for almost all $t \in \mathbb{Z}$ (i.e. the set of exceptional t with $|t| \leq T$ is $o(T)$ as $T \rightarrow \infty$).

Finally, with a slight abuse of notation we write $\text{Av}_{\mathbb{Z}}(\mathfrak{F}_{\mathbb{Z}}) := \{\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}}) \mid \mathcal{F} \in \mathfrak{F}_{\mathbb{Z}}\}$ and similarly for $\text{Av}_{\mathbb{Z}}(\mathfrak{F}_{i,\mathbb{Z}})$, etc.

Theorem 3. *We have*

$$\{\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}}) \mid \mathcal{F} \in \mathfrak{F}_{\mathbb{Z}}\} \supseteq \mathbb{Q} \cap [-1, 1].$$

In particular, $\text{Av}_{\mathbb{Z}}(\mathfrak{F}_{\mathbb{Z}})$ is dense in $[-1, 1]$. Moreover, the same result holds true also for $\text{Av}_{\mathbb{Z}}(\mathfrak{F}'_{\mathbb{Z}})$ and $\text{Av}_{\mathbb{Z}}(\mathfrak{F}_{i,\mathbb{Z}})$.

Under Chowla's and the square-free sieve conjectures we can also classify all average root numbers that can arise from families with periodic root number.

Theorem 4. *We have*

$$(1.7) \quad \text{Av}(\mathfrak{F}_{p,\mathbb{Z}}) \supseteq \{h/k \in \mathbb{Q} \cap [-1, 1] \mid h \text{ odd, and if } k \text{ even then } |h/k| \leq 1 - 2^{-v_2(k)}\}.$$

Moreover, assuming Conjecture 1 and Conjecture 2, the equality holds.

We can also obtain an analogue of Theorem 3 in the case of averages over $\mathbb{Q}$. Analogously to $\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}})$, we define

$$(1.8) \quad \text{Av}_{\mathbb{Q}}(\varepsilon_{\mathcal{F}}) := \lim_{T \rightarrow \infty} \frac{\pi^2}{12T^2} \sum_{\substack{|r|, |s| \leq T, \\ s > 0, (r,s)=1}} \varepsilon_{\mathcal{F}}(r/s)$$

if the limit exists. Also, we let $\mathfrak{F}_{\mathbb{Q}}$ be the set of families $\mathcal{F}$ where $\text{Av}_{\mathbb{Q}}(\mathcal{F})$ exists, and $\mathfrak{F}_{i,\mathbb{Q}}$ and $\mathfrak{F}'_{\mathbb{Q}}$ be the subsets of $\mathfrak{F}_{\mathbb{Q}}$ consisting of the isotrivial and non-isotrivial families.

Rizzo [Riz99], building on the work of Rohrlich [Roh93], proved that $\text{Av}_{\mathbb{Q}}(\mathfrak{F}_{i,\mathbb{Q}})$ (and thus $\text{Av}_{\mathbb{Q}}(\mathfrak{F}_{\mathbb{Q}})$) is dense in $[-1, 1]$. In a similar direction, Klagsbrun, Mazur and Rubin [KMR13] prove an analogous result for the parity of the ranks of the 2-Selmer groups in isotrivial families defined over number fields (with techniques which are completely different from the ones of the present paper). The following theorem refine Rizzo's result, showing $\text{Av}_{\mathbb{Q}}(\mathfrak{F}_{i,\mathbb{Q}})$ actually contains $[-1, 1] \cap \mathbb{Q}$. Moreover, also in this case we are able to address the case of non-isotrivial families, showing that $\text{Av}_{\mathbb{Q}}(\mathfrak{F}'_{\mathbb{Q}})$ is dense in $[-1, 1]$.

Theorem 5. *We have that $\text{Av}_{\mathbb{Q}}(\mathfrak{F}'_{\mathbb{Q}})$ is dense in $[-1, 1]$. Moreover, we have that $\text{Av}_{\mathbb{Z}}(\mathfrak{F}_{i, \mathbb{Q}}) \supseteq [-1, 1] \cap \mathbb{Q}$ (and thus, a fortiori, $\text{Av}_{\mathbb{Q}}(\mathfrak{F}_{\mathbb{Q}}) \supseteq [-1, 1] \cap \mathbb{Q}$).*

Notice that in the case of $\text{Av}_{\mathbb{Q}}(\mathfrak{F}'_{\mathbb{Q}})$ we do not get $[-1, 1] \cap \mathbb{Q}$. We remark that there are reasons to believe that in fact $\text{Av}_{\mathbb{Q}}(\mathfrak{F}'_{\mathbb{Q}}) \cap \mathbb{Q} = \{0\}$. Indeed, by the work of Helfgott (cf. [CCH05, Appendix A]) and Desjardins [Des16a] one has (conjecturally) that for a non-isotrivial family $\mathcal{F}$ with $\text{Av}_{\mathbb{Q}}(\varepsilon_{\mathcal{F}}) \neq 0$, the average root number of $\mathcal{F}$ over $\mathbb{Q}$ can be written as a convergent Euler product $\text{Av}_{\mathbb{Q}}(\varepsilon_{\mathcal{F}}) = c_{\infty} \prod_p (1 - r_p)$ for some $c_{\infty} \in \overline{\mathbb{Q}} \cap [-1, 1]$ and some r_p which are rational polynomials in p satisfying $0 \leq r_p(p) < 1$, $r_p \ll p^{-2}$ for all p and $r_p > 0$ for infinitely many p .⁵ In particular, one has $\text{Av}_{\mathbb{Q}}(\varepsilon_{\mathcal{F}}) \neq \pm 1$, and one also expects that such an infinite product is not algebraic.

We shall prove Theorem 3, 4 and 5 by considering subfamilies of $\mathcal{W}_a(t)$ where both t and the parameter a are replaced by polynomials in $\mathbb{Z}[t]$. By Theorem 1, we know exactly the root number for all the elliptic curves in these families, and so the problem becomes that of choosing suitably these polynomials. In the case of averages over $\mathbb{Q}$, we can reduce to the case where the ∞ -factor of the root number essentially determines $\varepsilon_{\mathcal{F}}(t)$, whereas in the case of Theorem 3 we work with the p -factor of the root number for a suitably chosen p . The proof of Theorem 4 is a bit more elaborate and requires dealing with the factors of the root number corresponding to all prime divisors of $6k$.

The organization of the paper is as follow. In Section 2 we discuss more in depth the work of Helfgott and we give our classification of the potentially parity-biased families with coefficients of low degree. In Section 3 we compute the ranks for the families given in (1.3). In Section 4 we compute the average root numbers of the families $\mathcal{W}_a$ and $\mathcal{V}_a$. In Section 5 we use the results proven in Section 4 to prove Theorem 3, 4 and 5. Finally, in Appendix A and B we give the local root numbers of the families $\mathcal{F}_s$ and $\mathcal{V}_a$. Finally, this work led to many technical computation (root number, local average of root number, ...), we used the PARI/GP software ([PAR16]) to intensively check them when it was relevant.

Acknowledgements. The authors would like to thank Jake Chinis, Julie Desjardins, Ottavio Rizzo, Joseph Silverman and Jamie Weigandt for helpful discussions. This work was initiated while the first author was a post-doctoral fellow at the Centre de Recherche Mathématiques (CRM) in Montréal, and completed during several visits of the third author at the CRM, and we are grateful to the CRM for providing very good facilities. The research of the second author is partially supported by the National Science and Engineering Research Council of Canada (NSERC). The third author was partially supported by the Région Franche-Comté (Projet Région).

2. THE CLASSIFICATION OF POTENTIALLY PARITY-BIASED FAMILIES OF LOW DEGREE

2.1. The work of Helfgott and its consequences. We start with a more detailed discussion of the work of Helfgott ([Hel09, Hel03]) which gives (conditionally) a necessary condition for a family to be potentially parity-biased. First, we state the following conjectures.

Conjecture 1 (Chowla's conjecture). *Let $P(x) \in \mathbb{Z}[x]$ be square-free. Then, $\sum_{n \leq N} \lambda(P(n)) = o(N)$ as $N \rightarrow \infty$, where $\lambda(n)$ is the Liouville function $\lambda(n) := \prod_{p|n} (-1)^{v_p(n)}$.*

Moreover, by *strong Chowla's conjecture* for a polynomial P we mean the assumption that Chowla's conjecture holds for $P(ax + b)$ for all $a, b \in \mathbb{Z}$, $a \neq 0$.

Conjecture 2 (Square-free sieve conjecture). *Let $P(x)$ be a square-free polynomial in $\mathbb{Z}[x]$. Then, the set of integers n such that $P(n)$ is divisible by the square of a prime which is larger than $\sqrt{n}$ has density 0.*

Conjectures 1 and 2 are believed to hold for all square-free polynomials P . Chowla's conjecture is known for polynomials of degree 1 only, whereas the square-free sieve conjecture is known for polynomials whose irreducible factors have degrees ≤ 3 ([Hel04]).

⁵In the proof of Corollaire 2.5.4. of [Des16a] it is shown that $r_p > 0$ for at least one p , but the same proof actually carries over to show that there are infinitely many such p .

Theorem 6 (Helfgott). *Let $\mathcal{F}$ be a family of elliptic curves. Let $M_{\mathcal{F}}(t)$ and $B_{\mathcal{F}}(t)$ be the polynomials defined by*

$$(2.1) \quad M_{\mathcal{F}}(t) := \prod_{\substack{v \text{ mult,} \\ v \neq -\deg}} Q_v(t), \quad B_{\mathcal{F}}(t) := \prod_{\substack{v \text{ quite bad,} \\ v \neq -\deg}} Q_v(t)$$

where the products are over the valuations v of $\mathbb{Q}(t)$ where $\mathcal{F}$ has multiplicative and quite bad⁶ reductions respectively and where $Q_v(t)$ is the polynomial associated to the place v . Then for all but finitely many $t \in \mathbb{Z}$ one has

$$\varepsilon_{\mathcal{F}}(t) = \text{sign}(g_{\infty}(t)) \lambda(M_{\mathcal{F}}(t)) \prod_{p \text{ prime}} g_p(t)$$

where $g_{\infty}(t)$ is a polynomial, S is a finite set of (rational) primes depending on $\mathcal{F}$ and $g_p : \mathbb{Q}_p \rightarrow \{\pm 1\}$ are functions satisfying

- a) $g_p(t)$ is locally constant outside a finite set of points;
- b) if $p \notin S$ then $g_p(t) = 1$ unless $v_p(B_{\mathcal{F}}(t)) \geq 2$.

Moreover, if $\mathcal{F}$ has at least one place of multiplicative reduction other than $-\deg$, then assuming the square-free sieve conjecture for $B_{\mathcal{F}}(t)$ and the strong Chowla's conjecture for $M_{\mathcal{F}}(t)$, one has $\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}}) = 0$.

If $\mathcal{F}$ has no place of multiplicative reduction other than $-\deg$ (i.e. $\mathcal{F}$ is potentially parity-biased), then assuming the square-free sieve conjecture for $B_{\mathcal{F}}(t)$ we have

$$(2.2) \quad \text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}}) = \frac{c_- + c_+}{2} \prod_p \int_{\mathbb{Z}_p} g_p(t) dt,$$

where dt denotes the usual p -adic measure and $c_{\pm} = \lim_{t \rightarrow \pm\infty} g_{\infty}(t)$.

The case where $\mathcal{F}$ is potentially parity-biased was also considered by Rizzo [Riz03] in two examples which already contain several of the important ideas for the general result. We also mention the recent work of Desjardins [Des16b] who revisited Helfgott's result, and relaxed some of the assumptions.

We now give a sketch of the proof of Helfgott's result, as it reveals quite clearly the way to proceed when computing $\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}})$.

Sketch of the proof of Theorem 6. The root number of an elliptic curve $\mathcal{F}(t)$ in the family $\mathcal{F}$ is defined as a product of local root numbers $\varepsilon_{\mathcal{F}}(t) = -\prod_p w_p(t)$, where $w_p(t)$ depends on the reduction type of $\mathcal{F}(t)$ modulo p . Naively, one might expect that $\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}}) = -\prod_p \int_{\mathbb{Z}_p} w_p(t) dt$ however this is false in general (the product on the right is typically non-convergent). One can however modify the $w_p(t)$ to some $w_p^*(t)$ so that one still has $\varepsilon(t) = -\prod_p w_p^*(t)$, but in this case (conjecturally) $\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}}) = -\prod_p \int_{\mathbb{Z}_p} w_p^*(t) dt$.

First, we recall that for $p \geq 5$ one has that $w_p(t) = 1$ if $\mathcal{F}(t)$ has good reduction at p , $w_p(t) = \left(\frac{j_p(t)}{p}\right)$ (where $(\cdot)$ is the Kroeneker symbol) if $\mathcal{F}(t)$ has bad, non-multiplicative reduction at p , where $-j_p(t) = 1, 2, 3$ depending on the reduction type⁷, and $w_p(t) = -\left(\frac{j_p(t)}{p}\right)$ if $\mathcal{F}(t)$ has multiplicative reduction at p where in this case $j_p(t)$ is the first non-zero p -adic digit of the invariant $c_6(t)$. Thus,

$$(2.3) \quad \varepsilon_{\mathcal{F}}(t) = -w_2(t)w_3(t)(-1)^{\#\{p: \mathcal{F}(t) \text{ has mult. red. at } p\}} \prod_{p \text{ bad}} \left(\frac{j_p(t)}{p}\right)$$

where the product is over primes p such that $\mathcal{F}(t)$ has bad reduction at p . Now, the key step is to observe that essentially $\mathcal{F}(t)$ has a certain reduction type at p if and only if there is a place $v \neq -\deg$

⁶That is, if no quadratic twist of $\mathcal{F}$ has good reduction at v .

⁷For example $j_p = -3$ if $v_p(c_4(t), c_6(t), \Delta(t)) \equiv (r, 2, 4) \pmod{12}$ for some $r \geq 2$ or $v_p(c_4, c_6, \Delta) \equiv (r, 4, 8) \pmod{12}$ for some $r \geq 3$.

over $\mathbb{Q}(t)$ where $\mathcal{F}$ has the same reduction type and $p|Q_v(t)$. The only exceptions to this are when p is in a finite set of primes S (depending on the family $\mathcal{F}$ only, essentially this amounts to excluding the finitely many primes that divide more than one Q_v) and when p divides $Q_v(t)$ with multiplicity greater than 1. It follows that

$$\begin{aligned} \varepsilon_{\mathcal{F}}(t) &= -(-1)^{\#\{p \notin S, p||Q_v(t) \text{ } v \text{ place of mult red.}\}} \prod_{p \in S} w_p(t) \cdot \prod_{\substack{v \text{ bad,} \\ v \neq -\deg}} \prod_{\substack{p||Q_v(t), \\ p \notin S}} \left(\frac{j_p(t)}{p} \right) \cdot \prod_{\substack{v \text{ bad,} \\ v \neq -\deg}} \prod_{\substack{p^2|Q_v(t), \\ p \notin S}} h_p(t) \\ &= (-1)^{\#\{p|M_{\mathcal{F}}(t)\}} \prod_{p \in S} w_p^*(t) \cdot \prod_{i=1}^3 \prod_{v \in V_i} \prod_p \left(\frac{-i}{p} \right)^{v_p(Q_v(t))} \\ &\quad \times \prod_{v \text{ mult.}} \prod_p \left(\frac{c'_6(t)}{p} \right)^{v_p(Q_v(t))} \cdot \prod_{\substack{v \text{ bad,} \\ v \neq -\deg}} \prod_{\substack{p^2|Q_v(t), \\ p \notin S}} h_p^*(t) \end{aligned}$$

for some finite set of primes S , some functions $h_p(t), h_p^*(t), w_p(t), w_p^*(t)$ which are p -locally constants on $\mathbb{Z}_p$ outside a finite set of points, and a suitable partition $V_1 \cup V_2 \cup V_3$ of the set $\{v \text{ bad}, v \neq -\deg\}$.⁸ Then,⁹

$$\varepsilon_{\mathcal{F}}(t) = (-1)^{\#\{p|M_{\mathcal{F}}(t)\}} \prod_{p \in S} w_p^*(t) \cdot \prod_{i=1}^3 \prod_{v \in V_i} \left(\frac{-i}{Q_v(t)} \right) \cdot \prod_{v \text{ mult.}} \left(\frac{c_6(t)}{Q_v(t)} \right) \cdot \prod_{\substack{v \text{ bad,} \\ v \neq -\deg}} \prod_{\substack{p^2|Q_v(t), \\ p \notin S}} h_p^*(t)$$

Now, applying repeatedly quadratic reciprocity one sees that the factor $\left(\frac{c_6(t)}{Q_v(t)} \right)$ also depends on the $\mathbb{Z}_q$ expansion of t at finitely many primes q and on the sign of a polynomial and the same is true for $\left(\frac{-i}{Q_v(t)} \right)$.¹⁰ Finally, one can verify directly that $h_p^*(t) = 1$ if $\mathcal{F}(t)$ has bad but not quite-bad reduction at p . Thus,

$$\varepsilon_{\mathcal{F}}(t) = \lambda(M_{\mathcal{F}}(t)) \text{sign}(h_{\infty}(t)) \prod_{p \in S'} w_p^{***}(t) \prod_{\substack{p^2|B_{\mathcal{F}}(t), \\ p \notin S'}} h_p^*(t)$$

for a finite set of primes S' , some $w_p^{***}(t)$ p -locally constant outside a finite set of points and a polynomial $h_{\infty}(t)$. Thus, we obtain the first assertion of Theorem 6. The other assertions are easy once one observes that the square-free sieve conjecture for $B_{\mathcal{F}}(t)$ gives

$$\lim_{T \rightarrow \infty} \frac{1}{T} \sum_{0 \leq \pm t \leq T} \varepsilon_{\mathcal{F}}(t) = \lim_{X \rightarrow \infty} \lim_{T \rightarrow \infty} \frac{c_{\pm}}{T} \sum_{0 \leq \pm t \leq T} \lambda(M_{\mathcal{F}}(\pm t)) \prod_{p \in S'} w_p^{***}(\pm t) \prod_{\substack{p^2|B_{\mathcal{F}}(\pm t), \\ p \notin S', \\ p \leq X}} h_p^*(\pm t).$$

Notice that the product on the right involves finitely many primes (for each X). Thus, if $M_{\mathcal{F}}(t) \neq 1$ then dividing into congruence classes modulo these primes one has that the strong Chowla's conjecture for $M_{\mathcal{F}}(t)$ gives that the average is 0. Otherwise, the limit over T coincides with the product of the

⁸For example V_3 is the set of places $w \neq -\deg$ of $\mathbb{Q}(t)$ such that $v_w(c_4(t), c_6(t), \Delta(t)) \equiv (r, 2, 4) \pmod{12}$ for some $r \geq 2$ or $v_p(c_4, c_6, \Delta) \equiv (r, 4, 8) \pmod{12}$ for some $r \geq 3$.

⁹We ignore the minor issue of the case where the top and bottom of the various Legendre symbol are not coprime.

¹⁰For example, if $Q_v(t) \neq 0$, then $\left(\frac{-1}{Q_v(t)} \right) = \text{sign}(Q_v(t))\chi(Q_v(t)_2)$, where χ is the non-principal character $\pmod{4}$ and $Q_v(t)_2 = Q_v(t)2^{-v_2(Q_v(t))}$.

p -adic integral (see [Hel09] or also [Riz03]) and, writing $h_p^*(t) = 1$ if $v_p(B_{\mathcal{F}}(t)) < 2$, we have

$$\begin{aligned} \lim_{T \rightarrow \infty} \frac{1}{T} \sum_{0 \leq \pm t \leq T} \varepsilon_{\mathcal{F}}(t) &= c_{\pm} \lim_{X \rightarrow \infty} \prod_{p \in S'} \int_{\mathbb{Z}_p} w_p^{***}(t) dt \prod_{\substack{p \notin S', \\ p \leq X}} \int_{\mathbb{Z}_p} h_p^*(t) dt \\ &= c_{\pm} \prod_{p \in S'} \int_{\mathbb{Z}_p} w_p^{***}(t) dt \prod_{p \notin S'} \int_{\mathbb{Z}_p} h_p^*(t) dt \end{aligned}$$

with $\int_{\mathbb{Z}_p} h_p^*(t) dt = 1 + O(p^{-2})$. $\square$

Notice that Theorem 6 implies, under Chowla's and the square-free sieve conjectures, that $\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}})$ exists for all families $\mathcal{F}$. Moreover, recalling Definition 1, we have the following implications

$$\begin{array}{ccccc} \text{elevated} & \implies & \text{Parity} & \xrightarrow[\text{Helfgott}]{\text{Conj.}} & \text{Potentially} \\ \text{rank} & & \text{biased} & & \text{parity-biased.} \end{array}$$

The first implication is trivial and the converse is false in general since there are examples with $\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}}) \notin \{-1, 0, 1\}$ (see [Riz03, Hel09] or also Theorem 1). The second implication comes from Theorem 6 and is conjectural in full generality. The converse is also false in general (see Theorem 1 with $a = 2$), however assuming the square-free sieve conjecture one has that every potentially biased family $\mathcal{F}$ has a parity-biased subfamily (obtained by taking t to be in an arithmetic progression and/or restricting to $t > 0$ ¹¹). Indeed, the potentially biased families are the ones for which some of the integrals in (2.2) are equal to 0 or with $c_+ = -c_-$. Fixing the sign of t and restricting t to be in a suitably selected congruence class one can make those integrals (as well as all the other ones) non-zero.

2.2. Potentially biased families. In this section, we find all potentially biased families such that $\deg a_i(t) \leq 2$. We first start by the case with a family $\mathcal{F}(t): y^2 = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t)$ where $\deg a_2 \leq 1$ and $\deg a_4, a_6 \leq 2$. We write $a_2(t) = ut + v$, $a_4(t) = at^2 + bt + c$ and $a_6(t) = dt^2 + et + f$. We denote by c_4, c_6, Δ and j the classical invariants of $\mathcal{F}(t)$. Notice that the potentially biased condition is equivalent to the fact that all the roots of Δ are also roots of c_4 . One can see that if Δ is constant then either $\Delta = 0$ or the family does not depend on t (i.e. $a = b = d = e = u = 0$).

We also notice that if $u^2 - 4a$ is a square, say $u^2 - 4a = r^2$ for $r \in \mathbb{Q}$, then the family doesn't change under the transformation

$$(2.4) \quad \begin{aligned} a &\leftrightarrow \frac{1}{2}(-4a + u^2 - ur), & u &\leftrightarrow \frac{1}{2}(-u + 3r), & b &\leftrightarrow b - uv + rv, \\ e &\leftrightarrow \frac{1}{2}(2e - cu + cr), & d &\leftrightarrow \frac{1}{2}(2d - bu + br - 2av + u^2v - urv) \end{aligned}$$

(and a suitable linear transformation in x).

Theorem 7. *Let $a_2(t), a_4(t)$ and $a_6(t)$ be polynomials in $\mathbb{Q}[t]$ with $\deg a_2(t) \leq 1$, $\deg a_4(t) \leq 2$, $\deg a_6(t) \leq 2$ and such that the curve $\mathcal{F}(t): y^2 = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t)$ is non-isotrivial and potentially parity-biased. Then the family has rank ≤ 1 over $\mathbb{Q}(t)$ and, up to some rational linear change of variables in the parameter t and in the variables x and y , the family is either*

$$\mathcal{F}_s: y^2 = x^3 + 3tx^2 + 3sx + st$$

for some $s \in \mathbb{Z}_{\neq 0}$ and with rank 1 if and only if $s = -12k^4$ with $k \in \mathbb{N}$; or

$$\mathcal{G}_w: wy^2 = x^3 + 3tx^2 + 3tx + t^2$$

for some $w \in \mathbb{Z}_{\neq 0}$ and with rank 1 if and only if w is a square or -2 times a square.

Proof. Here we shall only show that all non-isotrivial and potentially parity-biased families satisfying the above conditions are of the form $\mathcal{F}_s$ or $\mathcal{G}_w$. We will compute their ranks in Section 3, Propositions 5 and 8.

¹¹Alternatively one can for example replace t by t^2 .

We remind that $c_4 = 16(a_2^2 - 3a_4)$, $c_6 = 32(-2a_2^3 + 9a_4a_2 - 27a_6)$ and $1728\Delta = c_4^3 - c_6^2$. Thus, with our assumptions and the discussion above, we have $1 \leq \deg c_4 \leq 2$, $\deg c_6 \leq 3$ and one easily checks that $\deg \Delta$ can't be 1 and thus $2 \leq \deg \Delta \leq 6$.

Now, we observe that c_4 has to be square-free. Indeed, if $c_4 = \ell L^2$ for some $\ell \in \mathbb{Q}_{\neq 0}$ (for $\ell = 0$ the family is iso-trivial) and a degree one polynomial L , then since $\mathcal{F}$ is potentially parity-biased we can write Δ as $1728\Delta = kL^m$ for some $k \in \mathbb{Q}_{\neq 0}$ and some $2 \leq m \leq 6$. Then we have $c_6^2 = L^m(\ell P^{6-m} - k)$, so $m \in \{0, 2, 4\}$ (if $m = 6$, then the family is iso-trivial) and $\ell L^{6-m} - k$ is a square in $\mathbb{Q}(t)$ which is clearly not possible since $\ell L^{6-m} - k$ is square-free. Also, we must have $\deg(c_4) \geq 2$. Indeed, if $c_4 = L$, $1728\Delta = kL^m$, for some linear polynomial $L \in \mathbb{Q}(t)$, some $k \in \mathbb{Q}_{\neq 0}$ and some $m \in \mathbb{N}$, then we'd have $L^3 - kL^m$ is a square in $\mathbb{Q}(t)$ which is clearly not possible.

Now, suppose that c_4 is square-free of degree 2. Then, $c_4 = L_1L_2$ for some coprime linear polynomials $L_1, L_2 \in \mathbb{C}[t]$. We can write Δ as $1728\Delta = kL_1^mL_2^n$ for some $k \in \mathbb{Q}_{\neq 0}$ and some $m, n \in \mathbb{N}$ with $2 \leq m+n \leq 6$, $m \leq n$. Thus $L_1^mL_2^n(L_1^{3-m}L_2^{3-n} - k) = c_6^2$ is a square in $\mathbb{Q}(t)$. In particular, it can't be $m = n = 3$, nor $m = 0, n = 3$ (since $L_1^3 - k$ is square-free). Moreover, it can't be $m = 0, n = 2$ as this would imply that $L_1^3L_2 - k$ is a square in $\mathbb{C}(t)$ which is not possible (indeed, we can assume $L_1 = t$ and $L_2 = t - 1$, then for $k \neq 0$ the discriminant of $t^3(t-1) - k$ is zero only for $k = -\frac{27}{256}$ in which case $t^3(t-1) - k$ is not a square). Thus, we must have either $m = n = 2$ or $m = 2, n = 3$. Thus, we have two cases:

- (1) $c_4 = P$, $1728\Delta = kP^2$ for some $P \in \mathbb{Q}[t]$ of degree 2 and some $k \in \mathbb{Q}_{\neq 0}$;
- (2) $c_4 = L_1L_2$, $1728\Delta = kL_1^2L_2^3$ for some coprime $L_1, L_2 \in \mathbb{Q}[t]$ of degree 1 and some $k \in \mathbb{Q}_{\neq 0}$.

First, let's consider the case where c_4 has degree 2 and $1728\Delta = kc_4^2$. Notice that we can not have $a = 0$ and $u = 0$ at the same time (otherwise c_4 would be a degree ≤ 1 polynomial). Since $\deg \Delta = 4$, we must have $a = d = 0$ or $a = u^2/4$ and $d = (2ub - u^2v)/4$. By the transformations (2.4) the two cases lead to the same families, so it suffices to consider the case $a = d = 0$ only.

Now, we have $c_6^2 = c_4^2(c_4 - k)$ and so $c_4 - k$ is a square in $\mathbb{Q}[t]$, a condition which univocally determines k in terms of the other parameters. With this choice for k we have $c_4 - k = 16(ut + v - \frac{3b}{2u})^2 = (4a_2 - \frac{6b}{u})^2$. Thus, we have $c_6 = \pm c_4(4a_2 - \frac{6b}{u})$ and comparing the terms of degree 3 in t we see that we must take the minus sign. Expressing c_4 and c_6 in terms of the a_i and simplifying this equality becomes

$$6(a_4 - a_2b/u)a_2 - 54a_6 = -18a_4b/u$$

or, equivalently, $6(c - bv/u)a_2 + 18a_4b/u = 54a_6$. Comparing the terms of degree 1 and 2 in t we obtain

$$\begin{cases} 6(c - bv/u)u + 18b^2/u = 54e, \\ 6(c - bv/u)v + 18bc/u = 54f \end{cases} \Rightarrow \begin{cases} c = (9eu + bvu - 3b^2)/u^2, \\ f = (3ebu - b^3 + evu^2)u^3 \end{cases}$$

(remember we have $u \neq 0$) and so we are led to the families

$$y^2 = x^3 + (ut + v)x^2 + \left(bt + \frac{9eu + bvu - 3b^2}{u^2}\right)x + et + \frac{3ebu - b^3 + evu^2}{u^3}.$$

We make the changes $b \leftrightarrow -bu$ and $e \leftrightarrow eu$ in order to kill the denominator and we make the change of variables $ut + v \leftrightarrow t$. We arrive to

$$(2.5) \quad \mathcal{F}: y^2 = x^3 + tx^2 + (-bt - 3b^2 + 9e)x + et + b^3 - 3eb.$$

Finally, we make the changes of variables $t \leftrightarrow 3t - 3b/2$, $x \leftrightarrow x + b/2$ and write $e = s/3 + b^2/4$ and obtain $\mathcal{F}_s$, with associated invariants

$$(2.6) \quad \begin{aligned} c_4(t) &= 144(t^2 - s), \\ c_6(t) &= -1728t(t^2 - s), \\ \Delta(t) &= -1728s(t^2 - s)^2. \end{aligned}$$

Notice that if $d \neq 0$, then the changes $t \leftrightarrow t/d^2$, $x \leftrightarrow d^2x$, $y \leftrightarrow d^3y$ transform $\mathcal{F}_s$ into $\mathcal{F}_{sd^4}(t)$ and so in particular we can always reduce to the case where $s \in \mathbb{Z}_{\neq 0}$.

Now, let's consider the second case. Up to a linear change of variables in t we can assume c_4 has the form $c_4 = Ct(t-1)$ and $1728\Delta = 2^{12}kt^3(t-1)^2$ for some $k \neq 0$. Comparing this expression of c_4 with its definition, we see that we must have $C = 2^4(u^2 - 3a)$, $c = v^2/3$ and $b = \frac{1}{3}(u^2 + 2uv - 3a)$. Since $\deg \Delta = 5$, we have $a = 0$ or $4a - u^2 = 0$ and as before it suffices to consider the case $a = 0$ (and hence $u \neq 0$). Now, $c_6^2 = c_4^3 - 1728\Delta = 2^{12}u^6t^3(t-1)^2(t-1-k)$ and thus $k = -1$ and so $c_6 = \pm 2^6u^3t^2(t-1)$ and again we need to take the minus sign. Comparing the coefficients of the polynomials in t we find

$$\begin{cases} -864f + 32v^3 = 0 \\ -864e + 96u^2v + 96uv^2 = 0 \\ -864d + 96u^3 = 64u^3 \end{cases} \Rightarrow \begin{cases} f = v^3/27 \\ e = (u^2v + uv^2)/9 \\ d = u^3/27 \end{cases}$$

Making the change of variable $x \leftrightarrow x - v/3$, we then obtain that the dependence of v disappear and we obtain the families

$$y^2 = x^3 + tux^2 + \frac{1}{3}tu^2x + \frac{1}{27}u^3t^2.$$

Writing $u = 3w$ and making the change of variables $x \leftrightarrow wx$ and $y \leftrightarrow w^2y$ we obtain $\mathcal{G}_w(t)$ with

$$(2.7) \quad \begin{aligned} c_4(t) &= 12^2w^2t(t-1), \\ c_6(t) &= -12^3w^3t^2(t-1), \\ \Delta(t) &= -12^3w^6rt^3(t-1)^2. \end{aligned}$$

□

We can extend Theorem 7 to the case where $\deg a_2(t) = 2$. First we give the following Lemma which will allow us to exclude several cases. One could also rule out these cases by using Kodaira's classification of singular fibers [Mir95].

We remark that when performing the computations needed in the proofs of Lemma 3 and Theorem 7 we used Mathematica and PARI/GP.

Lemma 3. *Let R_1, R_2, S and L be polynomials in $\mathbb{C}[t]$ of degree 2, 2, 3 and 1 respectively. Let $k \in \mathbb{C} \setminus \{0\}$. Then*

- a) $R_1^3 - k$ can't be divisible by the square of a degree 2 polynomial in $\mathbb{C}[t]$.
- b) $R_1^3R_2 - k$ can't be a square in $\mathbb{C}[t]$.
- c) $LR_1^3 - k$ can't be divisible by the square of a degree 3 polynomial in $\mathbb{C}[t]$.
- d) $LS^3 - k$ can't be a square in $\mathbb{C}[t]$.
- e) $S^3 - k$ can't be divisible by the square of a degree 4 polynomial in $\mathbb{C}[t]$.
- f) $L^4R_1 - k$ can't be a square in $\mathbb{C}[t]$.

Proof. We only prove the first two statements, the proofs of the other ones being very similar.

