Journal de Théorie des Nombres de Bordeaux
anciennement Séminaire de Théorie des Nombres de Bordeaux

Julie DESJARDINS

Root number of twists of an elliptic curve

Tome 32, n° 1 (2020), p. 73-101.
<http://jtnb.centre-mersenne.org/item?id=JTNB_2020__32_1_73_0>

Journal de Théorie des Nombres
de Bordeaux **32** (2020), 73–101

Root number of twists of an elliptic curve

par Julie DESJARDINS

Résumé. Nous donnons une description explicite du comportement du signe (root number) dans la famille des tordues d'une courbe elliptique $E/\mathbb{Q}$ par les valeurs rationnelles d'un polynôme $f(t)$. En particulier, nous présentons un critère pour que la famille ait un signe constant sur $\mathbb{Q}$. Ceci complète un travail de Rohrlich : nous donnons les détails du comportement du signe lorsque E a mauvaise réduction sur $\mathbb{Q}^{ab}$ et nous traitons les cas $j(E) = 0, 1728$ qui n'étaient pas considérés précédemment.

Abstract. We give an explicit description of the behaviour of the root number in the family given by the twists of an elliptic curve $E/\mathbb{Q}$ by the rational values of a polynomial $f(T)$. In particular, we present a criterion for the family to have a constant root number over $\mathbb{Q}$. This completes work by Rohrlich: we detail the behaviour of the root number when E has bad reduction over $\mathbb{Q}^{ab}$ and we treat the cases $j(E) = 0, 1728$ which were not considered previously.

1. Introduction

This paper is concerned with the behaviour of the root number in a one-parameter family of twists of an elliptic curve by the values of a polynomial $f \in \mathbb{Z}[T]$, or equivalently, in the fibres of an isotrivial elliptic surface. We will see that the root number respects a certain type of periodicity, and we will give a criterion to predict when it is constant.

Let E be an elliptic curve over $\mathbb{Q}$. The *root number* $W(E)$ is defined as the product of the local root numbers $W_p(E) \in \{\pm 1\}$:

$$W(E) = \prod_{p \leq \infty} W_p(E),$$

where p runs through the finite and infinite places of $\mathbb{Q}$. These local factors, defined in terms of the epsilon factors of the Weil–Deligne representation of $\mathbb{Q}_p$ and explained in details by Rohrlich in [14], have the property that $W_p(E) = 1$ for all but finitely many p. Rohrlich [13] gives an explicit formula for the local root numbers in terms of the reduction of the elliptic curve E at a prime $p \neq 2, 3$. Moreover, we always have $W_\infty(E) = -1$. The remaining cases $p = 2, 3$ are covered by Halberstadt [9] (see also Rizzo [12]).

Manuscrit reçu le 10 janvier 2019, révisé le 20 mars 2020, accepté le 25 avril 2020.
2020 *Mathematics Subject Classification.* 11G05, 11G07.
Mots-clefs. elliptic curve, root number, twist.
The author was supported by the Max Planck Institut für Mathematik in Bonn.

Let $L(E,s)$ denote the L-function of E. Then $W(E)$ is equal to the sign of the functional equation of L by the Modularity Theorem over $\mathbb{Q}$. Note that over general number fields $K \neq \mathbb{Q}$, such an equality is only conjectural.

The Birch and Swinnerton-Dyer conjecture implies the following statement, known as the parity conjecture

$$W(E) = (-1)^{\operatorname{rank} E(\mathbb{Q})}.$$

A consequence of this conjectural equality is that it suffices to have $W(E) = -1$ for the rank of $E(\mathbb{Q})$ to be non-zero, and in particular for $E(\mathbb{Q})$ to be infinite.

By a *one-parameter family of elliptic curves* we mean the collection of the fibres of an elliptic surface over $\mathbb{Q}$ (with a section) given by a Weierstrass equation

$$\mathscr{E} : y^2 = x^3 + A(T)x + B(T),$$

where $A(T), B(T)$ are polynomials with coefficients in $\mathbb{Z}$, and the discriminant is denoted by $\Delta(T)$. For $t \in \mathbb{P}^1$ such that $\Delta(t) \neq 0$, the *fibre at* t, $\mathscr{E}_t : y^2 = x^3 + A(t)x + B(t)$, is an elliptic curve. In this paper we consider the case where the family is isotrivial, i.e. when its j-invariant function $t \mapsto j(\mathscr{E}_t) = \frac{4A(t)^3}{\Delta(t)}$ is constant. In that case, the curves $\mathscr{E}_t$ are twists of one another, and $\mathscr{E}$ can be seen as a subfamily of the families of all twists of $\mathscr{E}_1$:

(1) (quadratic twists, $j(\mathscr{E}) \neq 0, 1728$) $y^2 = x^3 + aH(T)^2x + bH(T)^3$,
(2) (quartic twists, $j(\mathscr{E}) = 1728$) $y^2 = x^3 + A(T)x$,
(3) (sextic twists, $j(\mathscr{E}) = 0$) $y^2 = x^3 + B(T)$,

where $a, b \neq 0$ and $H(T)$, $A(T)$, $B(T)$ are non-zero polynomials with integer coefficients.

In a previous article [6], the author proves that the function $t \mapsto W(\mathscr{E}_t)$ defined by the root number on a non-isotrivial family $\mathscr{E}$ is never periodic (i.e. constant on a congruence class of t). More precisely, she proves that the sets $W_\pm = \{t \in \mathbb{P}^1 \mid W(\mathscr{E}_t) = \pm 1\}$ are both infinite, which implies (under the parity conjecture) the Zariski-density of the rational points $\mathscr{E}(\mathbb{Q})$.

For families of twists thought, it can happen that $W(\mathscr{E}_t)$ takes the same value for every $t \in \mathbb{P}^1$ associated to a smooth $\mathscr{E}_t$, and (more alarmingly if one is interested in proving the Zariski-density) equal to $+1$, as observed previously in each of the two special cases:

(1) (Cassels and Schinzel [2]) $y^2 = x^3 - (1+T^4)^2x$,
(2) (Várilly-Alvarado [15]) $y^2 = x^3 + 27T^6 + 16$.

Observe that the first example is a K3 surface and that the second is a rational elliptic surface. These specific surfaces have however a Zariski-dense set of rational points - the proof can be found respectively in [10] and in [15, Example 7.1]. By the time the present article was published, the author and B. Naskręcki [7] released a preprint presenting a simple algorithm to find the generic rank of any elliptic surface of the form $y^2 = x^3 + AT^6 + B$, which generalizes Várilly-Alvarado's result.

It is not possible that all quadratic twists have the same root number, as observed by Dokchitser and Dokchitser [8]. However, they proved that the elliptic curve

$$y^2 = x^3 + x^2 - 12x - \frac{67}{4} \tag{1.1}$$

has root number +1 over every extension of $K = \mathbb{Q}(\sqrt[4]{-37})$. This curve has the additional property that any twist by an integer $t \in \mathbb{N}$ has root number +1 over $\mathbb{Q}$ and any twist by $-t$ has root number -1. Thus, polynomials f with only positive values (resp. only negative values) define a family of twists with constant root number +1 (resp. -1). For instance, $(T^2+1)y^2 = x^3+x^2-12x-\frac{67}{4}$ has constant root number +1. However, the density of the rational points is proven on every family of quadratic twists of an elliptic curve by a f with degree ≤ 2 [5, Theorem 4.2.].

