Root number in integer parameter families of elliptic curves

Julie Desjardins

Received: 16 February 2021 / Accepted: 21 April 2021 / Published online: 28 May 2021
© Crown 2021

Abstract
In a previous article [7], the author proves that the value of the root number varies in a non-isotrivial family of elliptic curves indexed by one parameter \( t \) running through \( \mathbb{Q} \). However, a well-known example of Washington has root number \(-1\) for every fiber when \( t \) runs through \( \mathbb{Z} \). Such examples are rare since, as proven in this paper, the root number of the integer fibers varies for a large class of families of elliptic curves. This result depends on the squarefree conjecture and Chowla’s conjecture, and is unconditional in many cases.

Résumé
Dans un article précédent [7], l’autrice démontre que la valeur du signe varie parmi une famille non isotriviale de courbes elliptiques indexée par un paramètre rationnel \( t \). Cependant, un exemple bien connu de Washington a comme signe \(-1\) pour toute fibre lorsque l’on se restreint aux valeurs entières de \( t \). Pareils exemples sont rares: ce papier démontre en effet que le signe des fibres entières varie pour une large classe de familles de courbes elliptiques. Ce résultat dépend de la Conjecture du Crible sans Facteur Carré et de la Conjecture de Chowla, et est inconditionnel dans plusieurs cas.

Keywords elliptic curves · rank · root number

Mathematics Subject Classification 11G05 · 11G40

1 Introduction

A family of elliptic curves \( \mathcal{E} \) over a number field \( K \) (or equivalently an elliptic surface with base \( \mathbb{P}^1 \)) is the family given by a Weierstrass equation

\[
\mathcal{E} : Y^2 = X^3 - 27c_4(T)X + 54c_6(T),
\]

where \( c_4, c_6 \in \mathbb{Z}[T] \) are such that the discriminant \( \Delta_{\mathcal{E}}(t) = \Delta(t) = \frac{c_4(t)^2 - c_6(t)^3}{1728} \) is non-zero (except for finitely many values of \( t \)). We call the family isotrivial if every fiber is a twist of one another (i.e. if the function \( j : t \mapsto j(t) \) is constant), and non-isotrivial otherwise.
A family of elliptic curves $\mathcal{E}$ can as well be seen as an elliptic curve over $\mathbb{Q}(T)$, and so it makes sense to speak about the generic rank of $\mathcal{E}$, as well as the reduction of $\mathcal{E}$ at a place $v$ of $\mathbb{Q}(T)$, whose type is described by a Kodaira symbol. Let us define $\mathcal{R}$ to be the set of places of multiplicative reduction and $\mathcal{B}$ the set of bad places that are not of Kodaira type $I_0^\circ$. Each place of $\mathbb{Q}(T)$ is either $-\deg$, or is said to be finite, and in that case it is associated to an irreducible polynomial $P$ (that we can suppose with integer coefficients and primitive). Let us call insipid (an irreducible polynomial $P$ associated to) a place of type

- $I_0^\circ$
- $II, II^*, IV$ or $IV^*$, and

$$\mu_3 \subseteq \mathbb{Q}[T]/P(T),$$

where $\mu_3$ is the group of third root of unity;

- $III$ or $III^*$, and

$$\mu_4 \subseteq \mathbb{Q}[T]/P(T),$$

where $\mu_4$ is the group of fourth root of unity.

In this article, we are interested in the integer fibers of a family of elliptic curves, meaning the curves $\mathcal{E}_t := \mathcal{E}(t)$ such that $t \in \mathbb{Z}$, and in particular, we want to find more about the distribution of their rank. We will use a useful substitute called the root number $W(\mathcal{E}_t)$ that is easier to compute.

Given an elliptic curve $E$ over $\mathbb{Q}$, the root number of $E$ is the product of the local root numbers:

$$W(E) = \prod_{p \text{ place of } \mathbb{Q}} W_p(E),$$

where $W_p(E) \in \{\pm 1\}$ is defined in terms of the epsilon factors of the Weil-Deligne representations of $\mathbb{Q}_p$ and equals to $+1$ except for a finite number of $p$. For a more detailed definition of these local root numbers, we refer to [5] and [20], and for explicit formulas we use the work of Rohrlich [19], as well as (when $p \neq 2, 3$) the tables of Halberstadt [11] completed by Rizzo [18].

Let $L(E, s)$ be the associated $L$-function. Then by the modularity theorem, $L$ admits the following functional equation

$$A_E^{(2-s)/2} (2\pi)^{s-2} \Gamma(2-s) L(E, 2-s) = W(E) A_E^{s/2} (2\pi)^{-s} \Gamma(s) L(E, s)$$

where $W(E) \in \{-1, +1\}$, the sign of the functional equation, is equal to the root number of $E$. For a general number field $K$, the existence of such a functional equation is not guaranteed, so we rely only on the definition (1). This equivalent definition leads to the equality: $W(E) = (-1)^{r_\text{an}(E)}$, where the analytic rank is $r_\text{an}(E) = \text{ord}_{s=1}(L(E, s))$. By (a weaker version of) the Birch and Swinnerton-Dyer conjecture, we have

$$r_\text{an}(E) \equiv r(E) \mod 2,$$

where $r(E)$ is the geometric rank of $E$. This justifies the following statement known as the parity conjecture

$$W(E) = (-1)^{r(E)}.$$

Given $\mathcal{E}$ a family of elliptic curves over $\mathbb{Q}$ and $A \subseteq \mathbb{Q}$ (in particular $A = \mathbb{Z}$ or $\mathbb{Q}$), we consider the sets $W_+(\mathcal{E}, A)$ and $W_-(\mathcal{E}, A)$ given by

$$W_\pm(\mathcal{E}, A) = \{ t \in A : \mathcal{E}_t \text{ is an elliptic curve and } W(\mathcal{E}_t) = \pm 1 \}.$$
The author proves in [7] that for a non-isotrivial family of elliptic curves whose discriminant respects some analytic number theory conjectures\(^1\) true for low degree, we have
\[
\#W_\pm(\mathcal{E}, \mathbb{Q}) = \infty.
\]
Beforehand, Manduchi already proved Theorem 1.1 in the particular case where the family considered admits a place of multiplicative reduction [17], and Helfgott studied the average root number over \(\mathbb{Q}\) and \(\mathbb{Z}\) in the preprint [12].

### 1.1 Main results

In this paper, we prove analogues of the results of [7] (on the variation of the root number in families of elliptic curves in one parameter running through \(\mathbb{Q}\)) when restricted to integer fibers. We show the following theorem.

**Theorem 1.1** Let \(\mathcal{E}\) be a family of elliptic curves over \(\mathbb{Q}\). Suppose that there exists at least one irreducible primitive polynomial \(P_0(T) \in \mathbb{Z}[T]\) associated to either a place that is not insipid for \(\mathcal{E}\) or to a place of type \(I^*_0\) and \(\deg P_0\) is odd.

Suppose moreover that

(i) \(M_{\mathcal{E}} = \prod \mathcal{P}_v\) (where the product runs through the places of multiplicative reduction) respects Chowla’s conjecture (4.4) or \(M_{\mathcal{E}} = 1\);

(ii) \(B_{\mathcal{E}} = \prod \mathcal{P}_v\) (where the product runs through the non-insipid places) respects the squarefree conjecture (4.1).

Then the sets \(W_+(\mathcal{E}, \mathbb{Z})\) and \(W_-(\mathcal{E}, \mathbb{Z})\) are both infinite.

Chowla’s conjecture (stated further on) is known to hold for linear polynomials \(P \in \mathbb{Z}[T]\). This conjecture gives an estimation of the proportion of values \(P(t)\) with a given parity of number of prime factors. The Squarefree conjecture (also stated further on), is known to hold when every irreducible factor of \(\Delta_{\mathcal{E}}\) has degree at most 3. This conjecture gives an estimation of the proportion of values \(P(t)\) that are squarefree (or “almost squarefree”). Our result is unconditional in the following cases:

**Corollary 1.2** Let \(\mathcal{E}\) be a family of elliptic curves with at least one finite place that is not insipid, or is of type \(I^*_0\) associated to a polynomial of odd degree.

Suppose moreover that \(\deg M_{\mathcal{E}} \leq 1\) and that \(\deg P \leq 3\) for any non-insipid places. Then the sets \(W_+(\mathcal{E}, \mathbb{Z})\) and \(W_-(\mathcal{E}, \mathbb{Z})\) are both infinite.

The proof of Theorem 1.1 is based on a one variable analogue of the “Squarefree Liouville Sieve” developed by the author in a previous paper [7] where she uses it to prove the variation of the root number on the rational fibers of a non-isotrivial family of elliptic curves. This sieve was inspired by the various squarefree sieves obtained consecutively by Hooley [15], Gouvêa and Mazur [10], Rohrlich [19] and Varilly-Alvarado [21]. The use of those sieves for similar purpose was already present in [17] and in [21].