- a) We can assume $R_1 = t^2 + 1$ or $R_1 = t^2$. In the second case the statement is obvious, thus assume $R_1 = t^2 + 1$. The discriminant of $R_1^3 - k$ is $6^6k^4(k-1)$ and thus it is zero only if $k = 1$, but $R_1^3 + 1 = t^2(3 + 3t^2 + t^4)$ and the second factor is not a square.
- b) We can assume $R_2 = t^2 + bt + c$ and $R_1 = t^2 + 1$ or $R_1 = t^2$; we consider the first case only, the second one being a bit simpler. If $C := R_1^3R_2 - k$ is the square of a degree 4 polynomials, then C and C' have at least 4 zeros in common and thus the first 4 subresultants of C and C' are zero. The fourth subresultant is a non-zero multiple of $(b^2 - 4c)(c - 1 + ib)^2(c - i - ib)^2$. If $c = b^2/4$, then the third subresultant is a non-zero multiple of $(4 + b^2)^2$ and thus we need $a = \pm 2i$, but with this choice the second subresultant is $2^{17} \cdot 3 \cdot 5 \cdot k^5 \neq 0$. If $c = 1 \pm ib$, then the third subresultant is zero when $b = 2i$ or $b = 0$ and in both cases the second subresultant is non-zero. Thus the first four subresultants of C and C' can't be all zeros and so C can't be the square of a degree 4 polynomial.

□

Theorem 8. *Let $a_2(t), a_4(t)$ and $a_6(t)$ be polynomials in $\mathbb{Q}[t]$ with $\deg a_2(t) = 2$, $\deg a_4(t) \leq 2$, $\deg a_6(t) \leq 2$ and such that the curve $\mathcal{F}(t): y^2 = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t)$ is non-isotrivial and potentially biased. Then, up to some rational linear changes of variables in the parameter t and in the variables x and y , the family is one of the following*

$$(2.8) \quad \begin{aligned} \mathcal{H}_w: & \quad wy^2 = x^3 + (8t^2 - 7t + 3)x^2 - 3(2t - 1)x + (t + 1), \text{ with } w \in \mathbb{Z}_{\neq 0}, \\ \mathcal{I}_w: & \quad wy^2 = x^3 + t(t - 7)x^2 - 6t(t - 6)x + 2t(5t - 27), \text{ with } w \in \mathbb{Z}_{\neq 0}, \\ \mathcal{J}_{m,w}: & \quad wy^2 = x^3 + 3t^2x^2 - 3mtx + m^2, \text{ with } m, w \in \mathbb{Z}_{\neq 0}, \\ \mathcal{L}_{w,s,v}: & \quad wy^2 = x^3 + 3(t^2 + v)x^2 + 3sx + s(t^2 + v), \text{ with } v \in \mathbb{Z}, r, w \in \mathbb{Z}_{\neq 0}. \end{aligned}$$

Moreover, the ranks of $\mathcal{H}_w$, $\mathcal{I}_w$ and $\mathcal{J}_{m,w}$ are ≤ 1 . Also, $\mathcal{I}_w$ and $\mathcal{J}_{m,w}$ have rank 1 if and only if w is a square, whereas $\text{rank}_{\mathbb{Q}(t)}(\mathcal{H}_w) = 1$ if and only if w is 2 times a square. Finally, the rank of $\mathcal{L}_{w,s,v}$ is always ≤ 3 and its value is given in equation (3.8) below in terms of the number of irreducible factors of certain polynomials.

Proof. We will compute the ranks in Section 3; here we only show that all the potentially biased are the ones given in (2.8).

First, we observe that the c_4 and the c_6 invariants of $\mathcal{F}$ have degree 4 and 6 respectively since $c_4 = 16a_2(t)^2 - 48a_4(t)$ and $c_6 = -64a_2(t)^3 + 288a_4(t)a_2(t) - 864a_6(t)$. Also, $3 \leq \deg(\Delta) \leq 8$. Indeed all the terms of degree ≥ 9 trivially cancel, whereas imposing that the coefficients of degree 5, 6, 7, 8 cancel we can determine d, e, f, c ; then, with this choices, the coefficients of degree 4 and 3 can be zero at the same time only if $bw - au = 0$ but in that case $\Delta = 0$.

Now, we notice that we can assume c_4 is square-free. Indeed, if it is not, write $c_4 = L_1^2 L_2 L_3$, with L_i linear polynomials in $\mathbb{C}[t]$, and, since the family is potentially parity-biased, $1728\Delta = kL_1^i L_2^j L_3^h$ with $i \in \{0, 2, 4\}$, $j, h \in \{0, 2, 3\}$, $3 \leq 2i + j + h \leq 8$, and $k \neq 0$. Thus,

$$c_6^2 = c_4^3 - 1728\Delta = L_1^{2i} L_2^j L_3^h (L_1^{6-2i} L_2^{3-j} L_3^{3-h} - k)$$

and in particular $L_1^{6-2i} L_2^{3-j} L_3^{3-h} - k$ is $L_2^{\frac{1-(-1)^j}{2}} L_3^{\frac{1-(-1)^h}{2}}$ times a square in $\mathbb{C}[t]$ (if $L_2 = L_3$ and $j = h = 3$, and so $i \in \{0, 2\}$, the condition would be that $L_1^{6-2i} - k$ is a square, which is clearly not possible). One can then easily rule out all the possibilities by Lemma 3.

Thus, we can assume $c_4 = L_1 L_2 L_3 L_4$ with $L_i \in \mathbb{C}[t]$ different linear polynomials. Since the family is potentially parity-biased and non-isotrivial, we have $1728\Delta = kL_1^i L_2^j L_3^h L_4^g$ with $k \neq 0$ and $i, j, h, g \in \{0, 2, 3\}$. Clearly at least two among i, j, h, g coincide and so we write $c_4 = L_1 L_2 P$ with P of degree 2, and $1728\Delta = kL_1^i L_2^j P^h$ and we can assume $i \leq j$. Also $3 \leq i + j + 2h \leq 8$. Then, the only possibilities are: $i = j = h = 2$ and $i = 0$ and either $j = h = 2$ or $j = 2, h = 3$ or $j = 3$ and $h = 2$ (we excluded the cases $i = 2, h = 2, j \in \{2, 3\}$ by b) and c) of Lemma 3, and $i = j = 3, h = 0$ by a)). It follows that there are only the following possibilities for c_4 where P_i and $P_{i,j}$ are polynomials in $\mathbb{Q}[t]$ of degree i , not necessary irreducible:

- (1) $c_4 = P_4$ and $\Delta = kP_4^2$,
- (2) $c_4 = P_{1,1}P_{1,2}P_2$ and $\Delta = kP_{1,2}^3P_2^2$,
- (3) $c_4 = P_{1,1}P_{1,2}P_2$ and $\Delta = kP_{1,2}^2P_2^3$,
- (4) $c_4 = P_3P_1$ and $\Delta = kP_3^2$,

with c_4 square-free in all cases.

Let's consider the case 1). Comparing the coefficients in t of the equation $c_6(t)^2 = c_4(t)^3 - kc_4(t)^2$ we obtain 9 equations in the various parameters (since the terms of degree > 8 in t are always equal). Imposing the equality of the coefficients coming from the degree 8, 7 and 6 we can easily express d, e and f in terms of the other variables. The coefficient of degree 5 factors and gives rise to two possibilities; one leads to $k = 0$ (after eliminating other variables looking at the coefficients of lower degrees) and so $\Delta = 0$, whereas the other one, eliminating b and c , leads to the following families (after a linear change

of variable in k)

$$y^2 = x^3 + a_2(t)x^2 + \left(\frac{a}{w}a_2(t) + 9k - \frac{3a^2}{w^2}\right)x + ka_2(t) - \frac{a^3}{w^3} + \frac{3ak}{w}$$

with $a_2(t) = wt^2 + ut + v$. Up to some change of variables, this is of the form (2.5), with t replaced by $a_2(t)$, so killing u with a change of variable in t , we see that we obtain families of the form $\mathcal{F}_h(p(t^2 + q))$ for some parameters $h, p, q \in \mathbb{Q}$ with $h, p \neq 0$. Writing $v = q, p = w, r = h/w^2$ and making the changes $x \leftrightarrow wx, y \leftrightarrow wy$ we obtain $\mathcal{L}_{w,s,v}(t)$ with invariants

$$(2.9) \quad \begin{aligned} c_4(t) &= 144(t^4 + 2t^2v + v^2 - s), \\ c_6(t) &= -1728(t^2 + v)(s - t^4 - 2t^2v - v^2), \\ \Delta(t) &= -1728s(t^4 + 2t^2v + v^2 - s)^2. \end{aligned}$$

Now, consider the case 2). We can assume $c_4(t)$ has simple zeros at 0 and 1 and that $\Delta(t)$ has a triple zero at 0. Thus, we can write $c_4(t)$ in the form $c_4(t) = -16w^2t(t-1)(t^2 + mt + n)$ and $\Delta(t)$ as $1728\Delta(t) = kt^3(t^2 + mt + n)^2$ for some $n, k \in \mathbb{Z}_{\neq 0}$ and some $m \in \mathbb{Z}$. Then, we express a, b, c, u in terms of m, n and the other parameters and we impose

$$(2.10) \quad c_6^2(t) = c_4(t)^3 - kt^3(t^2 + mt + n)^2$$

obtaining 9 equations for the parameters. The equations corresponding to the degrees 0, 2, 3 and 8 in t allow us to express f, e, k, d in terms of the other parameters. Then, we use a suitable linear combination of the equations from the degrees 5, 6 and 7 to obtain a linear equation in n , so that we can eliminate n as well. Then, (eliminating the denominator) the equations from the degrees 6 and 7 states that two polynomials in m are equal to 0. The common roots of these polynomials are $m = -1$ and $m = -\frac{11}{3}$. The former gives $k = 0$, i.e. $\Delta = 0$, whereas for $m = -\frac{11}{3}$ we see that (2.10) is verified and so we have new families. After a change of variable in x to reduce the degree in t of the coefficient of x , the families are

$$y^2 = x^3 + \frac{1}{3}(8w - 7tw + 3t^2w)x^2 + \frac{16}{27}(4w^2 - 3tw^2)x + \frac{64}{729}(8w^3 + 3tw^3).$$

We make the changes of variables $x \leftrightarrow \frac{8}{9}wx, t \leftrightarrow 8t/3, w \leftrightarrow 2w, y \leftrightarrow \frac{16}{27}w^2y$ and we arrive to $\mathcal{H}_w$ with

$$(2.11) \quad \begin{aligned} c_4(t) &= 16w^2t(8t - 3)(8t^2 - 11t + 8), \\ c_6(t) &= -64w^3t^2(8t^2 - 11t + 8)(64t^2 - 80t + 45), \\ \Delta(t) &= -512w^6t^3(8t^2 - 11t + 8)^2. \end{aligned}$$

Now, consider the case 3). Again we write $c_4(t)$ as $c_4(t) = -16w^2t(t-1)(t^2 + mt + n)$ and this time $\Delta(t)$ as $1728\Delta(t) = kt^2(t^2 + mt + n)^3$ with $k, n \neq 0$. We impose $c_6^2(t) = c_4(t)^3 + kt^2(t^2 + mt + n)^3 = 0$ and proceed as above, expressing f, k, e in terms of the other parameters, using the equations from the degrees 1, 8 and 7 in t . A suitable linear combination of the 5th and 6th equations give an equation of the form $(1 + m)^2(5 + 2m)d = Q(m, n, v, w)$ for some polynomial $Q(m, n, v, w)$. We have $Q(-1, n, v, w) = -\frac{(nw)^3}{27} \neq 0$ and thus we can assume $m \neq -1$. We now assume $5 + 2m \neq 0$, and we express d in terms of the other variables and with this choice the remaining equations don't depend on w and v anymore. Thus we are left with 4 independent equations equating polynomials in m, n to zero, the resultants in n of the 2nd and 3th polynomials and of the 4th and 5th polynomials have the only common zero $m = -\frac{5}{2}$ which we had excluded. Finally, we consider the case $m = -\frac{5}{2}$. With this choice we can quickly determine also n (whereas the dependence on v disappear also in this case) and, after some changes of variables in y, x, t we are led to the families $\mathcal{I}_w$ with

$$(2.12) \quad \begin{aligned} c_4(t) &= 16w^2(t - 4)t(t^2 - 10t + 27), \\ c_6(t) &= -64w^3(t - 1)t(t^2 - 10t + 27)^2, \\ \Delta(t) &= -64w^6t^2(t^2 - 10t + 27)^3. \end{aligned}$$

Finally let's consider case 4). With a change of variables we can write $c_4(t)$ as $c_4(t) = -16w^2t(t - \delta)(t^3 + mt + n)$ with $k, n \neq 0$, $\delta \in \{0, 1\}$ and $1728\Delta(t) = k(t^3 + mt + n)^2$. As above we express a, b, c, u in terms of the other variables and we impose $c_6^2(t) = c_4(t)^3 + k(t^3 + mt + n)^3 = 0$, from which we can easily eliminate d, e, k, f . If $\delta = 1$, then a linear combination of the remaining equations give $(3 + 4m)^4(2m - 10n - 1) = 0$ and in both cases one finds $k = 0$. Thus, we can take $\delta = 0$; this simplifies the remaining equations and we can eliminate m and f arriving to the families $\mathcal{J}_{n,w}$ with

$$(2.13) \quad \begin{aligned} c_4(t) &= 144w^2t(t^3 + n), \\ c_6(t) &= -864w^3(t^3 + n)(2t^3 + n), \\ \Delta(t) &= -432w^6n^2(t^3 + n)^2. \end{aligned}$$

Finally we observe that, up to rational linear changes of variables in t, x and y , one can always reduce to the case where the parameters w, r, v, n are in $\mathbb{Z}$. $\square$

Remark 1. *Note that, with the exception of $\mathcal{L}_{w,s,v}$, all the families of Theorem 7 and Theorem 8 don't have primes of bad reduction of degree greater than 3. In particular, the square-free sieve conjecture is known to hold for the associated polynomial B defined in (2.1). In the case of $\mathcal{L}_{w,s,v}$, one has that if $t^4 + 2t^2v + v^2 - s$ is irreducible (i.e. if s is not of the form n^2 nor $-4n^2(n^2 + v)$ for some $n \in \mathbb{N}$), then there is a prime of quite bad reduction of degree 4 for which the square-free sieve conjecture is not proven.*

Corollary 4. *Assume Chowla's conjecture and the square-free sieve conjecture for homogeneous square-free polynomials (Hypothesis $\mathcal{B}_1$ and $\mathcal{B}_2$ at page 5 in [Hel09]). Then, all non-isotrivial families $\mathcal{F}$ of the form (1.1), with $a_2(t), a_4(t), a_6(t) \in \mathbb{Q}[t]$ and $\deg(a_i) \leq 2$ for $i = 2, 4, 6$, for which we have $\text{Av}_{\mathbb{Q}}(\varepsilon_{\mathcal{F}}) \neq 0$ are of the form $\mathcal{F}_s$ or $\mathcal{G}_w$ up to some rational linear changes of variables in the parameter t and in the variables x and y .*

Proof. By Main Theorem 2 of [Hel09], we have that if the family $\mathcal{F}$ is not potentially parity-biased or it has multiplicative reduction at infinity, then $\text{Av}_{\mathbb{Q}}(\varepsilon_{\mathcal{F}}) = 0$. Thus, we just need to check which of the families in Theorems 7 and 8 have multiplicative reduction at infinity. By (2.6), (2.7), (2.9) and (2.11)-(2.13) one immediately sees that the only families with non-multiplicative reduction at infinity are $\mathcal{F}_s$ and $\mathcal{G}_w$. $\square$

3. RANKS OVER $\mathbb{Q}(t)$

In this section we compute the rank of the potentially parity-biased families given in Theorem 7 and Theorem 8 following the same approach as in [ALRM07]. Let $\mathcal{F}$ be a family of elliptic curves as defined by (1.1), and suppose that $\mathcal{F}$ is not isotrivial. The following conjecture gives a way to determine $r_{\mathcal{F}}$, the rank of $\mathcal{F}$ over $\mathbb{Q}(t)$, by considering averages of the traces of Frobenius at p of the specializations $\mathcal{F}(t)$, when t varies over $\mathbb{F}_p$. More precisely, writing the number of points of the specialization $\mathcal{F}(t)$ over the finite field $\mathbb{F}_p$ as $p + 1 - a_{\mathcal{F}(t)}(p)$ (with $a_{\mathcal{F}(t)}(p) = 0$ for p dividing the discriminant of $\mathcal{F}(t)$), we define

$$A_{\mathcal{F}}(p) := \frac{1}{p} \sum_{t=0}^{p-1} a_{\mathcal{F}(t)}(p).$$

Conjecture 3 (Nagao). *With the notation above, the rank of $\mathcal{F}$ over $\mathbb{Q}(t)$ is given by*

$$(3.1) \quad r_{\mathcal{F}} = \lim_{X \rightarrow \infty} \frac{1}{X} \sum_{p \leq X} -A_{\mathcal{F}}(p) \log(p)$$

where the sum runs through all prime numbers $p \leq X$.

As proved in [RS98], Tate's conjecture implies Nagao's conjecture, and thus Conjecture 3 holds for rational elliptic surfaces as Tate's conjecture holds in that case [RS98]. In particular, the conjecture

holds if $\deg a_i(t) \leq 2$ for $i = 2, 4, 6$, since in this case $\mathcal{F}$ is a rational elliptic surface (see [SS10, section 8]).

If $\deg a_i(t) \leq 2$, we have that $\deg_t(x^3 + a_2(t)x^2 + a_4(t)x + a_6(t)) \leq 2$ and we can rewrite (1.1) as

$$\mathcal{F}: y^2 = A(x)t^2 + B(x)t + C(x),$$

where $A(x), B(x)$ and $C(x)$ are in $\mathbb{Q}(x)$. Now, we have

$$(3.2) \quad \begin{aligned} \sum_{t \pmod{p}} a_{\mathcal{F}(t)}(p) &= - \sum_{t \pmod{p}} \sum_{x \pmod{p}} \left(\frac{x^3 + a_2(t)x^2 + a_4(t)x + a_6(t)}{p} \right) \\ &= - \sum_{x \pmod{p}} \sum_{t \pmod{p}} \left(\frac{A(x)t^2 + B(x)t + C(x)}{p} \right), \end{aligned}$$

and we can evaluate the sum over t for each fixed value of x .

We will need the following formulas (see for example [LN83, Theorem 5.48]):

$$(3.3) \quad \sum_{t=0}^{p-1} \left(\frac{Bt + C}{p} \right) = \begin{cases} p \left(\frac{C}{p} \right) & \text{if } p \mid B \\ 0 & \text{otherwise.} \end{cases}$$

If A is non-zero mod p , then

$$(3.4) \quad \sum_{t=0}^{p-1} \left(\frac{At^2 + Bt + C}{p} \right) = - \left(\frac{A}{p} \right) + \begin{cases} p \left(\frac{A}{p} \right) & \text{if } p \mid (B^2 - 4AC), \\ 0 & \text{otherwise.} \end{cases}$$

We now use the above setting to compute the rank of the families of Theorem 7 and 8 over $\mathbb{Q}(t)$.¹² In all cases we shall also give explicitly non-torsion points. Note that to prove that an explicit point, say $G \in \mathcal{F}(\mathbb{Q}(t))$, is non-torsion, it is sufficient to prove that it is neither a 3 nor a 4 torsion point (indeed, we only have to check a point is non-torsion when the rank of the family is $r_{\mathcal{F}} \geq 1$ which implies the torsion subgroup has cardinality at most 4, see [OS91]). In order to do this, it is sufficient to compute $2G$ and check that its y -coordinate is non-zero and that its x -coordinate is not the x -coordinate of G (indeed if $3G$ is zero then $2G = -G$ and the x -coordinates of G and $2G$ would coincide). We shall show this explicitly for Proposition 5 only, the computation being completely analogous in all other cases.

We first compute the ranks of the family $\mathcal{F}_s$, for which $A(x) = 0$.

Proposition 5. *Let $r \in \mathbb{Z}_{\neq 0}$ such and let $\mathcal{F}_s$ be the family*

$$\mathcal{F}_s: y^2 = x^3 + 3tx^2 + 3sx + st.$$

Then, $\text{rank}(\mathcal{F}_s) \leq 1$, and $\text{rank}(\mathcal{F}_s) = 1$ if and only if $s = -12k^4$, k in $\mathbb{N}$. Furthermore, if $s = -12k^4$, then $(-2k^2, 2^3k^3)$ is a non-torsion point of $\mathcal{F}_{-12k^4}(\mathbb{Q}(t))$.

Proof. We have $B(x) = 3x^2 + s$ and $C(x) = x^3 + 3sx$. If $-s/3$ is a square mod p , then the 2 roots of $B(x)$ are $\pm x_p$, where $x_p = \sqrt{-s/3}$, and $C(\pm x_p) = \pm \frac{8}{3}sx_p$. Then, using (3.1), (3.2) and (3.3), we have

¹²The study of more general formula for the rank whenever $\deg a_i(t) \leq 2$ is a work on progress and will appear in a forthcoming paper.

that

$$\begin{aligned}
\text{rank}(\mathcal{F}_s) &= \lim_{X \rightarrow \infty} \frac{1}{X} \sum_{p \leq X} \frac{\log p}{p} \sum_{x=0}^{p-1} \sum_{t=0}^{p-1} \left(\frac{B(x)t + C(x)}{p} \right) \\
&= \lim_{X \rightarrow \infty} \frac{1}{X} \sum_{\substack{p \leq X \\ \left(\frac{-3s}{p}\right)=1}} \log p \left(\left(\frac{6sx_p}{p} \right) + \left(\frac{-6sx_p}{p} \right) \right) \\
&= \lim_{X \rightarrow \infty} \frac{2}{X} \sum_{\substack{p \leq X \\ \left(\frac{-3s}{p}\right)=\left(\frac{-1}{p}\right)=1}} \log p \left(\frac{2x_p}{p} \right),
\end{aligned}$$

since for $\left(\frac{-3s}{p}\right) = \left(\frac{-1}{p}\right) = 1$ one has $\left(\frac{6sx_p}{p}\right) = \left(\frac{2x_p}{p}\right)$. Now if $-3s$ is neither a square nor minus a square in $\mathbb{Z}$, then the proportion of primes counted in the sum is $1/4$, and hence we obtain $\text{rank}(\mathcal{F}_s) < 1$, which implies that $\text{rank}(\mathcal{F}_s) = 0$. If $-3s = -n^2$ for some $n \in \mathbb{Z}_{\neq 0}$ then

$$\text{rank}(\mathcal{F}_s) = \lim_{X \rightarrow \infty} \frac{2}{X} \sum_{\substack{p \leq X \\ \left(\frac{-1}{p}\right)=1}} \log p \left(\frac{6n}{p} \right) \left(\frac{\delta_p}{p} \right),$$

where $\delta_p^2 \equiv -1 \pmod{p}$. Note that the sum does not depend on the choice of the sign of δ_p ; also, $\left(\frac{\delta_p}{p}\right) = 1$ if and only if $p \equiv 1 \pmod{8}$. We claim that there is a positive proportion of the primes $p \equiv 1 \pmod{4}$ such that

$$(3.5) \quad \left(\frac{6n}{p} \right) \left(\frac{\delta_p}{p} \right) = -1$$

so that in particular $\text{rank}(\mathcal{F}_s)$ has to be 0 also in this case. Indeed, if the square-free part of $6n$ is $2q$ with q odd, then take $p \equiv 5 \pmod{8}$ and $p \equiv b \pmod{q}$, where b is a quadratic non-residue modulo q so that by quadratic reciprocity one obtains (3.5). Similarly, if the square-free part of $6n$ is q with q odd, then take $p \equiv 5 \pmod{8}$ and $p \equiv b \pmod{q}$, where b is a non-zero quadratic residue modulo p .

Finally, if $-3s = n^2$, then

$$\text{rank}(\mathcal{F}_s) = \lim_{X \rightarrow \infty} \frac{2}{X} \sum_{\substack{p \leq X \\ \left(\frac{-1}{p}\right)=1}} \log p \left(\frac{6n}{p} \right).$$

If $6n \neq \pm k^2$, then the sum is 0; if $6n = \pm k^2$, then the sum is 1, and in that case we have that $s = -12k^4$. Finally, if $s = -12k^4$, then the point $G = (-2k^2, 8k^3)$ is a point on $\mathcal{F}_{-12k^4}(\mathbb{Q}(t))$ and we have

$$2G = \left(\frac{9t^2 - 12k^2t + 100k^4}{16k^2}, \frac{27t^3 + 18k^2t^2 + 324k^4t + 280k^6}{64k^3} \right)$$

and so G is neither a 3 nor a 4 torsion point. $\square$

Corollary 6. *Let $\mathcal{W}_a : y^2 = x^3 + tx^2 - a(t+3a)x + a^3$. Then $\text{rank}(\mathcal{W}_a) \leq 1$, and the rank is 1 if and only if $a = \pm n^2$.*

Proof. It follows from the fact that $\mathcal{W}_a(t)$ is isomorphic to $\mathcal{F}_{-3^5 4a^2}(12t + 18a)$. $\square$

Corollary 7. *Let $\mathcal{V}_a : y^2 = x^3 + 3tx^2 + 3atx + a^2t$. Then, $\text{rank}(\mathcal{V}_a) = 0$.*

Proof. It follows from the fact that $\mathcal{V}_a$ is isomorphic to $\mathcal{F}_{4a^2}(4t - 2a)$. $\square$

We now compute the rank of the remaining families of Theorem 7 and Theorem 8. First, we remark that for $\mathcal{F}$ as in (1.1) one has that the quadratic twist

$$\mathcal{F}^{(w)} : wy^2 = x^3 + a_4(t)x^2 + a_4(t)x + a_6(t),$$

satisfies $a_{\mathcal{F}^{(w)}(t)}(p) = \left(\frac{w}{p}\right)a_{\mathcal{F}(t)}(p)$. Then, using (3.3) and (3.4) one has

$$(3.6) \quad \begin{aligned} \text{rank}(\mathcal{F}^{(w)}) = \lim_{X \rightarrow \infty} \frac{1}{X} \sum_{p \leq X} \log p & \left(\sum_{\substack{x \pmod{p} \\ A(x) \equiv B(x) \equiv 0 \pmod{p}}} \left(\frac{wC(x)}{p} \right) \right. \\ & + \sum_{\substack{x \pmod{p} \\ A(x) \not\equiv 0 \pmod{p} \\ (B^2 - 4AC)(x) \equiv 0 \pmod{p}}} \left(\frac{wA(x)}{p} \right) - \frac{1}{p} \sum_{\substack{x \pmod{p} \\ A(x) \not\equiv 0 \pmod{p}}} \left(\frac{wA(x)}{p} \right) \Big). \end{aligned}$$

We note that the contribution from the first sum is zero unless A and B have common factors in $\mathbb{Q}[x]$, whereas the contribution from the last sum is

$$\begin{cases} -1 & \text{if } wA(x) = P(x)^2 \text{ for some } P(x) \in \mathbb{Q}[x], \deg P(x) \geq 1 \\ 0 & \text{otherwise} \end{cases}$$

using Weil's bound (or also (3.4) if A has degree 2).

We now use the above formula to compute the rank of the families $\mathcal{G}_w$, $\mathcal{I}_w$, $\mathcal{H}_w$, $\mathcal{J}_{m,w}$ and $\mathcal{L}_{w,s,v}$, the most delicate being the last one.

Proposition 8. *Let $w \in \mathbb{Z}_{\neq 0}$ and $\mathcal{G}_w$ be the family*

$$\mathcal{G}_w : wy^2 = x^3 + 3tx^2 + 3tx + t^2.$$

Then, the rank of $\mathcal{G}_w$ is ≤ 1 and $\text{rank}(\mathcal{G}_w) = 1$ if and only if w is a square or -2 times a square. Furthermore, if $w = 1$ (resp. $w = -2$) then the point $(0, t)$ (resp. $(-3, 2t)$) is a non-torsion point in $\mathcal{G}_w(\mathbb{Q}(t))$.

Proof. We use equation (3.6) with $A(x) = 1$, $B(x) = 3x(x+1)$ and $C(x) = x^3$ so that $(B^2 - 4AC)(x) = x^2(9x^2 + 14x + 9)$. Notice that the discriminant of $9x^2 + 14x + 9$ is -2^5 and thus for $p > 3$ one has that $B^2 - 4AC$ has 3 distinct roots in $\mathbb{F}_p$ if $\left(\frac{-2}{p}\right) = 1$ and has 1 root otherwise. Since $A(x_p) = 1$ for any root x_p of $(B^2 - 4AC)(x)$, we have

$$\begin{aligned} \text{rank}(\mathcal{G}_w) &= \lim_{X \rightarrow \infty} \frac{1}{X} \left(\sum_{\substack{p \leq X \\ \left(\frac{-2}{p}\right) = 1}} 3 \log p \left(\frac{w}{p} \right) + \sum_{\substack{p \leq X \\ \left(\frac{-2}{p}\right) = -1}} \log p \left(\frac{w}{p} \right) - \sum_{p \leq X} \log p \left(\frac{w}{p} \right) \right) \\ &= \lim_{X \rightarrow \infty} \frac{1}{X} \sum_{\substack{p \leq X \\ \left(\frac{-2}{p}\right) = 1}} 2 \log p \left(\frac{w}{p} \right) = \lim_{X \rightarrow \infty} \frac{1}{X} \sum_{p \leq X} \log p \left(\left(\frac{w}{p} \right) + \left(\frac{-2w}{p} \right) \right) \end{aligned}$$

and so the rank is 1 if w is a square or -2 times a square, and it is zero otherwise. $\square$

Proposition 9. *Let $w \in \mathbb{Z}_{\neq 0}$ and $\mathcal{I}_w$ be the family*

$$\mathcal{I}_w : wy^2 = x^3 + t(t-7)x^2 - 6t(t-6)x + 2t(5t-27)$$

Then, the rank of $\mathcal{I}_w$ is ≤ 1 and $\text{rank}(\mathcal{I}_w) = 1$ if and only if w is a square. Furthermore, if $w = 1$ then the point $(9/4, 5t/4 - 27/8)$ is a non-torsion point in $\mathcal{I}_1(\mathbb{Q}(t))$.

Proof. We use equation (3.6) with $A(x) = x^2 - 6x + 10$, $B(x) = -7x^2 + 36x - 54$ and $C(x) = x^3$ so that $B^2 - 4AC = -(4x - 9)(x^2 - 8x + 18)^2$. Note that $A(9/4) = 25/16 = (5/4)^2$. Also, the discriminant of $x^2 - 8x + 18$ is -8 , and so if -2 is a square modulo p then the roots of $x^2 - 8x + 18$ are $x_{p,\pm} = 4 \pm \delta_p$ where $\delta_p^2 = -2$ modulo p . Moreover, we have $A(x_{p,\pm}) = \pm 2\delta_p$ and so by equation (3.6), we obtain

$$\text{rank}(\mathcal{I}_w) = \lim_{X \rightarrow \infty} \frac{1}{X} \left(\sum_{p \leq X} \log p \left(\frac{w}{p} \right) + 2 \sum_{\substack{p \leq X \\ (\frac{-2}{p}) = (\frac{-1}{p}) = 1}} \log p \left(\frac{2\delta_p w}{p} \right) \right).$$

The contribution coming from the first sum is 1 if and only if w is a square (and 0 otherwise), whereas the contribution coming from the last sum is 0 (the proportion of primes counted in this sum is $1/4$). $\square$

Proposition 10. *Let $w \in \mathbb{Z}_{\neq 0}$ and $\mathcal{H}_w$ be the family*

$$\mathcal{H}_w: wy^2 = x^3 + (8t^2 - 7t + 3)x^2 - 3(2t - 1)x + (t + 1).$$

Then, the rank of $\mathcal{H}_w$ is ≤ 1 and $\text{rank}(\mathcal{H}_w) = 1$ if and only if w is 2 times a square. Furthermore, if $w = 2$ then $(-1, 2t)$ is a non-torsion point of $\mathcal{H}_2(\mathbb{Q}(t))$.

Proof. We have $A(x) = 8x^2$, $B(x) = -(x+1)(7x-1)$ and $C(x) = (x+1)^3$. In particular, for $p \neq 2$ we have $A(x) = 0 \pmod{p}$ if and only if $x = 0 \pmod{p}$. Also, notice that $A(x)$ is always 2 times a square. Then, using (3.6), we get

$$\text{rank}(\mathcal{H}_w) = \lim_{X \rightarrow \infty} \frac{1}{X} \left(\sum_{p \leq X} \log p \sum_{\substack{x \pmod{p} \\ (B^2 - 4AC)(x) \equiv 0 \pmod{p}}} \left(\frac{2w}{p} \right) - \sum_{p \leq X} \log p \left(\frac{2w}{p} \right) \right)$$

We compute that $B^2 - 4AC = -(x+1)^2(32x^3 - 17x^2 + 14x - 1)$, and we let $Q(x) = 32x^3 - 17x^2 + 14x - 1$ with discriminant $-2 \cdot (320)^2$. Then, we have

$$\text{rank}(\mathcal{H}_w) = \lim_{X \rightarrow \infty} \frac{1}{X} \left(\sum_{\substack{p \leq X \\ Q(x) \text{ has one root in } \mathbb{F}_p}} \log p \left(\frac{2w}{p} \right) + \sum_{\substack{p \leq X \\ Q(x) \text{ has three roots in } \mathbb{F}_p}} 3 \log p \left(\frac{2w}{p} \right) \right).$$

Now, $Q(x)$ has exactly 1 root in $\mathbb{F}_p$ if and only if $\left(\frac{-2 \cdot (320)^2}{p} \right) = -1$. Thus, the first sum contributes

$$\lim_{X \rightarrow \infty} \frac{1}{X} \sum_{p \leq X} \frac{\log p}{2} \left(\frac{2w}{p} \right) \left(1 - \left(\frac{-2}{p} \right) \right) = \begin{cases} \frac{1}{2} & \text{if } 2w \text{ is a rational square,} \\ -\frac{1}{2} & \text{if } -w \text{ is a rational square.} \end{cases}$$

Finally, since the Galois group of $Q(x)$ is S_3 , we have that the primes such that $Q(x)$ splits completely have density $\frac{1}{6}$, so that the contribution of the second sum is in $[-\frac{1}{2}, \frac{1}{2}]$. Also, such a contribution is positive if $2w$ or $-w$ are rational square (indeed in the second case $\left(\frac{2w}{p} \right) = \left(\frac{-2}{p} \right) = 1$ if Q splits completely in $\mathbb{F}_p$). Thus, since $\text{rank}(\mathcal{H}_w)$ is an integer, we must have that $\text{rank}(\mathcal{H}_w) = 1$ if $2w$ is a rational square and $\text{rank}(\mathcal{H}_w) = 0$ otherwise. $\square$

Proposition 11. *Let $m, w \in \mathbb{Z}_{\neq 0}$ and $\mathcal{J}_{m,w}$ be the family*

$$\mathcal{J}_{m,w}: wy^2 = x^3 + 3t^2x^2 - 3mtx + m^2.$$

Then, $\text{rank}(\mathcal{J}_{m,w}) \leq 1$ and $\text{rank}(\mathcal{J}_{m,w}) = 1$ if and only if w is a square. Furthermore, if $w = 1$ then $(0, m)$ is a non-torsion point in $\mathcal{J}_{m,1}(\mathbb{Q}(t))$.