In this article, we describe for which elliptic curves E the root number of a twist by $t \in \mathbb{Z}$ only depends on the sign of t (Lemma 4.2). Moreover, for general elliptic curves E we describe the behaviour of the root number (Theorem 1.2).

1.1. Notation. Throughout the paper we use two non-standard notations. Given an integer $\alpha \in \mathbb{Z}$ and a prime number, we denote by $\alpha_{(p)}$ the integer such that

$$\alpha = p^{v_p(\alpha)}\alpha_{(p)}.$$

Similarly, we define $\alpha_{(d)}$ with $d = \prod p_i^{e_i} \in \mathbb{N}$ as the integer

$$\alpha = \left(\prod_i p_i^{v_{p_i}(\alpha)}\right)\alpha_{(d)}.$$

We will denote by $sq(\alpha)$ and call the *square part* of α the integer

$$sq(\alpha) = \prod_{i \text{ such that } e_i \text{ is even}} p_i.$$

Incidentally, $sq(\alpha)_{(p)}$ refers to the integer

$$sq(\alpha)_{(p)} = \prod_i p_i,$$

where i ranges on e_i even and $p_i \neq p$. We also call $\operatorname{sgn}(\alpha)$ the sign of α.

1.2. Main results. We are interested in the behaviour of the root number in a one-parameter family of twists of elliptic curves, that is, to say in the fibres of an isotrivial elliptic surface.

Definition 1.1.

(1) A function $f : \mathscr{F} \subseteq \mathbb{Z} \to \{\pm 1\}$ is periodic (or N-periodic) if there exists a positive integer N such that for each $t, t' \in \mathscr{F}$

$$t \equiv t' \mod N \Rightarrow f(t) = f(t').$$

We denote a *congruence class modulo* N by $[t]$ (where $t \in \mathbb{Z}$ is a representative of the congruence class).

(2) A function $f : \mathscr{F} \subseteq \mathbb{Z} \to \{\pm 1\}$ is square-periodic (or (N, M)-square-periodic) if there exist positive integers N, M such that for $t, t' \in \mathscr{F}$ that we write in its factorisation into prime factors $t = p_1^{e_1} \cdot p_r^{e_r}$ and $t' = q_1^{e'_1} \cdot q_s^{e'_s}$, we have

$$t \equiv t' \mod N \text{ and } sq(t) \equiv sq(t') \mod M \Rightarrow f(t) = f(t'),$$

where $sq(t) = \prod_{e_i \text{ even}} p_i$ and $sq(t') = \prod_{e'_i \text{ even}} q_i$.

We call a *square-congruence class* $[t]_{sq} \mod N, M$ the set of the integers t' such that $t' \equiv t \mod N$ and $sq(t') \equiv sq(t) \mod M$.

Let E be the elliptic curve defined by the Weiestrass equation $y^2 = x^3 + ax + b$ and let $t \in \mathbb{Q} \setminus \{0\}$. Then the *twist by* t *of* E is the elliptic curve E_t given by the following Weiestrass equation:

(1) $E_t : y^2 = x^3 + at^2x + bt^3$ if $j(E) \neq 0, 1728$ (i.e. $ab \neq 0$),
(2) $E_t : y^2 = x^3 + atx$ if $j(E) = 1728$ (i.e. $b = 0$),
(3) $E_t : y^2 = x^3 + bt$ if $j(E) = 0$ (i.e. $a = 0$).

Note also the following isomorphisms for all $t \in \mathbb{Q} \setminus \{0\}$: $E_{t^2} \cong E$ if $j(E) \neq 0, 1728$, $E_{t^4} \cong E$ if $j(E) = 1728$, $E_{t^6} \cong E$ if $j(E) = 0$. As a consequence, for any $t = \frac{p}{q} \in \mathbb{Q} \setminus \{0\}$, the twist E_t is isomorphic to $E_{t'}$ for $t' = qp$ if $ab \neq 0$; $t' = pq^3$ if $b = 0$; $t' = pq^5$ if $a = 0$. It is thus sufficient to study the twists by integers.

The results of this article are summarized in the following theorem.

Theorem 1.2. *Let E be an elliptic curve and for $t \in \mathbb{Z}$ denote by E_t its twist by t.*

(1) *Suppose that $j(E) \neq 0, 1728$. Define $\mathscr{F}_2$ to be the set of square-free integers, and $\mathscr{F}_2^+$ (respectively $\mathscr{F}_2^-$) the subset of $t \in \mathscr{F}_2$ with* $\operatorname{sgn}(t) = +1$ *(resp.* $\operatorname{sgn}(t) = -1$*). Then*

(a) *The root number can be written as the following product*

$$W(E_t) = -W_2(E_t)W_3(E_t)\left(\frac{-1}{|t_{(6\Delta)}|}\right)\left(\prod_{p|\Delta_{(6)}} W_p(E_t)\right)$$

where $\left(\frac{\cdot}{\cdot}\right)$ is the Jacobi symbol.

(b) *the function $t \mapsto W(E_t)$ is periodic on $\mathscr{F}_2^\pm$.*

   (c) *The root number $W(E_t)$ is not constant when t runs through $\mathbb{Z} \setminus \{0\}$. However, if E satisfies the properties of Lemma 4.2, it is constant on $\mathbb{Z}_{<0}$ and $\mathbb{Z}_{>0}$.*

(2) *Suppose that $j(E) = 1728$. Define $\mathscr{F}_4$ to be the set of fourth-powerfree integers, and $\mathscr{F}_4^+$ (respectively $\mathscr{F}_4^-$) the subset of $t \in \mathscr{F}_4$ with* $\operatorname{sgn}(t) = +1$ *(resp.* $\operatorname{sgn}(t) = -1$*). Then*
   (a) *The root number can be written as the following product*

$$W(E_t) = -W_2(E_t)W_3(E_t)\left(\frac{-2}{|t_{(6)}|}\right)\left(\frac{-1}{sq(t)_{(6)}}\right).$$

   (b) *The function $t \mapsto W(E_t)$ is square-periodic on $\mathscr{F}_4^{\pm}$.*
   (c) *The root number $W(E_t)$ is not constant when t runs through $\mathbb{Z} \setminus \{0\}$.*

(3) *Suppose that $j(E) = 0$. Define $\mathscr{F}_6$ to be the set of sixth-powerfree integers, and $\mathscr{F}_6^+$ (respectively $\mathscr{F}_6^-$) the subset of $t \in \mathscr{F}_6$ with* $\operatorname{sgn}(t) = +1$ *(resp.* $\operatorname{sgn}(t) = -1$*). Then*
   (a) *The root number can be written as the following product*

$$W(E_t) = -W_2(E_t)W_3(E_t)\left(\frac{-1}{|t_{(6)}|}\right)\left(\frac{sq(t)_{(6)}}{3}\right).$$

   (b) *The function $t \mapsto W(E_t)$ is square-periodic on $\mathscr{F}_6^{\pm}$,*
   (c) *The root number $W(E_t)$ is not constant when t runs through $\mathbb{Z} \setminus \{0\}$.*

The article is organised as follows. In the rest of the introduction, we relate our results to previous work, in particular to Rohrlich's. In Section 2 we study the monodromy of the reduction on a family of twists in each of the three cases $j \in \mathbb{Q} \setminus \{0, 1728\}$, $j = 1728$ and $j = 0$, and in Section 3 we use it to describe the variation of the root number between an elliptic curve and one of its twists. We conclude the paper in Section 4 by proving Theorem 1.2 in each of the three cases.