In the preprint [12], Helfgott gives formulas for the computation of the average root number of the rational fibers of a non-isotrivial family of elliptic curves, and proves that it is equal to 0 whenever there is a place of multiplicative reduction. In [2], Helfgott together with Conrad and Conrad state without proving, that the average root number without multiplicative reduction is strictly contained between \(-1\) and \(1\) (the proof of this fact appears though in

\(^1\) Those conjectures (Chowla’s conjecture and the squarefree conjecture) are assumed in their homogeneous form in the main result of [7].
the author’s Ph.D dissertation). The average root number on the integer fibers of a family of elliptic curves with coefficients of small degrees are also discussed in [1] and [4].

The well-known Washington’s family

\[
\mathcal{V}: y^2 = x^3 + Tx^2 - (T + 3)x + 1
\]

introduced in [22] has the properties that

- ([18]) for all \( t \in \mathbb{Z} \), one has \( W(\mathcal{V}_t) = -1 \) (i.e. \( W_+ (\mathcal{V}, \mathbb{Z}) = \emptyset \));
- ([9]) it is proven numerically up to \( t < 1000 \) that the rank of \( \mathcal{V}_t \) is 1.

Of course, this example with constant root number on the integer fibers does not satisfy the hypothesis of our theorem - indeed the only finite place \( v \) where \( \mathcal{V} \) has bad reduction is insipid: it has type \( \text{II} \) and \( P_v(T) = T^2 + 3T + 9 \) is such that \( \mu_3 \subseteq \mathbb{Q}[T]/P_v(T) \) (by Remark 2).

### 1.2 Outline of the paper

In Sect. 2, we decompose the root number into contributions corresponding to the generic places. More precisely, Theorem 2.1 allows to write the root number function \( \mathbb{Z} \to \{ \pm 1 \} \) in the form

\[
\lambda(M_E (t)) \cdot \prod_{p|\delta} W_p(\mathcal{E}_t) \prod_{p \not| l_0,l_0^*} \mathcal{W}_p(u,v),
\]

where

- \( \delta \in \mathbb{N} \) depends on the coefficients of the Weierstrass equation of \( \mathcal{E} \),
- for an integer \( n \), \( \lambda(n) = (-1)^{\# \text{prime divisors of } n} \) is the Liouville function,
- \( \mathcal{W}_P \) depends on the type of reduction at an irreducible polynomial \( P \) and can be written as \( \mathcal{W}_P = g_P \cdot h_P \) for some functions \( g_P, h_P \).

In Sect. 3, we study the variation of the different components in this decomposition. In Sect. 4, we present the squarefree conjecture and Chowla’s conjecture, and we combine those conjectures to create the one variable version of the “Squarefree-Liouville” Sieve (Corollary 4.8) that we use in the proof of Theorem 1.1 in Sect. 5.

Many results of this paper are consequences (or “simply obtained 1-variable versions”) of results appearing in [7]. Here is a conversion table for the interested reader:

- Theorem 2.1 comes from [7, Theorem 3.4.]
- Proposition 3.1 comes from [7, Proposition 4.1.]
- Lemma 3.3 and Lemma 3.4 come respectively from [7, Lemma 4.2 and Lemma 4.3].
- Theorem 4.6 comes from [7, Theorem 2.9] and appeared originally in [6, Théorème 1.3.8]

Lemma 3.2, Proposition 3.6, 3.7 and 3.8 are new results. Observe moreover that, although Theorem 1.1 was proven in the special case where there is a place of multiplicative reduction by Manduchi in [17, Theorem 2], the proof of the general case in this article does not restrict to hers.
2 A formula for the global root number

Let $\mathcal{E}$ be the family of elliptic curves over $\mathbb{Q}$ with discriminant $\Delta_{\mathcal{E}}(T)$ described by the minimal Weierstrass equation

$$Y^2 = X^3 - 27c_4(T)X - 54c_6(T).$$

Define the integer:

$$\delta = 2 \cdot 3 \cdot n_4 \cdot n_6 \cdot n_\Delta \prod_{P, P' \mid \Delta_{\mathcal{E}}, P \neq P'} \text{Res}(P, P').$$

(2)

where $P, P'$ run through polynomials associated to generic places of bad reduction and $n_4, n_6$ and $n_\Delta$ are the numerators of the contents of the polynomials $c_4(T), c_6(T)$ and $\Delta_{\mathcal{E}}(T)$.

Moreover, we use from now on the following modified Jacobi symbol:

**Definition 1** For any integer $n \in \mathbb{Z}$ and prime number $p$, let $n_{(p)}$ denote the integer such that $n = p^{\nu_p(n)}n_{(p)}$.

For each pair of integers $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ and even integer $\delta$,

$$\left(\frac{a}{b}\right)_\delta = \prod_{p \nmid \delta} \left(\frac{a_{(p)}}{p}\right)^{v_p(b)}$$

(3)

where the product runs through the prime numbers $p \nmid \delta$ and $\left(\frac{a}{p}\right)$ is the Legendre symbol.

If $a, b, \delta$ are two-by-two coprime, then the symbol $(\frac{a}{p})_\delta$ is the classical Jacobi symbol.

We use moreover the Liouville function defined as follows:

**Definition 2** For a non-zero integer $n = \prod_p p^{v_p(n)}$, we denote by $\Omega(n) = \sum_p v_p(n)$ the number of its prime factors and we define Liouville’s function by the formula

$$\lambda(n) = (-1)^{\Omega(n)}.$$

2.1 Decomposition of the root number according to the generic places

We recall here (the one-variable version of) [7, Theorem 3.4.] that splits the formula of the root number of an integer fiber into contributions of places of bad reduction according to their Kodaira type. Those kind of expression can already be found in Helfgott’s preprint [12].

**Theorem 2.1** Let $\mathcal{E}$ be a family of elliptic curves over $\mathbb{Q}$. Let $\delta$ be defined as in (2). We recall that $M_{\mathcal{E}}$ is the product of the irreducible primitive $P \in \mathbb{Z}[T]$ associated to the places of multiplicative reduction of $\mathcal{E}$.

Then, the root number of $\mathcal{E}_t, t \in \mathbb{Z}$, can be written as

$$W(\mathcal{E}_t) = \lambda(M_{\mathcal{E}}(t)) \cdot \prod_{P \mid \delta} W_p(\mathcal{E}_t) \cdot \prod_{P \mid \Delta_{\mathcal{E}}} h_p(t)g_p(t).$$

The functions $h_p$ are given in Table 1 and

$$g_p(t) = \begin{cases} \left(\frac{\mathcal{E}_{P(t)}}{P(t)}\right)_\delta & \text{if } \mathcal{E} \text{ has additive reduction at } P \\ \left(\frac{-c_6(t)}{P(t)}\right)_\delta \left(\prod_{p \mid \delta} (-1)^{v_p(P(t))}\right) & \text{if } \mathcal{E} \text{ has multiplicative reduction at } P, \end{cases}$$
Table 1 Corrective functions $h_P$ of Theorem 2.1

| Type     | $h_P(t)$ |
|----------|----------|
| $I_0$    | 1        |
| $I_0^*$  | 1        |
| $II, II^*$ | $\prod_{p|\delta \atop p^2 \nmid P(t)} \left( \frac{-3}{p} \right) v_p(P(t)) \equiv 2, 4 \mod 6 +1$ otherwise. |
| $III, III^*$ | $\prod_{p|\delta \atop p^2 \nmid P(t)} \left( \frac{-1}{p} \right) v_p(P(t)) \equiv 2 \mod 4 +1$ otherwise. |
| $IV, IV^*$ | $\prod_{p|\delta \atop p^2 \nmid P(t)} \left( \frac{-3}{p} \right) v_p(P(t)) \equiv 2, 3, 4 \mod 6 +1$ otherwise. |
| $I_m^*(m \geq 1)$ | $\prod_{p|\delta \atop p^2 \nmid P(t)} \left( \frac{-c_6(t)(p)}{p} \right)^{v_p(P(t))-1}$ |
| $I_m (m \geq 1)$ | $\prod_{p|\delta \atop p^2 \nmid P(t)} \left( \frac{-c_6(t)(p)}{p} \right)^{v_p(P(t))-1}$ |

where $()_\delta$ is the modified Jacobi symbol of Definition 1 and

$$\varepsilon_P = \begin{cases} 
-1 & \text{if the type is } II, II^*, I_0^* \text{ or } I_m^*(m \geq 1) \\
-2 & \text{if the type is } III \text{ or } III^* \\
-3 & \text{if the type is } IV \text{ or } IV^*.
\end{cases}$$

Proof The details of the proof can be found in [7] where this formula is given for a rational fiber $\mathcal{E}_t, t \in \mathbb{Q}$. The general idea is the following. The root number can be expressed as

$$W(\mathcal{E}_t) = -\prod_{p|\delta} W_p(\mathcal{E}_t) \prod_{P|\Delta_\mathcal{E}} \mathcal{W}_P(t),$$

where for each $P$ primitive factor of $\Delta_\mathcal{E}$:

$$\mathcal{W}_P(t) = \prod_{p|\delta: p \nmid P(t)} W_p(\mathcal{E}_t).$$

Observe that in our case (with $t \in \mathbb{Z}$) there is no contribution to the root number of integer fibers coming from the infinite place $-\deg$.