Proof. In this case, we have $A(x) = 3x^2$, $B(x) = -3mx$, $C(x) = x^3 + m^2$ and $B^2(x) - 4A(x)C(x) = -3x^2(4x^3 + m^2)$. Let $Q(x) = 4x^3 + m^2$ and note that the discriminant of $Q(x)$ is $-3 \cdot (2m)^4$ and that

$A(x)$ is always 3 times a square. Also, $A(x)$ has a common root $x = 0$ and one has $C(0) = m^2$. Thus, using (3.6), we obtain

$$\text{rank}(\mathcal{J}_{m,w}) = \lim_{X \rightarrow \infty} \frac{1}{X} \sum_{p \leq X} \log p \left(\left(\frac{w}{p} \right) + \sum_{\substack{p \leq X \\ Q \text{ splits} \\ \text{completely in } \mathbb{F}_p}} 3 \left(\frac{3w}{p} \right) + \sum_{\substack{p \leq X \\ Q \text{ has one} \\ \text{root in } \mathbb{F}_p}} \left(\frac{3w}{p} \right) - \left(\frac{3w}{p} \right) \right).$$

The first term contributes 1 if w is a rational square and 0 otherwise and the last contributes 1 if $3w$ is rational square and 0 otherwise. As in the proof of Proposition 10 one then has that the third term contributes $\frac{1}{2}$ if $3w$ is a square, $-\frac{1}{2}$ if $-w$ is a square, and 0 otherwise. Thus, we must have that the second summand contributes $\frac{1}{2}$ if $3w$ or $-w$ are squares and 0 otherwise. $\square$

Proposition 12. *Let $v \in \mathbb{Z}$, $s, w \in \mathbb{Z}_{\neq 0}$ and $\mathcal{L}_{w,s,v}$ be the family*

$$(3.7) \quad \mathcal{L}_{w,s,v}: wy^2 = x^3 + 3(t^2 + v)x^2 + 3sx + s(t^2 + v).$$

Then the rank of $\mathcal{L}_{w,s,v}$ is ≤ 3 and all the cases can occur. More precisely, let

$$C(x) = x^3 + 3vx^2 + 3sx + sv, \quad R(x) = x^6 + (15sw - 27v^2w)x^4 + 48s^2w^2x^2 - 64(s^3w^3),$$

then

$$(3.8) \quad \text{rank}(\mathcal{L}_{w,s,v}) = \#\{\text{Irr. factors of } R(x)\} - \#\{\text{Irr. factors of } C(x)\} - \delta_1 + \delta_2,$$

where $\delta_2 \in \{0, 1\}$ with $\delta_2 = 1$ iff $-4w^2s$ is 3 times a 4-th power and

$$(3.9) \quad \delta_1 := \begin{cases} 2 & \text{if } s = v^2 \text{ or if } v = 0 \text{ and } -2sw \text{ is a square in } \mathbb{Q} \text{ whereas } -3s \text{ and } sw \text{ are not,} \\ 1 & \text{if } v = 0 \text{ and } -3s, rw \text{ and } -2sw \text{ are not squares in } \mathbb{Q}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. In this case we have $A(x) = 3x^2 + s$, $C(x) = x^3 + 3vx^2 + 3sx + sv$ and $B(x) = 0$. Using (3.6) we obtain

$$\begin{aligned} \text{rank}(\mathcal{E}_w) &= \lim_{X \rightarrow \infty} \frac{1}{X} \sum_{p \leq X} \log p \left(\sum_{\substack{x \pmod{p} \\ A(x) \equiv 0 \pmod{p}}} \left(\frac{wC(x)}{p} \right) + \sum_{\substack{x \pmod{p} \\ C(x) \equiv 0 \pmod{p}}} \left(\frac{wA(x)}{p} \right) \right) \\ &= \lim_{X \rightarrow \infty} \frac{1}{X} \sum_{p \leq X} \log p (S_1(p) + S_2(p)), \end{aligned}$$

say. We first consider $S_2(p)$. The discriminant of $C(x)$ is $-108s(s-v^2)^2$. If $s = v^2$, then $C(x) = (v+x)^3$ and so $S_2(p) = \left(\frac{wA(-v)}{p} \right) = \left(\frac{w4v^2}{p} \right) = \left(\frac{w}{p} \right)$ for p large enough. In particular

$$\lim_{X \rightarrow \infty} \frac{1}{X} \sum_{p \leq X} S_2(p) \log p = \begin{cases} 1 & w \text{ is a square in } \mathbb{Q}, \\ 0 & \text{otherwise.} \end{cases}$$

Now, assume $s \neq v^2$. We have

$$(3.10) \quad S_2(p) = \sum_{\substack{x \pmod{p} \\ wA(x) \equiv \square \pmod{p} \\ C(x) \equiv 0 \pmod{p}}} 2 - \sum_{\substack{x \pmod{p} \\ C(x) \equiv 0 \pmod{p}}} 1 = S'_2(p) - S''_2(p),$$

say. Then, since $C(x)$ is square-free, by Chebotarev's density theorem about the density of primes which splits, splits completely or are inert in a number field ([Lan94, VIII, §4, Th. 10]) we have

$$\lim_{X \rightarrow \infty} \frac{1}{X} \sum_{p \leq X} S''_2(p) \log p = \#\{\text{Irreducible factors of } C(x) \text{ in } \mathbb{Q}[x]\}.$$

Next, we rewrite $S'_2(p)$ as

$$S'_2(p) = \sum_{0 \neq \ell \pmod{p}} \sum_{\substack{x \pmod{p} \\ wA(x) \equiv \ell^2 \pmod{p} \\ C(x) \equiv 0 \pmod{p}}} 1$$

and we express the inner sum in terms of the resultant between $C(z)$ and $wA(z) - x^2$. To do this we notice that defining

$$R(x) := -\operatorname{Res}_z(C(z), wA(z) - x^2) = x^6 + (15sw - 27v^2w)x^4 + 48s^2w^2x^2 - 64(s^3w^3)$$

we have that $R(\ell) \equiv 0 \pmod{p}$ if and only if either $C(x)$ and $wA(x) - \ell^2$ have a common zero in $\mathbb{F}_p$ or if $C(x)$ and $wA(x) - \ell^2$ have a common irreducible factor of degree > 1 , i.e. if $(wA(x) - \ell^2) | C(x)$ with $wA(x) - \ell^2$ irreducible in $\mathbb{F}_p[x]$. Moreover, for p large enough C doesn't have multiple zeros over $\mathbb{F}_p$ and we have that the resultant $R(\ell)$ has a zero $\ell' \neq 0$ of multiplicity m if and only if there are m solutions $\pmod{p}$ of $wA(x) \equiv \ell'^2 \pmod{p}$, $C(x) \equiv 0 \pmod{p}$. Also, if $(wA(x) - \ell'^2) | C(x)$ with $wA(x) - \ell'^2$ irreducible in $\mathbb{F}_p[x]$, then ℓ' is a double root of $R(\ell)$. Thus,

$$S'_2(p) = \sum_{\substack{0 \neq \ell \pmod{p}, \\ R(\ell) \equiv 0 \pmod{p}}} m(\ell) - \sum_{\substack{0 \neq \ell \pmod{p}, \\ (wA(x) - \ell^2) | C(x) \text{ in } \mathbb{F}_p[x], \\ wA(x) - \ell^2 \text{ irreducible in } \mathbb{F}_p[x]}} 2,$$

where $m(\ell)$ is the multiplicity of ℓ as a zero of $R(\ell)$. Since $R(0) = -64s^3 \not\equiv 0 \pmod{p}$ for p large enough, then

$$\lim_{X \rightarrow \infty} \frac{1}{X} \sum_{p \leq X} \log p \sum_{\substack{0 \neq \ell \pmod{p}, \\ R(\ell) \equiv 0 \pmod{p}}} m(\ell) = \#\{\text{Irreducible factors of } R(x) \text{ in } \mathbb{Q}[x]\}.$$

Now we write $C(x)$ as $C(x) = L_1(A(x))x + L_2(A(x))$ with $L_1, L_2 \in \mathbb{Q}[x]$ of degree ≤ 1 . We have that $wA(x) - \ell^2$ divides $C(x)$ in $\mathbb{F}_p[x]$ if and only if $L_1(\ell^2/w)x + L_2(\ell^2/w)$ is identically zero in $\mathbb{F}_p[x]$ and so iff $L_1(\ell^2/w) = L_2(\ell^2/w) = 0$. The linear polynomials L_1 and L_2 can have a common root $\pmod{p}$ for infinitely many p only if one is multiple of the other, i.e. if $C(x) = (A(x) - a)(bx + c)$ for some $a, b, c \in \mathbb{Q}$. In particular, if $C(x)$ cannot be written in such form then

$$\lim_{X \rightarrow \infty} \frac{1}{X} \sum_{p \leq X} \log p \sum_{\substack{0 \neq \ell \pmod{p}, \\ (wA(x) - \ell^2) | C(x) \text{ in } \mathbb{F}_p[x], \\ wA(x) - \ell^2 \text{ irreducible in } \mathbb{F}_p[x]}} 1 = 0.$$

Otherwise, since the discriminant of $wA(x) - \ell^2$ is $-12w(-\ell^2 + sw)$, one has

$$\lim_{X \rightarrow \infty} \frac{1}{X} \sum_{p \leq X} \log p \sum_{\substack{0 \neq \ell \pmod{p}, \\ \ell^2 \equiv a \pmod{p}, \\ -3w(sw - a) \notin (\mathbb{F}_p)^2}} 1 = \lim_{X \rightarrow \infty} \frac{1}{X} \sum_{p \leq X} \log p \left(1 + \left(\frac{a}{p} \right) \right) \left(1 - \left(\frac{3w(a - sw)}{p} \right) \right)$$

and this is equal to 2 if $3w(a - sw)$ is not a square in $\mathbb{Q}$ and a is, equal to 1 if $a, 3w(a - sw)$ and $3aw(a - sw)$ are not squares in $\mathbb{Q}^*$, and it is equal to 0 otherwise. Also, we observe that looking at the first two subresultants of $wA(x) - a$ and $C(x)$, one has that $C(x)$ can have a factor of the form $A(x) - a$ only if $v = 0$ in which case $a = -8sw$. Thus,

$$\lim_{X \rightarrow \infty} \frac{1}{X} \sum_{p \leq X} S'_2(p) \log p = \#\{\text{Irreducible factors of } R(x) \text{ in } \mathbb{Q}[x]\} - \eta$$

where

$$\eta := \begin{cases} 2 & \text{if } v = 0 \text{ and } -3s, sw \text{ are not a square in } \mathbb{Q}, \text{ and } -2sw \text{ is a square in } \mathbb{Q}, \\ 1 & \text{if } v = 0 \text{ and } -3s, sw \text{ and } -2sw \text{ are not a square in } \mathbb{Q}, \\ 0 & \text{otherwise.} \end{cases}$$

Thus, for $s \neq v^2$ we have

$$\lim_{X \rightarrow \infty} \frac{1}{X} \sum_{p \leq X} S_2(p) \log p = \#\{\text{Irr. factors of } R(x)\} - \#\{\text{Irr. factors of } C(x)\} - \eta.$$

Since, for $s = v^2$ (in particular $v \neq 0$ and so $\eta = 0$) we have that R and C have respectively 6 and 3 irreducible factors, then in general we have

$$(3.11) \quad \lim_{X \rightarrow \infty} \frac{1}{X} \sum_{p \leq X} S_2(p) \log p = \#\{\text{Irr. factors of } R(x)\} - \#\{\text{Irr. factors of } C(x)\} - \delta_1.$$

where δ_1 is as in (3.9).

We now consider $S_1(p)$. We could proceed as for $S_2(p)$, but instead we follow a more direct approach. For p large enough, we have that $A(x)$ has two distinct zeros $\pm x_p \pmod p$ if and only if $\left(\frac{-3s}{p}\right) = 1$. In particular, $S_1(p) = 0$ for if $\left(\frac{-3s}{p}\right) \neq 1$. Also, we notice that if $\left(\frac{-3s}{p}\right) = 1$, then $C(\pm x_p) = \pm \frac{8s}{3} x_p$ and so $S_1(p) = \left(\frac{6wsx_p}{p}\right) \left(1 + \left(\frac{-1}{p}\right)\right) = \left(\frac{2wx_p}{p}\right) \left(1 + \left(\frac{-1}{p}\right)\right)$. Thus, proceeding as in the proof of Proposition 5 we have that

$$\lim_{X \rightarrow \infty} \frac{1}{X} \sum_{p \leq X} S_1(p) \log p = \lim_{X \rightarrow \infty} \frac{2}{X} \sum_{\substack{p \leq X, \\ \left(\frac{-3s}{p}\right) = \left(\frac{-1}{p}\right) = 1}} \left(\frac{2wx_p}{p}\right) = 0$$

unless $-3s$ is a square in $\mathbb{Q}$. If $s = -3k^2$ with $k \in \mathbb{Q}$, then $x_p = k$ and we have

$$\lim_{X \rightarrow \infty} \frac{1}{X} \sum_{p \leq X} S_1(p) \log p = \lim_{X \rightarrow \infty} \frac{1}{X} \sum_{p \leq X} \left(\frac{2wk}{p}\right) \left(1 + \left(\frac{-1}{p}\right)\right) = \begin{cases} 1 & 2wk \text{ is } \pm \text{ a square,} \\ 0 & \text{otherwise.} \end{cases}$$

Since $2wk \in \pm \mathbb{Q}^2$ if and only if s is $-\frac{3}{4w^2}$ times a 4-th power, then by the above computation and (3.11) we obtain (3.8).

We will give an example of a family $\mathcal{L}$ with rank 3 in the paragraph just after the proof of the Proposition and one can easily find families with rank 0, 1 and 2. Thus, it remains to show that $\text{rank}(\mathcal{L}_{w,s,v})$ is always ≤ 3 . To see this, we observe that the average value of $S_2(p) \log p$ given in (3.11) is always ≤ 2 . Indeed, by the definition of $S_2(p)$ we have

$$(3.12) \quad \begin{aligned} \lim_{X \rightarrow \infty} \frac{1}{X} \sum_{p \leq X} S_2(p) \log p &\leq \lim_{X \rightarrow \infty} \frac{1}{X} \sum_{p \leq X} \sum_{\substack{x \pmod p \\ C(x) \equiv 0 \pmod p}} 1 \\ &= \#\{\text{square-free irreducible factors of } C(x)\} \end{aligned}$$

and thus the average value of $S_2(p) \log p$ is ≤ 2 unless $C(x)$ is a product of three coprime linear factors (in which case $\delta_1 = 0$). Now, if $C(x)$ factors completely then its discriminant $-108s(s - v^2)^2$ must be a square, i.e. $s = -3k^2$ for some $k \in \mathbb{N}$. Now, if y is a root of $C(x)$ then from $C(y) = 0$ one obtains $v = \frac{y(y^2 - 9k^2)}{3(k^2 - y^2)}$ (we can take $y \neq \pm k$ since $C(\pm k) = \mp 8k^3$) and that the other roots of $C(x)$ are $\frac{k(y \pm 3k)}{k \mp y}$. Then,

$$R(x) = (wA(y) - x^2) \left(wA\left(\frac{k(y+3k)}{k-y}\right) - x^2\right) \left(wA\left(\frac{k(y-3k)}{k+y}\right) - x^2\right)$$

and these three quadratic polynomials factors if $wA(y)$ and $wA\left(\frac{k(y \pm 3k)}{k \mp y}\right)$ are squares, i.e. if $-3w(k^2 - y^2)$, $6kw(k + y)$ and $6kw(k - y)$ are squares (and the average of $S_2(p) \log p$ is exactly the number of

such integers which are rational squares). These are all squares if and only if $-3w$, $(k+y)/(k-y)$ and $6kw(k-y)$ are squares in $\mathbb{Q}$ and, in particular, for this to happen we need $w < 0$ and $|k| > |y|$. This implies that $6kw(k-y)$ is negative and thus can't be a square. Thus $R(x)$ has at most 5 irreducible factors and the proof of the proposition is complete. $\square$

We remark that in the Propositions 5 to 11, the generic points appear naturally from the proofs. For example, in Proposition 10 with $w = 2$, one takes the root 1 of $B^2 - 4AC$ and observe that $A(x)t^2 + B(x)t + C(x) = 64t^2$ so that $(-2, 8t)$ is a point in $\mathcal{H}_w$. The same phenomena holds also for Proposition 12 even if it's a bit less immediate. Let's illustrate this phenomena by looking at the two extremal cases: one where C is the product of 3 coprime linear factors over $\mathbb{Q}$ and one where C is irreducible of degree 3.

First, suppose that we are in the case where C has three roots. In the proof of Proposition 12 we showed that for this to happen we need $s = -3k^2$ for some $k \in \mathbb{N}$ and that in this case $\text{rank}(\mathcal{L}_{w,s,v})$ is equal to δ_2 plus the number of squares among $-3w(k-y)(k+y)$, $6kw(k+y)$ and $6kw(k-y)$. As said above it cannot happen that these three numbers are all squares, but it could be that two of them are and that at the same time $\delta_1 = 1$ so that $\text{rank}(\mathcal{L}) = 3$. Indeed, take

$$(3.13) \quad s = -3k^2, \quad v = \frac{y(y^2 - 9k^2)}{3(k^2 - y^2)}$$

and

$$(3.14) \quad y = 6(b^2 - a^2), \quad k = 6(b^2 + a^2), \quad w = \frac{\ell^2}{12(b^2 + a^2)},$$

with $a, b, \ell \in \mathbb{N}$. Then, $-4w^2s/3 = \ell^2$ is a square (and so $\delta_2 = 1$) and so are $6wk(k-y) = (6a\ell)^2$ and $6wk(k+y) = (6b\ell)^2$. These three conditions lead to generic points: with this choice for the parameters, the discriminant in t of $P(x) = A(x)t^2 + C(x)$ is a degree 5 polynomials with roots

$$x_1 = k, \quad x_2 = -k; \quad x_3 = y, \quad x_4 = -\frac{6(a^2 + b^2)(2a^2 + b^2)}{b^2}, \quad x_5 = \frac{6(a^2 + b^2)(a^2 + 2b^2)}{a^2}.$$

Now we have $P(x_2) = w(4k^2/\ell)^2$, $P(x_4) = w(2a/b^2\ell)^2$ and $P(x_5) = w(2b/a^2\ell)^2$. Thus, we get the points $(x_2, 4k^2/\ell)$ (the δ_2 contribution), $(x_4, 2a/b^2\ell)$ and $(x_5, 2b/a^2\ell)$ in $\mathcal{L}_{w,s,v}(\mathbb{Q}(t))$ (the $S_2(p)$ contribution) with the parameters s, w and v as in (3.13) and (3.14).

Suppose now that C is irreducible and that R factorizes as 2 irreducible factors. This means that the contribution coming from $S_2(p)$ gives 1. Since $R(x)$ is the resultant in y of $wA(y) - x^2$ and $C(y)$ with C irreducible of degree 3, we claim that $R(x)$ factors if and only if one (and so any) root ρ of C is such that $wA(\rho)$ is a square in $\mathbb{Q}(\rho)$. Indeed, let ρ_1, ρ_2, ρ_3 the 3 roots of C so that we have $R(x) = -(x^2 - wA(\rho_1))(x^2 - wA(\rho_2))(x^2 - wA(\rho_3))$. Let G be the Galois group of the Galois closure of $\mathbb{Q}(\rho_1)$ in $\overline{\mathbb{Q}}$, note that G contains a 3-cycle, σ , permuting the ρ_i . Let $H(x)$ be an irreducible factor of R defined over $\mathbb{Q}$, $H(x)$ can be written $H(x) = \prod_{\rho \in S_1} (x^2 - wA(\rho)) \prod_{\rho \in S_2} (x + \sqrt{wA(\rho)}) \prod_{\rho \in S_3} (x - \sqrt{wA(\rho)})$ where S_1, S_2, S_3 are disjoint subsets of $\{\rho_1, \rho_2, \rho_3\}$ and where the values $wA(\rho)$ are all distinct (by definition of S_i and the fact that H is squarefree). If S_2 (or S_3) is not empty then for some i , $\pm\sqrt{wA(\rho_i)}$ is a root of $H(x)$ and if $wA(\rho_i)$ is not a square in $\mathbb{Q}(wA(\rho_i))$ then the minimal polynomial of $\pm\sqrt{wA(\rho_i)}$ over $\mathbb{Q}(\rho_i)$ is $x^2 - wA(\rho_i)$ and divides H which is not possible. So we have $wA(\rho_i) = M(\rho_i)^2$ for some polynomial $M \in \mathbb{Q}[x]$ (with degree < 3). Since $M \in \mathbb{Q}[x]$ and σ permutes transitively the ρ_i , we obtain that $wA(\rho) = M(\rho)^2$ for all $\rho \in \{\rho_1, \rho_2, \rho_3\}$. So S_2 or S_3 is not empty if and only if $wA(\rho) = M(\rho)^2$ for all $\rho \in \{\rho_1, \rho_2, \rho_3\}$ (the converse being clear). In this case, we have $R(x) = K(x)K(-x)$ with $K(x) = (x - M(\rho_1))(x - M(\rho_2))(x - M(\rho_3))$ which is fixed by the action of G and so $K(x) \in \mathbb{Q}[x]$. Furthermore, the values $M(\rho_i)$ are conjugate and distinct (if $M(\rho_1) = M(\rho_2)$ then $M(\rho_3) = M(\rho_1)$ by the σ -action which would imply that $A(\rho_1) = A(\rho_2) = A(\rho_3)$: impossible with the degree 2 of A) so $K(x)$ is irreducible. Hence $R(x)$ factors into 2 irreducible factors of degree 3. Now, if $wA(\rho)$ is not a square in $\mathbb{Q}(wA(\rho))$ then $H(x) = \prod_{\rho \in S_1} (x^2 - wA(\rho))$. By the same argument, the values $wA(\rho)$ are conjugate and distinct so $H(x) = R(x)$ is irreducible.

Thus, coming back to the main discussion, we get that $wA(\rho)t^2 + C(\rho)$ is a square in $\mathbb{Q}(\rho)(t)$ and so we obtain a generic point $G = (\rho, \ell t/w^2)$ where $\ell^2 = wA(\rho) \in \mathcal{L}_{w,s,v}(\mathbb{Q}(\rho)(t))$. Thus, the trace $\text{tr}_{\mathbb{Q}(\rho)/\mathbb{Q}}(G)$ gives a point in $\mathcal{L}_{w,s,v}(\mathbb{Q}(t))$. For example, take $s = 1$, $v = 9$ and $w = 1$ so that

$$\mathcal{L}: y^2 = x^3 + (3t^2 + 27)x^2 + 3x + (t^2 + 9)$$

and the rank is 1. We have $R(x) = x^6 - 2172x^4 + 48x^2 - 64 = (x^3 - 46x^2 - 28x - 8)(x^3 + 46x^2 - 28x + 8)$ and if ρ is a root of $C(x)$ then $A(\rho) = (\rho^2/12 + \rho/2 - 1/4)^2$ so that $G = (\rho, t(\rho^2/12 + \rho/2 - 1/4)) \in \mathcal{L}_{w,s,v}(\mathbb{Q}(\rho)(t))$ and

$$\text{tr}_{\mathbb{Q}(\rho)/\mathbb{Q}}(G) = \left(\frac{15t^2 + 144}{t^2}, \frac{2(13t^4 + 216t^2 + 864)}{t^3} \right) \in \mathcal{L}_{w,s,v}(\mathbb{Q}(t)).$$

Note that for all the other families we could find generic points with coordinates in $\mathbb{Q}[t]$ but that in this case we found a point with non-polynomial coordinates. We remark however that there is a point which is polynomial in t over an algebraic extension of $\mathbb{Q}$.

It could appear as a little bit disappointing not to be able to find potentially parity-biased families with higher ranks. However, there are also geometric constraints on the rank due to the condition about the type of bad reduction. Indeed, let $E \rightarrow C$ be an elliptic surface defined over $\mathbb{C}$ with non-constant j -invariant and let $R_{\mathbb{C}}$ be the rank of the Mordell-Weil group over $\mathbb{C}$. Then, we have the following result due to Shioda (see [Sch88]).

Theorem 9 (Shioda). *With the above notation, we have $R_{\mathbb{C}} \leq -4 + 4g + n_1 + 2n_2 - 2p_g$, where*

- g is the genus of C ;
- n_1 is the number of singular fibers of the Néron model of type $\mathbf{I}_b$, $b > 0$;
- n_2 is the number of singular fibers of the Néron model of other types;
- p_g is the geometric genus of E .

Furthermore if $p_g = 0$ then $R_{\mathbb{C}} = -4 + 4g + n_1 + 2n_2$.

For the families of Theorem 7 and 8, we have $p_g = 0$ and $g = 0$ ($C \simeq \mathbb{P}^1$). The condition about the type of bad reduction implies that the number of singular fibers is the degree of the square-free part of Δ plus 1 coming from the place at infinity. Since the families are potentially parity-biased, none of the finite fibers can be of type $\mathbf{I}_b$, $b > 0$. Now if $\deg a_2(t) \leq 1$ then one obtains $R_{\mathbb{C}} = 2$, whereas if $\deg a_2(t) = 2$ then $R_{\mathbb{C}} \leq 6$.

4. THE ROOT NUMBERS

Let $\mathcal{F}$ be an elliptic surface given by (1.1), and let $\varepsilon_{\mathcal{F}}(t)$ be the root number of the specialization $\mathcal{F}(t)$. Then, we can compute $\varepsilon_{\mathcal{F}}(t)$ as a product

$$\varepsilon_{\mathcal{F}}(t) = - \prod_p w_p(t),$$

where the $w_p(t)$ are the local root numbers of the elliptic curve $\mathcal{F}(t)$ and are defined in terms of representations on the Weil-Deligne group of $\mathbb{Q}_p$. We remark that the -1 appearing in the formula corresponds to the root number at ∞ which is always -1 for any elliptic curve defined over $\mathbb{R}$. The local root numbers can be computed in terms of the reduction type of $\mathcal{F}(t)$ modulo p using tables due to Halberstadt, Connell and Rohrlich ([Hal98], [Con94], [Roh93]). We use them in the version given by Rizzo [Riz03] where the assumption that $\mathcal{F}$ is in minimal Weierstrass form is dropped.¹³

¹³We remark that there are the following misprints in Rizzo's table: in Table II if $(a, b, c) = (\geq 5, 6, 9)$ then the special condition is $c'_6 + 2 \not\equiv 3c_{4,4}(9)$; in Table III, the second line should have $(a, b, c) = (0, 0, \geq 0)$, also if $(a, b, c) = (2, 3, 1)$ then the Kodaira type is I_2^* .

After computing the root number of every specialization, we can compute the average root number. Notice that in general, it is false that

$$(4.1) \quad \text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}}) = - \prod_p \int_{\mathbb{Z}_p} w_p(t) dt.$$

However, it is easy to see that (4.1) is true if $\varepsilon_{\mathcal{F}}(t)$ is the product of *finitely many* functions which are p -adic locally constants almost everywhere (i.e. $w_p(t) = 1$ except for finitely many primes p), and this can be generalized if $\varepsilon_{\mathcal{F}}(t)$ is well approximated by a finite product. In [Hel09], those are called *almost finite* products of p -adic locally constant functions, and we cite his result.

Proposition 13 (Helfgott, Proposition 7.7). *Let S be a finite set of places of $\mathbb{Q}$, including ∞ . For every $v \in S$, let $g_v : \mathbb{Q}_v \rightarrow \mathbb{C}$ be a bounded function that is locally constant almost everywhere. For every $p \notin S$, let $h_p : \mathbb{Q}_p \rightarrow \mathbb{C}$ be a function that is locally constant almost everywhere and satisfies $|h_p(x)| \leq 1$ for all x . Let $B(x) \in \mathbb{Z}[x]$ be a non-zero polynomial, and assume that $h_p(x) = 1$ when $v_p(B(x)) \leq 1$. Let*

$$W(n) = \prod_{v \in S} g_v(n) \prod_{v \notin S} h_v(n).$$

If Conjecture 2 holds for B , then one has

$$\text{Av}_{\mathbb{Z}} W(n) = \frac{c_- + c_+}{2} \prod_{p \in S} \int_{\mathbb{Z}_p} g_p(x) dx \cdot \prod_{p \notin S} \int_{\mathbb{Z}_p} h_p(x) dx,$$

where $c_{\pm} = \lim_{t \rightarrow \pm\infty} \text{sgn}(g_{\infty}(t))$.

We remark that c_{∞} differs from the value of Proposition 7.7 of [Hel09] as he considers averages over positive integers, and we are using (1.2). Rizzo also proves a similar result in his paper [Riz03, Theorem 19] in the particular case that $B(x) = x$ (and then the result is unconditional).

Then, our strategy will be rewrite the root number as

$$\varepsilon_{\mathcal{F}}(t) = - \prod_p w_p^*(t),$$

where the modified local root numbers $w_p^*(t)$ are such that the product is finite or almost finite, and then we can compute the average root number with Proposition 13.

The average root numbers of Theorem 1 and Theorem 2 illustrate those 2 phenomenons. For the family of Theorem 1, the root number is a finite product and it is periodic, and the average root number is a rational number. For the family of Theorem 2, the root number is not given by an almost finite product in terms of the local root numbers $w_p(t)$, but can be written as an almost finite product in terms of the modified local root numbers $w_p^*(t)$, and the average root number is given by a convergent infinite Euler product, computed as in Proposition 13. Our result are unconditional, as the degree of the polynomial B is 2.

4.1. The generalized Washington family and proof of Theorem 1. As in the introduction, we fix $a \in \mathbb{Z}_{\neq 0}$ and we consider the family of elliptic curves

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

with

$$(4.2) \quad \begin{aligned} c_4(t) &= 16(t^2 + 3at + 9a^2); \\ c_6(t) &= -32(t^2 + 3at + 9a^2)(3a + 2t); \\ \Delta(t) &= 16a^2(t^2 + 3at + 9a^2)^2; \\ j(t) &= \frac{256}{a^2}(t^2 + 3at + 9a^2). \end{aligned}$$

Hence, $\mathcal{W}_a$ is a potentially parity-biased family. As explained after Theorem 9, the rank of $\mathcal{W}_a(t)$ over $\mathbb{C}(t)$ is 2 and, as proved in Corollary 6, the rank over $\mathbb{Q}(t)$ is ≤ 1 and it is equal to 1 if and only if a is a square or minus a square. In fact, the points $(0, a\sqrt{a})$ and $(a, a\sqrt{-a})$ are two points in $\mathcal{W}_a(t)(\mathbb{C}(t))$. By the action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, one can see that they are independent and the rank is thus 2 over $\mathbb{Q}(i, \sqrt{a})(t)$. Also, if a (resp. $-a$) is a square then $(0, a\sqrt{a})$ (resp. $(a, a\sqrt{a})$) is an infinite order point defined over $\mathbb{Q}(t)$. As stated in [Duc01], the point $(0, 1)$ can always be part of the generators of $\mathcal{W}_1(t)(\mathbb{Q})$ for any $t \in \mathbb{Z}$ such that $t^2 + 3t + 9$ is square-free.

Clearly, the family $\mathcal{W}_a(t)$ is a generalization of Washington's family (obtained with $a = 1$) and it is closed under quadratic twists: if $w \in \mathbb{Z}_{\neq 0}$ then the quadratic twist of $\mathcal{W}_a(t)$ by w defined by $\mathcal{W}_{a,w}(t): wy^2 = x^3 + tx^2 - a(3a + t)x + a^3$ is isomorphic to $\mathcal{F}_{aw}(wt)$. Furthermore, notice that $\mathcal{W}_{a/b}(r/s)$ is isomorphic to $\mathcal{W}_{abs^2}(b^2sr)$.

4.1.1. *The local root numbers of $\mathcal{W}_a(t)$.* In this section, we give formula for the local root numbers of $\mathcal{W}_a(t)$ for $t \in \mathbb{Z}$. In the following, we let $f_a(t) := (t^2 + 3at + 9a^2)$. Also, for convenience of notation, we indicate with $\varepsilon_a(t)$ the root number $\varepsilon_{\mathcal{W}_a}(t)$ and we denote by $w_p(t)$ (a will always be understood) the local root number at p of $\mathcal{W}_a(t)$. The formula below can be directly computed from Rizzo's tables ([Riz03]) and can be deduced from the general formula of the root number of $\mathcal{F}_s$ given in the appendix A.