1.3. Recollection on Rohrlich's results. Theorem 1.2 completes the following result on the variation of the root number of quadratic twists due to Rohrlich, and extends it to the case $ab = 0$: the quartic and sextic twists families.

Theorem 1.3 ([13, Theorem 2])**.** *Let $a, b \in \mathbb{Z}\setminus\{0\}$ such that $4a^3+27b^2 \neq 0$. Consider the elliptic curve given by the equation $E : y^2 = x^3 + ax + b$. Let $f(t) \in \mathbb{Z}[t]$ and the family of quadratic twists given by the equation*

$$E_{f(t)} : y^2 = x^3 + af(t)^2x + bf(t)^3.$$

Then, one of the two properties holds :

(1) *The sets W_+ and W_- are dense in $\mathbb{R}$.*

(2) *The sets* W_+ *and* W_- *are* $\{t \in \mathbb{Q} \mid f(t) < 0\}$ *and* $\{t \in \mathbb{Q} \mid f(t) > 0\}$ *(in either order).*

Moreover, given E:

As a conclusion of this theorem, one obtains :

(1) if E has good reduction over $\mathbb{Q}^{ab}$ then $E_{f(t)}$ has constant root number if and only if $f(t)$ takes the same sign for all $t \in \mathbb{Q}$,
(2) if E has bad reduction over $\mathbb{Q}^{ab}$, then
   (a) if $f(t)$ does not always take the same sign, then W_+ and W_- have infinite cardinality.
   (b) if $f(t) > 0$ (or < 0), then Rohrlich's theorem does not allow us to conclude directly. In order to know if the root number of the fibres is constant or not, the use of Theorem 1.2 is necessary. Here is how to proceed:
      (i) Find N the smallest integer such that for each $t, t' \in \mathscr{F}_2$ the congruence $t \equiv t' \mod N$ implies $W(\mathscr{E}_t) = W(\mathscr{E}_{t'})$, or in other terms the smallest N for which the root number function $t \longrightarrow W(E_t)$ is N-periodic. The existence of this N is given by Theorem 1.2. The value of N depends on the coefficients of a Weierstrass equation of E and can be found with the help of Corollary 4.5).
      (ii) Then determine in which of the equivalence classes modulo N are the values of the squarefree factors of $f(t)$. Take representatives $t_1, \dots, t_n$ such that each of the $f(t_i)$ represents a class modulo N (that can be obtained). If the root number of the fibres of $E_{f(t_i)}$ all have the same value, then the root number function is constant and we are in Rohrlich's case 2. Otherwise, it varies and we are in case 1.

Let us explain this with an example:

Example 1.4. Let $a = 2 \cdot 7 \cdot 17 = 238$ and $b = 2^3 \cdot 7 \cdot 17 = 952$, and $f(t) = t^{86} + 14$. We study the variation of the root number in the fibres of the family

$$E_{f(t)} : y^2 = x^3 + 238(t^{86} + 14)^2 x + 952(t^{86} + 14)^3.$$

Note that $E : y^2 = x^3 + 238x + 952$ has multiplicative reduction over $\mathbb{Q}^{ab}$ (since 173 is a place of multiplicative reduction over $\mathbb{Q}$). Indeed, we have $\Delta(E) = -2^9 \cdot 7^2 \cdot 17^2 \cdot 173$.

First find the integer N for which E is N-periodic. For this, observe that the bad places are 2, 7 (type *II*), 17 (type *II*) and 173 (type I_1). Then by

Corollary 4.5 the root number of E_t the twist by t is

$$W(E_t) = -\prod_{p=2,3,7,17,173} w_p(t),$$

where $w_p(t)$ are local contributions at each p determined as follows:

$$w_p(t) = \begin{cases} \operatorname{sgn}(t) D_2 \left(\frac{-1}{|t_{(2)}|}\right) W_2(E) & \text{for } p = 2 \\ (-1)^{v_3(t)} D_3 W_3(E) & \text{for } p = 3 \\ D_p \left(\frac{-1}{p}\right)^{v_p(t)} W_p(E) & \text{for } p = 7, 17 \\ \left(\frac{t_{(173)}}{173}\right) D_p W_p(E) & \text{for } p = 173, \end{cases}$$

and the $D_p \in \{\pm 1\}$ are the values depending on t such that $W_p(E_t) = D_p W_p(E)$. They are given by the Lemmas 3.4, 3.6 and 3.3. Although an appropriate D_p is not always given by Lemma 3.4 or 3.6 for $p = 2, 3$ in the case of a general elliptic curve, as is the case in this example. Example 1.6 explains what to do otherwise.

- For 2: we have $(v_2(a) + 4, v_2(b) + 5, v_2(\Delta)) = (5, 8, 9)$, $b_{(2)} \equiv 3 \mod 4$ and $a_{(2)} \equiv 7 \mod 8$. According to Lemma 3.4, $w_2(t)$ the local contribution at 2 of the root number of the twists by t takes the same value for any value of $t_{(2)}$ and of $v_2(t)$: $w_2(t) = +1$.
- For 3: we have $(v_3(a) + 1, v_3(b) + 3, v_3(\Delta)) = (1, 3, 0)$. According to Lemma 3.4, w_3 the local contribution at 3 of the root number of the twists by t will take the same value for any value of $t_{(3)}$ and of $v_3(t)$: $w_3(t) = +1$.

For primes $p \neq 2, 3$, Proposition 3.3 gives the value of D_p.

- For 7 and 17, the type of reduction is II and we have:

$$w_p(t) = \begin{cases} \left(\frac{3}{p}\right)\left(\frac{-1}{p}\right) W_p(E) & \text{if } p \mid t \\ W_p(E) & \text{if } p \nmid t. \end{cases}$$

  Since $7 \equiv 1 \mod 6$ we have $w_7(t) = W_7(E) = -1$ for all t squarefree integer, and since $17 \not\equiv 1 \mod 6$ we have

$$w_{17}(t) = \begin{cases} W_{17}(E) = +1 & \text{if } v_{17}(t) \text{ even} \\ -W_{17}(E) = -1 & \text{if } v_{17}(t) \text{ odd.} \end{cases}$$

- For 173: the reduction is multiplicative, we have

$$w_{173}(E_t) = \begin{cases} \left(\frac{t}{173}\right) W_{173}(E) = \left(\frac{t}{173}\right) & \text{if } 173 \nmid t \\ -\left(\frac{-6b_{(173)}}{173}\right)\left(\frac{t_{(173)}}{173}\right) W_{173}(E) = \left(\frac{t_{(173)}}{173}\right) & \text{if } 173 \mid t \end{cases}$$

  so we have simply $w_{173}(E_t) = \left(\frac{t_{(173)}}{173}\right)$.