Now, by the monodromy of the reduction type, each of the factors $W_p(\mathcal{E}_t)$ depends only on the type of $\mathcal{E}_t$ at $P$ and of $n = v_p(P(t))$. See Table 2 for a precise description of the changes in the types. This table can easily be deduced from Tate’s algorithm and appeared originally as [7, Lemma 3.3].

In particular if $n = 1$, then the type of reduction of $\mathcal{E}_t$ is the same as the type of $\mathcal{E}$ at $P$. We have thus in this case:

$$W_p(\mathcal{E}_t) = \begin{cases} 
\left( \frac{-\varepsilon_P}{p} \right) & \text{if } \mathcal{E} \text{ has additive reduction at } P \\
\left( \frac{-c_6(t)}{p} \right) & \text{if } \mathcal{E} \text{ has multiplicative reduction at } P.
\end{cases}$$
However, when \( n \geq 2 \), the type of reduction of \( \mathcal{E}_T \) is likely to change. For this reason, we introduce a corrective function, denoted by \( h_P \) and equal to \( \frac{g_P}{W_p} \) so we can write:

\[
W_p(t) = h_P(t) \left\{ \begin{array}{ll}
-\varepsilon_P & \text{if } \mathcal{E}_t \text{ has additive multiplication at } P \\
-\Omega(P(t)) & \text{if } \mathcal{E}_t \text{ has multiplicative multiplication at } P,
\end{array} \right.
\]

where \( \Omega(n) \) is the number of prime factors of the integer \( n \) and \( (\cdot)_\delta \) is the quadratic symbol defined in Definition 1.

To complete the proof, we need to prove that the functions in Table 1 are indeed the corrective functions \( h_P \). This is done case by case according to the Kodaira type of the reduction of \( \mathcal{E}_T \) at \( P \), using the monodromy given by Table 1 [7, Theorem 3.4].

3 Variation of the different components of the root number

3.1 The function \( \prod_{p \mid \delta} W_p(\mathcal{E}_t) \prod_{p \not\mid \delta} g_p(t) \)

As shown in [7, Prop. 4.1], the “first half” of the formula for the root number described in the previous section respects a certain periodicity:

**Proposition 3.1** Let \( \mathcal{E} \) be a family of elliptic curves over \( \mathbb{Q} \). Let \( \delta \) be the integer defined at equation 2.

Then, there exist an integer \( N_{\mathcal{E}} \in \mathbb{N}^* \) and a non-zero polynomial \( R_{\mathcal{E}} \in \mathbb{Z}[T] \) such that the function \( \varphi_{\mathcal{E}} : \mathbb{Z} \to \{-1, +1\} \) defined as

\[
t \mapsto \varphi_{\mathcal{E}}(t) := \prod_{p \mid \delta} W_p(\mathcal{E}_t) \prod_{p \not\mid \delta} g_p(t)
\]

has the property that \( \varphi_{\mathcal{E}}(t_1) = \varphi_{\mathcal{E}}(t_2) \) for every \( t_1, t_2 \in \mathbb{Z} \) such that

1. \( t_1 \equiv t_2 \mod N_{\mathcal{E}} \) and
2. for every irreducible factor \( R_i \) of \( R_{\mathcal{E}} \), one has that \( R_i(t_1) \) and \( R_i(t_2) \) have the same sign \( \epsilon_i \).

**Remark 1** Given these integer \( N_{\mathcal{E}} \) and polynomial \( R_{\mathcal{E}} \), assuming (1) and replacing Hypothesis (2) by:

2' for every irreducible factor \( R_i \) of \( R_{\mathcal{E}} \), one has that \( R_i(t_1) \) and \( R_i(t_2) \) have the same sign \( \epsilon_i \in \{-1, 1\} \) except for a given \( i_o \) such that \( R_{i_o}(t_1) \) and \( R_{i_o}(t_2) \) have opposite sign, then we get that \( \varphi_{\mathcal{E}}(t_1) = -\varphi_{\mathcal{E}}(t_2) \).

**Proof** For a detailed proof, we refer to [7, Prop. 4.1]. It is based on the following facts:

1. There exists an integer \( \alpha_p \) (that we can suppose minimal) such that the local root numbers at \( p \mid \delta \) of the fibers are such that \( W_p(\mathcal{E}_t) = W_p(\mathcal{E}_{t_2}) \) whenever \( t_1, t_2 \in \mathbb{Z} \) are such that \( t_1 \equiv t_2 \mod p^{\alpha_p} \).
2. The modified Jacobi symbol respects the property that for any polynomials \( g \) and \( f \) there exist an integer \( N_P \) and a polynomial \( R_P \) such that \( \left( \frac{f(t)}{g(t)} \right)_\delta \) depends only on the congruence class \( t \mod N_P \) and of the sign of the value \( R_P(t) \).
| Type of $E_T$ at $P(T)$ | $n = v_p(P(u, v))$ | Type of $E_I$ at $p$ | Type of $E_T$ at $P(T)$ | $n = v_p(P(u, v))$ | Type of $E_I$ at $p$ |
|------------------------|---------------------|----------------------|------------------------|---------------------|----------------------|
| $I_m$                  | $n \geq 1$          | $I_m$                | $I_m^n$                | 0 mod 2             | $I_{mn}$             |
| $II$                   | 0 mod 6             | $I_0$                | $II^*$                 | 0 mod 6             | $I_0$                |
|                        | 1 mod 6             | $II$                 | $I_0$                  | 1 mod 6             | $II^*$               |
|                        | 2 mod 6             | $IV$                 | $I_0^*$                | 2 mod 6             | $IV^*$               |
|                        | 3 mod 6             | $I_0^*$              | $III^*$                | 3 mod 6             | $I_0^*$              |
|                        | 4 mod 6             | $IV^*$               | $I_0$                  | 4 mod 6             | $IV$                 |
|                        | 5 mod 6             | $II^*$               | $I_0$                  | 5 mod 6             | $II$                 |
| $III$                  | 0 mod 2             | $I_0$                | $II^*$                 | 0 mod 4             | $I_0$                |
|                        | 1 mod 4             | $III$                | $I_0$                  | 1 mod 4             | $III^*$              |
|                        | 2 mod 4             | $I_0^*$              | $III^*$                | 2 mod 4             | $I_0^*$              |
|                        | 3 mod 4             | $III^*$              | $I_0$                  | 3 mod 4             | $III$                |
| $IV$                   | 0 mod 3             | $I_0$                | $IV^*$                 | 0 mod 3             | $I_0$                |
|                        | 1 mod 3             | $IV$                 | $I_0$                  | 1 mod 3             | $IV^*$               |
|                        | 2 mod 3             | $IV^*$               | $I_0$                  | 2 mod 3             | $IV$                 |
| $I_0^*$                | 0 mod 2             | $I_0$                | $I_0$                  | $n \geq 0$          | $I_0$                |
|                        | 1 mod 2             | $I_0^*$              | $I_0$                  |                      |                      |
We have for \( \left( \frac{\epsilon}{P(t)} \right)_\delta \), that \( R_P = P \), and if for instance \( \epsilon = -1 \), then \( N_P = 4 \).

For general \( f, g \) that we suppose such that \( \deg g \geq \deg f \) (otherwise, simply exchange \( f \) and \( g \)), we have \( R_P = f \cdot g \cdot (g - x^{\deg f - \deg g}) \cdots \) and we add to this product a finite number of factors \( g_i, i = 1, \cdots, \) of decreasing degree, defined by putting \( g_{-1} = f, g_0 = (g - x^{\deg g - \deg f}) \) and iterating the following: suppose \( g_i = (g_i - x^{\deg g_i - \deg g_{i-1}} g_{i-1}) \) is such that \( \deg g_i \leq \deg g_{i-1} \) (otherwise interchange their role), put \( g_{i+1} = g_{i-1} - x^{\deg g_{i-1} - \deg g_i} g_i \).

Repeat until \( \deg g_{i+1} = 0 \).

Therefore, we have that
\[
N_\epsilon = 24 \prod_{p \mid \delta} p^{\alpha_p} \prod_{P \in \mathcal{A}} N_P,
\]
and
\[
R_\epsilon = \prod_{P \in \mathcal{A}} R_P.
\]

\( \square \)

### 3.2 The function \( h_P \)

**Lemma 3.2** Let \( \mathcal{E} \) be a family of elliptic curves over \( \mathbb{Q} \) with a place of bad reduction associated to the primitive irreducible polynomial \( P \).