Case $p \geq 3$.

Proposition 14. *For $p \geq 3$ we have*

$$w_p(t) = \begin{cases} \left(\frac{-1}{p}\right)^{v_p(a)+v_p(f_a(t))} & \text{if } 0 \leq v_p(a) \leq v_p(t), \\ -\left(\frac{t_p}{p}\right) & \text{if } 0 \leq v_p(t) < v_p(a) \text{ and } v_p(t) \text{ is even,} \\ \left(\frac{-1}{p}\right) & \text{if } 0 \leq v_p(t) < v_p(a) \text{ and } v_p(t) \text{ is odd.} \end{cases}$$

Proof. We check only the case $p \geq 5$. The case of $p = 3$ is analogous but involves a much more lengthy case by case analysis of all possibilities using Table II of [Riz03]. We remark that it's quite surprising that the final formula for $p = 3$ turns out to be the same as for the case $p \geq 5$.

Let $p \geq 5$, and we first suppose that $0 \leq v_p(a) < v_p(t)$. Then, $v_p(f_a(t)) = 2v_p(a)$, and

$$v_p(c_4, c_6, \Delta) = (2v_p(a), 4v_p(a), 6v_p(a)).$$

We have to find the smallest triple (g, h, k) of nonnegative integers such that $g \equiv v_p(c_4) \pmod{4}$, $h \equiv v_p(c_6) \pmod{6}$ and $k \equiv v_p(\Delta) \pmod{12}$, and then we can read the value of $w_p(t)$ in the Tables of [Riz03] giving the root number of the minimal model. For convenience, we use the following notation between triplets of non-negative integers:

$$(g, h, k) \sim (g', h', k') \iff (g, h, k) = (g', h', k') - \lambda(4, 6, 12),$$

for an integer λ . Writing $v_p(a) = 2\ell + \tau$, with $\tau \in \{0, 1\}$, we have that

$$v_p(c_4, c_6, \Delta) \sim (2\tau, 3\tau, 6\tau)$$

and using Table I of [Riz03], we get that $w_p(t) = \left(\frac{-1}{p}\right)^{v_p(a)}$ when $0 \leq v_p(a) < v_p(t)$, which agrees with the statement of the proposition, as $v_p(f_a(t))$ is even in that case.

Suppose now that $0 \leq v_p(t) < v_p(a)$. Similarly to the first case, we write $v_p(t) = 2\ell + \tau$, $\tau \in \{0, 1\}$, and then $v_p(a) = 2\ell + \tau + (v_p(a) - v_p(t))$, with $v_p(a) - v_p(t) > 0$. This gives

$$\begin{aligned} v_p(c_4, c_6, \Delta) &= (4\ell + 2\tau, 6\ell + 3\tau, 12\ell + 6\tau + 2(v_p(a) - v_p(t))) \\ &\sim \begin{cases} (0, 0, 2(v_p(a) - v_p(t))) & \text{if } v_p(t) \text{ is even,} \\ (2, 3, 6 + 2(v_p(a) - v_p(t))) & \text{if } v_p(t) \text{ is odd,} \end{cases} \end{aligned}$$

and using Table II of [Riz03], we get

$$w_p(t) = \begin{cases} -\left(\frac{-c_6(t)_p}{p}\right) = -\left(\frac{t_p}{p}\right) & \text{if } v_p(t) \text{ is even,} \\ \left(\frac{-1}{p}\right) & \text{if } v_p(t) \text{ is odd.} \end{cases}$$

Finally, suppose that $v_p(t) = v_p(a)$. Then, $v_p(f_a(t)) = 2v_p(t) + v_p(t_p^2 + 3a_pt_p + 9a_p^2) = 2v_p(t) + v_p(f_{a_p}(t_p))$, and similarly, $v_p(2t + 3a) = v_p(t) + v_p(2t_p + 3a_p)$. We write $v_p(f_{a_p}(t_p)) = 6k + \tau$ with $0 \leq \tau \leq 5$ and $v_p(t) = 2\ell + \tau'$ with $0 \leq \tau' \leq 1$. We have

$$\begin{aligned} v_p(c_4, c_6, \Delta) &= (4\ell + 2\tau' + 6k + \tau, 6\ell + 3\tau' + 6k + \tau + v_p(2t_p + 3a_p), 12\ell + 6\tau' + 12k + 2\tau) \\ &\sim (2\tau' + 6k + \tau, 3\tau' + 6k + \tau + v_p(2t_p + 3a_p), 6\tau' + 12k + 2\tau) \\ (4.3) \quad &\sim (2k + 2\tau' + \tau, 3\tau' + \tau + v_p(2t_p + 3a_p), 6\tau' + 2\tau). \end{aligned}$$

We first suppose that $v_p(t) = v_p(a)$ is even. We note that if $v_p(2t_p + 3a_p) > 0$ then $v_p(f_{a_p}(t_p)) = 0$, i.e. $\tau = k = 0$. Replacing $\tau' = 0$ in (4.3), and using Table I of [Riz03], it is easy to see that

$$w_p(t) = \begin{cases} 1 & \tau = 0 \\ \left(\frac{-1}{p}\right) & \tau = 1, 3, 5 \\ \left(\frac{-3}{p}\right) & \tau = 2, 4 \end{cases}$$

To see that this agrees with the statement of the proposition, we remark that if $v_p(f_{a_p}(t_p)) > 0$, then $t_p^2 + 3a_pt_p + 9a_p^2$ has a root modulo p and its discriminant $-3a_p^2$ is a square modulo p , hence, $(-3/p) = 1$.

We now suppose that $v_p(t) = v_p(a)$ is odd, i.e. $\tau' = 1$. Replacing in (4.3) and using Table I of [Riz03], we have

$$(v_p(c_4), v_p(c_6), v_p(\Delta)) \sim (2 + 2k + 2\tau, 3 + v_p(3a_p + 2t_p) + \tau, 6 + 2\tau),$$

and it is easy to see that

$$w_p(t) = \begin{cases} \left(\frac{-1}{p}\right) & \tau = 0, 2, 4 \\ \left(\frac{-3}{p}\right) & \tau = 1, 5 \\ 1 & \tau = 3. \end{cases}$$

Again, using the fact that $\left(\frac{-3}{p}\right) = 1$ when $\tau > 0$, this agrees with the statement of the proposition. $\square$

Case $p = 2$. For $a \in \mathbb{Z}_{\neq 0}$ and $t \in \mathbb{Z}$, we set $s_a(t) \in \{\pm 1\}$ such that $w_2(t) \equiv s_a(t)f_a(t)_2 \pmod{4}$.

Proposition 15. *The values $s_a(t)$ are given by the following cases.*

- For $0 \leq v_2(a) \leq v_2(t)$ and $v_2(a)$ even then $s_a(t) = 1$ if and only if

$$\begin{cases} a_2 = \pm 1 \pmod{8} \\ \text{or} \\ a_2 = 3 \pmod{8} \quad \text{and } 2^{-v_2(a)}t \equiv 1, 2, 3 \pmod{4} \\ \text{or} \\ a_2 = 5 \pmod{8} \quad \text{and } 2^{-v_2(a)}t \equiv 0, 2, 3 \pmod{4} \end{cases}.$$
- For $0 \leq v_2(a) \leq v_2(t)$ and $v_2(a)$ odd then $s_a(t) = 1$ if and only if

$$\begin{cases} a_2 = 1 \pmod{4} \quad \text{and } 2^{-v_2(a)}t \equiv 1, 2 \pmod{4} \\ \text{or} \\ a_2 = 3 \pmod{4} \quad \text{and } 2^{-v_2(a)}t \equiv 0, 1 \pmod{4} \end{cases}.$$
- For $v_2(a) = v_2(t) + 1$ and $v_2(t)$ even then $s_a(t) = 1$ if and only if

$$\begin{cases} a_2 = 1 \pmod{4} \quad \text{and } t_2 \equiv 1, 3 \pmod{8} \\ \text{or} \\ a_2 = 3 \pmod{4} \quad \text{and } t_2 \equiv 1, 7 \pmod{8} \end{cases}.$$

- For $v_2(a) = v_2(t) + 1$ and $v_2(t)$ odd then $s_a(t) = 1$ if and only if $t_2 \equiv a_2 \pmod{4}$.
- For $v_2(a) = v_2(t) + 2$ and $v_2(t)$ even then $s_a(t) = 1$ if and only if

$$\begin{cases} a_2 = 1 \pmod{4} & \text{and } t_2 \equiv 3, 5, 7 \pmod{8} \\ \text{or} \\ a_2 = 3 \pmod{4} & \text{and } t_2 \equiv 1, 3, 7 \pmod{8} \end{cases}.$$

- For $v_2(a) = v_2(t) + 2$ and $v_2(t)$ odd then $s_a(t) = 1$ if and only if $t_2 \equiv 1 \pmod{4}$.
- For $v_2(a) \geq v_2(t) + 3$ and $v_2(t)$ even then $s_a(t) = 1$ if and only if

$$\begin{cases} v_2(a) = v_2(t) + 3 & \text{and } t_2 \equiv 3, 5, 7 \pmod{8} \\ \text{or} \\ v_2(a) = v_2(t) + 4 & \text{and } t_2 \equiv 1 \pmod{4} \\ \text{or} \\ v_2(a) \geq v_2(t) + 5 & \text{and } t_2 \equiv 5 \pmod{8} \end{cases}.$$

- For $v_2(a) \geq v_2(t) + 3$ and $v_2(t)$ odd then $s_a(t) = 1$ if and only if $t_2 \equiv 1 \pmod{4}$.

Proof. As for Proposition 14, one performs a rather lengthy case by case analysis of all possibilities using Table III of [Riz03]). $\square$

Remark 2. Note that if $v_2(a) = v_2(t) + 4$ then in any case $s_a(t) \equiv t_2 \pmod{4}$ and that if $v_2(a) \geq v_2(t) + 3$ and $v_2(t)$ odd, then $s_a(t) \equiv t_2 \pmod{4}$. These facts will be important in the proofs of Theorems 3, 4 and 5.

The root number of $\mathcal{W}_a$ and proof of the first part of Theorem 1. By the previous section we have $\varepsilon_a(t) = -\prod_p w_p(t)$ we now show how to transform this product into

$$(4.4) \quad \varepsilon_a(t) \equiv -s_a(t) \gcd(a_2, t) \prod_{p \mid \frac{a_2}{\gcd(a_2, t)}} (-1)^{1+v_p(t)} \left(\frac{t_p}{p} \right)^{1+v_p(t)} \pmod{4}.$$

as given in Theorem 1. We recall that $t_p := p^{-v_p(t)}t$ and thus $a_2 := 2^{-v_2(a)}a$.

Proof. Let $p \geq 3$. From the definition $f_a(t) := (t^2 + 3at + 9a^2)$ one has that if $0 \leq v_p(t) < v_p(a)$, then $v_p(f_a(t)) = 2v_p(t)$. Hence, by Proposition 14, if $0 \leq v_p(t) < v_p(a)$ then

$$w_p(t) = \left(\frac{-1}{p} \right)^{v_p(f_a(t)) + v_p(a)} \left(-\left(\frac{t_p}{p} \right) \right)^{1+v_p(t)} \left(\frac{-1}{p} \right)^{v_p(t) + v_p(a)}.$$

Thus,

$$\prod_{p \geq 3} w_p(t) = \prod_{p \geq 3} \left(\frac{-1}{p} \right)^{v_p(f_a(t)) + v_p(a)} \cdot \prod_{\substack{p \geq 3 \\ 0 \leq v_p(t) < v_p(a)}} \left(-\left(\frac{t_p}{p} \right) \right)^{1+v_p(t)} \left(\frac{-1}{p} \right)^{v_p(t) + v_p(a)}$$

Using the fact that $\left(\frac{-1}{p} \right) \equiv p \pmod{4}$, we have

$$\prod_{p \geq 3} \left(\frac{-1}{p} \right)^{v_p(f_a(t)) + v_p(a)} \equiv |(af_a(t))_2| \equiv |a_2| f_a(t)_2 \pmod{4}.$$

since $f_a(t) > 0$ for all t . Now, for a prime p , we have $0 \leq v_p(t) < v_p(a)$ if and only if $p \mid \frac{a}{\gcd(a, t)}$. In this case we also have $v_p(t) + v_p(a) \equiv v_p(a/\gcd(a, t)) \pmod{2}$. Furthermore, the odd prime factors of

$\frac{a}{\gcd(a,t)}$ are the prime factors of $(a/\gcd(a,t))_2$ and $(a/\gcd(a,t))_2 = \frac{a_2}{\gcd(a_2,t)}$. So,

$$\begin{aligned} \prod_{\substack{p \geq 3 \\ 0 \leq v_p(t) < v_p(a)}} \left(-\left(\frac{t_p}{p}\right)\right)^{1+v_p(t)} \left(\frac{-1}{p}\right)^{v_p(t)+v_p(a)} &= \prod_{p \mid \frac{a_2}{\gcd(a_2,t)}} \left(-\left(\frac{t_p}{p}\right)\right)^{1+v_p(t)} \left(\frac{-1}{p}\right)^{v_p(a_2/\gcd(a_2,t))} \\ &\equiv \frac{|a_2|}{\gcd(a_2,t)} \prod_{p \mid \frac{a_2}{\gcd(a_2,t)}} \left(-\left(\frac{t_p}{p}\right)\right)^{1+v_p(t)} \pmod{4} \end{aligned}$$

Finally, recalling that by definition $w_2(t) \equiv s_a(t)f_a(t)_2 \pmod{4}$, we have

$$\begin{aligned} \varepsilon_a(t) &= - \prod_{p \geq 2} w_p(t) \\ &\equiv -s_a(t) \frac{(f_a(t)_2)^2 |a_2|^2}{\gcd(a_2,t)} \prod_{p \mid \frac{a_2}{\gcd(a_2,t)}} \left(-\left(\frac{t_p}{p}\right)\right)^{1+v_p(t)} \pmod{4} \\ &\equiv -s_a(t) \gcd(a_2,t) \prod_{p \mid \frac{a_2}{\gcd(a_2,t)}} (-1)^{1+v_p(t)} \left(\frac{t_p}{p}\right)^{1+v_p(t)} \pmod{4} \end{aligned}$$

as claimed. $\square$

Corollary 16 (O. Rizzo). *Let $\mathcal{W}_1: y^2 = x^3 + tx^2 - (t+3)x + 1$ be the Washington's family. Then the root number of E_t is -1 for every $t \in \mathbb{Z}$.*

4.1.2. *The average root number for $\mathcal{W}_a(t)$ and the proof of the second part of Theorem 1.* In this section, we give a closed formula for the average root number of $\mathcal{F}_a(t)$.

Proposition 17. *The average root number of the family $\mathcal{W}_a$ is*

$$\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{W}_a}) = - \prod_{p \mid 2a} E_{\mathcal{W}_a}(p),$$

where for p odd we have

$$E_{\mathcal{W}_a}(p) = \begin{cases} \frac{1 - p^{-2\lfloor v_p(a)/2 \rfloor}}{p+1} + p^{-v_p(a)} & \text{if } p \equiv 1 \pmod{4}, \\ -\frac{p-1}{p^2+1} \left(1 - (-p^{-2})^{\lfloor v_p(a)/2 \rfloor}\right) + (-1)^{v_p(a)} p^{-v_p(a)} & \text{if } p \equiv 3 \pmod{4} \end{cases}$$

and for $p = 2$,

$$E_{\mathcal{W}_a}(2) = \begin{cases} 1 & \text{if } a \equiv \pm 1 \pmod{8}, \\ 1/2 & \text{if } a \equiv \pm 3 \pmod{8}, \\ 0 & \text{if } v_2(a) = 1, \\ 1/2 & \text{if } v_2(a) = 2 \text{ and } a_2 \equiv \pm 1 \pmod{8}, \\ 3/8 & \text{if } v_2(a) = 2 \text{ and } a_2 \equiv \pm 3 \pmod{8}, \\ 1/4 & \text{if } v_2(a) = 3, \\ 2^{1-v_2(a)} - \frac{2^{v_2(a)-4}-1}{3 \times 2^{v_2(a)-4}} & \text{if } v_2(a) \geq 4 \text{ and } v_2(a) \text{ even and } a_2 \equiv \pm 1 \pmod{8}, \\ 3/2^{v_2(a)+1} - \frac{2^{v_2(a)-4}-1}{3 \times 2^{v_2(a)-4}} & \text{if } v_2(a) \geq 4 \text{ and } v_2(a) \text{ even and } a_2 \equiv \pm 3 \pmod{8}, \\ 2^{1-v_2(a)} + \frac{1-2^{v_2(a)-3}}{3 \times 2^{v_2(a)-3}} & \text{if } v_2(a) \geq 5 \text{ and } v_2(a) \text{ odd.} \end{cases}$$

Proof. Since $\left(\frac{-1}{p}\right) \equiv 1 \pmod{4}$ for p odd, then we can rewrite (4.4) as

$$\varepsilon_a(t) = -s_a(t) \prod_{p|a_2} \left(\frac{-1}{p}\right)^{\min(v_p(a_2), v_p(t))} \prod_{p \mid \frac{a_2}{\gcd(a_2, t)}} (-1)^{1+v_p(t)} \left(\frac{t_p}{p}\right)^{1+v_p(t)} = - \prod_{p|2a} w_p^*(t),$$

where $w_2^*(t) := s_a(t)$ for p odd

$$w_p^*(t) := \begin{cases} \left(\frac{-1}{p}\right)^{v_p(t)} (-1)^{1+v_p(t)} \left(\frac{t_p}{p}\right)^{1+v_p(t)} & v_p(t) < v_p(a), \\ \left(\frac{-1}{p}\right)^{v_p(a)} & v_p(t) \geq v_p(a). \end{cases}$$

Then, the average root number is given by

$$\text{Av}_{\mathbb{Z}}(\varepsilon_a) = - \prod_{p|2a} \int_{\mathbb{Z}_p} w_p^*(t) d\mu(t).$$

For $p \mid a$ odd, we have

$$\int_{\mathbb{Z}_p} w_p(t) d\mu(t) = \sum_{e=0}^{v_p(a)-1} \left(\frac{-1}{p}\right)^e \frac{(-1)^{e+1}}{p^{e+1}} \sum_{d \in (\mathbb{Z}/p\mathbb{Z})^*} \left(\frac{d}{p}\right)^{e+1} + \left(\frac{-1}{p}\right)^{v_p(a)} \sum_{e=v_p(a)}^{\infty} \sum_{d \in (\mathbb{Z}/p\mathbb{Z})^*} \frac{1}{p^{e+1}}.$$

Let $N_a = \lfloor \frac{v_p(a)-2}{2} \rfloor + 1$. The first sum is

$$\sum_{e=0, e \text{ odd}}^{v_p(a)-1} \left(\frac{-1}{p}\right)^e \frac{p-1}{p} \frac{1}{p^e} = \begin{cases} \frac{1-p^{-2N_a}}{p+1} & p \equiv 1 \pmod{4}, \\ -\frac{p-1}{p^2+1} (1 - (-p^{-2})^{N_a}) & p \equiv 3 \pmod{4}, \end{cases}$$

and the second sum is

$$\left(\frac{-1}{p}\right)^{v_p(a)} \frac{p-1}{p^{v_p(a)+1}} \sum_{e=0}^{\infty} \frac{1}{p^e} = \left(\frac{-1}{p}\right)^{v_p(a)} p^{-v_p(a)}.$$

Thus,

$$(4.5) \quad \int_{\mathbb{Z}_p} w_p(t) d\mu(t) = \begin{cases} \frac{1-p^{-2N_a}}{p+1} + p^{-v_p(a)} & p \equiv 1 \pmod{4} \\ -\frac{p-1}{p^2+1} (1 - (-p^{-2})^{N_a}) + (-1)^{v_p(a)} p^{-v_p(a)} & p \equiv 3 \pmod{4} \end{cases}$$

For $p = 2$ we consider several cases depending on $v_2(a)$ and $a_2 \pmod{8}$.

The case $v_2(a) = 0$. First, looking at the values of $s_a(t)$, we note that if $a \equiv \pm 1 \pmod{8}$ then $s_a(t) = 1$ for all t and $\int_{\mathbb{Z}_2} s_a(t) dt = 1$. Otherwise, we write

$$\int_{\mathbb{Z}_2} s_a(t) dt = \int_{v_2(t)=0} s_a(t) dt + \int_{v_2(t)=1} s_a(t) dt + \int_{v_2(t) \geq 2} s_a(t) dt$$

where in any case, if d is odd then $s_a(d2^e)$ depend on $d \pmod{4}$. If $a \equiv 3 \pmod{8}$ then

$$\int_{v_2(t)=0} s_a(t) dt = \frac{1}{2^{0+2}} \sum_{d \in (\mathbb{Z}/4\mathbb{Z})^\times} s_a(d) = \frac{1}{2^2} (s_a(1) + s_a(3)) = \frac{1}{2}$$

and

$$\int_{v_2(t)=1} s_a(t) dt = \frac{1}{2^{1+2}} \sum_{d \in (\mathbb{Z}/4\mathbb{Z})^\times} s_a(2d) = \frac{1}{2^3} (s_a(2) + s_a(6)) = \frac{1}{2^2}$$

and

$$\int_{v_2(t) \geq 2} s_a(t) dt = \sum_{e \geq 2} \frac{1}{2^{e+2}} \sum_{d \in (\mathbb{Z}/4\mathbb{Z})^\times} s_a(2^e d) = \sum_{e \geq 2} (s_a(2^e) + s_a(2^e 3)) = \sum_{e \geq 2} \frac{-1}{2^{e+1}} = -\frac{1}{2^2}.$$

Summing up the various contributions we obtain $\int_{\mathbb{Z}_2} s_a(t) dt = \frac{1}{2}$. If $a \equiv 5 \pmod{8}$, then the same method leads to the same result:

$$\int_{\mathbb{Z}_2} s_a(t) dt = \int_{v_2(t)=0} s_a(t) dt + \int_{v_2(t)=1} s_a(t) dt + \int_{v_2(t) \geq 2} s_a(t) dt = 0 + \frac{1}{2^2} + \frac{1}{2^2} = \frac{1}{2}.$$

Hence, summarizing the above computations, we have

$$(4.6) \quad \int_{\mathbb{Z}_2} s_a(t) dt = \begin{cases} 1 & \text{if } a \equiv \pm 1 \pmod{8}, \\ \frac{1}{2} & \text{if } a \equiv \pm 3 \pmod{8}. \end{cases}$$

The case $v_2(a) = 1$. We have

$$\int_{\mathbb{Z}_2} s_a(t) dt = \int_{v_2(t)=0} s_a(t) dt + \int_{v_2(t)=1} s_a(t) dt + \int_{v_2(t) \geq 2} s_a(t) dt$$

where, from the table for $s_a(t)$ we have $\int_{v_2(t)=0} s_a(t) dt = \int_{v_2(t)=1} s_a(t) dt = 0$ and

$$\int_{v_2(t) \geq 2} s_a(t) dt = \sum_{e \geq 2} \frac{1}{2^{e+2}} (s_a(2^e) + s_a(2^e 3)) = (-1)^{(a_0-1)/2} \left(\frac{2}{2^{2+2}} + \sum_{e \geq 3} \frac{-2}{2^{e+2}} \right) = 0.$$

Thus if $v_2(a) = 1$, then

$$(4.7) \quad \int_{\mathbb{Z}_2} s_a(t) dt = 0.$$

The case $v_2(a) = 2$. We have

$$\int_{\mathbb{Z}_2} s_a(t) dt = \int_{v_2(t)=0} s_a(t) dt + \int_{v_2(t)=1} s_a(t) dt + \int_{v_2(t)=2} s_a(t) dt + \int_{v_2(t)=3} s_a(t) dt + \int_{v_2(t) \geq 4} s_a(t) dt$$

with $\int_{v_2(t)=0} s_a(t) dt = \frac{1}{2^{0+3}} (s_a(1) + s_a(3) + s_a(5) + s_a(7)) = \frac{1}{2^2}$, $\int_{v_2(t)=1} s_a(t) dt = 0$. Furthermore, we obtain

$$\int_{v_2(t)=2} s_a(t) dt = \frac{1}{2^4} \times \begin{cases} 2 & \text{if } a_2 \equiv \pm 1 \pmod{8} \\ 2 & \text{if } a_2 \equiv 3 \pmod{8} \\ 0 & \text{if } a_2 \equiv 5 \pmod{8} \end{cases}$$

and $\int_{v_2(t)=3} s_a(t) dt = \frac{2}{2^5}$. Finally,

$$\int_{v_2(t) \geq 4} s_a(t) dt = \frac{1}{2^6} \times \begin{cases} 4 & \text{if } a_2 \equiv \pm 1 \pmod{8} \\ -4 & \text{if } a_2 \equiv 3 \pmod{8} \\ 4 & \text{if } a_2 \equiv 5 \pmod{8} \end{cases}$$

and so

$$(4.8) \quad \int_{\mathbb{Z}_2} s_a(t) dt = \begin{cases} \frac{1}{2} & \text{if } v_2(a) = 2 \text{ and } a_2 \equiv \pm 1 \pmod{8}, \\ \frac{3}{8} & \text{if } v_2(a) = 2 \text{ and } a_2 \equiv \pm 3 \pmod{8}. \end{cases}$$

The case $v_2(a) = 3$. In this case, we have

$$\begin{aligned} \int_{v_2(t)=0} s_a(t) dt &= \frac{1}{2^2}, & \int_{v_2(t)=1} s_a(t) dt &= \int_{v_2(t)=2} s_a(t) dt = 0, \\ \int_{v_2(t)=3} s_a(t) dt &= - \int_{v_2(t) \geq 4} s_a(t) dt = (-1)^{(a_0-1)/2} \frac{1}{2^5}. \end{aligned}$$

Thus, if $v_2(a) = 3$ then

$$(4.9) \quad \int_{\mathbb{Z}_2} s_a(t) dt = \frac{1}{4}.$$

The case $v_2(a) \geq 4$ with $v_2(a)$ even. In this case we have

$$\int_{\mathbb{Z}_2} s_a(t) dt = \int_{v_2(t) < v_2(a)} s_a(t) dt + \int_{v_2(t)=v_2(a)} s_a(t) dt + \int_{v_2(t)=v_2(a)+1} s_a(t) dt + \int_{v_2(t) \geq v_2(a)+2} s_a(t) dt.$$

With the same techniques as before,

$$\begin{aligned} \int_{v_2(t)=v_2(a)} s_a(t) dt &= \frac{1}{2^{v_2(a)+1}} \begin{cases} 1 & \text{if } a_2 \equiv \pm 1 \pmod{8}, \\ 1 & \text{if } a_2 \equiv 3 \pmod{8}, \\ 0 & \text{if } a_2 \equiv 5 \pmod{8}, \end{cases} \\ \int_{v_2(t)=v_2(a)+1} s_a(t) dt &= \frac{1}{2^{v_2(a)+2}}, \\ \int_{v_2(t) \geq v_2(a)+2} s_a(t) dt &= \frac{1}{2^{v_2(a)+2}} \begin{cases} 1 & \text{if } a_2 \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } a_2 \equiv 3 \pmod{8}, \\ 1 & \text{if } a_2 \equiv 5 \pmod{8}. \end{cases} \end{aligned}$$

Now,

$$\int_{v_2(t) < v_2(a)} s_a(t) dt = \int_{v_2(t)=v_2(a)-2} s_a(t) dt + \int_{v_2(t)=v_2(a)-4} s_a(t) dt + \sum_{\substack{j=4 \\ j \text{ even}}} \int_{v_2(t)=v_2(a)-2-j} s_a(t) dt$$

The first integral of the right hand side is $\frac{1}{2^{v_2(a)}}$, the second one is 0 and

$$\begin{aligned} \sum_{\substack{j=4 \\ j \text{ even}}}^{v_2(a)-2} \int_{v_2(t)=v_2(a)-2-j} s_a(t) dt &= \sum_{\substack{j=0 \\ j \text{ even}}}^{v_2(a)-6} \int_{v_2(t)=v_2(a)-6-j} s_a(t) dt \\ &= \sum_{\substack{j=0 \\ j \text{ even}}}^{v_2(a)-6} \frac{1}{2^{v_2(a)-6-j+3}} (-2) = -\frac{2^{v_2(a)-4} - 1}{3 \times 2^{v_2(a)-4}}. \end{aligned}$$

Thus, collecting the above results, we have that if $a = 2^{v_2(a)} a_2$ with a_2 odd and $v_2(a) \geq 4$ even, then

$$(4.10) \quad \int_{\mathbb{Z}_2} s_a(t) dt = \frac{1}{2^{v_2(a)}} - \frac{2^{v_2(a)-4} - 1}{3 \times 2^{v_2(a)-4}} + \begin{cases} \frac{1}{2^{v_2(a)}} & \text{if } a_2 \equiv \pm 1 \pmod{8}, \\ \frac{1}{2^{v_2(a)+1}} & \text{if } a_2 \equiv \pm 3 \pmod{8}. \end{cases}$$

The case $v_2(a) \geq 5$ with $v_2(a)$ odd. In this case we have

$$\int_{\mathbb{Z}_2} s_a(t) dt = \int_{v_2(t) < v_2(a)} s_a(t) dt + \int_{v_2(t)=v_2(a)} s_a(t) dt + \int_{v_2(t)=v_2(a)+1} s_a(t) dt + \int_{v_2(t) \geq v_2(a)+2} s_a(t) dt.$$

The integral $\int_{v_2(t)=v_2(a)} s_a(t) dt$ is zero and $\int_{v_2(t)=v_2(a)+1} s_a(t) dt = - \int_{v_2(t) \geq v_2(a)+2} s_a(t) dt$. Then as above,

$$\int_{v_2(t) < v_2(a)} s_a(t) dt = \sum_{\substack{j=0 \\ j \text{ even}}}^{v_2(a)-1} \int_{v_2(t)=j} s_a(t) dt = \sum_{\substack{j=0 \\ j \text{ even}}}^{v_2(a)-1} \int_{v_2(t)=v_2(a)-1-j} s_a(t) dt.$$

Now, $\int_{v_2(t)=v_2(a)-1} s_a(t)dt = 0$, $\int_{v_2(t)=v_2(a)-3} s_a(t)dt = \frac{1}{2^{v_2(a)-1}}$ and

$$\begin{aligned} \sum_{\substack{j=4 \\ j \text{ even}}}^{v_2(a)-1} \int_{v_2(t)=v_2(a)-1-j} s_a(t)dt &= \sum_{\substack{j=0 \\ j \text{ even}}}^{v_2(a)-5} \int_{v_2(t)=v_2(a)-5-j} s_a(t)dt = \sum_{\substack{j=0 \\ j \text{ even}}}^{v_2(a)-5} \frac{-1}{2^{v_2(a)-3-j}} \\ &= -\frac{2^{v_2(a)-3} - 1}{3 \times 2^{v_2(a)-3}}. \end{aligned}$$

Thus, if $v_2(a) \geq 5$ with $v_2(a)$ odd, then

$$(4.11) \quad \int_{\mathbb{Z}_2} s_a(t)dt = \frac{1}{2^{v_2(a)-1}} + \frac{1 - 2^{v_2(a)-3}}{3 \times 2^{v_2(a)-3}}.$$

Thus, by (4.5) and (4.6)-(4.11) the proof of Proposition 17 is complete. $\square$

4.1.3. Families with elevated rank. We can use the family $\mathcal{W}_a(t)$ in order to find families with elevated rank over $\mathbb{Z}$. First, we notice the following corollary

Corollary 18. *Let $a, b \in \mathbb{Z}$ with $a \equiv \pm 1 \pmod{8}$ and $\gcd(a, b) = 1$. Then for all $t \in \mathbb{Z}$, we have*

$$\varepsilon_a(at + b) = - \prod_{p|a} - \left(\frac{b}{p} \right) = (-1)^{1+\lambda(\kappa(a))} \left(\frac{b}{\kappa(a)} \right),$$

where $\kappa(a) := \prod_{p|a} p$ is the kernel of a and λ is the Louville function.

Proof. This is a direct application of Theorem 1. $\square$

In particular, Corollary 18 gives that the root number of $\mathcal{W}_{p^2}(pt + a)$ is 1 for all $t \in \mathbb{Z}$ when a is a quadratic residue mod p and the root number of $\mathcal{W}_p(pt + b)$ is -1 for all t when b is a quadratic non-residue mod p . This proves Corollary 2.

We can also give examples of families of rank 2 and 3 with elevated rank by considering families of the form $\mathcal{W}_a(p(t))$ where $p(t)$ is a degree 2 polynomial. Indeed, for $a \in \mathbb{N}$ consider the family

$$\mathcal{W}_a^\dagger(t) := \mathcal{W}_{a^2}(2t^2 - 2at - a^2).$$

We then have that

$$\mathcal{W}_a^\dagger(t) = \mathcal{W}_{a^2}(2t^2 - 2at - a^2) \simeq \mathcal{F}_{-12(3a)^4}(6(2t - a)^2) \simeq \mathcal{L}_{6, -3^3 a^4, 0}(2t - a).$$

Now, writing $s = -3^3 a^4$, $w = 6$ and $v = 0$ one has that $-4w^2 r = 3(12a)^4$, $-3r = (3a)^4$ and the polynomials $C(x)$ and $R(x)$ of Proposition 12 factor into 3 and 5 irreducible polynomials respectively. Thus, by Proposition 12, we have that $\mathcal{W}_a^\dagger$ has rank 3 over $\mathbb{Q}(t)$ for all a .