As a consequence, we see that $W(E_t)$ takes the same value on the congruence classes modulo $17^2 \cdot 173$, so that the root number of the twists is N-periodic for $N = 17^2 \cdot 173$. It is however somehow more convenient in this case to observe the more precise fact that it takes the same value for t and t' such that $t_{(173)} \equiv t'_{(173)} \mod 173$ and with $v_{17}(t) \equiv v_{17}(t') \mod 2$.

An easy consequence of Fermat's little theorem is that $f(t) = t^{86} + 14$ takes the values among $\{13, 14, 15\} \mod 173$. Thus we have

$$w_{173}(f(t)) = \left(\frac{f(t)_{(173)}}{173}\right).$$

This Jacobi symbol is equal to $+1$ for all squarefree t (since $(\frac{13}{173}) = (\frac{14}{173}) = (\frac{15}{173}) = +1$).

It is not so hard to check that $f(t)$ takes values among

$$\{1, 5, 6, 10, 12, 13, 15, 16\} \mod 17,$$

and in particular that $17 \nmid f(t)$ for any value of t. Thus $w_{17}(f(t)) = +1$.

This proves that the root number is constant on the family $E_{f(t)}$ and always takes the value $+1$.

Sometimes, the computation of N is not even necessary since a basic check proves that the root number varies:

Example 1.5. If we twist $E : y^2 = x^3 + 238x + 952$ by the polynomial $g(t) = t^{86} + 1$ instead: we have $W(E_{g(0)}) = W(E) = 1$ and $W(E_{g(1)}) = W(E_2) = -1$ so the root number is not constant on the family $E_{g(t)}$. (When we look in detail, we see that the variation comes from w_{173}: we have $w_{173}(1) = +1$ and $w_{173}(2) = -1$. The other contributions are such that $w_p(1) = w_p(2)$.)

In some other cases, it is more convenient to take a shortcut when we search for N, in particular when the local root number at 2 or 3 is not listed in Lemma 3.4 or 3.6. Here is an example:

Example 1.6. In our first examples, finding the appropriate N was easy because the functions $w_2(t)$ and $w_3(t)$ were constant by Lemma 3.4 and 3.6. Let us choose another base curve, say $E' : y^2 = x^3 + 2 \cdot 17x + 2^2 \cdot 17$, and study the family of twists of E' by the values of the function $h(t) = 8t^{30} + 5$:

$$E'_{h(t)} : y^2 = x^3 + 34(8t^{30} + 5)^2 x + 68(8t^{30} + 5)^3.$$

The discriminant of E' is $\Delta(E') = -2^8 17^2 61$, so the reduction of E' at 17 has type II and the reduction at 61 is I_1. The root number can be written as

$$W(E'_t) = -\prod_{p=2,3,17,61} w_p(t),$$

with $w_p(t)$ as in Corollary 4.5. Let us find them explicitly in this case.

- For 2: we have $(v_2(a)+4, v_2(b)+5, v_2(\Delta)) = (5,7,8)$, and this triple is not listed in Lemma 3.4 as one with $w_2(t)$ constant on the family E'_t. Some additional work must be done here with Rizzo's table III [12]. From there we extract the formula (for odd t):

$$W_2(E'_t) = \begin{cases} +1 & \text{if } 6\cdot 17t^2 + 27\cdot 17t^3 \equiv 1 \mod 8 \\ & \text{or if } 27\cdot 17t^3 \equiv 5 \mod 8, \\ -1 & \text{otherwise.} \end{cases}$$

  In our choice of $h(t) = 8t^{30}+5$, not only is $h(t)$ always positive and odd, but it is also always such that $h(t) \equiv 5 \mod 8$. Consequently, $102h(t)^2 + 459h(t)^3 \equiv 59925 \equiv 5 \mod 8$ and $459h(t)^3 \equiv 7 \mod 8$ for any t. This means that $W_2(E'_{h(t)}) = W_2(E') = -1$ (in particular $D_2 = +1$ for all t), and thus that

$$w_2(h(t)) = \operatorname{sgn}(h(t)) \left(\frac{-1}{h(t)}\right) D_2 W_2(E') = -1$$

  for all $t \in \mathbb{Z}$.
- By Lemma 3.6, $w_3(t) = +1$ for all t.
- Similarly as in Example 1.4, we have

$$w_{17}(t) = \begin{cases} +1 & \text{if } v_{17}(t) \text{ even,} \\ -1 & \text{if } v_{17}(t) \text{ odd} \end{cases}$$

  and

$$w_{61}(t) = \begin{cases} -\left(\frac{t}{61}\right) & \text{if } 61 \nmid t \\ \left(\frac{t}{61}\right) & \text{if } 61 \mid t. \end{cases}$$

As a consequence, the root number $W(E'_{h(t)})$ is $17^2\cdot 61$-periodic. We can be even more precise. A consequence of Fermat's little theorem is that $h(t) = 8t^{30}+5$ takes the values among $\{5,13,58\} \mod 61$. We have thus $w_{61}(h(t)) = -\left(\frac{h(t)}{61}\right) = -1$ for all t. The polynomial $h(t)$ takes values among $\{1,3,4,5,6,7,9,13,14\}$ modulo 17 and hence we always have $w_{17}(h(t)) = +1$ for all t. Thus we have for every $t \in \mathbb{Z}$:

$$W(E'_{h(t)}) = -(-1)(+1)(+1)(-1) = -1.$$

1.4. More formulae. Birch and Stephens [1] prove formulae for the root number of $y^2 = x^3 - Dx$, and for the root number of $z^3 = x^3 + A$ (this curve can be rewritten as the equation $y^2 = x^3 - 432A^2$). Liverance [11] completes these results by giving a formula for the root number of $y^2 = x^3 + D$ in the general case.

The formulae given in the points (3a) and (2a) of Theorem 1.2 have a flavor different from that found in those two papers, in particular, it distinguishes between primes $p \geq 5$ according to whether or not $p^2 \mid t$, in a similar way to the formulae of Várilly-Alvarado [15, Propositions 4.4 and 4.8].

Connell [3] computer-implemented the root number formulae from those of Rohrlich [13], Liverance [11], Birch and Stephens [1].