Suppose that there exist \( t_1, t_2 \in \mathbb{Z} \) such that we have

1. \( P(t_1) = c^2l \), where \( l \) is squarefree and \( \gcd(c, l) = 1 \),
2. \( P(t_2) = (c_0q_0)^2\eta, \) where \( \eta \) is squarefree, \( \gcd(c, \eta) = 1 \), for a certain integer \( q_0 \),

for some \( c \in \mathbb{Z} \).

A. Suppose that \( q_0 \neq 2, 3 \) is a prime number such that

i) \( c_0(t_2)(q_0) \equiv 1 \mod q_0 \) if the reduction of \( \mathcal{E} \) at \( P \) is additive or potentially multiplicative,

ii) \( \left( -\frac{1}{q_0} \right) = -1 \) if the reduction of \( \mathcal{E} \) at \( P \) is \( II, II^*, IV \) or \( IV^* \),

iii) \( \left( -\frac{1}{q_0} \right) = -1 \) if the reduction of \( \mathcal{E} \) at \( P \) is \( III \) or \( III^* \),

then \( h_P(t_1) = -h_P(t_2) \);

B. Suppose that \( q_0 = 1 \), then \( h_P(t_1) = h_P(t_2) \).

**Proof** Let \( P \) be a 1-variable irreducible polynomial associated to a place of \( \mathcal{E} \) that is neither of type \( I_0 \) nor of type \( I_0^* \). The function \( h_P \) is a product over the square factors of \( P(t) \) not dividing \( \delta \). By hypothesis 1 and 2, the square factors of \( P(t_1) \) and \( P(t_2) \) are the same except for \( q_0 \). Hence,
\[
h_P(t_1) = \lambda_P h_P(t_2),
\]
where \( \lambda_P \) depends on the type of reduction of \( \mathcal{E} \) at \( P \).

- Suppose the reduction at \( P \) has type \( II, II^*, IV \) or \( IV^* \). Then \( \lambda_P = \left( -\frac{3}{p} \right) \) and by hypothesis, it is equal to \( -1 \). Hence \( h_P(t_1) = -h_P(t_2) \).
- Suppose the reduction at \( P \) has type \( III, III^* \). Then \( \lambda_P = \left( -\frac{1}{p} \right) \) and by hypothesis, it is equal to \( -1 \). Hence \( h_P(t_1) = -h_P(t_2) \).
Suppose the reduction at \( P \) has type \( I_n^* \) or \( I_m \) \((m \geq 1)\). Then \( \lambda_P = \left( -\frac{c_6(t_1)(p)}{p} \right) \).

We put \( \alpha := P(t_1) = c^2I \) and \( \beta := P(t_2) = c^2q_0^2 \eta \). Then by Theorem 2.1, one has

\[
h_P(t_2) = \prod_{p|\delta; p|q_0} \left\{\begin{array}{ll}
\left( -\frac{-c_6(t_2)(p)}{p} \right) & \text{if } 2\nu_p(q_0c) \equiv 2, 4 \mod 6 \\
+1 & \text{otherwise.}
\end{array}\right.
\]

\[
= -\left( -\frac{c_6(t_1)(q_0)}{q_0} \right) \prod_{p|\delta; p|c} \left\{\begin{array}{ll}
\left( -\frac{-c_6(t_1)(p)}{p} \right) & \text{if } \nu_p(c) \text{ is even,} \\
+1 & \text{otherwise.}
\end{array}\right.
\]

\[
= -\left( -\frac{c_6(t_1)(q_0)}{q_0} \right) \cdot h_P(t_1).
\]

By assumption on \( q_0 \), one has \( q_0^{-2} \frac{-c_6(t_1)}{P(t_1)^2} \equiv 1 \mod q_0 \). If we put \( P(t_1) = q_0^2 \mu \) where \( \mu \) is an integer coprime to \( q_0 \), one has \( q_0^{-6}(-c_6(t_1)) \equiv \mu^2 \mod q_0 \). Thus, one has

\[
\left( -\frac{-c_6(t_1)(q_0)}{q_0} \right) = +1.
\]

Thus we have the equality

\[
h_P(t_1) = -h_P(t_2).
\]

- If \( q_0 = 1 \), then the products in \( h_P(t_1) \) and \( h_P(t_2) \) have exactly the same factors. Thus \( h_P(t_1) = h_P(t_2) \).

\[\square\]

Be aware however, that in certain cases a number \( q_0 \) with properties A ii) or iii) does not exist - this is the subject of the next subsection.

### 3.2.1 Existence of \( q_0 \)

If the reduction at a polynomial \( P \) is such that

- \( P \) has type \( I^*_0 \) then the theorem does not apply. Indeed, \( h_P(t) = +1 \) for all \( t \in \mathbb{Z} \).
- \( P \) has type \( II^*, IV, IV^* \) then we use the following Lemma.

**Lemma 3.3** Let \( P \in \mathbb{Z}[T] \) be a polynomial associated to a place of type \( II, II^*, IV \) or \( IV^* \). We assume that

\[
\mu_3 \subseteq \mathbb{Q}[T]/P(T),
\]

where \( \mu_3 \) is the group of third roots of unity.

Then for all \( t \in \mathbb{Z} \) one has \( h_P(t) = +1 \).

**Proof** Let \( P(T) \in \mathbb{Z}[T] \) be an irreducible polynomial and let \( K = \mathbb{Q}[T]/P(T) \). Suppose that \( \mathbb{Q}(\mu_3) \subseteq K \). In [8, Proposition 2.2], it is proven that there exist \( A, B \in \mathbb{Z}[T] \) such that \( P = A^2 + 3B^2 \) and this implies that for every \( t \in \mathbb{Z} \), if \( p \mid P(t) \) for some prime number, then \( p \equiv 1 \mod 3 \). This means that any \( p \) dividing a value of \( P \) is such that \( \left( \frac{-3}{p} \right) = +1 \).

We have:

\[
h_P(t) = \prod_{p|\delta; p^2 \mid P(t)} \left\{\begin{array}{ll}
\left( -\frac{-3}{p} \right) & \text{if } \nu_p(P(t)) \equiv 2, 4 \mod 6 \\
+1 & \text{otherwise}
\end{array}\right.
\]
Remark 2 One can easily give examples of polynomials $P \in \mathbb{Z}[T]$ satisfying the hypothesis $\mu_3 \subseteq \mathbb{Q}[T]/P_i(T)$ for every irreducible factors $P_i$ of $P$. We have in particular those of the form

$$P(T) = 3A(T)^2 + B(T)^2,$$

where $A(T), B(T) \in \mathbb{Z}[T]^*$ are coprime. This polynomial is not necessarily irreducible in general, but for every irreducible factor $P_i$ and the corresponding field $K_i = \mathbb{Q}[T]/(P_i(T)) = \mathbb{Q}(\alpha_i)$ where $\alpha_i$ is a root of $P_i$, one has $3A(\alpha_i)^2 + B(\alpha_i)^2 = 0$, thus $-3 = (B(\alpha_i)A(\alpha_i)^{-1})^2$ and this proves that $\mu_3 \subseteq K_i$.

If a polynomial $P$ does not satisfy the property (4), then there exist a prime number $p_o$ and an integer $t$ such that $p_o^2 | P(t)$ and \( \left( \frac{-3}{p_o} \right) = -1 \).

• $P$ has type $III$, $III^*$

Lemma 3.4 Let $P \in \mathbb{Z}[T]$ be an irreducible polynomial associated to a place of type $II$, $II^*$, $IV$ or $IV^*$. Assume that

$$\mu_4 \subseteq \mathbb{Q}[T]/P(T),$$

where $\mu_4$ is the group of the fourth roots of unity.

Then for all $t \in \mathbb{Z}$, one has $h_P(t) = +1$.

Proof The proof is similar to Lemma 3.3. □

Remark 3 One can easily give examples of polynomials satisfying the hypothesis $\mu_4 \subseteq \mathbb{Q}[T]/(P_i(T))$ for every factor $P_i$; in particular those of the form

$$P(T) = A(T)^2 + B(T)^2,$$

where $A(T), B(T) \in \mathbb{Z}[T]^*$ are coprime.

If a polynomial $P$ does not satisfy the property (5), then there exist a prime number $p_o$ and an integer $t$ such that $p_o^2 | P(t)$ and \( \left( \frac{-1}{p_o} \right) = -1 \).

• The reduction at $P$ is multiplicative or potentially multiplicative

Now, we present a general result on values of polynomials which will allow us to prove the existence of $t_1, t_2$ and $q_0$ for which the hypothesis A i) of Lemma 3.2 is satisfied.

Lemma 3.5 [17, Lemma 2.3] Let $Q(T)$ and $P(T) \in \mathbb{Z}[T]$ be such that $Q(T)$ is non-constant. Let $\text{Res}(P, Q)$ be the resultant of $P$ and of $Q$, and let $\Delta_Q$ be the discriminant of $Q$. Suppose $\text{Res}(P, Q)$ and $\Delta_Q$ are non-zero. Let $\mathcal{P}_0$ be a finite set of prime numbers.