Corollary 19. *Let p be a prime number $\equiv \pm 1 \pmod{8}$, and let $\mathcal{W}_{p, \ell}^\dagger(t) := \mathcal{W}_p^\dagger(pt + \ell)$ for $\ell \in \mathbb{Z}$. Then for $(p, \ell) = 1$, $\mathcal{W}_{p, \ell}^\dagger(t)$ is a rank 3 family with elevated rank over $\mathbb{Z}$.*

Proof. For any odd prime p , an easy application of Theorem 1 gives that the root number of $\mathcal{W}_p^\dagger(t)$ is

$$\varepsilon_{\mathcal{W}_p^\dagger}(t) = \begin{cases} \left(\frac{2}{p} \right) & \text{if } p \nmid t \\ -1 & \text{if } p \mid t \end{cases}$$

for any $t \in \mathbb{Z}$. Replacing t by $pt + \ell$, and using the fact that $p \equiv \pm 1 \pmod{8}$, we get the result. $\square$

It's not difficult to construct in a similar way rank 2 families with elevated rank. For example, one such family is given by $\mathcal{W}_4(-3t^2 - 4t - 21)$.

4.1.4. *Twists of Washington's family.* In this section, we consider quadratic twists of the original Washington's family (see [KN92], [Bye97] for some studies about Washington's twists). Let $d \in \mathbb{Z}_{\neq 0}$, the twist by w of Washington's family is given by

$$\mathcal{W}_1^{(d)}(t): y^2 = x^3 + dtx^2 - (t+3)d^2x + d^3.$$

We easily see that the family $\mathcal{W}_1^{(d)}(t)$ is in fact the family $\mathcal{W}_d(dt)$. So in the formula of Theorem 1, the product is empty and equal to one, hence $\varepsilon_{\mathcal{W}_1^{(d)}}(t) \equiv -|d_2|s_d(dt) \pmod{4}$. The value of $s_d(dt)$ is given by the first two cases of Proposition 15, furthermore, we have $2^{-v_2(d)}dt = d_2t$.

Proposition 20. *The root number, $\varepsilon_{\mathcal{W}_1^{(d)}}(t)$ of $\mathcal{W}_1^{(d)}(t)$ is given by the following cases.*

If $v_2(d)$ is even, then

- *if $d_2 \equiv \pm 1 \pmod{8}$ then $\varepsilon_{\mathcal{W}_1^{(d)}}(t) \equiv -|d_2| \pmod{4}$;*
- *if $d_2 \equiv 3 \pmod{8}$ then $\varepsilon_{\mathcal{W}_1^{(d)}}(t) = \text{sgn}(d_2)$ if and only if $t \equiv 1, 2, 3 \pmod{4}$;*
- *if $d_2 \equiv 5 \pmod{8}$ then $\varepsilon_{\mathcal{W}_1^{(d)}}(t) = \text{sgn}(d_2)$ if and only if $t \equiv 1 \pmod{4}$.*

If $v_2(d)$ is odd then $\varepsilon_{\mathcal{W}_1^{(d)}}(t) = \text{sgn}(d_2)$ if and only if $t \equiv 0, 3 \pmod{4}$.

One can also consider the twist by

$$d_u(t) = u^3 + tu^2 - (t+3)u + 1 = u(u-1)t + u^3 - 3u + 1$$

for any $u \in \mathbb{Z}$ (one could also take u to be a polynomial in t). In this case, the generic point $(ud_u(t), d_u(t)^2)$ is a non-torsion point of $\mathcal{W}_1^{(d_u(t))}$. So the rank of $\mathcal{W}_1^{(d_u(t))}$ over $\mathbb{Q}(t)$ is at least 1. Moreover from Proposition 20 we can deduce the following result.

Corollary 21. *Let $u \in \mathbb{Z}$.*

- *If $u \equiv 1 \pmod{4}$ then $\varepsilon_{\mathcal{W}_1^{(d_u(t))}}(t) = 1$ if and only if $d_u(t) > 0$.*
- *If $u \equiv 0 \pmod{4}$ then $\varepsilon_{\mathcal{W}_1^{(d_u(t))}}(t) = 1$ if and only if $d_u(t) < 0$.*

Proof. Assume that $u \equiv 1 \pmod{4}$ then $d_t(u) \equiv -1 \pmod{8}$ for all t and we apply Proposition 20: $\varepsilon(E_{d_t(u)}(t)) \equiv -|d_t(u)| \equiv \text{sgn}(d_t(u))$. If $u \equiv 0 \pmod{4}$ then $d_t(u) \equiv 1 \pmod{8}$ for all t and we apply the same method. $\square$

As an example, let's consider the case $u = 5$, so that $d_t(5) = 20t + 111$. In this case $\varepsilon_{\mathcal{W}_1^{(20t+111)}}(t) > 0$ if and only if $t \geq -5$ and there are at least 2 independent points of $\mathcal{W}_1^{(20t+111)}$:

$$(5(20t+111), (20t+111)^2) \quad \text{and} \quad \left(-\frac{20t+111}{4}, \frac{(20t+111)^2}{8} \right).$$

4.2. **The family $\mathcal{V}_a$ and the proof of Theorem 2.** First we give the root number for the family

$$\mathcal{V}_a: y^2 = x^3 + 3tx^2 + 3atx + a^2t$$

for which we have

$$\begin{aligned} c_4(t) &= 2^4 3^2 t(t-a), \\ c_6(t) &= -2^5 3^3 t(t-a)(2t-a), \\ \Delta(t) &= -2^4 3^3 a^2 t^2 (t-a)^2, \\ j(t) &= -\frac{2^8 3^3}{a^2} t(t-a). \end{aligned}$$

In the following we shall always assume $t \neq 0, a$, so that $\Delta(t) \neq 0$. Also, for convenience of notation, we will use in this section $\varepsilon_a(t)$ for the root number of $\mathcal{V}_a(t)$, and $w_p(t)$ for the local root number at p of $\mathcal{V}_a(t)$. Then,

$$\varepsilon_a(t) = - \prod_p w_p(t).$$

4.2.1. *The local root numbers of $\mathcal{V}_a$.* The local root numbers for $\mathcal{V}_a$ can be obtained by performing a simple but quite lengthy case by case analysis from Rizzo's table [Riz03] as in the proof of Proposition 14. We give the final results only, here for $p \geq 5$ and in Appendix B for $p = 2, 3$.

Lemma 22. *Let $p \geq 5$. Then, for $0 \leq v_p(a) \leq v_p(t)$ one has*

$$w_p(t) = \begin{cases} \left(\frac{-3}{p}\right)\left(\frac{3}{p}\right)^{v_p(t)+v_p(t-a)+v_p(a)} & \text{if } 6 \nmid v_p(t-a) - v_p(t) + 3v_p(a), \\ 1 & \text{if } 6 \mid v_p(t-a) - v_p(t) + 3v_p(a), \end{cases}$$

whereas if $0 \leq v_p(t) < v_p(a)$ then

$$w_p(t) = \begin{cases} -\left(\frac{3t_p}{p}\right) & \text{if } v_p(t) \text{ is even,} \\ \left(\frac{-1}{p}\right) & \text{if } v_p(t) \text{ is odd.} \end{cases}$$

We now modify the local root numbers $w_p(t)$ in order to apply Proposition 13. We will write $\varepsilon_a(t)$ as

$$\varepsilon_a(t) = - \prod_p w_p(t) = - \prod_p w_p^*(t),$$

for some $w_p^*(t)$ satisfying $w_p^*(t) = 1$ for $v_p(t(t-s)) \leq 1$ for all primes $p \nmid 6a$.

Let $p \geq 5$, and suppose that $v_p(a) = 0$ and $p \mid \Delta(t) = -2^4 3^3 a^2 t^2 (t-a)^2$ (if not, $w_p(t) = 1$). Then, we have 2 cases: either $v_p(t) = 0$ and $v_p(t-a) > 0$, or $v_p(t) > 0$ and $v_p(t-a) = 0$. Thus, Lemma 22 gives in this case

$$w_p(t) = \begin{cases} \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)^{v_p(t-a)+1} & v_p(t) = 0, v_p(t-a) > 0 \text{ and } 6 \nmid v_p(t-a), \\ \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)^{v_p(t)+1} & v_p(t) > 0, v_p(t-a) = 0 \text{ and } 6 \nmid v_p(t), \\ 1 & \text{if } v_p(t) = 0, v_p(t-a) > 0 \text{ and } 6 \mid v_p(t-a) \text{ or if } v_p(t) > 0, 6 \mid v_p(t). \end{cases}$$

Then, for all $p \neq 2, 3$, we define

$$(4.12) \quad w_p^*(t) := w_p(t) \left(\frac{-1}{p}\right)^{v_p(t-a)} \left(\frac{-1}{p}\right)^{v_p(t)},$$

so that for $p \nmid 6a$ we have $w_p^*(t) = 1$ for $v_p(t(t-a)) \leq 1$.

Lemma 23. *For $p \geq 5$, let $w_p^*(t)$ be defined by (4.12). Let $w_2^*(t), w_3^*(t), w_\infty^*(t) \in \{\pm 1\}$ be defined by*

$$\begin{aligned} w_3^*(t) &= (-1)^{v_3(t)} (-1)^{v_3(t-a)} w_3(t) \\ w_2^*(t) &\equiv t_2(t-a)_2 w_2(p) \pmod{4} \\ w_\infty^*(t) &= \text{sgn}(t(t-a)) \end{aligned}$$

Then,

$$\varepsilon_a(t) = -w_\infty^*(t) \prod_p w_p^*(t).$$

Proof. Using (4.12), we have

$$\prod_{p \neq 2, 3} w_p^*(t) = \prod_{p \neq 2, 3} \left(\frac{-1}{p}\right)^{v_p(t)} \left(\frac{-1}{p}\right)^{v_p(t-a)} \prod_{p \neq 2, 3} w_p(t).$$

Since $\left(\frac{-1}{p}\right) \equiv p \pmod{4}$, then

$$\begin{aligned} \prod_{p \neq 2,3} \left(\frac{-1}{p}\right)^{v_p(t)} \left(\frac{-1}{p}\right)^{v_p(t-a)} &\equiv (-1)^{v_3(t)} (-1)^{v_3(t-a)} \prod_{p \neq 2} p^{v_p(t)} p^{v_p(t-a)} \pmod{4} \\ &\equiv (-1)^{v_3(t)} (-1)^{v_3(t-a)} |t_2(t-a)_2| \pmod{4}, \end{aligned}$$

which proves the result. $\square$

4.2.2. *The average root number for $\mathcal{V}_a(t)$.* Using Lemma 23 and Proposition 13, we then have

$$(4.13) \quad \text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{V}_a}) = - \prod_p \int_{\mathbb{Z}_p} w_p^*(t) dt,$$

since $t(t-a)$ is positive except for finitely many values of t . Computing the p -adic integrals we will obtain the following proposition, thus completing the proof of Theorem 2.

Proposition 24. *The average root number of the family $\mathcal{V}_a$ is given by the Euler product*

$$\text{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{V}_a}) = - \prod_p E_{\mathcal{V}_a}(p),$$

where the Euler factors for $p = 2$ and $p = 3$ are given by

$$\begin{aligned} E_{\mathcal{V}_a}(2) &= \begin{cases} -1/2 & \text{if } v_2(a) = 0 \\ 0 & \text{if } v_2(a) = 1 \\ 1/8 & \text{if } v_2(a) = 2 \\ 2^{1-v_2(a)} + \frac{1}{3}(4^{-(v_2(a)-3)/2} - 1) & \text{if } v_2(a) \geq 3 \text{ with } v_2(a) \text{ odd} \\ 2^{-v_2(a)-1} + \frac{1}{3}(4^{-(v_2(a)-4)/2} - 1) & \text{if } v_2(a) \geq 4 \text{ with } v_2(a) \text{ even,} \end{cases} \\ E_{\mathcal{V}_a}(3) &= \begin{cases} \frac{6}{7} \frac{1}{3^{v_3(a)+2}} + \frac{3}{4}(3^{-v_3(a)} - 1) & \text{if } v_3(a) \equiv 0 \pmod{2} \\ \frac{6}{7} \frac{1}{3^{v_3(a)+2}} + \frac{3}{4}(3^{-v_3(a)+1} - 1) & \text{if } v_3(a) \equiv 1 \pmod{2}, \end{cases} \end{aligned}$$

whereas for $p \geq 5$, the Euler factors are

$$E_{\mathcal{V}_a}(p) = \left(\frac{-1}{p}\right) \frac{1 - p^{j-v_p(a)}}{p+1} + \left(\frac{-1}{p}\right)^j \frac{1}{p^{v_p(a)}} \begin{cases} 1 & p \equiv 1 \pmod{3}, \\ \left(1 - \frac{4(p-1)(p^{1-j} + p^{3+j})}{p^6 - 1}\right) & p \equiv 2 \pmod{3}, \end{cases}$$

where $v_p(a) \equiv j \pmod{2}$ with $j \in \{0, 1\}$. In particular, for $v_p(a) = 0$ and $p \geq 5$, we have

$$E_{\mathcal{V}_a}(p) = \begin{cases} 1 & p \equiv 1 \pmod{3}, \\ \left(1 - \frac{4(p-1)(p+p^3)}{p^6 - 1}\right) & p \equiv 2 \pmod{3}. \end{cases}$$

When computing the p -adic integrals we shall need the following Lemma.

Lemma 25. *For $k \in \mathbb{Z}_{\geq 0}$, let $S_k := \{t \in \mathbb{Z}_p : v_p(t) = v_p(a), v_p(t-a) = v_p(a) + k\}$, then S_k has measure*

$$\mu(S_k) = \begin{cases} \frac{p-2}{p^{v_p(a)+1}} & \text{if } k = 0 \\ \frac{p-1}{p^{v_p(a)+k+1}} & \text{if } k \geq 1 \end{cases}$$

Proof. Let χ_k be the characteristic function of S_k . If $k = 0$, then

$$\mu(S_k) = \frac{1}{p^{v_p(a)+1}} \sum_{d \in (\mathbb{Z}/p\mathbb{Z})^*} \chi_0(p^{v_p(a)}d),$$

and $\chi_0(p^{v_p(a)}d) = 1$ iff $p^{v_p(a)}d - p^{v_p(a)}a_p \not\equiv 0 \pmod{p^{v_p(a)+1}}$ and thus iff $d \not\equiv a_p \pmod{p}$, which gives the result. In the same way, considering the contribution of $d \equiv a_p \pmod{p}$ only, we have

$$\mu(t \in \mathbb{Z}_p : v_p(t) = v_p(a), v_p(t-a) \geq v_p(a) + 1) = \frac{1}{p^{v_p(a)+1}}$$

and similarly, for any $k \geq 1$,

$$\mu(t \in \mathbb{Z}_p : v_p(t) = v_p(a), v_p(t-a) \geq v_p(a) + k) = \frac{1}{p^{v_p(a)+k}}.$$

Then,

$$\mu(S_k) = \frac{1}{p^{v_p(a)+k}} - \frac{1}{p^{v_p(a)+k+1}} = \frac{p-1}{p^{v_p(a)+k+1}}$$

completing the proof of the Lemma. $\square$

First, we shall compute $\int_{\mathbb{Z}_p} w_p^*(t) dt$ for $p \geq 5$.

Proposition 26. *Let $p \geq 5$. Then $\int_{\mathbb{Z}_p} w_p^*(t) dt = E_{\mathcal{V}_a}(p)$.*

Proof. We shall consider three cases, according to whether $v_p(t)$ is smaller, equal, or larger than $v_p(a)$.

The case $0 \leq v_p(t) < v_p(a)$. We have that $v_p(a) > 0$, and $v_p(t-a) = v_p(t)$ and so by (4.12) in this case we have $w_p^*(t) = w_p(t)$. Using Lemma 22, we have

$$\int_{0 \leq v_p(t) < v_p(a)} w_p^*(t) dt = - \int_{0 \leq v_p(t) < v_p(a)} \left(\frac{3t_p}{p} \right) dt + \int_{0 \leq v_p(t) < v_p(a)} \left(\frac{-1}{p} \right) dt.$$

It is easy to see that the first integral is 0 and that so is the second if $v_p(a) = 1$ (the domain of integration is empty). Thus, suppose $v_p(a) \geq 2$. Then, letting $v_p(a) \equiv j \pmod{2}$ with $j \in \{0, 1\}$

$$(4.14) \quad \int_{0 \leq v_p(t) < v_p(a)} w_p^*(t) dt = \left(\frac{-1}{p} \right) \sum_{0 \leq 2k+1 < v_p(a)} \frac{p-1}{p^{2k+2}} = \left(\frac{-1}{p} \right) \frac{1}{p+1} (1 - p^{j-v_p(a)}).$$

Notice that the expression on the right is 0 if $v_p(a) = 0$.

The case $v_p(t) = v_p(a)$. We let $v_p(t-a) = v_p(a) + k$, with $k \geq 0$. We have

$$(4.15) \quad w_p^*(t) = \begin{cases} \left(\frac{-3}{p} \right)^{k+1} \left(\frac{3}{p} \right)^{v_p(a)} & \text{if } 3v_p(a) + k \not\equiv 0 \pmod{6}, \\ \left(\frac{-1}{p} \right)^k & \text{if } 3v_p(a) + k \equiv 0 \pmod{6}, \end{cases}$$

and

$$\begin{aligned} \int_{v_p(t)=v_p(a)} w_p^*(t) dt &= \sum_{k=0}^{\infty} \int_{\substack{v_p(t)=v_p(a) \\ v_p(t-a)=v_p(a)+k}} w_p^*(t) dt \\ &= \sum_{k=0}^{\infty} \mu(t \in \mathbb{Z}_p : v_p(t) = v_p(a), v_p(t-a) = v_p(a) + k) w_p^*(t), \end{aligned}$$

with $w_p^*(t)$ as in (4.15). Thus, by Lemma 25 we have

$$\begin{aligned} \int_{v_p(t)=v_p(a)} w_p^*(t) dt &= \frac{p-2}{p^{v_p(a)+1}} \left(\frac{-1}{p}\right)^j + \sum_{\substack{k=1 \\ k \not\equiv 3j \pmod{6}}}^{\infty} \frac{p-1}{p^{v_p(a)+1+k}} \left(\frac{-3}{p}\right)^{k+1} \left(\frac{3}{p}\right)^j \\ &\quad + \sum_{\substack{k=1 \\ k \equiv 3j \pmod{6}}}^{\infty} \frac{p-1}{p^{v_p(a)+1+k}} \left(\frac{-1}{p}\right)^j. \end{aligned}$$

The sum over k in the first line gives

$$\begin{aligned} \frac{p-1}{p^{v_p(a)+1}} \left(\frac{-3}{p}\right) \left(\frac{3}{p}\right)^j \sum_{k=1}^{\infty} p^{-k} \left(\frac{-3}{p}\right)^k - \frac{p-1}{p^{v_p(a)+1}} \left(\frac{-1}{p}\right)^j \left(\frac{-3}{p}\right) \sum_{\substack{k=1 \\ k \equiv 3j \pmod{6}}}^{\infty} p^{-k} \\ = \frac{p-1}{p^{v_p(a)+1}} \left(\frac{3}{p}\right)^j \frac{1}{p - \left(\frac{-3}{p}\right)} - \frac{p-1}{p^{v_p(a)+1}} \left(\frac{-1}{p}\right)^j \left(\frac{-3}{p}\right) \frac{p^{3j}}{p^6 - 1} \end{aligned}$$

whereas the sum over k in the second line adds up to

$$\frac{(p-1)p^{3j}}{p^{v_p(a)+1}(p^6 - 1)} \left(\frac{-1}{p}\right)^j$$

Then, since $\left(\frac{-3}{p}\right) = 1$ if $p \equiv 1 \pmod{3}$ and $\left(\frac{-3}{p}\right) = -1$ if $p \equiv 2 \pmod{3}$, we have

$$\int_{v_p(t)=v_p(a)} w_p^*(t) dt = \left(\frac{-1}{p}\right)^j \begin{cases} \frac{p-1}{p^{v_p(a)+1}} & p \equiv 1 \pmod{3}, \\ \frac{1}{p^{v_p(a)+1}} \left(p - 2 + (-1)^j \frac{p-1}{p+1} + \frac{2p^{3j}(p-1)}{p^6 - 1}\right) & p \equiv 2 \pmod{3}. \end{cases}$$

The case $0 \leq v_p(a) < v_p(t)$. In this case, $v_p(t-a) = v_p(a)$, and by Lemma 22 and (4.12) we get

$$\left(\frac{-1}{p}\right)^{v_p(a)} w_p^*(t) = \begin{cases} \left(\frac{-3}{p}\right)^{v_p(t)+1} & v_p(t) - 4v_p(a) \not\equiv 0 \pmod{6} \\ 1 & v_p(t) - 4v_p(a) \equiv 0 \pmod{6}, \end{cases}$$

which gives

$$\left(\frac{-1}{p}\right)^{v_p(a)} \int_{0 \leq v_p(a) < v_p(t)} w_p^*(p) dt = \sum_{\substack{e > v_p(a) \\ e - 4v_p(a) \not\equiv 0 \pmod{6}}} \frac{p-1}{p^{e+1}} \left(\frac{-3}{p}\right)^{e+1} + \sum_{\substack{e > v_p(a) \\ e - 4v_p(a) \equiv 0 \pmod{6}}} \frac{p-1}{p^{e+1}}.$$

Thus, for $v_p(a) \equiv j \pmod{2}$ with $j \in \{0, 1\}$ the first sum is

$$\begin{aligned} \sum_{e > v_p(a)} \frac{p-1}{p^{e+1}} \left(\frac{-3}{p}\right)^{e+1} - \left(\frac{-3}{p}\right) \sum_{e > -\frac{1}{2}v_p(a)} \frac{p-1}{p^{4v_p(a)+6e+1}} \\ = \left(\frac{-3}{p}\right)^{v_p(s)} \frac{p-1}{p^{v_p(s)+1}} \frac{1}{p - \left(\frac{-3}{p}\right)} - \left(\frac{-3}{p}\right) \frac{(p-1)p^{3j}}{p^{v_p(a)+1}(p^6 - 1)} \end{aligned}$$

whereas the second gives

$$\sum_{\substack{e > v_p(a) \\ e - 4v_p(a) \equiv 0 \pmod{6}}} \frac{p-1}{p^{e+1}} = \frac{(p-1)p^{3j}}{p^{v_p(a)+1}(p^6 - 1)}.$$

Thus,

$$(4.16) \quad \int_{v_p(t) > v_p(a)} w_p^*(t) dt = \left(\frac{-1}{p}\right)^j \begin{cases} \frac{1}{p^{v_p(s)+1}} & p \equiv 1 \pmod{3}, \\ \frac{(-1)^j}{p^{v_p(s)+1}} \frac{p-1}{p+1} + \frac{2(p-1)p^{3j}}{p^{v_p(a)+1}(p^6-1)} & p \equiv 2 \pmod{3}. \end{cases}$$

Finally, summing

$$\int_{\mathbb{Z}_p} w_p^*(t) dt = \int_{0 \leq v_p(t) < v_p(a)} w_p^*(t) dt + \int_{v_p(t) = v_p(a)} w_p^*(t) dt + \int_{0 \leq v_p(a) < v_p(t)} w_p^*(t) dt,$$

we get the result. $\square$

Proposition 27. *We have $\int_{\mathbb{Z}_3} w_3^*(t) dt = E_{\mathcal{V}_a}(3)$.*

Proof. We recall that

$$w_3^*(t) = (-1)^{v_3(t)} (-1)^{v_3(t-a)} w_3(t),$$

and that the values of $w_3(t)$ are given in Proposition 42 of Appendix B.

The case $0 \leq v_3(a) < v_3(t)$. In this case we have $v_3(t-a) = v_3(a)$. Also, from Appendix B, we have that $w_3(t)$ depends only on $v_3(t)$ and $(t-a)_3 \pmod{9}$ (and possibly a_3 and $v_3(a)$). Thus, if $v_3(t) \equiv v_3(a) \pmod{3}$, we have that

$$\int_{v_3(t)=e} w_3^*(t) dt = \frac{(-1)^{v_3(a)+e}}{3^{e+2}} \sum_{d \in (\mathbb{Z}/9\mathbb{Z})^*} w_{3,a}(dp^e) = \frac{2(-1)^{v_3(a)+e}}{3^{e+2}}.$$

If $v_3(t) - v_3(a) \not\equiv 0 \pmod{3}$, then the integral is easily seen to be 0. This gives that

$$\begin{aligned} \int_{0 \leq v_3(a) < v_3(t)} w_3^*(t) dt &= \frac{2(-1)^{v_3(a)}}{9} \sum_{\substack{e > v_3(a) \\ e \equiv v_3(a) \pmod{3}}} \frac{(-1)^e}{3^e} \\ &= \frac{2}{3^{v_3(a)+2}} \sum_{n=1}^{\infty} (-1/3)^{3n} = \frac{-1}{14 \cdot 3^{v_3(a)+2}}. \end{aligned}$$

The case $0 \leq v_3(t) = v_3(a)$. Let $e = v_3(t) = v_3(a)$ and $v_3(t-a) = e + k$ with $k \geq 1$ so that $w_3^*(t) = (-1)^k w_3(t)$. First, we consider the case $k \geq 1$. If $k \equiv 0 \pmod{3}$ (and then $k \geq 3$), then $w_3(t)$ is determined by a congruence modulo 9 on $(t-a)_3$, and we compute

$$\int_{\substack{v_3(t)=v_3(a)=e, \\ v_3(t-a)=e+k}} w_3^*(t) dt = \frac{(-1)^k}{3^{e+k+2}} \sum_{\substack{d \in (\mathbb{Z}/3^{k+2}\mathbb{Z})^* \\ d \equiv a_3 \pmod{3^k} \\ d \not\equiv a_3 \pmod{3^{k+1}}}} w_3((d-a_3)_3) = 2 \frac{(-1)^k}{3^{e+k+2}}.$$

For $k \not\equiv 0 \pmod{3}$ and $k \geq 1$ we easily get

$$\int_{\substack{v_3(t)=v_3(a)=e \\ v_3(t-a)=e+k}} w_3^*(t) dt = 0$$

and thus

$$(4.17) \quad \int_{\substack{v_3(t)=v_3(a)=e \\ v_3(t-a) > e}} w_3^*(t) dt = \frac{2}{3^{e+2}} \sum_{\substack{k=1 \\ k \equiv 0 \pmod{3}}}^{\infty} (-1)^k / 3^k = -\frac{1}{14} \frac{1}{3^{2+v_3(a)}}.$$

Next, $k = 0$, that is $e = v_3(t) = v_3(a) = v_3(t-a)$. Then, we must have $v_3(2t-a) = e + \ell$ with $\ell \geq 1$. Also, in this case $w_3^*(t) = w_3(t)$. If $\ell \geq 2$, then $w_3(t) = 1$ and

$$\int_{\substack{v_3(t)=v_3(a)=e, \\ v_3(2t-a)=e+\ell}} w_3^*(t) dt = \frac{2}{3^{e+\ell+1}},$$

whereas the integral is quickly seen to be 0 if $\ell = 1$. Thus,

$$(4.18) \quad \int_{v_3(t)=v_3(a)=e, v_3(t-a)=e} w_3^*(t) dt = \frac{2}{3^{e+1}} \sum_{k=2}^{\infty} 3^{-k} = \frac{1}{3^{v_3(a)+2}}.$$

Summing the contributions (4.17) and (4.18), we get

$$\int_{v_3(t)=v_3(a)} w_3^*(t) dt = \frac{13}{14} \frac{1}{3^{v_3(a)+2}}.$$

The case $0 \leq v_3(t) < v_3(a)$. We let $v_3(t) = e$. In this case we have $v_3(t-a) = v_3(t) = e$, and so $w_3^*(t) = w_3(t)$. If $e \equiv 0 \pmod{2}$ and $e < v_3(a) - 1$ then $w - 3(t) = -1$ and so we find

$$\int_{v_3(t)=e} w_3^*(t) dt = \frac{-2}{3^{e+1}},$$

whereas in all other cases the above integral is 0. Thus,

$$\int_{0 \leq v_3(t) < v_3(a)} w_3^*(t) dt = -\frac{2}{3} \sum_{\substack{0 \leq e \leq v_3(a)-2, \\ e \equiv 0 \pmod{2}}} \frac{1}{3^e} = \frac{-2}{3} \sum_{0 \leq n \leq N} \frac{1}{9^n} = \frac{3}{4} (9^{-(N+1)} - 1),$$

where $N = \lfloor \frac{v_3(a)-2}{2} \rfloor$.

Then, summing the contribution of the three cases we obtain the proposition. $\square$

Proposition 28. *We have $\int_{\mathbb{Z}_2} w_2^*(t) dt = E_{\mathcal{V}_a}(2)$.*

Proof. The proof of the proposition is given by a series of lemmas, which compute the contribution to $\int_{\mathbb{Z}_2} w_2^*(t) dt$ in 4 cases depending on the relative valuations of t and a . To obtain Proposition 28, it is then enough to sum the 4 contributions.

Before proceeding with the lemmas we recall that for $t \notin [0, a]$ (note that excluding a finite number of values of t does not influence the various averages) we have

$$w_2^*(t) \equiv t_2(t-a)_2 w_2(t) \pmod{4}.$$

and that the values of $w_2(t)$ are given in Proposition 43 in Appendix B. $\square$

Lemma 29. *Let χ_4 be non-principal character modulo 4. If $v_2(a)$ is even, then*

$$\int_{0 \leq v_2(a) < v_2(t)} w_2^*(t) dt = -\frac{1}{2^{v_2(a)+2}} + \chi_4(a_2) \frac{1}{2^{v_2(a)+4}} - \chi_4(a_2) \frac{29}{63} \frac{1}{2^{2+v_2(a)}}.$$

If $v_2(a)$ is odd,

$$\int_{0 \leq v_2(a) < v_2(t)} w_2^*(t) dt = \chi_4(a_2) \frac{1}{2^{v_2(a)+5}} - \chi_4(a_2) \frac{46}{63} \frac{1}{2^{v_2(a)+4}}.$$

Proof. We first remark that if $0 \leq v_2(a) < v_2(t) = e$, then

$$t_2(t-a)_2 \equiv \begin{cases} -t_2 a_2 \pmod{4} & \text{if } v_2(t) - v_2(a) \geq 2, \\ t_2 a_2 \pmod{4} & \text{if } v_2(t) - v_2(a) = 1. \end{cases}$$

We first suppose that $v_2(a)$ is even. If $v_2(t) - v_2(a) \equiv 0, 2 \pmod{6}$, and $v_2(t) \neq v_2(a) + 2$, then since $w_2^*(t) \equiv t_2 a_2 \pmod{4}$, it is clear that

$$\int_{v_2(t)=e} w_2^*(t) dt = 0.$$

If $v_2(t) - v_2(a) \equiv 1, 3, 4, 5 \pmod{6}$, and $v_2(t) - v_2(a) > 1$, then $w_2^*(t) \equiv -a_2 \pmod{4}$, and

$$\int_{v_2(t)=e} w_2^*(t) dt = \frac{1}{2^{e+1}} \sum_{d \in (\mathbb{Z}/2\mathbb{Z})^*} w_2^*(dp^e) = -\chi_4(a_2) \frac{1}{2^{e+1}}.$$

Then, if $v_2(a)$ is even, we then have that

$$(4.19) \quad \sum_{e \geq v_2(a)+3} \int_{v_2(t)=e} w_2^*(t) dt = -\chi_4(a_2) \sum_{\substack{e \geq v_2(a)+3 \\ e-v_2(a) \not\equiv 0,2 \pmod{6}}} \frac{1}{2^{e+1}} = -\frac{\chi_4(a_2)}{2^{v_2(a)+2}} \frac{29}{63}.$$

If $v_2(t) - v_2(a) = 1$, then $w_2^*(t) \equiv -t_2 a_2^{-1} t_2 a_2 \pmod{4} \equiv -1 \pmod{4}$, so $w_2^*(t) = -1$ and we have

$$\int_{v_2(t)=v_2(a)+1} w_2^*(t) dt = \frac{-1}{2^{v_2(a)+2}}.$$

Finally, if $v_2(t) - v_2(a) = 2$, then we compute

$$w_2^*(d2^e) \equiv -da_2 w_2(d2^e) \pmod{4} = \begin{cases} 1 & d \equiv 1 \pmod{8}, \\ 1 & d \equiv 3, 7 \pmod{8}, a_2 \equiv 1 \pmod{4}, \\ -1 & d \equiv 3, 7 \pmod{8}, a_2 \equiv 3 \pmod{4}, \\ -1 & d \equiv 5 \pmod{8}, \end{cases}$$

and so

$$\int_{v_2(t)=v_2(a)+2} w_2^*(t) dt = \frac{1}{2^{e+3}} \sum_{d \in (\mathbb{Z}/8\mathbb{Z})^*} w_2^*(dp^e) = \frac{\chi_4(a_2)}{2^{v_2(a)+4}}.$$

Adding the contributions for $v_p(t) = v_p(a) + 1$ and $v_p(t) = v_p(a) + 2$ to (4.19), we get the result for $v_2(a)$ even.