2. Monodromy of the reduction

2.1. For quadratic twists. Let E be the elliptic curve given by the Weierstrass equation $E : y^2 = x^3 + ax + b$, where $a, b \in \mathbb{Z} \setminus \{0\}$ and let Δ be its discriminant, that we suppose minimal. For every $t \in \mathbb{Z} \setminus \{0\}$, consider the twist of E by t, $E_t : y^2 = x^3 + at^2x + bt^3$. Tate's algorithm allows us to show the following lemma:

Lemma 2.1. *We have:*

(1) *If $v_p(t)$ is even, then E and E_t have the same type of reduction at p.*
(2) *If $v_p(t)$ is odd, then the type of E_t and E are among the following possibilities (the order is not important)*
   (a) *I_0 and I_0^**
   (b) *I_m and I_m^**
   (c) *II and IV**
   (d) *II* and IV*
   (e) *III and III**

2.2. For quartic twists. Let E be the elliptic curve given by the Weierstrass equation $E : y^2 = x^3 + ax$, where $a \in \mathbb{Z}$ is a non-zero fourth-powerfree integer. For every $t \in \mathbb{Z} \setminus \{0\}$, consider the twist of E by t:

$$E_t : y^2 = x^3 + atx.$$

The discriminant is $\Delta(E_t) = -2^6a^3t^3$. Tate's algorithm allows us to show the following lemma:

Lemma 2.2. *The reduction at $p \neq 2, 3$ of E_t has type I_0, III, I_0^*, III* if $v_p(at) \equiv 0, 1, 2, 3 \mod 4$ respectively.*

2.3. For sextic twists. Let E be the elliptic curve given by the Weierstrass equation $E : y^2 = x^3 + b$, where $b \in \mathbb{Z}$ is a non-zero sixth-powerfree integer. For every $t \in \mathbb{Z} \setminus \{0\}$, consider the twist of E by t:

$$E_t : y^2 = x^3 + bt.$$

The discriminant is $\Delta(E_t) = -2^4 3^3 b^2 t^2$. Tate's algorithm allows to show the following lemma:

Lemma 2.3. *The reduction at $p \neq 2, 3$ of E_t has type I_0, II, IV, I_0^*, IV*, II* if $v_p(bt) \equiv 0, 1, 2, 3, 4, 5 \mod 6$ respectively.*

3. Behaviour of the local root number

3.1. Local root number of a quadratic twist. For $p \neq 2,3$ a simple formula gives the local root number of an elliptic curve E according to the type of its reduction:

Proposition 3.1 ([13, Proposition 2]). *Let $p \geq 5$ be a rational prime, and let $E/\mathbb{Q}_p$ be an elliptic curve given by the Weierstrass equation*

$$E : y^2 = x^3 + ax + b,$$

where $(a,b) \in \mathbb{Z}^2 \setminus (0,0)$. Then

$$W_p(E) = \begin{cases} 1 & \text{if the reduction of } E \text{ at } p \text{ has type } I_0; \\ \left(\frac{-1}{p}\right) & \text{if the reduction has type } II,\ II^*,\ I_m^* \text{ or } I_0^*; \\ \left(\frac{-2}{p}\right) & \text{if the reduction has type } III \text{ or } III^*; \\ \left(\frac{-3}{p}\right) & \text{if the reduction has type } IV \text{ or } IV^*; \\ -\left(\frac{6b}{p}\right) & \text{if the reduction has type } I_m; \end{cases}$$

However, it is not as simple when p is 2 or 3. According to [12, 1.1], to determine the local root number at $p = 2,3$ of an elliptic curve, we must find the smallest vector (α,β,γ) with nonnegative entries such that

$$(\alpha,\beta,\delta) = (v_p(c_4), v_p(c_6), v_p(\Delta)) + k(4,6,12)$$

for $k \in \mathbb{Z}$, where c_4, c_6 and Δ are the usual quantities associated to a Weierstrass equation.

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve. For every $t \in \mathbb{Z} \setminus \{0\}$, define E_t to be the quadratic twist

$$E_t : y^2 = x^3 + at^2x + bt^3,$$

with $a, b \in \mathbb{Z}$. The Weierstrass coefficients of the twisted curve are:

$$c_4 = -2^4 \cdot 3 \cdot a \cdot t^2 \quad c_6 = -2^5 \cdot 3^3 \cdot b \cdot t^3 \quad \Delta = -2^4 \cdot (4a^3 + 27b^2)t^6,$$

whence

$$(\alpha,\beta,\delta) = (v_p(a), v_p(b), v_p(\Delta)) + (2v_p(t), 3v_p(t), 6v_p(t)) + \begin{cases} (4,5,0) & \text{if } p = 2 \\ (1,3,0) & \text{if } p = 3 \end{cases}$$

The root number is given by the entry of Rizzo's Table II (if $p = 3$) or Table III (if $p = 2$) corresponding to (α,β,δ).

3.1.1. *Periodicity.*

Lemma 3.2. *For every prime p, the function $t \mapsto W_p(E_t)$ is periodic.*

Proof. Let t be an integer, and let $t = t_0 t_{(\Delta)}$ be a decomposition such that t_0 is a product of prime factors of Δ (the discriminant of E) and $t_{(\Delta)}$ is an integer coprime with Δ. Let $\Delta_{E_t} = \Delta t^6$ be the discriminant of E_t. By Tate's algorithm, the reduction at p depends only on the triple $(v_p(c_4), v_p(c_6), v_p(\Delta t^6))$.

If $p \geq 5$ and $v_p(t) = 2$, we have $v_p(\Delta_{E_t}) = v_p(\Delta) + 12 v_p(t_{(\Delta)})$. Since $p \nmid t_{(\Delta)}$, then $v_p(\Delta_{E_t}) = v_p(\Delta)$. Yet, we know that the root number of a curve stays the same under a twist by a twelfth-power. Knowing t modulo p^2 suffices thus to know $W_p(E_t)$.

For $p = 2, 3$ and $l = 4, 6$, let $c_{l,p}$ be the integers such that $c_l = p^{v_p(t)} c_{l,p}$. The formulae found in the tables in [9] depend only of the 2-adic and 3-adic valuation of c_4 and c_6 as well as the remainder of $c_{4,2}$, $c_{4,3}$, $c_{6,2}$, $c_{6,3}$ modulo a certain power of 2 or 3. $\square$

3.1.2. *Variation of the local root number at p ≥ 5 when twisting.* Let $p \neq 2, 3$ be a prime number, and $t \in \mathbb{Z} \setminus \{0\}$ a squarefree integer. In the following, we compare $W_p(E)$ and $W_p(E_t)$.

Proposition 3.3. *Put $D_p \in \{-1, +1\}$ the integer such that $W_p(E) = D_p W_p(E_t)$. We have*

(1) *if $p \nmid t$*

$$D_p = \begin{cases} +1 & \text{if } E \text{ has good or additive reduction} \\ \left(\frac{t}{p}\right) & \text{if } E \text{ has multiplicative reduction} \end{cases}$$

(2) *if $p \mid t$*

$$D_p = \begin{cases} +1 & \text{if } E \text{ has type } III \text{ or } III^* \\ \left(\frac{-1}{p}\right) & \text{if } E \text{ has type } I_0 \text{ or } I_0^* \\ \left(\frac{3}{p}\right) & \text{if } E \text{ has type } II, II^*, IV, IV^* \\ -\left(\frac{-6 b_{(p)} t_{(p)}}{p}\right) & \text{if } E \text{ has type } I_m \text{ or } I_m^* \ (m \geq 1) \end{cases}$$

Proof. The value of D_p depends of the type of reduction at p of E.