Then there exist a prime number $p_0 \notin \mathcal{P}_0$ and $n$ a positive integer such that $p_0^2 | Q(n)$ and $p_0^{-2}P(n)Q(n) \equiv 1 \mod p_0$. In particular, $p_0^2 || Q(n)$ and $p_0 | P(n)$.

We refer to [17] for a proof of this elementary lemma. Observe that there is no need of the Squarefree conjecture in Lemma 3.5.

Thus, for any family of elliptic curves $\mathcal{E}$ with a place of type $I_m$ or $I_m^*$ ($m \geq 1$) whose associated polynomial is $Q$, put $P = -\frac{c_6(t)}{Q(t)^3}$. Manduchi’s lemma on $P$ and $Q$ guarantees the existence of a $p_0$ such that $p_0^{-2}P(t)Q(t) \equiv c_6(t) \cdot \square \mod p_0 \equiv 1 \mod p_0$, and thus \( \left( \frac{-c_6(t)}{p_0} \right) = +1 \).
3.3 Variation of the global root number

**Proposition 3.6** Let \( \mathcal{E} \) be a family of elliptic curves. Let \( N_{\mathcal{E}} \) be the integer and \( R_{\mathcal{E}}(T) \) be the polynomial given by Proposition 3.1. Let \( t_1, t_2 \in \mathbb{Z} \), and suppose they satisfy the following properties.

1. We have \( t_1 \equiv t_2 \mod N_{\mathcal{E}} \), a non-zero congruence class.
2. We have \( \lambda(M(t_1)) = \lambda(M(t_2)) \).
3. For every primitive factor \( R_i \) of \( R_{\mathcal{E}} \) and \( j = 1, 2 \) one has \( R_i(t_j) > 0 \).
4. For a certain \( Q_0 \) and some \( c \in \mathbb{Z} \), one has
   
   \[ Q_0(t_1) = c^2 l \text{ and } Q_0(t_2) = c^2 l' Q, \]
   
   where \( l, l' \) are squarefree integers coprime to \( N_{\mathcal{E}} \), and \( Q \in \mathbb{Z} \).

Then, we have

\[ W(\mathcal{E}_{t_1}) = -W(\mathcal{E}_{t_2}). \]

**Proof** By Theorem 2.1, we have:

\[ W(\mathcal{E}_{t_1}) = \lambda(M_{\mathcal{E}}(t_1)) \prod_{p \mid \delta} W_p(\mathcal{E}_{t_1}) \prod_{p \in \mathbb{M}} g_p(t_1) \prod_{p \in \mathbb{B}} h_p(t_1). \]

By Hypotheses (1), (2) and (3), we have

\[ W(\mathcal{E}_{t_1}) = \lambda(M_{\mathcal{E}}(t_2)) \prod_{p \mid \delta} W_p(\mathcal{E}_{t_2}) \prod_{p \in \mathbb{M}} g_p(t_2) \prod_{p \in \mathbb{B}} h_p(t_1). \]

The rest of the proof is based essentially on Propositions 3.6 or 3.7. By hypotheses (4), \( h_{Q_0}(t_1) = -h_{Q_0}(t_2) \) and finally by Hypotheses (5), for every \( Q \neq Q_0 \) of bad reduction, \( h_Q(t_1) = h_Q(t_2) \). Hence

\[ W(\mathcal{E}_{t_1}) = -\lambda(M_{\mathcal{E}}(t_2)) \prod_{p \mid \delta} W_p(\mathcal{E}_{t_2}) \prod_{p \in \mathbb{M}} g_p(t_2) \prod_{p \in \mathbb{B}} h_p(t_2) \]

\[ = -W(\mathcal{E}_{t_2}) \]

\( \square \)

Very similarly, we have:

**Proposition 3.7** Do the same hypotheses (1) to (3) as in Proposition 3.6, and suppose additionally that for a certain \( Q_0 \) and some \( c \in \mathbb{Z} \), one have \( Q_0(t_1) = c^2 l \) and \( Q_0(t_2) = c^2 l'^2 \) where \( l, l' \) are squarefree integers coprime to \( N_{\mathcal{E}} \). Then

\[ W(\mathcal{E}_{t_1}) = W(\mathcal{E}_{t_2}). \]

There is also another approach to making the root number vary:
Proposition 3.8 Let $E$ be a family of elliptic curves over $\mathbb{Q}$ with no place $I_m$ nor $I_m^\ast$. Let $N_E$ be the integer and $R_E(T)$ be the polynomial given by Proposition 3.1. Let $t_1, t_2 \in \mathbb{Z}$. Suppose they satisfy the following properties.

1. We have $t_1 \equiv t_2 \mod N_E$, a non-zero congruence class.
2. For a fixed primitive factor $R_i$ of $R_E$ one has $R_i(t_1) > 0$ and $R_i(t_2) < 0$.
3. For every other primitive factor $R_i$ of $R_E$ one has $R_i(t_1) > 0$ and $R_i(t_2) > 0$.
4. For every place of bad (but not insipid) reduction, one has $Q(t_1) = c_0^2 l_Q$ and $Q(t_2) = c_0^2 l_Q'$, where $l_Q$ and $l_Q'$ are squarefree integers coprime to $N_E$.

Then, we have $W(E(t_1)) = -W(E(t_2))$.

Proof The crux of the proof is the function $\varphi_E : \mathbb{Z} \to \{-1, +1\}$ defined in Proposition 3.1 as

$$t \mapsto \varphi_E(t) := \prod_{p \mid \delta} W_p(E(t)) \prod_{P \in \mathfrak{B}} g_P(t).$$

Let $R_E = \prod_i R_i$ be the polynomial given by Proposition 3.1. For a fixed primitive factor $R_i$ of $R_E$ one has $R_i(t_1) > 0$ and $R_i(t_2) < 0$. For every other primitive factor $R_i$ of $R_E$ one has $R_i(t_1) > 0$ and $R_i(t_2) > 0$. Then by construction of $R$, we have $\varphi_E(t_1) = -\varphi_E(t_2)$.

The other parts of the root number formula do not vary by Proposition 3.7. Hence $W(E(t_1)) = -W(E(t_2))$. 

\[\square\]

4 Analytical conjectures and sieves

In this section, we recall the two analytical number theory conjectures applied on a polynomial $f(T) \in \mathbb{Z}[T]$ that appear in Theorem 1.1:

1. Chowla’s conjecture,
2. Squarefree conjecture.

They respectively correspond to asymptotic approximations of the proportion of the values of $f(t)$ with the following properties:

1. a certain parity of the number of prime factors,
2. a fixed square part.

Notice that we recall here exclusively the statements in the case where $f(t)$ is one-variable polynomial since it is sufficient for our purpose, and that for details of the 2-variable homogenous case, we refer the interested reader to our previous paper [7, Section 2].

We will make a certain number of assumptions on the polynomial $f(T)$ throughout this section: first, it is natural to assume that $f$ is primitive (i.e. that its content is equal to 1), and second, that $f$ is squarefree (i.e. that there is no polynomial $f_0$ such that $f_0^2 \mid f$), which is the same as supposing that its discriminant $D_f$ is non-zero.

We denote by $|\cdot|$ the usual absolute value on $\mathbb{R}$ or the max norm on $\mathbb{R}^2$. Let $A = a + N\mathbb{Z}$ (where $N \neq 0$) be an arithmetic progression. We also introduce the notations

$$\mathbb{Z}(X) = \{t \in \mathbb{Z} \mid |t| \leq X\}, \quad \mathcal{A}(X) := \{t \in A \mid |t| \leq X\} \quad \text{and} \quad A(X) := \mathbb{Z}(X),$$

so that $A(X)$ is roughly proportional to $X$. More precisely, we have $A(X) \sim \frac{X}{N}$. 

\[\square\]
4.1 Squarefree conjecture

This conjecture estimates the proportion of squarefree values of a polynomial in an arithmetic progression.

Notations. Put \( \delta_f := \gcd \{ f(t) \mid t \in \mathbb{Z} \} \), then let \( d_f \) be the smallest integer such that \( \delta_f / d_f \) is squarefree. Write \( d_f = \prod p^{v_p} \). We denote by \( t_f(p) \) the number of solutions modulo \( p^{2+v_p} \) of \( f(t)d_f^{-1} \equiv 0 \mod p^2 \), or \( f(t) \equiv 0 \mod p^{2+v_p} \) and we put

\[
C_f := \prod_p \left( 1 - \frac{t_f(p)}{p^{2+v_p}} \right).
\]

Note that the product defining \( C_f \) is absolutely convergent since \( t_f(p) = O(1) \).