We now suppose that $v_2(a)$ is odd. If $v_2(t) - v_2(a) \equiv 0, 2, 4 \pmod{6}$, or $v_2(t) - v_2(a) \equiv 1 \pmod{6}$ and $v_2(t) \neq v_2(a) + 1$, then $w_2^*(t) \equiv -t_2^2 a_2 \equiv -a_2 \pmod{4}$ and so, as before,

$$\int_{v_2(t)=e} w_2^*(t) dt = -\chi_4(a_2) \frac{1}{2^{e+1}}.$$

If $v_2(t) - v_2(a) \equiv 3, 5 \pmod{6}$ and $v_2(t) - v_2(a) \neq 3$, then $w_2^*(t) \equiv t_2 a_2 \pmod{4}$ and so

$$\int_{v_2(t)=e} w_2^*(t) dt = 0.$$

Thus, if $v_2(a)$ is odd, we then have that

$$(4.20) \quad \sum_{e \geq v_2(a)+4} \int_{v_2(t)=e} w_2^*(t) dt = -\chi_4(a_2) \sum_{\substack{e \geq v_2(a)+4 \\ e-v_2(a) \not\equiv 3,5 \pmod{6}}} \frac{1}{2^{e+1}} = -\frac{\chi_4(a_2)}{2^{v_2(a)+4}} \frac{46}{63}.$$

We then have to treat the 2 remaining cases $v_2(t) = v_2(a) + 1$ and $v_2(t) = v_2(a) + 3$. In the latter case, we have that

$$w_2^*(t) \equiv \begin{cases} t_2 a_2 & t_2 \equiv 5 \pmod{8}, \\ -t_2 a_2 & t_2 \not\equiv 5 \pmod{8}, \end{cases}$$

and then

$$\int_{v_2(t)=v_2(a)+3} w_2^*(t) dt = \frac{1}{2^{e+3}} \sum_{d \in (\mathbb{Z}/8\mathbb{Z})^*} w_2^*(dp^e) = \frac{\chi_4(a_2)}{2^{e+2}}.$$

Finally, if $v_2(t) - v_2(a) = 1$, then we have

$$w_2^*(t) = \chi_4(a_2) \begin{cases} 1 & t_2 \equiv 1 \pmod{8} \\ -1 & t_2 \equiv 3 \pmod{8}, a_2 \equiv 1 \pmod{4} \\ 1 & t_2 \equiv 3 \pmod{8}, a_2 \equiv 3 \pmod{4} \\ -1 & t_2 \equiv 5 \pmod{8} \\ 1 & t_2 \equiv 7 \pmod{8}, a_2 \equiv 1 \pmod{4} \\ -1 & t_2 \equiv 7 \pmod{8}, a_2 \equiv 3 \pmod{4} \end{cases}$$

and so

$$\int_{v_2(t)=v_2(a)+1} w_2^*(t) dt = \frac{1}{2^{e+3}} \sum_{d \in (\mathbb{Z}/8\mathbb{Z})^*} w_2^*(dp^e) = 0.$$

Adding the contributions of $v_p(t) = v_p(a) + 1$ and $v_p(t) = v_p(a) + 3$ to (4.20), we get the result. $\square$

Lemma 30. *Suppose that $v_2(a) \geq 2$. Then,*

$$\int_{0 \leq v_2(t) \leq v_2(a)-2} w_2^*(t) dt = \begin{cases} \frac{1}{4} & v_2(a) = 2 \\ 2^{1-v_2(a)} + \frac{1}{3}(4^{-(v_2(a)-3)/2} - 1) & v_2(a) \geq 3 \text{ odd} \\ 2^{-v_2(a)} + \frac{1}{3}(4^{-(v_2(a)-4)/2} - 1) & v_2(a) \geq 4 \text{ even} \end{cases}$$

Proof. Since $e = v_p(t) \leq v_p(a) - 2$, we have that $(t - a)_2 = t_2 - 2^k a_2$ for $k = v_2(a) - v_2(t) \geq 2$, and $(t - a)_2 \equiv t_2 \pmod{4}$, which gives $w_2^*(t) = w_2(t)$. First, suppose that $v_2(t)$ is even. Then, it is easy to see from Proposition 43 of Appendix B that

$$\int_{v_2(t)=e} w_{2,r}^*(t) dt = \begin{cases} \frac{1}{2^{v_2(a)}} & e = v_2(a) - 2, \\ \frac{1}{2^{v_2(a)-1}} & e = v_2(a) - 3, \\ 0 & e = v_2(a) - 4, \\ \frac{-1}{2^{e+2}} & e \geq v_2(a) - 5. \end{cases}$$

We now suppose that $v_2(t)$ is odd. Then, it is clear that

$$\int_{v_2(t)=e} w_2^*(t) dt = 0.$$

Thus, summing all contributions

$$\int_{0 \leq v_2(t) \leq v_2(a)-2} w_2^*(t) dt = \sum_{\substack{0 \leq e \leq v_2(a)-2 \\ e \text{ even}}} \int_{v_2(t)=e} w_2^*(t) dt,$$

we get the result. $\square$

Lemma 31. *We have*

$$\int_{v_2(t)=v_2(a)-1} w_2^*(t) dt = 0.$$

Proof. If $v_2(t) = v_2(a) - 1$, then $(t - a)_2 = t_2 - 2a_2$, and one check that $t_2 - 2a_2 \equiv 1 \pmod{4} \iff t_2 \equiv -1 \pmod{4}$, which gives

$$w_2^*(t) \equiv t_2(t - a)_2 w_2(t) \equiv -w_2(t) \pmod{4}.$$

From Proposition 43 of Appendix B, we then easily deduce that

$$\int_{v_2(t)=v_2(a)-1} w_2^*(t) dt = 0$$

for all cases. $\square$

Lemma 32. *If $v_2(a)$ is even, then*

$$\int_{v_2(t)=v_2(a)} w_2^*(t) dt = -\chi_4(a_2) \frac{1}{2^{v_2(a)+4}} - \frac{1}{2^{v_2(a)+2}} + \chi_4(a_2) \frac{1}{2^{v_2(a)+2}} \frac{29}{63}.$$

If $v_2(a)$ is odd, then

$$\int_{v_2(t)=v_2(a)} w_2^*(t) dt = -\chi_4(a_2) \frac{1}{2^{v_2(a)+5}} + \chi_4(a_2) \frac{1}{2^{v_2(a)+4}} \frac{46}{63}.$$

Proof. Let $e = v_2(t) = v_2(a)$ and $v_2(t-a) = e+k$. Notice that $k \geq 1$ since $t_2 - a_2 \equiv 0 \pmod{2}$. We first suppose that $v_2(a)$ is even. If $k \equiv 0, 2 \pmod{6}$, $k \geq 3$, then $w_2^*(t) \equiv -t_2(t-a)_2 \equiv -s_2(t-a)_2 \pmod{4}$ and so

$$\int_{\substack{v_2(t)=v_2(a)=e \\ v_2(t-a)=e+k}} dt = \frac{-1}{2^{e+k+2}} \sum_{a \in (\mathbb{Z}/4\mathbb{Z})^*} w_2^*(2^e(s_2 + a2^k)) = 0.$$

If $k \equiv 1, 3, 4, 5 \pmod{6}$, $k \geq 3$, then $w_2^*(t) \equiv s_2 \pmod{4}$, and

$$\int_{\substack{v_2(t)=v_2(a)=e \\ v_2(t-a)=e+k}} w_2^*(t) dt = \chi_4(a_2) \frac{1}{2^{e+k+1}}.$$

We then have that

$$(4.21) \quad \int_{\substack{e=v_2(t)=v_2(a) \\ v_2(t-a) \geq e+3}} w_2^*(t) dt = \chi_4(a_2) \sum_{\substack{k \geq 3 \\ k \not\equiv 0, 2 \pmod{6}}} \frac{1}{2^{k+v_2(a)+1}} = \chi_4(a_2) \frac{1}{2^{v_2(a)+2}} \frac{29}{63}.$$

We now have to compute the contribution for $v_2(t-a) = v_2(a) + 1$ and $v_2(t-a) = v_2(a) + 2$. For the first case $v_2(t-a) = v_2(a) + 1$, by Proposition 43 we have

$$(4.22) \quad \int_{\substack{e=v_2(t)=v_2(a) \\ v_2(t-a)=e+1}} w_2^*(t) dt = \frac{1}{2^{e+3}} \sum_{a \in (\mathbb{Z}/4\mathbb{Z})^*} \chi_4(a(a_2 + 2a)) w_2(2^e(a_2 + 2a)) = -2^{-e-2}.$$

For the second case $v_2(t-a) = v_2(a) + 2$, we have $w_2^*(t) \equiv s_2(t-s_2)w_2(t) \pmod{4}$ and so

$$(4.23) \quad \int_{\substack{e=v_2(t)=v_2(a) \\ v_2(t-a)=e+2}} w_2^*(t) dt = \frac{\chi_4(s_2)}{2^{e+5}} \sum_{a \in (\mathbb{Z}/8\mathbb{Z})^*} \chi_4(a) w_2(2^e(a_2 + 4a)) = -\chi_4(s_2) 2^{-e-4},$$

since $w_2(2^e(a_2 + 4a)) = 1$ only in the cases $a \equiv 1, 3, 7 \pmod{8}$ if $a_2 \equiv 1 \pmod{4}$, or $a \equiv 1, 3, 5 \pmod{8}$ if $a_2 \equiv 3 \pmod{4}$. Summing (4.22), (4.23) and (4.21), we get the result when $v_2(a)$ is even.

Suppose now that $e = v_2(a) = v_2(t)$ is odd. If $k = v_2(t-a) - v_2(a) \equiv 0, 1, 2, 4 \pmod{6}$, and $k \geq 4$, then $w_2^*(t) \equiv t_2(t-a)_2 w_2(t) \equiv t_2 \equiv s_2 \pmod{4}$, and

$$\int_{\substack{e=v_2(t)=v_2(a) \\ v_2(t-a)=e+k}} w_2^*(t) dt = \chi_4(s_2) \frac{1}{2^{e+k+1}}.$$

If $k = v_2(t-a) - v_2(a) \equiv 3, 5 \pmod{6}$, and $k \geq 4$, then $w_2^*(t) \equiv t_2(t-a)_2 w_2(t) \equiv -s_2(t-a)_2 \pmod{4}$ and, as before,

$$\int_{\substack{e=v_2(t)=v_2(a) \\ v_2(t-a)=e+k}} w_2^*(t) dt = 0.$$

Summing the contributions above, we get that

$$(4.24) \quad \int_{\substack{v_2(t)=v_2(a) \\ v_2(t-a) \geq v_2(a)+4}} w_2^*(t) dt = \chi_4(a_2) \sum_{\substack{k \geq 4 \\ k \not\equiv 3, 5 \pmod{6}}} \frac{1}{2^{v_2(a)+k+1}} = \chi_4(a_2) \frac{1}{2^{v_2(a)+4}} \frac{46}{63}.$$

We now have to compute the contributions for $v_2(t-a) = v_2(a) + 1$ and $v_2(t-a) = v_2(a) + 3$. For the first case $v_2(t-a) = v_2(a) + 1$, we have

$$(4.25) \quad \int_{\substack{e=v_2(t)=v_2(a) \\ v_2(t-a)=e+1}} w_2^*(t) dt = \sum_{a \in (\mathbb{Z}/8\mathbb{Z})^*} \chi_4(a(a_2 + 2a)) w_2(2^e(a_2 + 2a)) = 0$$

since $w_2(2^e(a_2 + 2a)) = 1$ only in the cases $a \equiv 1, 7 \pmod{8}$ if $a_2 \equiv 1 \pmod{4}$ or $a \equiv 1, 3 \pmod{8}$ if $a_2 \equiv 3 \pmod{4}$. Finally, if $v_2(t-a) = v_2(a) + 3$, we find

$$(4.26) \quad \int_{\substack{e=v_2(t)=v_2(a) \\ v_2(t-a)=e+3}} w_2^*(t) dt = -\chi_4(a_2) \frac{1}{2^{v_2(a)+5}}.$$

Summing (4.24), (4.25) and (4.26), we get the result when $v_2(a)$ is odd. $\square$

5. THE DENSITY OF AVERAGE ROOT NUMBERS

We shall prove Theorem 3, 4 and 5 by considering subfamilies of $\mathcal{W}_a(t)$ of the form $\mathcal{W}_{a(t)}(Q(t))$ where $a(t)$ and $Q(t)$ are polynomials in $\mathbb{Z}[t]$. Thanks to Theorem 1, we know exactly the root number for all the elliptic curves in these families, and so we just need to choose $a(t)$ and $Q(t)$ so that we obtain the desired averages. In the case of averages over $\mathbb{Q}$, we can reduce to the case where the ∞ -factor of the (modified) root number essentially determines the root number, whereas in the case of averages over $\mathbb{Z}$, we reduce to the case where the root number is determined by its p -factor for a suitably chosen p . The proof of Theorem 4 is more elaborate and requires working with all prime divisors of k .

Proof of Theorem 3. We first prove that $\text{Av}_{\mathbb{Z}}(\mathfrak{F}'_{\mathbb{Z}}) \supseteq \mathbb{Q} \cap [-1, 1]$.

For any $h/k \in \mathbb{Q}$ with $(h, k) = 1$, $k > 0$ we need to show that there exists a non-isotrivial family $\mathcal{E}$ such that $\text{Av}_{\mathbb{Z}}(\mathcal{E}) = h/k$. First notice that we can assume $0 \neq |h/k| < 1$, since by Theorem 1 we have that $\mathcal{W}_2(1+4t)$, $\mathcal{W}_1(t)$ and $\mathcal{W}_3(1+12t)$ are non-isotrivial families with root numbers constantly equal to $(-1)^t$, -1 and 1 respectively. Also, let $h = \pm|h|$.

Let p be a prime such that $p+1 = 2rk$ for $r \geq 1$. By Dirichlet's Theorem on primes in arithmetic progressions we can always find such a prime. Let $m = p+1 - 2r|h|$ so that $0 < m < p$ and m is even. Let

$$P(t) = \mp p \prod_{i=1}^m (t-i), \quad a(t) = 2^4 p P(t), \quad Q(t) = (4pt^2 + 1)P(t),$$

so that by (4.2) one easily sees that $\mathcal{W}_{a(t)}(Q(t))$ is a potentially parity-biased non-isotrivial family.

We shall assume $t \neq 1, \dots, m$ so that $P(t) \neq 0$ and we let $\varepsilon(t)$ be the root number of $\mathcal{W}_{a(t)}(Q(t))$. First, notice that

$$\gcd(a(t)_2, Q(t)) = |P(t)_2| = \frac{|a(t)_2|}{p}.$$

Then, by (1.4) for $t \neq 1, \dots, m$ we have

$$\begin{aligned} \varepsilon(t) &\equiv -s_{a(t)}(Q(t)) \gcd(a(t)_2, Q(t)) \prod_{\substack{q \mid \frac{a(t)_2}{\gcd(a(t)_2, Q(t))} \\ q \text{ prime}}} (-1)^{1+v_q(Q(t))} \left(\frac{Q(t)_q}{q} \right)^{1+v_q(Q(t))} \pmod{4} \\ &\equiv -s_{a(t)}(Q(t)) |P(t)_2| (-1)^{1+v_p(Q(t))} \left(\frac{Q(t)_p}{p} \right)^{1+v_p(Q(t))} \pmod{4} \\ &\equiv -Q(t)_2 |Q(t)_2| (-1)^{1+v_p(Q(t))} \left(\frac{Q(t)_p}{p} \right)^{1+v_p(Q(t))} \pmod{4} \end{aligned}$$

since $v_2(a(t)) = 4 + v_2(Q(t))$ and thus by Remark 2 after Proposition 15 we have $s_{a(t)} \equiv Q(t)_2 \pmod{4}$. Now, for $t \neq 1, \dots, m$ an integer we have that $|Q(t)| = \mp Q(t)$, so that

$$\varepsilon(t) = \pm (-1)^{1+v_p(Q(t))} \left(\frac{Q(t)_p}{p} \right)^{1+v_p(Q(t))}.$$

Now notice that $v_p(Q(t)) = 1$ unless $t \equiv 1, \dots, m \pmod{p}$, whereas if $t \equiv i \pmod{p}$ with $i \in \{1, \dots, m\}$ then $v_p(Q(t)) = 1 + v_p(t - i)$ and $Q(t)_p = (4pt^2 + 1)\kappa_i(t - i)_p$ where $\kappa_i = \mp \prod_{j \neq i} (j - i)$. It follows that

$$\begin{aligned}
\frac{1}{2X} \sum_{|t| \leq X} \varepsilon(t) &= \pm \int_{\mathbb{Z}_p} (-1)^{1+v_p(Q(t))} \left(\frac{Q(t)_p}{p} \right)^{1+v_p(Q(t))} d\mu_p \\
&= \pm \frac{p-m}{p} \pm \sum_{i=1}^m \int_{t \in i+p\mathbb{Z}_p} (-1)^{v_p(t-i)} \left(\frac{\kappa_i(t-i)_p}{p} \right)^{v_p(t-i)} dt \\
&= \pm \frac{p-m}{p} \pm \sum_{i=1}^m \sum_{\ell=1}^{\infty} (-1)^{\ell} \left(\frac{\kappa_i}{p} \right)^{\ell} \int_{t \in i+p^{\ell}\mathbb{Z}_p^*} \left(\frac{(t-i)_p}{p} \right)^{\ell} dt \\
&= \pm \frac{p-m}{p} \pm \sum_{i=1}^m \sum_{\ell=1}^{\infty} (-1)^{\ell} \left(\frac{\kappa_i}{p} \right)^{\ell} \frac{1}{p^{\ell}} \int_{x \in \mathbb{Z}_p^*} \left(\frac{x}{p} \right)^{\ell} dt \\
&= \pm \frac{p-m}{p} \pm \sum_{i=1}^m \sum_{\substack{\ell=1, \\ \ell \text{ even}}}^{\infty} \frac{1}{p^{\ell}} \frac{p-1}{p} = \pm \frac{p-m}{p} \pm m \sum_{\ell=0}^{\infty} \frac{p-1}{p^{3+2\ell}} \\
&= \pm \frac{p-m}{p} \pm m \frac{p-1}{p(p^2-1)} = \pm \left(1 - \frac{m}{p+1} \right) = \pm \frac{2r|h|}{2rk} = \frac{h}{k},
\end{aligned}$$

and $\text{Av}_{\mathbb{Z}}(\mathfrak{F}'_{\mathbb{Z}}) \supseteq \mathbb{Q} \cap [0, 1]$ as desired.

To show that we also have that $\text{Av}_{\mathbb{Z}}(\mathfrak{F}_{i,\mathbb{Z}}) \supseteq \mathbb{Q} \cap [0, 1]$, we proceed as above taking $Q(t) = P(t)$ instead of $Q(t) = (4pt^2 + 1)P(t)$. $\square$

We now move to the proof of Theorem 5, about the density of average of the root number over the rational. Given a family of elliptic curve $\mathcal{F}$, we first state a result to compute $\text{Av}_{\mathbb{Q}}(\varepsilon_{\mathcal{F}})$ as defined by (1.8). As for the averages over the integers, we write the root number as an *almost finite* product of local root number, and we use the following result.

Proposition 33 (Helfgott, Proposition 7.8). *Let S be a finite set of places of $\mathbb{Q}$, including ∞ . For every $v \in S$, let $g_v : \mathbb{Q}_v \times \mathbb{Q}_v \rightarrow \mathbb{C}$ be a bounded function that is locally constant outside a finite set of lines through the origin. For every $p \notin S$, let $h_p : \mathbb{Q}_p \times \mathbb{Q}_p \rightarrow \mathbb{C}$ be a function that is locally constant outside a finite set of lines through the origin, and satisfying $|h_p(x, y)| \leq 1$ for all $x, y \in \mathbb{Q}_p$. Let $B(x, y) \in \mathbb{Z}[x, y]$ be a non-zero homogeneous polynomial of degree at most 6, and assume that $h_p(x, y) = 1$ when $v_p(B(x, y)) \leq 1$. Let*

$$W(x, y) = \prod_{v \in S} g_v(x, y) \prod_{p \notin S} h_p(x, y).$$

Then,

$$\begin{aligned}
\text{Av}_{\mathbb{Z}^2, \text{coprime}} W(x, y) &:= \lim_{N \rightarrow \infty} \frac{\sum_{(x, y) \in [-N, N]^2, (x, y) = 1} W(x, y)}{\#\{(x, y) \in [-N, N]^2 \mid (x, y) = 1\}} \\
&= c_{\infty} \prod_{p \in S} \frac{1}{1-p^{-2}} \int_{O_p} g_p(x, y) dx dy \cdot \prod_{p \notin S} \frac{1}{1-p^{-2}} \int_{O_p} h_p(x, y) dx dy
\end{aligned}$$

where $O_p = (\mathbb{Z}_p \times \mathbb{Z}_p) \setminus (p\mathbb{Z}_p \times p\mathbb{Z}_p)$, and

$$c_{\infty} = \lim_{N \rightarrow \infty} \frac{1}{2N^2} \int_{-N}^N \int_{-N}^N g_{\infty}(x, y) dx dy.$$

We remark that our version of [Hel09, Proposition 7.8] is unconditional, as we are assuming that $\deg B \leq 6$.

Proof of Theorem 5. We first prove that $\text{Av}_{\mathbb{Q}}(\mathfrak{F}'_{\mathbb{Q}})$ is dense in $[0, 1]$.

For $X \geq 2$, let

$$m_X := \prod_{2 \leq p \leq X} p \quad \text{and} \quad n_X := m_X^{2\lfloor f(X) \rfloor + 1},$$

where $f(x)$ is any positive function such that $f(X)$ and $\log X/f(X)$ tend to infinity. Let $P(t)$ be a polynomial with integer coefficients of even degree $2d > 0$ and define

$$Q_X(t) := -P(t)(1 + n_X t^2), \quad a_X(t) := -2^4 P(t)(1 + n_X t^2)^2.$$

Notice that by the equations of the invariants (4.2) for the family $\mathcal{W}_a(t)$, $\mathcal{W}_{a_X(t)}(Q_X(t))$ is a non-isotrivial potentially parity-biased family.

Now, let $r/s \in \mathbb{Q}$ with $(r, s) = 1$, $s > 0$. We have the isomorphism of elliptic curves

$$\mathcal{W}_{a_X(r/s)}(Q_X(r/s)) \simeq \mathcal{W}_{s^{2d+4}a_X(r/s)}(s^{2d+4}Q_X(r/s)) = \mathcal{W}_{a_X(r,s)}(Q_X(r,s)),$$

where

$$\begin{aligned} P(r, s) &:= s^{2d} P(r/s), \\ Q_X(r, s) &:= s^{2d+4} Q_X(r/s) = -s^2 P(r, s)(s^2 + n_X r^2), \\ a_X(r, s) &:= s^{2d+4} a_X(r/s) = -2^4 P(r, s)(s^2 + n_X r^2)^2 \end{aligned}$$

are homogeneous polynomial in r and s which are non-zero for all but finitely many r/s . In the following we shall ignore such values as they give a negligible contribution to the average. Also, we let $\varepsilon(r/s)$ be the root number of the elliptic curve given by $\mathcal{W}_{a_X(r,s)}(Q_X(r,s))$ (or, i.e., by $\mathcal{W}_{a_X(r/s)}(Q_X(r/s))$). Using Theorem 1, we have

$$\begin{aligned} \varepsilon(r/s) &\equiv -s_{a_X(r,s)}(Q_X(r,s)) \gcd(a_X(r,s)_2, Q_X(r,s)) \times \\ (5.1) \quad &\times \prod_{p|g_X(r,s)} (-1)^{1+v_p(Q_X(r,s))} \left(\frac{Q_X(r,s)_p}{p} \right)^{1+v_p(Q_X(r,s))} \pmod{4}. \end{aligned}$$

where

$$g_X(r, s) := \frac{|a_X(r, s)_2|}{\gcd(a_X(r, s)_2, Q_X(r, s))}$$

Now, we have

$$\gcd(a_X(r, s)_2, Q_X(r, s)) = |P(r, s)_2(s^2 + n_X r^2)_2|(s^2 + n_X r^2, s_2^2)$$

and thus

$$g_X(r, s) := \frac{|a_X(r, s)_2|}{\gcd(a_X(r, s)_2, Q_X(r, s))} = \frac{(s^2 + n_X r^2)_2}{(s^2 + n_X r^2, s_2^2)}.$$

Notice that, for $3 \leq p \leq X$, we have $v_p(n_X)$ and $v_p(s^2)$ have opposite parities and so $v_p(s^2 + n_X r^2) = \min(v_p(s^2), v_p(n_X r^2))$, since $(r, s) = 1$. In particular, we have $p \nmid g_X(r, s)$ for $3 \leq p \leq X$. Moreover, for $p > X$ then $p|g_X(r, s)$ if and only if $p | s^2 + n_X r^2$ since $p \nmid s$ then. In that case, we have

$$v_p(Q_X(r, s)) = v_p(s^2 + n_X r^2) + v_p(P(r, s)).$$

Let E_X be the set of primes $p > X$ such that there exist r, s such that $p | s^2 + n_X r^2$ and $p | P(r, s)$. Since $p \nmid s$ this implies $P(t)$ and $1 + n_X t^2$ has a common solution modulo p and thus p divides the

resultant R_X of these two polynomials. We notice that $R_X = O(n_X)$. It follows that

$$\begin{aligned} & \prod_{p|g_X(r,s)} (-1)^{1+v_p(Q_X(r,s))} \left(\frac{Q_X(r,s)_p}{p} \right)^{1+v_p(Q_X(r,s))} \\ &= \prod_{\substack{p>X, p \notin E_X \\ v_p(s^2+n_X r^2) \geq 2}} (-1)^{1+v_p(s^2+n_X t^2)} \left(\frac{Q_X(r,s)_p}{p} \right)^{1+v_p(s^2+n_X r^2)} \\ & \quad \times \prod_{\substack{p>X, p \in E_X, \\ v_p(s^2+n_X r^2) \geq 1}} (-1)^{1+v_p(s^2+n_X r^2)+v_p(P(r,s))} \left(\frac{Q_X(r,s)_p}{p} \right)^{1+v_p(s^2+n_X r^2)+v_p(P(r,s))}. \end{aligned}$$

We now simplify the first part of (5.1). For all but finitely many values of r, s we have

$$v_2(Q_X(r,s)) = 2v_2(s) + v_2(P(r,s)) + v_2(s^2 + n_X t^2) = 2v_2(s) + v_2(P(r,s)) + \min(2v_2(s), 2\lfloor f(X) \rfloor + 1),$$

$$v_2(a_X(r,s)) = 4 + v_2(P(r,s)) + 2v_2(s^2 + n_X t^2) = 4 + v_2(P(r,s)) + 2\min(2v_2(s), 2\lfloor f(X) \rfloor + 1),$$

and thus if $v_2(s) \leq \lfloor f(X) \rfloor$, then $v_2(a_X(r,s)) = v_2(Q_X(r,s)) + 4$, and thus by Remark 2 after Proposition 15, we have $s_{a_X(r,s)} \equiv Q_X(r,s)_2 \pmod{4}$. Then, for $v_2(s) \leq \lfloor f(X) \rfloor$,

$$\begin{aligned} & s_{a_X(r,s)}(Q_X(r,s)) \gcd(a_X(r,s)_2, Q_X(r,s)) \\ & \equiv -s_2^2 P(r,s)_2 (s^2 + n_X r^2)_2 |P(r,s)_2 (s^2 + n_X r^2)_2| (s^2 + n_X r^2, s_2^2) \pmod{4} \\ & \equiv -\operatorname{sgn}(P(r,s)) (s^2 + n_X r^2, s_2^2) \pmod{4}. \end{aligned}$$

Notice that since $(r,s) = 1$ we have

$$(s^2 + n_X r^2, s_2^2) = \prod_{3 \leq p \leq X} p^{\min(2v_p(s), 2\lfloor f(X) \rfloor + 1)} \equiv \prod_{\substack{3 \leq p \leq X, \\ v_p(s) > \lfloor f(X) \rfloor}} p \pmod{4}.$$

If $v_2(s) \geq \lfloor f(X) \rfloor$, then it also follows from Proposition 15 that

$$s_{a_X(r,s)}(Q_X(r,s)) \gcd(a_X(r,s)_2, Q_X(r,s)) \equiv -\operatorname{sgn}(P(r,s)) f_2(r,s) \prod_{\substack{3 \leq p \leq X, \\ v_p(s) > \lfloor f(X) \rfloor}} p \pmod{4},$$

where $f_2(r,s)$ is a 2-locally constant function.

Replacing the above in (5.1), we have proven that

$$\begin{aligned} \varepsilon(r/s) &= \operatorname{sgn}(P(r,s)) f_{2,X}(r,s) \prod_{\substack{3 \leq p \leq X, \\ v_p(s) > \lfloor f(X) \rfloor}} \left(\frac{-1}{p} \right) \\ & \quad \times \prod_{\substack{p>X, p \notin E_X \\ v_p(s^2+n_X r^2) \geq 2}} (-1)^{1+v_p(s^2+n_X t^2)} \left(\frac{Q_X(r,s)_p}{p} \right)^{1+v_p(s^2+n_X r^2)} \\ & \quad \times \prod_{\substack{p>X, p \in E_X, \\ v_p(s^2+n_X r^2) \geq 1}} (-1)^{1+v_p(s^2+n_X r^2)+v_p(P(r,s))} \left(\frac{Q_X(r,s)_p}{p} \right)^{1+v_p(s^2+n_X r^2)+v_p(P(r,s))}, \end{aligned}$$

where $f_{2,X}(r,s) = 1$ if $v_2(s) \leq \lfloor f(X) \rfloor$. Then, for $3 \leq p \leq X$, we write

$$f_{p,X}(r,s) = \begin{cases} \left(\frac{-1}{p} \right) & \text{if } v_p(s) > \lfloor f(X) \rfloor \\ 1 & \text{otherwise.} \end{cases}$$

For $p > X$, $p \notin E_X$ we write

$$h_{p,X}(r, s) = \begin{cases} 1 & \text{if } v_p(s^2 + n_X r^2) < 2 \\ (-1)^{1+v_p(s^2+n_X r^2)} \left(\frac{Q_X(r, s)_p}{p} \right)^{1+v_p(s^2+n_X r^2)} & \text{otherwise.} \end{cases}$$

Finally, for $p > X$, $p \in E_X$ we write

$$g_{p,X}(r, s) = \begin{cases} 1 & \text{if } v_p(s^2 + n_X r^2) = 0 \\ (-1)^{1+v_p(s^2+n_X r^2)+v_p(P(r, s))} \left(\frac{Q_X(r, s)_p}{p} \right)^{1+v_p(s^2+n_X r^2)+v_p(P(r, s))} & \text{otherwise.} \end{cases}$$

Thus, we have

$$\varepsilon(r/s) = \text{sgn}(P(r, s)) \prod_{2 \leq p \leq X} f_{p,X}(r, s) \prod_{\substack{p > X \\ p \in E_X}} g_{p,X}(r, s) \prod_{\substack{p > X \\ p \notin E_X}} h_{p,X}(r, s).$$

The conditions for Proposition 33 with $S = X \cup E_X$ (which is a finite set) and $B(x, y) = x^2 + n_X y^2$ are satisfied and thus

$$\begin{aligned} \text{Av}_{\mathbb{Q}}(\varepsilon) &= \text{Av}_{\mathbb{Z}^2, \text{coprime}}(\epsilon_{a_X}(r, s)(Q_X(r, s))) \\ (5.2) \quad &= c_{\infty}(P) \prod_{2 \leq p \leq X} \frac{1}{1-p^{-2}} \int_{O_p} f_{p,X}(r, s) dr ds \times \\ &\quad \times \prod_{\substack{p > X \\ p \in E_X}} \frac{1}{1-p^{-2}} \int_{O_p} g_{p,X}(r, s) dr ds \prod_{\substack{p > X \\ p \notin E_X}} \frac{1}{1-p^{-2}} \int_{O_p} h_{p,X}(r, s) dr ds, \end{aligned}$$

where

$$c_{\infty}(P) = \lim_{N \rightarrow \infty} \frac{1}{4N^2} \int_{-N}^N \int_{-N}^N \text{sgn}(P(x, y)) dx dy.$$

We will now show that the three products over p all contributes $1 + o(1)$ as $X \rightarrow \infty$. First, we notice that for $p \leq X$, we have $f_{p,X}(r, s) = 1$ if $v_p(s) \leq \lfloor f(X) \rfloor$ and thus

$$\begin{aligned} \int_{O_p} f_{p,X}(r, s) dr ds &= \int_{O_p} 1 dr ds + O(\mu(\{(r, s) \in O_p : v_p(s) \geq \lfloor f(X) \rfloor + 1\})) \\ &= (1 - p^{-2}) + O(p^{-\lfloor f(X) \rfloor - 1}). \end{aligned}$$

Also, for $p \notin E_X$, we have $h_{p,X}(r, s) = 1$ if $v_p(s^2 + n_X r^2) < 2$ and so

$$\begin{aligned} \int_{O_p} h_{p,X}(r, s) dr ds &= \int_{O_p} 1 dr ds + O(\mu(\{(r, s) \in O_p : v_p(s^2 + n_X r^2) \geq 2\})) \\ &= (1 - p^{-2}) + O\left(\frac{1}{p^2}\right), \end{aligned}$$

and in the same way for $p \in E_X$ we obtain

$$(5.3) \quad \int_{O_p} g_{p,X}(r, s) dr ds = (1 - p^{-2}) + O\left(\frac{1}{p}\right).$$

With the above formulas it's then clear that the first two products over p in (5.2) are $1 + o(1)$ as $X \rightarrow \infty$. We now show that the same holds for the last product. We let $e(X)$ be the cardinality of E_X , which is the set of the prime divisors $p > X$ of an integer $R_X \ll n_X$. Then we have

$$X^{e(X)} < \prod_{p > X, p | R_X} p \ll n_X = \prod_{p \leq X} p^{2\lfloor f(X) \rfloor + 1} \ll e^{O(f(X)X)}$$

and thus $e(X) \ll \frac{f(X)X}{\log X}$. Then,

$$\log \prod_{\substack{p > X \\ p \in E_X}} (1 + O(1/p)) \ll \sum_{\substack{p > X \\ p \in E_X}} \log(1 + O(1/p)) \ll \sum_{\substack{p > X \\ p \in E_X}} \frac{1}{p} \ll \frac{e(X)}{X} \ll \frac{f(X)}{\log X} = o(1)$$

as $X \rightarrow \infty$, by hypothesis. Thus, by (5.3), we have that also the last product over p in (5.2) is $1 + o(1)$ and so

$$(5.4) \quad \lim_{X \rightarrow \infty} \text{Av}_{\mathbb{Q}}(\varepsilon) = c_{\infty}(P).$$

Finally, we compute that

$$\begin{aligned} c_{\infty}(P) &= \lim_{N \rightarrow \infty} \frac{1}{4N^2} \int_{-N}^N \int_{-N}^N \text{sgn}(P(x, y)) \, dx dy \\ &= \frac{1}{4} \int_{-1}^1 \int_{-1}^1 \text{sgn}(P(x/y)) \, dx dy = \frac{1}{2} \int_0^1 \int_{-1/y}^{1/y} \text{sgn}(P(x)) y \, dx dy \\ &= \frac{1}{2} \int_{-\infty}^{\infty} \int_0^{\min(1, 1/|x|)} \text{sgn}(P(x)) y \, dy dx \\ &= \frac{1}{4} \int_{-1}^1 \text{sgn}(P(x)) \, dx + \frac{1}{4} \int_1^{\infty} \frac{\text{sgn}(P(x)) + \text{sgn}(P(-x))}{x^2} \, dx. \end{aligned}$$

Thus, replacing in (5.4), we get

$$\lim_{X \rightarrow \infty} \text{Av}_{\mathbb{Q}}(\varepsilon) = \frac{1}{4} \int_{-1}^1 \text{sgn}(P(x)) \, dx + \frac{1}{4} \int_1^{\infty} \frac{\text{sgn}(P(x)) + \text{sgn}(P(-x))}{x^2} \, dx.$$

To conclude, it is enough to show that the set of values taken by $c_{\infty}(P)$ as P varies among polynomials of even degree in $\mathbb{Z}[t]$ is dense in $[0, 1]$. If $|h/k| \leq 1$, then taking

$$P(x) = k^2(x^2 - (1 - h/k)^2),$$

one obtains $c_{\infty}(P) = h/k$ and so $\text{Av}_{\mathbb{Q}}(\mathfrak{F}'_{\mathbb{Q}})$ is dense in $[0, 1]$.