(1) If $p \nmid t$ and the reduction of E is not multiplicative, one has $D_p = +1$. If the reduction has type I_m, then

$$D_p = \left(\frac{t}{p}\right),$$

because

$$W_p(E_t) = -\left(\frac{-6 b_{(p)} t^3}{p}\right) = -\left(\frac{-6 b_{(p)}}{p}\right)\left(\frac{t}{p}\right) = W_p(E_t)\left(\frac{t}{p}\right).$$

(2) If $p \mid t$, one of the following cases occurs, according to the type of variation of E at p.

(a) If E has type I_0, then E_t has type I_0^*. Conversely, if E_t has type I_0^*, then E_{pt} has type I_0. The local root number at p changes from $(\frac{-1}{p})$ to $+1$. We have $D_p = (\frac{-1}{p})$.

(b) If E has type II, then E_t has type IV^*. Conversely, if E_t has type IV^*, then E_{pt} has type II. The local root number at p changes from $(\frac{-1}{p})$ to $(\frac{-3}{p})$. We have $D_p = (\frac{3}{p})$.

(c) If E has type III, then E_t has type III^* and conversely. The local root number at p changes from $(\frac{-2}{p})$ to $(\frac{-2}{p})$. We have $D_p = +1$.

(d) If E has type I_m^*, then E_t has type I_m and conversely. The local root number at p changes from $(\frac{-1}{p})$ to $-\left(\frac{-6b_{(p)}t_{(p)}}{p}\right)$. We have $D_p = -\left(\frac{6b_{(p)}t_{(p)}}{p}\right)$.

$I_0^* \leftrightarrow I_0$	$II \leftrightarrow IV^*$
$\left(\frac{-1}{p}\right) \xrightarrow{D_p=(\frac{-1}{p})} +1$	$\left(\frac{-1}{p}\right) \xrightarrow{D_p=(\frac{3}{p})} \left(\frac{-3}{p}\right)$
$III \leftrightarrow III^*$	$I_m^* \leftrightarrow I_m$
$\left(\frac{-2}{p}\right) \xrightarrow{D_p=+1} \left(\frac{-1}{p}\right)$	$\left(\frac{-1}{p}\right) \xrightarrow{D_p=-\left(\frac{6b_{(p)}t_{(p)}}{p}\right)} -\left(\frac{-6b_{(p)}t_{(p)}}{p}\right).$

□

3.1.3. *Local root number at* $p = 2$.

Lemma 3.4. *We have* $W_2(E_t) = \epsilon_2 \cdot \mathrm{sgn}(t)(\frac{-1}{|t_{(2)}|})$ *(for a fixed* $\epsilon_2 \in \{-1, +1\}$*) for all* $t \in \mathbb{Z}$ *if and only if the triple* $(v_2(a) + 4, v_2(b) + 5, v_2(\Delta))$ *is among the following:*

(1) $(0, 0, 0)$ *or* $(2, 3, 6)$ *(then* $\epsilon_2 \equiv -b_{(2)} \mod 4$*); or*

(2) $(3, 5, 3)$ *or* $(5, 8, 9)$ *and*

  (a) $a_{(2)} \equiv 3 \mod 8$ *and* $b_{(2)} \equiv 3 \mod 4$*; or* $a_{(2)} \equiv 7 \mod 8$ *and* $b_{(2)} \equiv 1 \mod 4$ *(then* $\epsilon_2 = -1$*)*

  (b) $a_{(2)} \equiv 3 \mod 8$ *and* $b_{(2)} \equiv 1 \mod 4$*; or* $a_{(2)} \equiv 7 \mod 8$ *and* $b_{(2)} \equiv 3 \mod 4$ *(then* $\epsilon_2 = +1$*)*

(3) $(\geq 4, 3, 0)$ *or* $(\geq 6, 6, 6)$ *(then* $\epsilon_2 \equiv b_{(2)} \mod 4$*).*

We deduce the following:

Corollary 3.5. *The cases listed in Theorem 3.4 are the only one such that for every* $t \in \mathbb{Z} \setminus \{0\}$*, one has*

$$W(E_t) = \mathrm{sgn}(t) \left(\frac{-1}{|t_{(2)}|}\right) W(E),$$

where D_2 is the integer depending on t such that $W_2(E_t) = D_2 W_2(E)$. In particular, we have $D_2 = \epsilon_2 \cdot \mathrm{sgn}(t)(\frac{-1}{|t_{(2)}|})$ and so the function w_2 defined in Corollary 4.5 is constant and $w_2(t) = \epsilon_2$.

Proof. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve and let Δ be its discriminant. For every squarefree $t \in \mathbb{Z} \setminus \{0\}$, consider the twist of E by t, $E_t : ty^2 = x^3 + ax + b$.

We list here the conditions of the coefficients a, b and Δ for the root number at 2 of the fibres E_t to be $W_2(t) = \mathrm{sgn}(t)(\frac{-1}{t_{(2)}})$ for all positive t and $-(\frac{-1}{-t_{(2)}})$ for all negative t. We can classify the curves E by their triple $(v_2(a) + 4, v_3(b) + 5, v_2(\Delta))$: a formula for their local root number at 2 is given by the table of Rizzo [12, Table III]. (In Rizzo, the notation with the c-invariants is preferred. Note that $(c_6)_{(2)} = 3b_{(2)}$ and that $(c_4)_{(2)} = 3^3 a_{(2)}$.). The first step is to select the surfaces such that $W_2(E_t) = \epsilon \cdot \mathrm{sgn}(t)(\frac{-1}{|t|})$ when $2 \nmid t$, for a fixed $\epsilon \in \{\pm 1\}$. To find the triples and determine the additional conditions, we proceed in the following way. (We only give three examples here, the other cases being treated in a similar manner.)

If $(v_2(a) + 4, v_2(b) + 5, v_2(\Delta)) = (0, 0, 0)$, then Rizzo's table gives the following formula for the root number of the fibres in odd t:

$$W_2(E_t) = \begin{cases} +1 & \text{if } b_{(2)}t^3 \equiv 1 \mod 4 \\ -1 & \text{otherwise.} \end{cases}$$

We want $W_2(E_t) = +1 \Leftrightarrow t \equiv 1 \mod 4$, which is possible if and only if $b_{(2)} \equiv 1 \mod 4$.

For some triples though, the local root number at 2 of E_t does not behave the way we want. For instance in the case of the triple $(v_2(a) + 4, v_2(b) + 5, v_2(\Delta)) = (3, 3, 0)$. In this case, the local root number is

$$W_2(E_t) = \begin{cases} +1 & \text{if } a_{(2)}t^2 \equiv 3 \mod 4 \text{ and if } b_{(2)}t \equiv \pm 3 \mod 8, \\ & \text{if } a_{(2)}t^2 \equiv 1 \mod 4 \text{ and if } b_{(2)}t \equiv 1, 3 \mod 8, \\ -1 & \text{otherwise.} \end{cases}$$

In any case of $a_{(2)} \mod 4$ and $b_{(2)} \mod 8$, there will be values of $t \mod 8$ such that $W_2(E_t) \neq \mathrm{sgn}(t)\left(\frac{-1}{|t|}\right)$. For instance, if $b_{(2)} \equiv 3 \mod 4$ and $a_{(2)} \equiv 1 \mod 16$, then $W_2(E_t) = +1$ if and only if $t \equiv 5 \mod 8$.