To study the “almost" squarefree values we proceed as follows. Let \( \phi : \mathbb{Z} \to \mathcal{A} \) the bijection with \( \phi(t) = a + Nt \). We put \( g := f \circ \phi \), \( d_{f,\mathcal{A}} := d_g = \prod p^{\mu_p} \), and define \( t_{f,\mathcal{A}}(p) \) as the number of solutions modulo \( p^{2+\mu_p} \) of \( g(t)d_{f,\mathcal{A}}^{-1} \equiv 0 \mod p^{2+\mu_p} \),

\[
C_{f,\mathcal{A}} := \frac{1}{N} \prod_{p|N} \left( 1 - \frac{t_{f,\mathcal{A}}(p)}{p^{2+\mu_p}} \right)
\]

and let \( Sq_{f,\mathcal{A}}(X) \) to be the number of elements \( t \in \mathcal{A}(X) \) such that \( f(t) \) is squarefree. We can write the Squarefree conjecture in the following form:

**Conjecture 4.1** (Squarefree Conjecture on arithmetic progressions)

\[
Sq_{f,\mathcal{A}}(X) = C_{f,\mathcal{A}}X + o(X)
\]

It is known to hold in the following cases:

**Theorem 4.2** (Hooley [15]) Let \( f \in \mathbb{Z}[T] \) be a primitive squarefree polynomial with integer coefficients in one variable. Suppose that every irreducible factor of \( f \) has degree at most 3. Then \( f \) verifies the Squarefree conjecture on arithmetic progressions.

It leads to the following squarefree sieve\(^3\):

**Corollary 4.3** Let \( f(T) \in \mathbb{Z}[T] \) be a polynomial such that no square of a non-unit in \( \mathbb{Z}[T] \) divides \( f(T) \), and such that every factor of \( f \) has degree \( \leq 3 \).

Fix

- a sequence \( S = (p_1, \ldots, p_s) \) of distinct prime numbers and
- a sequence \( T = (t_1, \ldots, t_s) \) of non-negative integers.

Let \( N \) be an integer such that \( p_1^{t_1+1} \cdots p_s^{t_s+1} | N \) and that \( p^2 | N \) for all primes \( p \leq (\deg f) \).

Suppose that there exists an integer \( a \) such that

1. \( f(a) \not\equiv 0 \mod p^2 \), whenever \( p | N \) and \( p \neq p_i \) for any \( i \),
2. and such that \( v_{p_i}(f(a)) = t_i \) for every \( i = 1, \ldots, s \).

Then there are infinitely many integers \( t \) such that

1. \( t \equiv a \mod N \),
2. and such that \( f(t) = p_1^{t_1} \cdots p_s^{t_s} \cdot l \), where \( l \) is squarefree and \( v_{p_i}(l) = 0 \) for all \( i = 1, \ldots, s \).

**Remark 4** Let \( R \in \mathbb{Z} \) be an integer, than we can as well require that the infinitely many integers \( t \) given by the sieve are such that \( t \geq R \) (or equivalently such that \( t \leq R \)).

\(^2\) We allow the squarefree part of the values of \( f \) to be a certain fixed integer.

\(^3\) A homogeneous squarefree sieve is given in [10] and is unconditional for 2-variable homogeneous \( f \in \mathbb{Z}[X, Y] \) whose irreducible factor have all degree less than 6.
4.2 Chowla’s conjecture

This second conjecture estimates the proportion of the values \( f(t) \) with a certain parity of the number of prime factors. Recall that Liouville’s function (Definition 2) already appears since section 2.

**Conjecture 4.4** (Chowla’s conjecture) Let \( f \) be a primitive squarefree polynomial with integer coefficients. The following estimation holds for every arithmetic progression \( A \):

\[
\sum_{t \in A(X)} \lambda(f(t)) = o(X)
\]  

(7)

A 2-variable homogeneous version is known to hold for polynomials up to degree 3. This is proven for non-irreducible homogeneous polynomials in [14], and for irreducible polynomials in [13] and more recently in [16]. In our 1-variable case however Conjecture 4.4 is known to hold in the following case:

**Theorem 4.5** (Hadamard – de la Vallée Poussin) Let \( f \in \mathbb{Z}[T] \) be a squarefree polynomial. Chowla’s conjecture holds if \( f \) is linear.

4.3 Combination of the conjectures

In [7, Theorem 2.9], the author proves an analytical theorem for homogeneous polynomials of two variables indicating a sort of independence between the two properties of the values of a polynomial

- being “squarefree”
- having the same “parity of the number of factors”.

In this paper we need the following 1-variable analogue of that result, whose proof can be found in [6, Théorème 1.3.8]:

**Theorem 4.6** [7, Theorem 2.9] Fix an element \( \epsilon \in \{1, -1\} \). Let \( f, g, h \in \mathbb{Z}[T] \) be squarefree primitive polynomials with no common factor. Assume the Squarefree conjecture holds for \( f \) and \( g \) and that Chowla’s conjecture holds for \( f \). Then for any arithmetic progression \( A = N\mathbb{Z} + a \) (where \( a, N \neq 0 \) are integers such that \( a \) and \( N \) are coprime), define \( T(X) \) to be the number of pairs of integers \( t \in A(X) \) such that

1. \( \frac{f(t)g(t)}{d_{fg,A}} \) is not divisible by \( p^2 \) for any prime \( p \) such that \( p \nmid N \);
2. \( \lambda(f(t)) = \epsilon \)
3. for all factor \( h_i \) of \( h \), one has \( h_i(t) > 0 \).

Then

\[
T(X) = \frac{C_{fg,A}}{2} X + o(X).
\]

(8)

Combining Theorem 4.6 with Theorem 4.2 and Theorem 4.5, we obtain:

**Corollary 4.7** Fix \( \epsilon \in \{1, -1\} \). Let \( f, g, h \in \mathbb{Z}[T] \) be squarefree polynomials. Assume that every factor of \( g \) has degree at most 3 and that \( \deg f = 1 \). For an arithmetic progression \( A \), let \( T(X) \) be the counting function as defined in Theorem 4.6. Then the following estimate holds

\[
T(X) = \frac{C_{fg,A}}{2} X + o(X).
\]

(9)
4.3.1 A one variable version of the “Squarefree-Liouville” Sieve

**Corollary 4.8** Let \( f(T), g(T) \in \mathbb{Z}[T] \) be polynomials. Assume that they are coprime, that no square of a nonunit in \( \mathbb{Z}[T] \) divides \( f(T) \) or \( g(T) \), that every irreducible factor of \( g \) has degree \( \leq 3 \), and that \( \deg f \leq 1 \).

Let \( R(T) \in \mathbb{Z}[T] \) be a polynomial and \( R = \gamma \cdot \prod_{0 \leq i \leq r} R_i \) its decomposition in primitive factors. Suppose \( \text{sgn}(\gamma) = +1 \).

Fix
- a sequence \( S = (p_1, \ldots, p_s) \) of distinct prime numbers and
- a sequence \( T = (t_1, \ldots, t_s, t'_1, \ldots, t'_s) \) of nonnegative integers.

Let \( N \) be an integer such that \( p_1 t_1 + p'_1 t'_1 + \cdots + p_s t_s + p'_s t'_s \mid N \) and that \( p^2 \mid N \) for all primes \( p < (\deg f + \deg g) \).

Suppose that there exists an integer \( a \) such that

1. \( f(a)g(a) \equiv 0 \mod p^2 \), whenever \( p \mid N \) and \( p \neq p_i \) for any \( i \),
2. for every \( 1 \leq i \leq r \), one has \( R_i(t) > 0 \),
3. \( v_{p_i}(f(a)) = t_i \) and \( v_{p_i}(g(a)) = t'_i \) for every \( i = 1, \ldots, s \)
4. and \( \lambda(f(a)) = \epsilon \).

Then there are infinitely many integers \( t \) such that

1. \( u \equiv a \mod N \),
2. for every \( i \), one has \( R_i(t) > 0 \),
3. \( \lambda(f(t)) = \epsilon \),
4. and \( f(t) = p_1^{t_1} \cdots p_s^{t_s} \cdot l \), and \( g(t) = p'_1^{t'_1} \cdots p'_s^{t'_s} l' \) where \( l \) and \( l' \) are squarefree and \( v_{p_i}(l) = v_{p_i}(l') = 0 \) for all \( i = 1, \ldots, s \).

5 Proof of the theorem 1.1

**Theorem 5.1** (=Theorem 1.1) Let \( \mathcal{E} \) be a family of elliptic curves over \( \mathbb{Q} \). Suppose that there exists at least one polynomial \( P_o(T) \in \mathbb{Q}[T] \) such that the reduction of \( \mathcal{E} \) at \( P_o(T) \) is either

1. multiplicative;
2. additive potentially multiplicative;
3. semi-stable and \( \deg P_o \) is odd;
4. or additive potentially good and if the Kodaira symbol of the reduction is
   - (a) \( II, II^*, IV \) or \( IV^* \), then
     \[ \mu_3 \not\subseteq \mathbb{Q}[T]/P_o(T); \]
   - (b) \( III \) or \( III^* \), then
     \[ \mu_3 \not\subseteq \mathbb{Q}[T]/P_o(T). \]

Suppose moreover that

1. \( M_{\mathcal{E}} = \prod_{P \in \mathcal{M}} P \) respects Chowla’s conjecture;
2. \( B_{\mathcal{E}} = \prod_{P \in \mathcal{B}} P \) respects the squarefree conjecture.