Next, we show that $\text{Av}_{\mathbb{Q}}(\mathfrak{F}_{i, \mathbb{Q}}) \supseteq \mathbb{Q} \cap [0, 1]$. Given a polynomial $P(t) \in \mathbb{Z}[t]$ of even degree $2d > 0$ we take

$$\begin{aligned} Q(t) &:= -P(t), & a(t) &:= -2^4 P(t), \\ Q(r, s) &:= s^{2d} Q(r/s), & a(r, s) &:= s^{2d} a(r/s), & P(r, s) &:= s^{2d} P(r/s). \end{aligned}$$

for $(r, s) = 1, s > 0$. Then, $\mathcal{W}_{a(t)}(Q(t))$ gives a potentially parity-biased elliptic surface, which is isotrivial. Also, as before we call $\varepsilon(r/s)$ the root number of the specialization $\mathcal{W}_{a(r/s)}(Q(t)) \simeq \mathcal{W}_{a(r, s)}(Q(r, s))$. Then, assume $t = r/s$ is not a zero of $P(t)$. We have

$$\gcd(a(r, s)_2, Q(r, s)) = |a(r, s)_2| = |P(r, s)_2|.$$

Also, $v_2(a(r, s)) = v_2(Q(r, s)) + 4$. Thus by Remark 2 after Proposition 15, we have

$$s_{a(r, s)}(Q(r, s)) \equiv Q(r, s)_2 \equiv -P(r, s)_2 \pmod{4}.$$

It follows that

$$\varepsilon_{a(s/t)}(Q(s/t)) = \varepsilon_{a(r, s)}(Q(r, s)) \equiv P(r, s)_2 |P(r, s)_2| \equiv \text{sgn}(P(r, s)) \pmod{4}.$$

Thus, using Proposition 33, we have

$$\begin{aligned} \text{Av}_{\mathbb{Q}}(\varepsilon_{a(t)}(Q(t))) &= \lim_{N \rightarrow \infty} \frac{1}{4N^2} \int_{-N}^N \int_{-N}^N \text{sgn}(P(x, y)) \, dx dy \\ &= \frac{1}{4} \int_{-1}^1 \text{sgn}(P(x)) \, dx + \frac{1}{4} \int_1^{\infty} \frac{\text{sgn}(P(x)) + \text{sgn}(P(-x))}{x^2} \, dx. \end{aligned}$$

Choosing $P(x)$ appropriately as above, we obtain $\text{Av}_{\mathbb{Q}}(\mathfrak{F}_{i,\mathbb{Q}}) \supseteq \mathbb{Q} \cap [0, 1]$. $\square$

In order to prove Theorem 4 we need a few Lemmas.

Lemma 34. *Let $\phi, \eta_1, \eta_2 : \mathbb{Z} \rightarrow \mathbb{C}_{\neq 0}$ be periodic functions of period n_1, n_1 and n_2 respectively with $(n_1, n_2) = 1$. Assume there exists $\delta > 0$ such that*

$$|\{t \in \mathbb{N} \mid t \leq N, \phi(t) \neq \eta_1(t)\eta_2(t)\}| < \delta N$$

for all large enough N . Then there exists $\xi \in \mathbb{C}_{\neq 0}$ such that

$$|\{t \in \mathbb{N} \mid t \leq N, \phi(t) \neq \xi \cdot \eta_1(t)\}| < 2\delta N$$

for all large enough N .

Proof. There exists a residue class i modulo n_1 such that for all large enough N

$$|\{t \in \mathbb{N} \mid t \leq N, \eta_2(i + n_1 t) \neq \xi\}| < \delta N$$

where $\xi = \frac{\phi(i+n_1 t)}{\eta_1(i+n_1 t)}$. Since $(n_1, n_2) = 1$ then the above inequality is equivalent to

$$|\{t \in \mathbb{N} \mid t \leq N, \eta_2(t) \neq \xi\}| < \delta N$$

for N large enough and thus the result follows. $\square$

Lemma 35. *Let $\phi : \mathbb{Z} \rightarrow \mathbb{C}_{\neq 0}$ be a periodic function of period ℓ and let $\eta(t) = \prod_{i=1}^k h_{p_i}(t)$ with $h_{p_i} : \mathbb{Z} \rightarrow \mathbb{C}_{\neq 0}$ periodic modulo $p_i^{r_i}$ and $p_1, \dots, p_k$ distinct primes. Assume we have*

$$|\{t \in \mathbb{N} \mid t \leq N, \phi(t) \neq \eta(t)\}| < N/4\ell^2$$

for all large enough N . Then for each $p|\ell$ there exist $\rho \in \mathbb{C}_{\neq 0}$ and a function $h_p^*(t)$ periodic modulo $p^{v_p(\ell)}$ such that $\phi(t) = \rho \prod_{p|\ell} h_p^*(t)$ for all t .

Proof. Let $n := p_1^{r_1} \cdots p_k^{r_k}$. Increasing n if necessary, we can assume $\ell = p_1^{s_1} \cdots p_u^{s_u}$ where $s_i \leq r_i$, $u \leq k$ and $p_1, \dots, p_u$ are distinct primes. We prove the result by induction over the number u of distinct primes of ℓ . If $u = 0$, then the result is trivial. Now, let $u \geq 1$ and assume the result is true if ℓ has $u - 1$ distinct prime factors.

Let $\eta_1(t) = \prod_{j=2}^u h_{p_j}(t)$ and $\eta_2(t) = h_{p_1}(t) \prod_{j=u+1}^k h_{p_j}(t)$ so that $\eta(t) = \eta_1(t)\eta_2(t)$. Then for all $i = 1, \dots, p_1^{s_1}$ we have that $\phi(i + p_1^{s_1}t)$ and $\eta_1(i + p_1^{s_1}t)$ are periodic modulo $n_1 := p_2^{r_2} \cdots p_u^{r_u}$ whereas $\eta_2(i + p_1^{s_1}t)$ is periodic modulo $n_2 := n/n_1 p_1^{s_1}$. Notice that $(n_1, n_2) = 1$. Moreover, we have

$$|\{t \in \mathbb{N} \mid t \leq N, \phi(i + p_1^{s_1}t) \neq \eta_1(i + p_1^{s_1}t)\eta_2(i + p_1^{s_1}t)\}| < p_1^{s_1} \cdot N/4\ell^2$$

for all large enough N . Then, by Lemma 34, there exists $\xi_i \in \mathbb{C}_{\neq 0}$ such that

$$|\{t \in \mathbb{N} \mid t \leq N, \phi(i + p_1^{s_1}t) \neq \xi_i \eta_1(i + p_1^{s_1}t)\}| < 2p_1^{s_1} N/4\ell^2$$

for all large enough N . Equivalently, writing $h_{p_1}^*(t) := \xi_i$ if $t \equiv i \pmod{p_1^{s_1}}$, we have

$$(5.5) \quad |\{t \in \mathbb{N} \mid t \leq N, \frac{\phi(t)}{h_{p_1}^*(t)} \neq \eta_1(t)\}| < p_1^{s_1} N/2\ell^2$$

for large enough N . Also, for all $j = 1, \dots, \ell/p_1^{s_1}$ we have that $\frac{\phi(j + \ell/p_1^{s_1}t)}{h_{p_1}^*(j + \ell/p_1^{s_1}t)}$ is periodic modulo $p_1^{s_1}$ and $\eta_1(j + \ell/p_1^{s_1}t)$ is periodic modulo $p_1^{s_1} n_1/\ell$ and so, since $(p_1^{s_1}, p_1^{s_1} n_1/\ell) = 1$, by Lemma 34 we have that there exists $\psi_j \in \mathbb{C}$ such that

$$|\{t \in \mathbb{N} \mid t \leq N, \frac{\phi(j + \ell/p_1^{s_1}t)}{h_{p_1}^*(j + \ell/p_1^{s_1}t)} \neq \psi_j\}| < p_1^{s_1} N/\ell^2$$

for large enough N (notice that since $\ell/p_1^{s_1}$ is coprime with the period $p_1^{s_1}$ having t or $j + \ell/p_1^{s_1}t$ doesn't change the estimate on the right for N large enough). Thus, since $p_1^{s_1} N/\ell^2 \leq N/p_1^{s_1}$ and $\frac{\phi(j + \ell/p_1^{s_1}t)}{h_{p_1}^*(j + \ell/p_1^{s_1}t)}$

is periodic modulo $p_1^{s_1}$, then the set on the left has to be empty which means that $\frac{\phi(t)}{h_{p_1}^*(t)}$ is periodic modulo $\ell/p_1^{s_1}$. Finally, notice that $p_1^{s_1}N/2\ell^2 \leq N/4(\ell/p_1^{s_1})^2$ and so by (5.5) we can apply the inductive hypothesis to $\frac{\phi(t)}{h_{p_1}^*(t)}$ and the Lemma follows. $\square$

Corollary 36. *Assume Conjectures 1 and 2. Let $\mathcal{F}$ a family of elliptic curves as defined by (1.1) and such that $\varepsilon_{\mathcal{F}}(t)$, the root number of the specializations $\mathcal{F}(t)$, is a periodic function of t with period ℓ with $o(1)$ exceptions for $|t| \leq T$ as $T \rightarrow \infty$. Then, up to $o(1)$ exceptions, we have*

$$\varepsilon_{\mathcal{F}}(t) = \rho \prod_{p|\ell} h_p(t)$$

where $h_p : \mathbb{Z} \rightarrow \{\pm 1\}$ is periodic modulo $p^{v_p(\ell)}$ and $\rho \in \{\pm 1\}$.

Proof. By Theorem 6, the root number can be written as

$$\varepsilon_{\mathcal{F}}(t) = \text{sign}(g_{\infty}(t)) \lambda(M_{\mathcal{F}}(t)) \prod_{p \text{ prime}} g_p(t)$$

up to finitely many exceptions, where $g_p(t) = 1$ if $p \notin S$ and $p^2 \nmid B_{\mathcal{F}}(t)$. Under Conjectures 1 and 2, by Theorem 6, we have that $\varepsilon_{\mathcal{F}}(t)$ has average 0 as t varies among any fixed arithmetic progression unless $M_{\mathcal{F}}(t) = 1$. Thus, since $\varepsilon_{\mathcal{F}}(t)$ is periodic up to $o(1)$ exceptions, we must have $M_{\mathcal{F}}(t) = 1$. Similarly, the periodicity of $\varepsilon_{\mathcal{F}}(t)$ implies that $\text{sign}(g_{\infty}(t))$ is constant, except for a finite number of values of t .

Under Conjecture 2, for any fixed $\varepsilon > 0$ there exists $N_0 > 0$ such that

$$|\{1 \leq n \leq N \mid p^2 \mid B_{\mathcal{F}}(n) \Rightarrow p \leq N_0\}| \geq (1 - \varepsilon)N.$$

for all $N \geq 1$ (see e.g. the proof of Proposition 7.7 in [Hel09]). Now, let $S_0 = S \cup \{p \leq N_0\}$. Since $g_p(t)$ is locally constant outside a finite set of points for all p , then there exist an integer $k \in \mathbb{N}$ (depending on ε) and functions $g_p^* : \mathbb{Z} \rightarrow \{\pm 1\}$ which are periodic of period p^k such that

$$\prod_{p \in S_0} g_p(t) = \prod_{p \in S_0} g_p^*(t)$$

for t in all but c residue classes $r_1, \dots, r_c$ modulo $\ell := \prod_p p^k$ with $c \leq \varepsilon \ell$. Indeed, if $g_p(t)$ is locally constant on $\mathbb{Z}_p \setminus \{x_1, \dots, x_{c_p}\}$, then $g_p(i + tp^s)$ is p -locally constant (in $t \in \mathbb{Z}_p$) for all $1 \leq i \leq p^s$ with $i \not\equiv x_1, \dots, x_{c_p} \pmod{p^s}$. In particular, since $\mathbb{Z}_p$ is compact then for all $i \not\equiv x_1, \dots, x_{c_p} \pmod{p^s}$ one has that $g_p(i + tp^s)$ is periodic modulo p^{s_i} for some s_i . Thus, writing $g_p^*(t) := g_p(t)$ if $t \not\equiv x_1, \dots, x_{c_p} \pmod{p^s}$ and $g_p^*(t) := 1$ otherwise, we have that $g_p^*(t)$ is periodic modulo p^{k_p} where $k_p := s + \max_i s_i$. Taking s large enough so that $p^{-m} \leq \varepsilon/r$, we then have that $g_p^*(t)$ coincides with $g_p(t)$ for all but εp^{k_p} congruence classes modulo p^{k_p} . Proceeding in the same way for all $p \in S_0$ and taking $k = \max_p k_p$ we obtain the claimed result.

Now, we define

$$I_N = \{1 \leq n \leq N \mid p^2 \mid B_{\mathcal{F}}(n) \Rightarrow p \leq N_0, n \not\equiv r_j \pmod{m} \text{ for } j = 1, \dots, c\},$$

so that

$$|I(N)| \geq (1 - 3\varepsilon)N$$

for N large enough. For all $t \in I_N$ we have

$$\varepsilon_{\mathcal{F}}(t) = \prod_{p \in S_0} g_p^*(t)$$

and so, taking $3\varepsilon < 1/4\ell^2$ and using Lemma 35, we get the claimed result. $\square$

Corollary 36 easily gives that $\text{Av}(\mathfrak{F}_{p,\mathbb{Z}})$ is contained in the set on the right of (1.7) (see the end of the proof of Theorem 4 below for the details). We now give two Lemmas which are needed in the opposite direction. In order to construct subfamilies of $\mathcal{F}_a(t)$ with periodic root numbers with specified averages, we are led to the problem of finding polynomials in $\mathbb{Z}/p^\ell\mathbb{Z}[t]$ with a prescribed number of zeros m . This is not always possible for all choices (for example there is no polynomial in $\mathbb{Z}/8\mathbb{Z}[t]$ with exactly 7 zeros), but we can always find an $r \geq \ell$ and a polynomial in $\mathbb{Z}/p^r\mathbb{Z}[t]$ such that a portion of exactly m/p^ℓ residue classes modulo $p^r\mathbb{Z}$ are zeros.

Lemma 37. *Let p be a prime and let $\ell, u \geq 1$ and let m be such that $0 \leq m \leq p^\ell$. Then, there exists $r \geq 0$ arbitrary large such that there exists a polynomial $P(t) \in \mathbb{Z}[t]$ with exactly mp^r zeros $(\text{mod } p^{r+\ell})$ and with $v_p(P(t)) \leq r + \ell - u$ whenever t is not one of such zeros.*

Proof. We order the numbers $0 \leq j < p^\ell$ in the following way: given $0 \leq h, k < p^\ell$ we say $h >^* k$ iff writing $h = a_0 + a_1p + \dots + a_{\ell-1}p^{\ell-1}$, $k = b_0 + b_1p + \dots + b_{\ell-1}p^{\ell-1}$, then $a_d < b_d$ where $d = v_p(k - h)$. Then, we order the numbers $0 \leq j < p^\ell$ as $b_0 >^* b_1 >^* \dots >^* b_{p^\ell-1}$, with

$$\begin{aligned} b_0 &= 0 >^* b_1 = p^{\ell-1} >^* 2p^{\ell-1} >^* \dots >^* (p-1)p^{\ell-1} >^* p^{\ell-2} \geq p^{\ell-2} + p^{\ell-1} >^* \dots \\ &>^* p^{\ell-2} + (p-1)p^{\ell-1} >^* 2p^{\ell-2} >^* 2p^{\ell-2} + p^{\ell-1} >^* \dots >^* p^\ell - 1 = b_{p^\ell-1}. \end{aligned}$$

Notice that with this choice for all $0 \leq i < p^\ell$ we have that $v_p(b_j - b_i)$ is decreasing in j with $i < j \leq p^\ell$. In particular, for any sequence of non-negative real numbers $\kappa_0, \dots, \kappa_{p^\ell-1}$ we have that $\sum_{i=0}^b \kappa_i v_p(b_j - b_i)$ is also decreasing in j for $0 \leq b < j < p^\ell$.

Next, for any positive integer s , define recursively the sequence c_j for $0 \leq j < m$ in the following way:

$$c_0 = s/\ell, \quad \ell c_j = s - \sum_{i=0}^{j-1} c_i v_p(b_j - b_i).$$

We have that $c_j > 0$ for all j . Indeed, this is obvious for $j \leq 1$ and if we assume by induction that it is true for $j \leq k$ with $k < m-1$, then

$$\begin{aligned} \ell(c_k - c_{k+1}) &= \sum_{i=0}^k c_i v_p(b_{k+1} - b_i) - \sum_{i=0}^{k-1} c_i v_p(b_k - b_i) \\ &= c_k v_p(b_{k+1} - b_k) + \sum_{i=0}^{k-1} c_i v_p(b_{k+1} - b_i) - \sum_{i=0}^{k-1} c_i v_p(b_k - b_i) \\ &\leq c_k v_p(b_{k+1} - b_k). \end{aligned}$$

Thus,

$$c_{k+1} \geq c_k(1 - v_p(b_{k+1} - b_k)/\ell) \geq c_k/\ell > 0.$$

Moreover, it's clear that $c_i \ell^m / s$ is an integer, so that taking s to be any multiple of $\ell^m u$ we have that c_i is an integer greater than or equal to u .

Now, let $P(t) := \prod_{0 \leq i < m} (t - b_i)^{c_i}$. For $t \equiv b_j \pmod{p^\ell}$ with $j \geq m$, we have

$$\begin{aligned} v_p(P(t)) &= \sum_{i=0}^{m-1} c_i v_p(b_j - b_i) = c_{m-1} v_p(b_j - b_{m-1}) + \sum_{i=0}^{m-2} c_i v_p(b_j - b_i) \\ &\leq c_{m-1} v_p(b_j - b_{m-1}) + \sum_{i=0}^{m-2} c_i v_p(b_{m-1} - b_i) \\ &= s - c_{m-1}(\ell - v_p(b_j - b_{m-1})) \leq s - c_{m-1} \leq s - u, \end{aligned}$$

since $b_j \not\equiv b_{m-1} \pmod{p^\ell}$. Finally, if $t \equiv b_j \pmod{p^\ell}$ with $0 \leq j \leq m-1$, then

$$v_p(P(t)) \geq \sum_{i=0}^{j-1} c_i v_p(b_j - b_i) + c_j \ell = s.$$

Thus, the Lemma follows with $r = s - \ell$. $\square$

Lemma 38. *Let $0 \neq |h/k| < 1$ with $(h, k) = 1$ and let $p_1, \dots, p_g$ be the (distinct) prime factors of k . Then there exists $d_1, \dots, d_g \in \mathbb{Z}$, $r_1, \dots, r_g \in \mathbb{N}$ such that $-1 < d_i/p_i^{r_i} < 1$ for $i = 1, \dots, g$ and $h/k = \prod_{i=1}^g d_i/p_i^{r_i}$. Moreover, we can choose $d_1, \dots, d_g$ so that $d_1 \cdots d_g | (hk)^\infty$.*

Proof. We prove the Lemma by induction on the number of distinct prime factors of k , the result being obvious if k has only one prime factor. Thus, assume that k has $g+1$ prime factors and that the Lemma is true whenever k has g prime factors with $g \geq 1$. Let p, q be two distinct prime factors of k . Since $\log p$ and $\log q$ are linearly independent we can find arbitrarily large $u, v \in \mathbb{N}$ such that $|h/k| < q^v/p^u < 1$. In particular, writing $h' = h \cdot p^u/(p^u, k)$, $k' = k \cdot q^v/(p^u, k)$ then we have $\frac{h}{k} = \frac{h'}{k'} \frac{q^v}{p^u}$ and, if u is large enough, k' has g prime factors and $0 \neq |h'/k'| < 1$ and so the result follows by the inductive hypothesis. $\square$

Proof of Theorem 4. Let $(h, k) = 1$ with $k \geq 1$, h odd and, if k even then $|h/k| \leq (2^{v_2(k)} - 1)/2^{v_2(k)}$. We now construct a subfamily of $\mathcal{F}_a(t)$ with average root number h/k . As in the proof of Theorem 5 we can assume $h/k \neq 0, \pm 1$.

For simplicity we assume k is divisible by 2, but it's not a power of 2. The same proof works with obvious modifications also without these conditions. Then, we can write h/k as

$$\frac{h}{k} = \frac{2^{v_2(k)} - 1}{2^{v_2(k)}} \frac{h'}{k'}$$

with $-1 < h'/k' < 1$, and h', k' odd. We use Lemma 38 to write h'/k' as $h'/k' = \prod_{i=1}^g (d_i/p_i^{u_i})$ where $p_1, \dots, p_g$ are the (distinct) prime factors of k' , $u_1, \dots, u_g$ are positive integers and $-p^{u_i} < d_i < p^{u_i}$ with d_i odd. In particular

$$\frac{h}{k} = \frac{d_0}{2^{u_0}} \frac{d_1}{p_1^{u_1}} \cdots \frac{d_g}{p_g^{u_g}},$$

where $u_0 = v_2(k) + 1$, and $d_0 = 2^{u_0} - 1$. We will also use the notation $p_0 = 2$.

For $i = 1, \dots, g$, let m_i be such that $d_i = 2m_i - p_i^{u_i}$, so that $0 < m_i < p_i^{u_i}$, and let

$$m'_i := \begin{cases} m_i & \text{if } p_i \equiv 3 \pmod{4}, \\ p_i^{u_i} - m_i & \text{if } p_i \equiv 1 \pmod{4}. \end{cases}$$

By Lemma 37, there exist $r_i \in \mathbb{N}$ and a polynomial Q_i such that the set Z_i of zeros of $Q_i(t)$ modulo $p_i^{r_i+u_i}$ has cardinality $m'_i p_i^{r_i}$, and $v_{p_i}(Q_i(t)) \leq r_i + u_i - 1$ if $t \notin Z_i$. Then, let

$$B_i(t) = p_i Q_i(t)^2 - p_i^{2r_i+2u_i}$$

Notice that if $t \pmod{p_i^{r_i+u_i}}$ is not in Z_i , then $v_{p_i}(B_i(t)) = 1 + 2v_p(Q_i(t)) \leq 2r_i + 2u_i - 1$ is odd and

$$\gcd(p_i^{2r_i+2u_i+1}, B_i(t)) = p_i^{1+2v_p(Q_i(t))} \equiv p_i \pmod{4}.$$

Instead, if $t \pmod{p_i^{r_i+u_i}}$ is in Z_i , then $v_{p_i}(B_i(t)) = 2r_i + 2u_i$ and $B_i(t)_{p_i} \equiv -1 \pmod{p_i}$ so that $\left(\frac{B_i(t)_{p_i}}{p_i}\right) = \left(\frac{-1}{p_i}\right) \equiv p_i \pmod{4}$. Also, in this case

$$\gcd(p_i^{2r_i+2u_i+1}, B_i(t)) = p_i^{2r_i+2u_i} \equiv 1 \pmod{4}.$$

Thus, summarizing both cases

$$\begin{aligned} (p_i^{2r_i+2u_i+1}, B_i(t))(-1)^{1+v_{p_i}(B_i(t))} \left(\frac{B_i(t)p_i}{p_i} \right)^{1+v_{p_i}(B_i(t))} &\equiv \begin{cases} -p_i \pmod{4} & \text{if } t \pmod{p} \in Z_i \\ p_i \pmod{4} & \text{if } t \pmod{p} \notin Z_i \end{cases} \\ &\equiv \begin{cases} 1 \pmod{4} & \text{if } t \pmod{p} \in S_i \\ -1 \pmod{4} & \text{if } t \pmod{p} \notin S_i \end{cases} \end{aligned}$$

where S_i is equal to Z_i if $p_i \equiv 3 \pmod{4}$, and it is equal to its complement (in $\mathbb{Z}/p_i^{r_i+u_i}\mathbb{Z}$) if $p_i \equiv 1 \pmod{4}$. Notice that in both cases we have that $|S_i| = m_i p_i^{r_i}$.

Next, we use Lemma 37 to find $r_0 \in \mathbb{N}$ and a polynomial Q_0 such that the set Z_0 of zeros of $Q_0(t)$ modulo $2^{r_0+u_0}$ has cardinality $(2^{u_0} - 1)2^{r_0}$ and $v_2(Q_0(t)) \leq r_0 + u_0 - 2$ whenever $t \pmod{2^{r_0+u_0}}$ is not in Z_0 . Then, we define

$$B_0(t) = 2Q_0(t)^2 - 2^{2r_0+2u_0-1}.$$

If $t \pmod{2^{r_0+u_0}} \notin Z_0$, then $v_2(B_0(t)) = 1 + 2v_2(Q_0(t)) \leq 2r_0 + 2u_0 - 3$ is odd and $B_0(t)_2 \equiv (Q_0(t)_2)^2 \equiv 1 \pmod{4}$. If $t \pmod{2^{r_0+u_0}} \in Z_0$, then $v_2(B_0(t)) = 2r_0 + 2u_0 - 1$ and $B_0(t)_2 \equiv -1 \pmod{4}$. By Remark 2 after Proposition 15, in both cases we have $s_{2^{2r_0+2u_0+3}}(B_0(t)) \equiv B_0(t)_2 \pmod{4}$ and so

$$s_{2^{2r_0+2u_0+3}}(B_0(t)) \equiv \begin{cases} 1 \pmod{4} & \text{if } t \pmod{p} \in S_0, \\ -1 \pmod{4} & \text{if } t \pmod{p} \notin S_0, \end{cases}$$

where S_0 is the complement of Z_0 in $\mathbb{Z}/2^{r_0+u_0}\mathbb{Z}$, so that $|S_0| = 2^{r_0}$.

We can now define $a = 4 \prod_{i=0}^g p_i^{2r_i+2u_i+1}$ and

$$Q(t) = \sum_{i=0}^g (p_0 \cdots p_g / p_i)^r x_{p_i}^r B_i(t),$$

where x_{p_i} is the inverse of $p_0 \cdots p_g / p_i$ modulo p_i and where $r = 2 \max_{i=0, \dots, g} (u_i + r_i + 1)$. It follows that the sign $\varepsilon(t)$ of the elliptic curve $\mathcal{W}_a(Q(t))$ is

$$\begin{aligned} \varepsilon(t) &\equiv -s_a(B_0(t)) \prod_{i=1}^g \gcd(p_i^{2u_i+2r_i+1}, B_i(t))(-1)^{1+v_{p_i}(B_i(t))} \left(\frac{B_i(t)p_i}{p_i} \right)^{1+v_{p_i}(B_i(t))} \pmod{4} \\ &\equiv - \prod_{i=0}^g h_i(t) \pmod{4} \end{aligned}$$

where $h_i(t) = 1$ if $t \pmod{p_i^{r_i+u_i}}$ is in S_i and it is equal to $h_i(t) = -1$ otherwise. Thus, by the Chinese remainder theorem

$$\begin{aligned} \text{Av}_{\mathbb{Z}}(\varepsilon) &= - \prod_{i=0}^g \left(2 \frac{|S_i|}{p_i^{u_i+r_i}} - 1 \right) = - \left(\frac{2^{r_0+1}}{2^{r_0+u_0}} - 1 \right) \prod_{i=1}^g \left(2 \frac{m_i p_i^{r_i}}{p_i^{u_i+r_i}} - 1 \right) \\ &= \frac{2^{u_0} - 2}{2^{u_0}} \prod_{i=1}^g \frac{d_i}{p_i^{u_i}} = \frac{h}{k}, \end{aligned}$$

as desired.

For the converse, let's assume Conjecture 1 and Conjecture 2, and prove that the equality holds in (1.7). By Corollary 36, we have that if the root number $\varepsilon_{\mathcal{F}}$ of a family of elliptic curves $\mathcal{F}$ is periodic modulo ℓ up to $o(1)$ exceptions then

$$\varepsilon_{\mathcal{F}}(t) = \rho \prod_{p|\ell} h_p(t)$$

up to $o(1)$ exceptions, where $h_p : \mathbb{Z} \rightarrow \{\pm 1\}$ is periodic modulo $p^{v_p(\ell)}$ and $\rho \in \{\pm 1\}$. Thus, by the Chinese remainder theorem we have

$$\text{Av}_{\mathbb{Z}}(\varepsilon_F) = \prod_{p|\ell} \left(\sum_{m \pmod{p^{v_p(\ell)}}} h_p(m) \right) = \prod_{p|\ell} \left(1 - \frac{2\kappa_p}{p^{v_p(\ell)}} \right) = \frac{2^{v_2(\ell)-1} - \kappa_2}{2^{v_2(\ell)-1}} \prod_{2 \nmid p|\ell} \left(\frac{p^{v_p(\ell)} - 2\kappa_p}{p^{v_p(\ell)}} \right)$$

where $\kappa_p := |\{t \pmod{p^{v_p(\ell)}} \mid h_p(t) = -1\}|$. Since the product over $2 \nmid p|\ell$ is a rational number with numerator and denominator which are both odd, it follows that if $\text{Av}_{\mathbb{Z}}(\varepsilon_F) = \frac{h}{k}$ with $(h, k) = 1$, then $|\frac{h}{k}| \leq \frac{2^{v_2(k)} - 1}{2^{v_2(k)}}$. $\square$

REFERENCES

- [ALRM07] Scott Arms, Álvaro Lozano-Robledo, and Steven J. Miller. Constructing one-parameter families of elliptic curves with moderate rank. *J. Number Theory*, 123(2):388–402, 2007.
- [BKL⁺15] Manjul Bhargava, Daniel M. Kane, Hendrik W. Lenstra, Jr., Bjorn Poonen, and Eric Rains. Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves. *Camb. J. Math.*, 3(3):275–321, 2015.
- [Bye97] Dongho Byeon. Quadratic twists of elliptic curves associated to the simplest cubic fields. *Proc. Japan Acad. Ser. A Math. Sci.*, 73(10):185–186, 1997.
- [CCH05] B. Conrad, K. Conrad, and H. Helfgott. Root numbers and ranks in positive characteristic. *Adv. Math.*, 198(2):684–731, 2005.
- [Con94] Ian Connell. Calculating root numbers of elliptic curves over $\mathbf{Q}$. *Manuscripta Math.*, 82(1):93–104, 1994.
- [DD09] Tim Dokchitser and Vladimir Dokchitser. Elliptic curves with all quadratic twists of positive rank. *Acta Arith.*, 137(2):193–197, 2009.
- [Des16a] Julie Desjardins. Densité des points rationnels sur les surfaces elliptiques et les surfaces de del pezzo de degré 1. *PhD thesis, Université Paris Diderot, Institut de mathématiques de Jussieu Rive Gauche, available at <https://webusers.imj-prg.fr/~julie.desjardins/these.pdf>*, 2016.
- [Des16b] Julie Desjardins. On the variation of the root number in families of elliptic curves. *Preprint, arXiv:math/1610.07440*, 2016.
- [DJ14] Christophe Delaunay and Frédéric Jouhet. p^ℓ -torsion points in finite abelian groups and combinatorial identities. *Adv. Math.*, 258:13–45, 2014.
- [Duq01] Sylvain Duquesne. Integral points on elliptic curves defined by simplest cubic fields. *Experiment. Math.*, 10(1):91–102, 2001.
- [Far05] David Farmer. Modeling families of l-functions. *Preprint, arXiv:math/0511107v1*, 2005.
- [Hal98] Emmanuel Halberstadt. Signes locaux des courbes elliptiques en 2 et 3. *C. R. Acad. Sci. Paris Sér. I Math.*, 326(9):1047–1052, 1998.
- [Hel03] Harald Helfgott. Root numbers and the parity problem. *Preprint, arXiv:math/0305435*, 2003.
- [Hel04] Harald Helfgott. On the square-free sieve. *Acta Arith.*, 115(4):349–402, 2004.
- [Hel09] Harald Helfgott. On the behaviour of root numbers in families of elliptic curves. *Preprint, arXiv:math/0408141v3*, 2009.
- [KMR13] Zev Klagsbrun, Barry Mazur, and Karl Rubin. Disparity in Selmer ranks of quadratic twists of elliptic curves. *Ann. of Math. (2)*, 178(1):287–320, 2013.
- [KN92] Mayumi Kawachi and Shin Nakano. The 2-class groups of cubic fields and 2-descents on elliptic curves. *Tohoku Math. J. (2)*, 44(4):557–565, 1992.
- [Kow13] Emmanuel Kowalski. Families of cusp forms. *Publ. Math. Besançon Algèbre Théorie Nr.*, pages 5–40, 2013.
- [Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.
- [LN83] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1983. With a foreword by P. M. Cohn.
- [Mir95] Rick Miranda. An overview of algebraic surfaces. *Notes for Lectures at the Summer School on Algebraic Geometry, Bilkent International Center for Advanced Studies, Bilkent University, Ankara, Turkey*, 1995.
- [OS91] Keiji Oguiso and Tetsuji Shioda. The Mordell-Weil lattice of a rational elliptic surface. *Comment. Math. Univ. St. Paul.*, 40(1):83–99, 1991.
- [PAR16] Group PARI. PARI/GP, version 2.8.1. *Bordeaux*, 2016.
- [PR12] Bjorn Poonen and Eric Rains. Random maximal isotropic subspaces and Selmer groups. *J. Amer. Math. Soc.*, 25(1):245–269, 2012.
- [Riz99] Ottavio Rizzo. Average root numbers in families of elliptic curves. *Proc. Amer. Math. Soc.*, 127(6):1597–1603, 1999.