Proceding in a similar manner for all the other triples, we determine the triple, and the special conditions for which $t \mapsto W_2(E_t)$ behaves like $\mathrm{sgn}(t)\left(\frac{-1}{|t_{(2)}|}\right)$. We obtain the list given in Table 3.1. We have double checked every computation with the computation software MAGMA.

TABLE 3.1. Cases where $W_2(E_t) = \epsilon \cdot \mathrm{sgn}(t) \cdot \left(\frac{-1}{|t|}\right)$ for every *odd* squarefree $t \in \mathbb{Z} - 0$.

$(v_2(a)+4, v_2(b)+5, v_2(\Delta))$ (of a minimal model)	Special conditions	ϵ
$(0,0,0)$	$b_{(2)} \equiv 1 \mod 4$	$+1$
	$b_{(2)} \equiv 3 \mod 4$	-1
$(\geq 4,3,0)$	$b_{(2)} \equiv 1 \mod 4,$	$+1$
	$b_{(2)} \equiv 3 \mod 4$	-1
$(2,3,\geq 4)$	$b_{(2)} \equiv 1 \mod 4,$	-1
	$b_{(2)} \equiv 3 \mod 4,$	$+1$
$(\geq 4,4,2)$	$b_{(2)} \equiv 1 \mod 4$	$+1$
	$b_{(2)} \equiv 3 \mod 4$	-1
$(3,5,3)$	$a_{(2)} \equiv 3,5 \mod 8,\ b_{(2)} \equiv 3 \mod 4$	-1
	$a_{(2)} \equiv 1,7 \mod 16,\ b_{(2)} \equiv 1 \mod 4$	
	$a_{(2)} \equiv 3,5 \mod 8,\ b_{(2)} \equiv 1 \mod 4$	$+1$
	$a_{(2)} \equiv 1,7 \mod 16,\ b_{(2)} \equiv 3 \mod 4$	
$(5,8,9)$	$a_{(2)} \equiv 5,7 \mod 8,\ b_{(2)} \equiv 3 \mod 4$	$+1$
	$a_{(2)} \equiv 1,3 \mod 16,\ b_{(2)} \equiv 1 \mod 4$	
	$a_{(2)} \equiv 5,7 \mod 8,\ b_{(2)} \equiv 1 \mod 4$	-1
	$a_{(2)} \equiv 1,3 \mod 16,\ b_{(2)} \equiv 3 \mod 4$	
$(\geq 6,6,6)$	$b_{(2)} \equiv 1 \mod 4$	$+1$
	$b_{(2)} \equiv 3 \mod 4$	-1
$(4,6,7)$	$b_{(2)} \equiv 3 \mod 4,\ a_{(2)} \equiv 7 \mod 8$	$+1$
	$b_{(2)} \equiv 1 \mod 4,\ a_{(2)} \equiv 7 \mod 8$	-1
$(\geq 7,7,8)$	$b_{(2)} \equiv 1 \mod 4$	$+1$
	$b_{(2)} \equiv 3 \mod 4$	-1
$(6,8,10)$	$a_{(2)}b_{(2)} \equiv 3 \mod 4$	$+1$
	$a_{(2)}b_{(2)} \equiv 1 \mod 4$	-1
$(\geq 7,8,10)$	$b_{(2)} \equiv 1 \mod 4$	$+1$
	$b_{(2)} \equiv 3 \mod 4$	-1

The final step is to retain only the triples such that $W_2(E_{2t}) = W_2(E_t)$. For every case of the list, we check if the triple $(v_2(a)+2, v_2(b)+3, v_2(\Delta)+6)$ (the triple associated to a fibre at $2t$ for $t \in \mathbb{Z}$ odd) also gives a local root number at 2 equal to $W_2(\mathscr{E}_{2t}) = \epsilon \cdot \mathrm{sgn}(t) \left(\frac{1}{|t|}\right)$ (for the same ϵ). A list of the monodromy of the triples, as well as whether or not those pairs figure in Table 3.1. This way we find the cases listed in the statement of the theorem (note that for $(3,5,3)$ and $(5,8,9)$ this only works for specific classes of $a_{(2)}$ and $b_{(2)}$). □

TABLE 3.2.

Monodromy of $(v_2(a)+4, v_2(b)+5, v_2(\Delta))$	Are triples in Table 3.1
$(0,0,0) \longleftrightarrow (2,3,6)$	yes, yes
$(0,0,>0) \longleftrightarrow (2,3,>6)$	no, no
$(3,3,0) \longleftrightarrow (5,5,6)$	no, no
$(\geq 4,3,0) \longleftrightarrow (\geq 6,6,6)$	yes, yes
$(2,4,0) \longleftrightarrow (4,7,6)$	no, no
$(2,\geq 5,0) \longleftrightarrow (4,\geq 8,6)$	no, no
$(2,3,1) \longleftrightarrow (4,6,7)$	no, no
$(2,3,2) \longleftrightarrow (4,6,8)$	no, no
$(2,3,3) \longleftrightarrow (4,6,7)$	no, no
$(2,3,\geq 4) \longleftrightarrow (4,6,\geq 8)$	yes, no
$(3,4,2) \longleftrightarrow (5,7,8)$	no, no
$(3,5,3) \longleftrightarrow (5,8,9)$	yes, yes
$(4,4,2) \longleftrightarrow (6,7,8)$	yes, no
$(\geq 5,4,2) \longleftrightarrow (\geq 7,7,8)$	yes, no
$(4,5,4) \longleftrightarrow (6,8,10)$	no, yes
$(\geq 5,5,4) \longleftrightarrow (\geq 7,8,10)$	no, yes

3.1.4. *Local root number at $p = 3$.*

Lemma 3.6. *We have $W_3(E_t) = \epsilon_3 \cdot (-1)^{v_3(t)}$ for all $t \in \mathbb{Z}$ (for a fixed $\epsilon_3 = \pm 1$) if and only if the triple of values $(v_3(a)+1, v_3(b)+3, v_3(\Delta))$ is one of the following:*

(1) $(0,0,0)$, $(1,\geq 3,0)$, *and* $(1,2,0)$ *with* $a_{(3)} \equiv 2 \mod 3$ *(then* $\epsilon_3 = +1$*)*
(2) $(2,3,6)$, $(3,\geq 6,6)$, *and* $(3,5,6)$ *with* $a_{(3)} \equiv 2 \mod 3$ *(then* $\epsilon_3 = -1$*)*

Corollary 3.7. *The cases listed in Theorem 3.6 are the only ones such that for every $t \in \mathbb{Z} \setminus \{0\}$, one has*

$$W(E_t) = (-1)^{v_3(t)} W(E).$$

In particular, we have $D_3 = \epsilon_3 \cdot (-1)^{v_3(t)} W(E)$ (D_3 is the integer depending on t such that $W_3(E_t) = D_3 W_3(E)$) and so the function w_3 defined in Example 1.4 or Corollary 4.5 is constant and $w_3(t) = \epsilon_3$.