Then the sets \( W_+(\mathcal{E}, \mathbb{Z}) \) and \( W_-(\mathcal{E}, \mathbb{Z}) \) are both infinite.
The general strategy is to construct infinitely many pairs of integers $(t_1, t_2)$ such that $W(\mathcal{E}_{t_1}) = -W(\mathcal{E}_{t_2})$.

Recall that a place (or an irreducible polynomial associated to this place) is insipid if it is of type
- $I_0^*$
- $I_1, II^*, IV$ or $IV^*$, and
- $\mu_3 \subseteq \mathbb{Q}[T]/P(T)$;
- or $III$ or $III^*$, and
- $\mu_4 \subseteq \mathbb{Q}[T]/P(T)$.

**Proof** Let $\frac{n_4}{d_4}, \frac{n_6}{d_6}, \frac{n_\Delta}{d_\Delta}$ be the respective coprime numerators and denominators of the contents of the polynomials $c_4(T), c_6(T), \Delta(T)$ associated to $\mathcal{E}$. (Observe that the only factors of $d_4, d_6, d_\Delta$ are 2 or 3.) Put as in Section 2

$$\delta = 2 \cdot 3 \cdot n_4 \cdot n_6 \cdot n_\Delta \prod_{Q, Q' \in \mathcal{B}} \text{Res}(Q, Q').$$

Let $N = N_{\mathcal{E}}$ be the integer and $R_\mathcal{E}$ be the polynomial given by Proposition 3.1 (choose the minimal such integer $N_{\mathcal{E}}$ and polynomial $R_\mathcal{E}$ of lowest degree). Write $R_\mathcal{E} = R = \gamma R_1 \cdots R_r$, the decomposition in primitive polynomial. Let us choose $R$ such that $\text{sign}(\gamma) = +1$. By definition, the function $t \mapsto \prod_{p|\delta} W_p(\mathcal{E}_t) \prod_{P \in \mathcal{B}} g_P(t)$ is constant when $t$ stays in a congruence class modulo $N$ and when $t$ is in a connected component of

$$\mathbb{R} - \{t \in \mathbb{R} | R(t) = 0\}.$$

For each $p | N$, put $\alpha_p = v_p(N)$. Moreover, write $N = 2^{\alpha_2} 3^{\alpha_3} p_1^{\alpha_{p_1}} \cdots p_s^{\alpha_{p_s}}$ the factorisation into distinct prime numbers.

Put

$$S = (2, 3, p_1, \ldots, p_s),$$

and

$$T = (0, \ldots, 0).$$

Let $a_2 \mod 2^{\alpha_2}$ be a congruence class such that for all $P_i$ of bad reduction (except the insipid ones):

$$P_i(a_2) \not\equiv 0 \mod 2^{\alpha_2}.$$

Let $a_3 \mod 3^{\alpha_3}$ be a congruence class such that for all $P_i$ of bad reduction (except the insipid ones):

$$P_i(a_3) \not\equiv 0 \mod 3^{\alpha_3}.$$

Let also, for each $p | N$ such that $p \neq 2, 3$, be classes $\alpha_p \mod p^{\alpha_p}$ such that for all $P_i$ of bad reduction (except the insipid ones) we have:

$$P_i(\alpha_p) \not\equiv 0 \mod p^{\alpha_p}.$$

As by assumption the polynomial $P_i$ have content 1, such classes $\alpha_p$ exist for every $p | N$. 

\[\text{Springer}\]
By the Chinese Remainder Theorem, there exist integers \( a \) satisfying
\[
 a \equiv \begin{cases} 
 a_2 \mod 2^{a_2}, \\
 a_3 \mod 3^{a_3}, \\
 a_p \mod p^{a_p} & \text{for all } p \mid N.
\end{cases}
\] (10)

Now we use the hypotheses: there exists an irreducible polynomial such that the reduction respects one of the properties from 1 to 4.

- Suppose that we can choose \( P_o \) to have multiplicative reduction (property 1). Then
  i. choose \( a_p \) such that \( R_i(t) > 0 \) for all \( 1 \leq i \leq r \).
  ii. put \( f := M_{\mathcal{E}} \).

- Suppose that there’s no multiplicative place and that \( P_o \) is not insipid (property 2 or 4), then
  i. choose \( a \) (as in (10)) such that \( R_i(t) > 0 \) for all \( 1 \leq i \leq r \) except for \( R_{i_0} < 0 \).
  ii. put \( f := 1 \).

- Suppose that \( P \) of reduction type \( I^*_0 \) with deg \( P \) odd (property 3), then
  i. choose \( a \) (as in (10)) such that \( R_i(t) > 0 \) for all \( 1 \leq i \leq r \) except for \( R_{i_0} = P_o \) where \( R_{i_0} < 0 \).
  ii. put \( f := 1 \).

In any case, put \( g = \prod P \), where \( P \) runs through the non-insipid polynomials.

If \( f \neq 1 \) (property 1: there exists a finite place of multiplicative reduction), use the Liouville-Squarefree Sieve given by Corollary 4.8 on \( f, g, S, T, N \) and \( a \) as previously, to prove that there exists a set \( \mathcal{F}_1 \) of infinitely many \( t \in \mathbb{Z} \) such that
\[
g(t) = l, \quad \text{and } \lambda(f(t)) = +1
\]
where \( l \) is a squarefree integer coprime to each \( p \in S \) by our choice of \( S \) and \( T \). This set \( \mathcal{F}_1 \) may be chosen such that \( \forall t \in \mathcal{F}_1, R_i(t) > 0 \) for all \( 1 \leq i \leq r \).

If \( f = 1 \), use similarly the Squarefree Sieve given by Corollary 4.3 on \( g, S, T, N \) and \( a \), to obtain the set \( \mathcal{F}_1 \). As previously, the set \( \mathcal{F}_1 \) may be chosen such that \( \forall t \in \mathcal{F}_1, R_i(t) > 0 \) for all \( 1 \leq i \leq r \).

By Proposition 3.6 part B, we have that for all \( t, t' \in \mathcal{F}_1 \),
\[
W(\mathcal{E}_t) = W(\mathcal{E}_{t'}). 
\]

Suppose that the \( P_o \) that we fixed has type \( I^*_0 \) and has odd degree (property 3). Then we similarly define \( \mathcal{F}_2 \) such that for all \( P \neq P_o \) one has \( R_P(t) > 0 \), and \( R_{P_o}(t) < 0 \). By Proposition 3.6, all the elements of \( \mathcal{F}_2 \) are such that their fibers on \( \mathcal{E} \) have the same root number. Then by Proposition 3.8 every pair \((t_1, t_2)\) with \( t_1 \in \mathcal{F}_1 \), and \( t_2 \in \mathcal{F}_2 \), is such that
\[
W(\mathcal{E}_{t_1}) = -W(\mathcal{E}_{t_2}).
\]

For the other cases, according to the type of \( P_o \), choose a prime number \( q_0 \) with one of the following properties:

(1) Suppose that \( P_o \) has type \( I^*_m \) or \( I_m \) (property 1 or 2). Put \( P(T) = -c_6(T)/Q(T)^3 \). By Lemma 3.5 applied to \( P(T), Q(T) \) and \( S =: \mathcal{P}_0 \), there exist \( q_0 \neq S \) and \( m_0 \leq 0 \) an integer such that \( q_0^2 \mid Q(m_0) \) and that \(-q_0^{-2}P(m_0)Q(m_0)\) is a square modulo \( q_0 \).
(2) Suppose that $P_o$ has type $II, II^*, IV, IV^*$ (property 4 (a)), then let $q_o$ be such that \( \left( \frac{-3}{q_o} \right) = -1 \). This prime exists whenever $P_o$ is not insipid by Remark 2.

(3) Suppose that $P_o$ has type $III, III^*$ (property 4 (b)), then let $q_0$ be such that $\left( \frac{-1}{q_0} \right) = -1$. This prime exists whenever $P_o$ is not insipid by Remark 3.

Consider the sequences

$$ S' = (2, 3, p_1, \ldots, p_s, q_0) $$

and

$$ T' = (0, \ldots, 0, 2). $$

By the Chinese Remainder Theorem, there exists an integer $a'$ satisfying both (10) and

$$ a' \equiv m_0 \mod q_0^3. $$

We can choose it such that $R_i(t) > 0$ for all $1 \leq i \leq r$.