- [Riz03] Ottavio G. Rizzo. Average root numbers for a nonconstant family of elliptic curves. *Compositio Math.*, 136(1):1–23, 2003.
- [Roh93] David E. Rohrlich. Variation of the root number in families of elliptic curves. *Compositio Math.*, 87(2):119–151, 1993.
- [Rom05] Fausto Romano. Sulla distribuzione della parità del rango di famiglie di curve ellittiche. *Master thesis, supervised by Ottavio Rizzo, Corso di laurea di Matematica, Università degli Studi di Milan*, 2005.
- [RS98] Michael Rosen and Joseph H. Silverman. On the rank of an elliptic surface. *Invent. Math.*, 133(1):43–67, 1998.
- [Sar08] Peter Sarnak. Definition of families of l -functions. *letter to H. Iwaniec, P. Michel, A. Venkatesh and others*, 2008.
- [Sch88] Charles F. Schwartz. On a family of elliptic surfaces with Mordell-Weil rank 4. *Proc. Amer. Math. Soc.*, 102(1):1–8, 1988.
- [SS10] Matthias Schütt and Tetsuji Shioda. Elliptic surfaces. *Preprint, arXiv:math/0907.0298v3*, 2010.
- [Was87] Lawrence C. Washington. Class numbers of the simplest cubic fields. *Math. Comp.*, 48(177):371–384, 1987.

APPENDIX A. ROOT NUMBER OF $\mathcal{F}_s$

The proofs of the propositions in Appendix A and B can be obtained by a long case by case analysis in the same way as in the proof of Proposition 14.

In this appendix we give the local root numbers for the family

$$\mathcal{F}_s: y^2 = x^3 + 3tx^2 + 3sx + st$$

for which we have

$$\begin{aligned} c_4 &= 2^4 \times 3^2(t^2 - s), \\ c_6 &= -2^6 \times 3^3 \times t(t^2 - s), \\ \Delta &= -2^6 3^3 s(t^2 - s)^2, \\ j &= \frac{-2^6 3^3}{s}(t^2 - s). \end{aligned}$$

For a prime p , we denote by $w_p(t)$ the local root number of $\mathcal{F}_s$ at p .

Proposition 39. *If $p \geq 5$, we have:*

- if $0 \leq v_p(s) < 2v_p(t)$ then if $v_p(s)$ is even $w_p(t) = \left(\frac{-1}{p}\right)^{v_p(s)/2}$ and otherwise $w_p(t) = \left(\frac{-2}{p}\right)$ (this case also holds for $t = 0$ for which $v_p(t) = +\infty$);
- if $0 \leq 2v_p(t) < v_p(s)$ then if $v_p(t)$ is even $w_p(t) = -\left(\frac{3t_p}{p}\right)$ and otherwise $w_p(t) = \left(\frac{-1}{p}\right)$;
- if $0 \leq 2v_p(t) = v_p(s)$ then
 - if $v_p(t^2 - s) \equiv v_p(t) \pmod{2}$ then if $v_p(t^2 - s) + v_p(t) \equiv 0 \pmod{3}$ then $w_p(t) = 1$ otherwise $w_p(t) = \left(\frac{-3}{p}\right)$;
 - if $v_p(t^2 - s) \not\equiv v_p(t) \pmod{2}$ then $w_p(t) = \left(\frac{-1}{p}\right)$.

Proposition 40. *If $p = 3$, we have:*

- if $0 \leq v_3(s) < 2v_3(t)$:
 - if $v_3(s) \equiv 0 \pmod{4}$ if $v_3(t) = 1 + v_3(s)/2$ then $w_3(t) = 1$ if and only if $t_3 \equiv 1 \pmod{3}$ if $v_3(t) > 1 + v_3(s)/2$ then $w_3(t) = 1$;
 - if $v_3(s) \equiv 1 \pmod{4}$ if $v_3(t) = 1/2 + v_3(s)/2$ then $w_3(t) = 1$ if and only if $s_3 \equiv 1 \pmod{3}$ if $v_3(t) > 1/2 + v_3(s)/2$ then $w_3(t) = -1$;
 - if $v_3(s) \equiv 2 \pmod{4}$ if $v_3(t) = 1 + v_3(s)/2$ then $w_3(t) = 1$ if and only if $t_3 \not\equiv s_3 \pmod{3}$ if $v_3(t) > 1 + v_3(s)/2$ then $w_3(t) = 1$;
 - if $v_3(s) \equiv 3 \pmod{4}$ then $w_3(t) = 1$.
- If $0 \leq 2v_3(t) < v_3(s)$:
 - if $v_3(t) \equiv 0 \pmod{2}$ if $v_3(s) - 2v_3(t) = 1$ then $w_3(t) = 1$, if $v_3(s) - 2v_3(t) = 2$ then $w_3(t) = 1$ if and only if $t_3 \equiv s_3 \pmod{3}$ and if $v_3(s) - 2v_3(t) \geq 3$ then $w_3(t) = -1$;

- if $v_3(t) \equiv 1 \pmod{2}$ if $v_3(s) - 2v_3(t) = 1$ then $w_3(t) = 1$ if and only if $s_3 \equiv 1 \pmod{3}$, if $v_3(s) - 2v_3(t) = 2$ then $w_3(t) = 1$ if and only if $t_3 \equiv 2 \pmod{3}$, if $v_3(s) - 2v_3(t) = 3$ then $w_3(t) = 1$ and if $v_3(s) - 2v_3(t) \geq 4$ then $w_3(t) = 1$ if and only if $t_3 \equiv 2 \pmod{3}$.
- If $0 \leq 2v_3(t) = v_3(s)$ and $v_3(t)$ even:
 - if $v_3(t^2 - s) = 2v_3(t)$ then $w_3(t) = 1$ if and only if $s_3 \equiv 2 \pmod{3}$ and $s_3 t_3 \not\equiv 2, 4 \pmod{9}$;
 - if $v_3(t^2 - s) - 2v_3(t) \equiv 0 \pmod{6}$ and $v_3(t^2 - s) - 2v_3(t) > 0$ then $w_3(t) = 1$ if and only if $t_3(t^2 - s)_3 \not\equiv 7, 8 \pmod{9}$;
 - if $v_3(t^2 - s) - 2v_3(t) \equiv 1$ or $2 \pmod{6}$ then $w_3(t) = 1$ if and only if $t_3(t^2 - s)_3 \equiv 1 \pmod{3}$;
 - if $v_3(t^2 - s) - 2v_3(t) \equiv 3$ then $w_3(t) = 1$ if and only if $t_3(t^2 - s)_3 \not\equiv 1, 2 \pmod{9}$;
 - if $v_3(t^2 - s) - 2v_3(t) \equiv 4$ or $5 \pmod{6}$ then $w_3(t) = 1$ if and only if $t_3(t^2 - s)_3 \equiv 2 \pmod{3}$.
- If $0 \leq 2v_3(t) = v_3(s)$ and $v_3(t)$ odd:
 - if $v_3(t^2 - s) = 2v_3(t)$ then $w_3(t) = 1$ if and only if $s_3 \equiv 2 \pmod{3}$ and $s_3 t_3 \not\equiv 2, 4 \pmod{9}$;
 - if $v_3(t^2 - s) - 2v_3(t) \equiv 0 \pmod{6}$ and $v_3(t^2 - s) - 2v_3(t) > 0$ then $w_3(t) = 1$ if and only if $t_3(t^2 - s)_3 \not\equiv 1, 2 \pmod{9}$;
 - if $v_3(t^2 - s) - 2v_3(t) \equiv 1$ or $2 \pmod{6}$ then $w_3(t) = 1$ if and only if $t_3(t^2 - s)_3 \equiv 2 \pmod{3}$;
 - if $v_3(t^2 - s) - 2v_3(t) \equiv 3 \pmod{6}$ then $w_3(t) = 1$ if and only if $t_3(t^2 - s)_3 \not\equiv 7, 8 \pmod{9}$;
 - if $v_3(t^2 - s) - 2v_3(t) \equiv 4$ or $5 \pmod{6}$ then $w_3(t) = 1$ if and only if $t_3(t^2 - s)_3 \equiv 1 \pmod{3}$.

Proposition 41. *If $p = 2$, we have:*

- if $0 \leq v_2(s) < 2v_2(t)$:
 - if $v_2(s) \equiv 0 \pmod{4}$ then
 - * if $v_2(t) - v_2(s)/2 = 1$ then $w_2(t) = 1$ if and only if

$$\begin{cases} s_2 \equiv 3 \pmod{4} \\ \text{or} \\ s_2 \equiv 1 \text{ or } 13 \pmod{16} \text{ and } t_2 \equiv 3 \pmod{4} \\ \text{or} \\ s_2 \equiv 5 \text{ or } 9 \pmod{16} \text{ and } t_2 \equiv 1 \pmod{4}; \end{cases}$$
 - * if $v_2(t) - v_2(s)/2 = 2$ then $w_2(t) = 1$ if and only if $s_2 \equiv 5 \text{ or } 9 \pmod{16}$;
 - * if $v_2(t) - v_2(s)/2 \geq 2$ then $w_2(t) = 1$ if and only if $s_2 \equiv 1 \text{ or } 13 \pmod{16}$.
 - If $v_2(s) \equiv 1 \pmod{4}$, if $v_2(t) - v_2(s)/2 = 1/2$ then $w_2(t) = 1$ if and only if

$$\begin{cases} s_2 \equiv 1 \text{ or } 3 \pmod{8} \text{ and } t_2 \equiv 3 \pmod{4} \\ \text{or} \\ s_2 \equiv 5 \text{ or } 7 \pmod{8} \text{ and } t_2 \equiv 1 \pmod{4}, \end{cases}$$
 and if $v_2(t) - v_2(s)/2 \geq 1$ then $w_2(t) = 1$ if and only if $s_2 \equiv 5 \text{ or } 7 \pmod{8}$.
- if $v_2(s) \equiv 2 \pmod{4}$ then
 - * if $v_2(t) - v_2(s)/2 = 1$ then $w_2(t) = 1$ if and only if

$$\begin{cases} s_2 \equiv 1 \pmod{4} \\ \text{or} \\ s_2 \equiv 3 \text{ or } 7 \pmod{16} \text{ and } t_2 \equiv 1 \pmod{4} \\ \text{or} \\ s_2 \equiv 11 \text{ or } 15 \pmod{16} \text{ and } t_2 \equiv 3 \pmod{4}; \end{cases}$$
 - * if $v_2(t) - v_2(s)/2 = 2$ then $w_2(t) = 1$ if and only if $s_2 \equiv 7 \text{ or } 11 \pmod{16}$;
 - * if $v_2(t) - v_2(s)/2 \geq 2$ then $w_2(t) = 1$ if and only if $s_2 \equiv 3 \text{ or } 15 \pmod{16}$.

– if $v_2(s) \equiv 3 \pmod{4}$, if $v_2(t) - v_2(s)/2 = 1/2$ then $w_2(t) = 1$ if and only if

$$\begin{cases} s_2 \equiv 1 \text{ or } 7 \pmod{8} \text{ and } t_2 \equiv 1 \pmod{4} \\ \text{or} \\ s_2 \equiv 3 \text{ or } 5 \pmod{8} \text{ and } t_2 \equiv 3 \pmod{4}, \end{cases}$$

and if $v_2(t) - v_2(s)/2 \geq 1$ then $w_2(t) = 1$ if and only if $s_2 \equiv 1 \text{ or } 3 \pmod{8}$.

- If $0 \leq 2v_2(t) < v_2(s)$ and $v_2(t)$ even:
 - if $v_2(s) - 2v_2(t) = 1$ then $w_2(t) = 1$ if and only if $r_2 \equiv 1 \pmod{4}$ and $t_2 \equiv 1 \text{ or } 7 \pmod{8}$ or if $s_2 \equiv 3 \pmod{4}$ and $t_2 \equiv 1 \text{ or } 3 \pmod{8}$;
 - if $v_2(s) - 2v_2(t) = 2$ then $w_2(t) = 1$ if and only if $s_2 \equiv 1 \pmod{8}$ and $t_2 \equiv 3, 5 \text{ or } 7 \pmod{8}$ or if $s_2 \equiv 5 \pmod{8}$ and $t_2 \equiv 1, 3 \text{ or } 7 \pmod{8}$;
 - if $v_2(s) - 2v_2(t) = 3$ then $w_2(t) = 1$ if and only if $s_2 \equiv 1 \pmod{4}$ and $t_2 \equiv 3 \text{ or } 5 \pmod{8}$ or if $s_2 \equiv 3 \pmod{4}$ and $t_2 \equiv 1 \text{ or } 3 \pmod{8}$;
 - if $v_2(s) - 2v_2(t) = 4$ then $w_2(t) = 1$ if and only if $t_2 \equiv 1 \pmod{4}$ or if $s_2 \equiv 1 \pmod{4}$ and $t_2 \equiv 3 \pmod{8}$ or if $s_2 \equiv 3 \pmod{4}$ and $t_2 \equiv 7 \pmod{8}$;
 - if $v_2(s) - 2v_2(t) = 5$ then $w_2(t) = 1$ if and only if $t_2 \equiv 1 \pmod{4}$ or if $t_2 \equiv 7 \pmod{8}$;
 - if $v_2(s) - 2v_2(t) = 6$ then $w_2(t) = 1$ if and only if $t_2 \equiv 3 \pmod{4}$;
 - if $v_2(s) - 2v_2(t) \geq 7$ then $w_2(t) = 1$ if and only if $t_2 \equiv 7 \pmod{8}$.
- If $0 \leq 2v_2(t) < v_2(s)$ and $v_2(t)$ odd:
 - if $v_2(s) - 2v_2(t) = 1$ then $w_2(t) = 1$ if and only if $t_2 \equiv r_2$ or $s_2 + 2 \pmod{8}$;
 - if $v_2(s) - 2v_2(t) = 2$ then $w_2(t) = 1$ if and only if $t_2 \equiv s_2 \pmod{4}$;
 - if $v_2(s) - 2v_2(t) = 3$ then $w_2(t) = 1$ if and only if $s_2 \equiv 3 \pmod{4}$;
 - if $v_2(s) - 2v_2(t) \geq 4$ then $w_2(t) = 1$ if and only if $t_2 \equiv 3 \pmod{4}$.
- If $0 \leq 2v_2(t) = v_2(s)$ and $v_2(t)$ even:
 - if $v_2(t^2 - s) - 2v_2(t) \equiv 0 \pmod{6}$ then $w_2(t) = 1$ if and only if $t_2 \equiv (t^2 - s)_2 \pmod{4}$;
 - if $v_2(t^2 - s) - 2v_2(t) = 1$ then $w_2(t) = 1$ if and only if $t_2 \equiv 1 \pmod{4}$ and $t_2(t^2 - s)_2 \equiv 1 \text{ or } 7 \pmod{8}$ or if $t_2 \equiv 3 \pmod{4}$ and $t_2(t^2 - s)_2 \equiv 5 \text{ or } 7 \pmod{8}$;
 - if $v_2(t^2 - s) - 2v_2(t) \equiv 1 \pmod{6}$ and $v_2(t^2 - s) - 2v_2(t) > 1$ then $w_2(t) = -1$;
 - if $v_2(t^2 - s) - 2v_2(t) = 2$ then $w_2(t) = 1$ if and only if $t_2 \equiv 3 \pmod{4}$;
 - if $v_2(t^2 - s) - 2v_2(t) \equiv 2 \pmod{6}$ and $v_2(t^2 - s) - 2v_2(t) > 2$ then $w_2(t) = 1$ if and only if $t_2 \equiv (t^2 - s)_2 \pmod{4}$;
 - if $v_2(t^2 - s) - 2v_2(t) = 3$ then $w_2(t) = 1$ if and only if $t_2 \equiv 1 \pmod{4}$ and $t_2(t^2 - s)_2 \equiv 5 \text{ or } 7 \pmod{8}$ or if $t_2 \equiv 3 \pmod{4}$ and $t_2(t^2 - s)_2 \equiv 3 \text{ or } 5 \pmod{8}$;
 - if $v_2(t^2 - s) - 2v_2(t) \equiv 3 \pmod{6}$ and $v_2(t^2 - s) - 2v_2(t) > 3$ then $w_2(t) = 1$ if and only if $t_2 \equiv (t^2 - s)_2 \pmod{4}$;
 - if $v_2(t^2 - s) - 2v_2(t) \equiv 4 \pmod{6}$ then $w_2(t) = 1$ if and only if $t_2 \equiv (t^2 - s)_2 \pmod{4}$;
 - if $v_2(t^2 - s) - 2v_2(t) = 5$ then $w_2(t) = 1$ if and only if $t_2(t^2 - s)_2 \equiv 1, 3 \text{ or } 7 \pmod{8}$;
 - if $v_2(t^2 - s) - 2v_2(t) \equiv 5 \pmod{6}$ and $v_2(t^2 - s) - 2v_2(t) > 5$ then $w_2(t) = -1$.
- If $0 \leq 2v_2(t) = v_2(s)$ and $v_2(t)$ odd:
 - if $v_2(t^2 - s) - 2v_2(t) \equiv 0 \pmod{6}$ then $w_2(t) = 1$ if and only if $t_2 \equiv (t^2 - s)_2 \pmod{4}$;
 - if $v_2(t^2 - s) - 2v_2(t) = 1$ then $w_2(t) = 1$ if and only if $t_2 \equiv 3 \pmod{8}$ or if $t_2 \equiv 1 \pmod{8}$ and $(t^2 - s)_2 \equiv 1 \text{ or } 5 \pmod{8}$ or if $t_2 \equiv 5 \pmod{8}$ and $(t^2 - s)_2 \equiv 3 \text{ or } 7 \pmod{8}$;
 - if $v_2(t^2 - s) - 2v_2(t) \equiv 1 \pmod{6}$ and $v_2(t^2 - s) - 2v_2(t) > 1$ then $w_2(t) = 1$ if and only if $t_2 \equiv (t^2 - s)_2 \pmod{4}$;
 - if $v_2(t^2 - s) - 2v_2(t) = 2$ then $w_2(t) = 1$ if and only if $t_2 \equiv (t^2 - s)_2 \equiv 1 \pmod{4}$ or if $t_2 \equiv 7 \pmod{8}$ and $(t^2 - s)_2 \equiv 1 \pmod{4}$;
 - if $v_2(t^2 - s) - 2v_2(t) \equiv 2 \pmod{6}$ and $v_2(t^2 - s) - 2v_2(t) > 2$ then $w_2(t) = -1$;
 - if $v_2(t^2 - s) - 2v_2(t) = 3$ then $w_2(t) = 1$ if and only if $(t^2 - s)_2 \equiv 3 \pmod{4}$;
 - if $v_2(t^2 - s) - 2v_2(t) \equiv 3 \pmod{6}$ and $v_2(t^2 - s) - 2v_2(t) > 3$ then $w_2(t) = 1$ if and only if $t_2 \equiv (t^2 - s)_2 \pmod{4}$;

- if $v_2(t^2 - s) - 2v_2(t) = 4$ then $w_2(t) = 1$ if and only if $t_2 \equiv 1 \pmod{4}$ and $t_2(t^2 - s)_2 \equiv 3, 5$ or $7 \pmod{8}$ of if $t_2 \equiv 3 \pmod{4}$ and $t_2(t^2 - s)_2 \equiv 1, 3$ or $7 \pmod{8}$;
- if $v_2(t^2 - s) - 2v_2(t) \equiv 4 \pmod{6}$ and $v_2(t^2 - s) - 2v_2(t) > 4$ then $w_2(t) = -1$;
- if $v_2(t^2 - s) - 2v_2(t) \equiv 5 \pmod{6}$ then $w_2(t) = 1$ if and only if $t_2 \equiv (t^2 - s)_2 \pmod{4}$.

APPENDIX B. ROOT NUMBER AT 2 AND 3 FOR $\mathcal{V}_a(t)$

We give the local root number at $p = 2$ and $p = 3$ for the family

$$\mathcal{V}_a: y^2 = x^3 + 3tx^2 + 3atx + a^2t.$$

The local root number at $p \geq 5$ is given in Lemma 22. For the family $\mathcal{V}_a$ we have

$$\begin{aligned} c_4 &= 2^4 3^2 t(t - a), \\ c_6 &= -2^5 3^3 t(t - a)(2t - a), \\ \Delta &= -2^4 3^3 a^2 t^2 (t - a)^2, \\ j &= \frac{-2^8 3^3}{a^2} t(t - a). \end{aligned}$$

For a prime p , we denote by $w_p(t)$ the local root number of $\mathcal{V}_a(t)$ at p . We shall also assume $t \neq 0, a$.

Proposition 42. *We have*

- For $0 \leq v_3(a) < v_3(t)$ then
 - if $v_3(t) - v_3(a) \equiv 0 \pmod{3}$, then $w_3(t) = -1$ if and only if

$$(-1)^{v_3(t)} a_3^2 t_3 \equiv 5 \text{ or } 7 \pmod{9};$$
 - if $v_3(t) - v_3(a) \equiv 1 \text{ or } 2 \pmod{6}$, then $w_3(t) = -1$ if and only if

$$(-1)^{v_3(a)} t_3 \equiv 1 \pmod{3};$$
 - if $v_3(t) - v_3(a) \equiv 4 \text{ or } 5 \pmod{6}$, then $w_3(t) = -1$ if and only if

$$(-1)^{v_3(a)} t_3 \equiv 2 \pmod{3}.$$
- If $0 \leq v_3(t) = v_3(a)$ and $v_3(t - a) - v_3(t) > 0$ then
 - if $v_3(t - a) - v_3(a) \equiv 0 \pmod{3}$, then $w_3(t) = -1$ if and only if

$$(-1)^{v_3(t)} a_3^2 (t - a)_3 \equiv 5 \text{ or } 7 \pmod{9};$$
 - if $v_3(t - a) - v_3(a) \equiv 1 \text{ or } 2 \pmod{6}$, then $w_3(t) = -1$ if and only if

$$(-1)^{v_3(a)} (t - a)_3 \equiv 1 \pmod{3};$$
 - if $v_3(t - a) - v_3(a) \equiv 4 \text{ or } 5 \pmod{6}$, then $w_3(t) = -1$ if and only if

$$(-1)^{v_3(a)} (t - a)_3 \equiv 1 \pmod{3}.$$
- If $0 \leq v_3(t) < v_3(a)$ then
 - if $v_3(2t - a) - v_3(a) = 1$, $w_3 = 1$ if and only if $(2t_3 - a_3) \equiv (-1)^{v_3(a)} 6 \pmod{9}$;
 - if $v_3(2t - a) - v_3(a) > 1$, then $w_3 = 1$.
- If $0 \leq v_3(t) < v_3(a)$ then
 - if $v_3(t) \equiv 0 \pmod{2}$ and $v_3(a) - v_3(t) = 1$, $w_3(t) = 1$ if and only if $t_3 \equiv 1 \pmod{3}$;
 - if $v_3(t) \equiv 0 \pmod{2}$ and $v_3(a) - v_3(t) > 1$, then $w_3(t) = -1$;
 - if $v_3(t) \equiv 1 \pmod{2}$ then $w_3(t) = 1$ if and only if $t_3 \equiv 2 \pmod{3}$.

Proposition 43. *We have*

- For $0 \leq v_2(a) < v_2(t)$ and $v_2(a)$ even then
 - if $v_2(t) - v_2(a) \equiv 0 \pmod{6}$, $w_2(t) = -1$;
 - if $v_2(t) - v_2(a) = 1$ then $w_2(t) = -1$ if and only if $t_2 \equiv a_2 \pmod{4}$;
 - if $v_2(t) - v_2(a) \equiv 1 \pmod{6}$ and $v_2(t) - v_2(a) > 1$ then $w_2(t) \equiv t_2 \pmod{4}$;

- if $v_2(t) - v_2(a) = 2$ then $w_2(t) = 1$ if and only one of the following conditions hold

$$\begin{cases} t_2 \equiv 3 \pmod{4} \\ \text{or} \\ t_2 \equiv 1 \pmod{8} \text{ and } a_2 \equiv 3 \text{ or } 7 \pmod{8} ; \\ \text{or} \\ t_2 \equiv 5 \pmod{8} \text{ and } a_2 \equiv 1 \text{ or } 5 \pmod{8} \end{cases}$$
- if $v_2(t) - v_2(a) \equiv 2 \pmod{6}$ and $v_2(t) - v_2(a) > 2$ then $w_2(t) = -1$;
- if $v_2(t) - v_2(a) \equiv 3, 4 \text{ or } 5 \pmod{6}$ then $w_2(t) \equiv t_2 \pmod{4}$.
- For $0 \leq v_2(a) < v_2(t)$ and $v_2(a)$ odd then
 - if $v_2(t) - v_2(a) \equiv 0, 2 \text{ or } 4 \pmod{6}$ then $w_2(t) \equiv t_2 \pmod{4}$;
 - if $v_2(t) - v_2(a) = 1$ then $w_2(t) = 1$ if and only if one of the following conditions hold

$$\begin{cases} t_2 \equiv 1 \pmod{8} \\ \text{or} \\ (t_2, a_2) \equiv (3, 1), (3, 5), (7, 3) \text{ or } (7, 7) \pmod{8} \end{cases} ;$$
 - if $v_2(t) - v_2(a) \equiv 1 \pmod{6}$ and $v_2(t) - v_2(a) > 1$ then $w_2(t) \equiv t_2 \pmod{4}$;
 - if $v_2(t) - v_2(a) = 3$ then $w_2(t) = -1$ if and only if $t_2 \equiv 5 \pmod{8}$;
 - if $v_2(t) - v_2(a) \equiv 3 \pmod{6}$ and $v_2(t) - v_2(a) > 3$ then $w_2(t) = -1$;
 - if $v_2(t) - v_2(a) \equiv 5 \pmod{6}$ then $w_2(t) = -1$.
- For $0 \leq v_2(t) < v_2(a) - 1$ and $v_2(t)$ even then
 - if $v_2(a) - v_2(t) = 2$ then $w_2(t) = 1$ if and only if one of the following conditions hold

$$\begin{cases} t_2 \equiv 1, 5, 7 \pmod{8} \text{ and } a_2 \equiv 1 \pmod{4} \\ \text{or} \\ t_2 \equiv 1, 3, 5 \pmod{8} \text{ and } a_2 \equiv 3 \pmod{4} \end{cases} ;$$
 - if $v_2(a) - v_2(t) = 3$ then $w_2(t) = 1$ if and only if $t_2 \equiv 1, 5, 7 \pmod{8}$;
 - if $v_2(a) - v_2(t) = 4$ then $w_2(t) = 1$ if and only if $t_2 \equiv 3 \pmod{4}$;
 - if $v_2(a) - v_2(t) \geq 5$ then $w_2(t) = 1$ if and only if $t_2 \equiv 7 \pmod{8}$.
- For $0 \leq v_2(t) < v_2(a) - 1$ and $v_2(t)$ odd then $w_2(t) = 1$ if and only if $t_2 \equiv 3 \pmod{4}$.
- For $0 \leq v_2(t) = v_2(a) - 1$ and $v_2(t)$ even then $w_2(t) = 1$ if and only if one of the following conditions hold

$$\begin{cases} t_2 \equiv 7 \pmod{8} \\ \text{or} \\ t_2 \equiv 1 \pmod{8} \text{ and } a_2 \equiv 1 \pmod{4} \\ \text{or} \\ t_2 \equiv 5 \pmod{8} \text{ and } a_2 \equiv 3 \pmod{4} \end{cases}$$
- For $0 \leq v_2(t) = v_2(a) - 1$ and $v_2(t)$ odd then $w_2(t) = -1$ if and only if $t_2 \equiv a_2 \pmod{4}$.
- For $0 \leq v_2(t) = v_2(a)$ and $v_2(t)$ even then
 - if $v_2(t - a) - v_2(a) \equiv 0 \pmod{6}$ then $w_2(t) = -1$;
 - if $v_2(t - a) - v_2(a) = 1$ then $w_2(t) = 1$ if and only if $(t_2, a_2) \equiv (1, 3), (3, 1), (5, 7) \text{ or } (7, 5) \pmod{8}$;
 - if $v_2(t - a) - v_2(a) \equiv 1 \pmod{6}$ and $v_2(t - a) - v_2(a) > 1$ then $w_2(t) = 1$ if and only if $(t - a)_2 \equiv 1 \pmod{4}$;
 - if $v_2(t - a) - v_2(a) = 2$ then $w_2(t) = 1$ if and only if one of the following conditions hold

$$\begin{cases} t_2 - a_2 \equiv 12 \pmod{16} \\ \text{or} \\ a_2 \equiv 1 \pmod{4} \text{ and } t_2 \equiv a_2 + 4 \pmod{32} \\ \text{or} \\ a_2 \equiv 3 \pmod{4} \text{ and } t_2 \equiv a_2 + 20 \pmod{32}; \end{cases}$$
 - if $v_2(t - a) - v_2(a) \equiv 2 \pmod{6}$ and $v_2(t - a) - v_2(a) > 2$ then $w_2(t) = -1$;

- $v_2(t-a) - v_2(t) \equiv 3, 4 \text{ or } 5 \pmod{6}$ then $w_2(t) \equiv (t-a)_2 \pmod{4}$.
- For $0 \leq v_2(t) = v_2(a)$ and $v_2(t)$ odd then
 - if $v_2(t-a) - v_2(a) \equiv 0 \pmod{6}$ then $w_2(t) \equiv (t-a)_2 \pmod{4}$;
 - if $v_2(t-a) - v_2(a) = 1$ then $w_2(t) = 1$ if and only if one of the following conditions hold

$$\left\{ \begin{array}{l} t_2 - a_2 \equiv 2 \pmod{16} \\ \text{or} \\ a_2 \equiv 1 \pmod{4} \text{ and } t_2 \equiv a_2 + 14 \pmod{16} \\ \text{or} \\ a_2 \equiv 3 \pmod{4} \text{ and } t_2 \equiv a_2 + 6 \pmod{16}; \end{array} \right.$$
 - if $v_2(t-a) - v_2(a) \equiv 1 \pmod{6}$ and $v_2(t-a) - v_2(a) > 1$ then $w_2(t) \equiv (t-a)_2 \pmod{4}$;
 - if $v_2(t-a) - v_2(a) \equiv 2 \pmod{6}$ then $w_2(t) \equiv (t-a)_2 \pmod{4}$;
 - if $v_2(t-a) - v_2(a) = 3$ then $w_2(t) = -1$ if and only if $(t-a)_2 \equiv 5 \pmod{8}$;
 - if $v_2(t-a) - v_2(a) \equiv 3 \pmod{6}$ and $v_2(t-a) - v_2(a) > 3$ then $w_2(t) = -1$;
 - if $v_2(t-a) - v_2(a) \equiv 4 \pmod{6}$ then $w_2(t) \equiv (t-a)_2 \pmod{4}$;
 - if $v_2(t-a) - v_2(a) \equiv 5 \pmod{6}$ then $w_2(t) = -1$.

DIMA - DIPARTIMENTO DI MATEMATICA, VIA DODECANESO, 35, 16146 GENOVA - ITALY

E-mail address: `bettin@dimma.unige.it`

DEPARTMENT OF MATHEMATICS AND STATISTICS CONCORDIA UNIVERSITY, 1455 DE MAISONNEUVE WEST MONTRÉAL, QUÉBEC CANADA H3G 1M8

E-mail address: `cdavid@mathstat.concordia.ca`

LABORATOIRE DE MATHÉMATIQUES DE BESANÇON, UNIV. BOURGOGNE FRANCHE-COMTÉ, CNRS UMR 6623, 16 ROUTE DE GRAY, 25030 BESANÇON CEDEX, FRANCE

E-mail address: `christophe.delaunay@univ-fcomte.fr`