By using either Corollary 4.8 or Corollary 4.3 (according to whether or not $f = 1$) on

$$(f, P_o, S', T' \text{ and } a')$$

we obtain $F_2$, a set of infinitely many $t \in \mathbb{Z}$ such that

$$ P_o(t) = q_0^d l_t, \quad (\text{and } \lambda(f(t)) = +1), $$

where $l$ is a squarefree integer coprime to every element of $S'$ and where $q_0^{-6} c_6(t)$ is a square modulo $q_0$. As previously, we choose $F_2$ such that $\forall t \in F_2$ one has $R_i(t) > 0$ for all $1 \leq i \leq r$ – except in case $P_o$ is insipid: for all $i \neq i_0$, with the exception that $R_{i_0}(t) < 0$. By Proposition 3.6, all the elements of $F_2$ are such that their fibers on $E$ have the same root number.

To end the proof, we use Proposition 3.6 part A to show that for all $t_1 \in F_1$, and every $t_2 \in F_2$, one has

$$ W(E_{t_1}) = -W(E_{t_2}). $$

\[ \square \]

**Remark 5** An alternative proof for the case where $E$ has multiplicative reduction can be found in Manduchi’s article where she proves the following:

**Theorem 5.2** [17, Theorem 2] Let $E$ be a non-isotrivial family of elliptic curves satisfying the hypotheses of Corollary 1.2 with a linear place of multiplicative reduction on $E$ outside of $-\deg$. Then the sets $W_\pm(E, \mathbb{Z})$ are both infinite.

In her proof, she focuses rather on making the Liouville function vary.

### 6 Families with coefficients of bounded degrees

Let $E$ be a family of elliptic curves given for $t \in \mathbb{Q}$ by the Weierstrass equation

$$ E_t : y^2 = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t) $$

where $\deg a_i \leq 2$ for $i = 2, 4, 6$. Suppose that there is no place of multiplicative reduction other than possibly $-\deg$ (or in other words *potentially parity-biased*), then Bettin, David ...
and Delauney prove in recent work [1, Theorem 7 and 8] that there are essentially 6 different classes of non-isotrivial such families, namely:

\[ F_s(t) : y^2 = x^3 + 3tx^2 + 3sx + st, \text{ with } s \in \mathbb{Z}_{\neq 0}; \]  
\[ G_w(t) : wy^2 = x^3 + 3tx^2 + 3tx + t^2, \text{ with } w \in \mathbb{Z}_{\neq 0}; \]  
\[ H_w(t) : wy^2 = x^3 + (8t^2 - 7t + 3)x^2 - 3(2t - 1)x + (t + 1), \text{ with } w \in \mathbb{Z}_{\neq 0}; \]  
\[ J_w(t) : wy^2 = x^3 + t(t - 7)x^2 - 6t(t - 6)x + 2(5t - 27), \text{ with } w \in \mathbb{Z}_{\neq 0}; \]  
\[ J_{m,w}(t) : wy^2 = x^3 + 3t^2x^2 - 3mtx + m^2, \text{ with } m, w \in \mathbb{Z}_{\neq 0}; \]  
\[ \mathcal{L}_{w,s,v}(t) : wy^2 = x^3 + 3(t^2 + v)x^2 + 3sx + s(t^2 + v), \text{ with } s \in \mathbb{Z}_{\neq 0}. \]

Observe that those families have no place of multiplicative reduction except possibly at \(-\deg\). The bad places of those surfaces are:

For \(F_s\): \(t^2 - s (II)\), \(-\deg (I_4^s)\);
For \(G_w\): \(t - 1 (II), t (III), -\deg (I_7^s)\);
For \(H_w\): \(t (III), t^2 - 11/8t + 1 (II), -\deg (I_5)\);
For \(J_w\): \(t (II), t^2 - 10t + 27 (III), -\deg (I_4)\);
For \(J_{m,w}\): \(t^3 + m (II), -\deg (I_6)\);
For \(\mathcal{L}_{w,s,v}\): \(t^4 + 2vt^2 + v^2 - s (II), -\deg (I_4)\).

As a corollary of Theorem 1.1, any family isomorphic to one of the form \(G_w, H_w, J_w\) and \(J_{m,w}\) have infinitely many integer fibers with negative (resp. positive) root number. Hence, the only surfaces among those six families to which our Theorem 1.1 do not apply are of the form \(F_s\) with \(s = -3s^2\) and \(\mathcal{L}\) in very special circumstances.

In [4], Chinis computes the average root number on the families \(F_s\), and shows that \(F_s\) is \textit{parity biased} over \(\mathbb{Z}\) (i.e. the average root number over \(\mathbb{Z}\) is not 0) if and only if \(s \equiv 1, 3, 5 \text{ mod } 8\). The \textit{average root number} of a family of elliptic curve \(E\) over \(\mathbb{Z}\) is defined as

\[ \text{Av}_\mathbb{Z}(W(E)) := \lim_{T \to \infty} \frac{1}{2T} \sum_{|t| \leq T} W(E_t), \]

provided that the limit exists. However, even knowing that \(| \text{Av}_\mathbb{Z}(W(E)) | = 1\) would not be enough to determine whether or not the root number is constant. A work in progress by the author and Rena Chu aims at finding conditions on \(s, a, b \in \mathbb{Z}\) for \(F_s(at + b)\) to have constant root number [3].

Acknowledgements This article was triggered by an email conversation with Fernando Gouvêa. I thank him for his interest. I also wish to thank Rena Chu, Marc Hindry and Arul Shankar for helpful discussions and the anonymous referees for several useful suggestions and a very detailed list of typos.

References

1. Bettin, S., David, C., Delaunay, C.: Non-isotrivial elliptic surfaces with non-zero average root number. J. Number Theory 191, 1–84 (2018)
2. Conrad, B., Conrad, K., Helm, H.: Root numbers and ranks in positive characteristic. Adv. Math. 198(2), 684–731 (2005)
3. Chu, R., Desjardins, J.: Constant root number on integer fibres of elliptic surfaces. arXiv:2011.02386 (2020)
4. Chinis, J.: Computing the average root number of an elliptic surface. J. Number Theory 194, 83–116 (2019)
5. Deligne, P.: Les constantes des équations fonctionnelles des fonctions L. In: Modular Functions of One Variable, II (Proceedings of International Summer School, University of Antwerp, Antwerp, 1972). Lecture Notes in Mathematics, vol. 349, pp. 501–597. Springer, Berlin (1973)

6. Desjardins, J.: Densité des points rationnels sur les surfaces elliptiques et les surfaces de del Pezzo de degré 1. Ph.D. thesis, Université Paris-Diderot—Paris VII (2016)

7. Desjardins, J.: On the variation of the root number of the fibers of families of elliptic curves. J. Lond. Math. Soc. 99(2), 295–331 (2018)

8. Desjardins, J., Naskręcki, B.: Geometry of the Del Pezzo surface $y^2 = x^3 + Am^6 + Bn^6$. arXiv:1911.02684 (2019)

9. Duquesne, S.: Integral points on elliptic curves defined by simplest cubic fields. Exp. Math. 10(1), 91–102 (2001)

10. Gouvêa, F., Mazur, B.: The square-free sieve and the rank of elliptic curves. J. Am. Math. Soc. 4(1), 1–23 (1991)

11. Halberstadt, E.: Signes locaux des courbes elliptiques en 2 et 3. C. R. Acad. Sci. Paris Sér. I Math. 326(9), 1047–1052 (1998)

12. Helfgott, H.A.: On the behaviour of root numbers in families of elliptic curves. arXiv:math/0408141v3 (2003)

13. Helfgott, H.A.: The parity problem for irreducible cubic forms. arXiv:math/0501177 (2005)

14. Helfgott, H.A.: The parity problem for reducible cubic forms. J. Lond. Math. Soc. (2) 73(2), 415–435 (2006)

15. Hooley, C.: On the power free values of polynomials. Mathematika 14, 21–26 (1967)

16. Lachand, Armand: Fonctions arithmétiques et formes binaires irréductibles de degré 3. Annales de l’Institut Fourier 68(3), 1297–1363 (2018)

17. Manduchi, E.: Root numbers of fibers of elliptic surfaces. Compositio Math. 99(1), 33–58 (1995)

18. Rizzo, O.G.: Average root numbers for a nonconstant family of elliptic curves. Compositio Math. 136(1), 1–23 (2003)

19. Rohrlich, D.E.: Variation of the root number in families of elliptic curves. Compositio Math. 87(2), 119–151 (1993)

20. Tate, J.: Algorithm for determining the type of a singular fibre in an elliptic pencil. In: Lecture Notes in Mathematics, Modular functions of one variable IV (Antwerpen 1972), vol. 476, pp 33–52 (1975)

21. Várilly-Alvarado, A.: Density of rational points on isotrivial rational elliptic surfaces. Algebra Number Theory 5, 659–690 (2011)

22. Washington, L.C.: Class numbers of the simplest cubic fields. Math. Comp. 48(1), 371–384 (1987)

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.