Proof. Let $t \in \mathbb{Z} \setminus \{0\}$ be an integer.

Suppose that t satisfies $3 \nmid t$. Then the local root number at 3 is given by the entry of [12, Table II] corresponding to $(v_3(a)+1, v_3(b)+3, v_3(\Delta))$. If $v_3(t)$ is odd, then the triple is $(v_3(a)+3, v_3(b)+6, v_3(\Delta)+6)$ and the corresponding entry gives the local root number. We double-checked every computation using the software MAGMA.

We start by selecting the triples such that $W_3(E_t) = W_3(E) = \epsilon_3$ for all $t \in \mathbb{Z}$ prime to 3 (for some fixed $\epsilon_3 \in \{\pm 1\}$). The list is given in Table 3.3.

TABLE 3.3. Cases where $W_3(E_t) = \epsilon_3$ for every squarefree $t \in \mathbb{Z} \setminus 0$ not divisible by 3.

$(v_3(a)+1, v_3(b)+3, v_3(\Delta))$	Special conditions	ϵ_3
$(0,0,0)$,		$+1$
$(1,\geq 3,0)$,		$+1$
$(1,2,0)$,		$+1$
$(2,\geq 5,3)$		$+1$,
$(2,3,3)$	if $a_{(3)} \equiv 1 \mod 3$, $b_{(3)} \equiv 4,5 \mod 9$	$+1$,
$(2,3,4)$		$+1$,
$(2,3,6)$		-1
$(2,3,\geq 7)$		-1
$(2,3,4)$ $(2,\geq 5,3)$		$+1$ $+1$
$(\geq 3,3,3)$	$b_{(2)} \equiv 1,8 \mod 9$	$+1$
$(3,5,6)$	if $a_{(3)} \equiv 1 \mod 3$ $a_{(3)} \equiv 2 \mod 3$	$+1$ -1
$(3,\geq 6,6)$		-1
$(4,6,9)$	if $a_{(3)} \equiv 1 \mod 3$, $b_{(3)} \equiv 4,5 \mod 9$	$+1$,
$(4,\geq 8,9)$		$+1$
$(\geq 5,6,9)$	$b_{(2)} \equiv 1,8 \mod 9$	$+1$

Now, we check among those triples whether they have the property that $W(E_{3t}) = -W(E_t)$, by verifying that both the triple of E and the triple of a twist by 3 are in Table 3.3 (these facts are listed in Table 3.4) and comparing the values of ϵ_3. We retain only $(0,0,0)$, $(2,3,6)$, $(1,\geq 3,0)$ $(3,\geq 6,6)$, and finally $(1,2,0)$ and $(3,5,6)$ with the additional condition that $a_{(3)} \equiv 2 \mod 3$. It is important to notice that in the following cases, although the triple $(v_3(a)+1, v_3(b)+3, v_2(\Delta))$ and the triple of a quadratic twist by 3 are both in Table 3.3, we have $W_3(E_t) = W_3(E_{3t})$ rather than $W(E_t) = -W(E_{3t})$ as required: $(2,3,3)$ and $(4,6,9)$ with the additional condition that $a_{(3)} \equiv 1 \mod 3$ and $b_{(3)} \equiv 4,5 \mod 9$, and $(\geq 3,3,3)$ and $(\geq 5,6,9)$ with the additional condition that $b_{(3)} \equiv \pm 1 \mod 9$.

A yes in the second column of Table 3.4 means that the triple is in Table 3.3, but under special conditions. If there is no special condition to take account of, they the table tells the value of the function $W_3(\mathscr{E}_t)$. □

3.2. Root number of a quartic twist.

Lemma 3.8 ([15, Lemme 4.7]). *Let t be a non-zero integer and define the elliptic curve $E_t : y^2 = x^3 + tx$. We denote by $W_2(t)$ and $W_3(t)$ its local root*

TABLE 3.4.

Monodromy of $(v_3(a)+1, v_3(b)+3, v_3(\Delta))$	Are triples in Table 3.3
$(0,0,0) \longleftrightarrow (2,3,6)$	$+1$, -1
$(0,0,>0) \longleftrightarrow (2,3,>6)$	no, -1
$(1,2,0) \longleftrightarrow (3,5,6)$	$+1$, yes
$(1,\geq 3,0) \longleftrightarrow (3,\geq 6,6)$	$+1$, -1
$(\geq 2,2,1) \longleftrightarrow (\geq 4,5,7)$	no, no
$(2,3,3) \longleftrightarrow (4,6,9)$	yes, yes
$(\geq 3,3,3) \longleftrightarrow (\geq 5,6,9)$	yes, yes
$(2,4,3) \longleftrightarrow (4,7,9)$	no, no
$.(2,\geq 5,3) \longleftrightarrow (4,\geq 8,9)$	$+1$, $+1$
$(2,3,4) \longleftrightarrow (4,6,10)$	$+1$, no
$(2,3,5) \longleftrightarrow (4,6,11)$	no, no
$(\geq 3,4,5) \longleftrightarrow (\geq 5,7,11)$	no, no

numbers at 2 and 3. Let $t_{(2)}$ be the integer such that $t = 2^{v_2(t)}t_{(2)}$. Then

$$W_2(t) = \begin{cases} -1 & \text{if } v_2(t) \equiv 1 \text{ or } 3 \mod 4 \text{ and } t_{(2)} \equiv 1,3 \mod 8; \\ & \text{or if } v_2(t) \equiv 0 \mod 4 \text{ and } t_{(2)} \equiv 1,5,9,11,13,15 \text{ mod} 16; \\ & \text{or if } v_2(t) \equiv 2 \mod 4 \text{ and } t_{(2)} \equiv 1,3,5,7,11,15 \text{ mod} 16; \\ +1 & \text{otherwise.} \end{cases}$$

$$W_3(t) = \begin{cases} -1 & \text{if } v_3(t) \equiv 2 \mod 4; \\ +1 & \text{otherwise.} \end{cases}$$

We may reformulate this theorem as follows:

Lemma 3.9. *The function of the local root number at 2 on the fourth-powerfree integers, defined as $t \mapsto W_2(\mathscr{E}_t)$, is 2^4-periodic on $\mathscr{F}_4$ and it takes the value -1 if and only if $t \in [2^k a]$ the congruence class mod 2^4, where $k = 1,3 \mod 4$ and $a \equiv 1,3 \mod 8$; or $k = 0$ and $a \equiv 1,5,9,11,13,15 \mod 16$; or $k = 2$ and $a \equiv 1,3,5,7,11,15 \mod 16$.*

Lemma 3.10. *The function of the local root number at 3 on the fourth-powerfree integers, defined as $t \mapsto W_3(\mathscr{E}_t)$, is 3^4-periodic on $\mathscr{F}_4$ and it takes the value -1 if and only if $t \in [3^2 a]$ the congruence class mod 3^4, where $a \in \mathbb{Z}$.*

3.3. Root number of a sextic twist.

Lemma 3.11 ([15, Lemma 4.1])**.** *Let t be a non-zero integer and the elliptic curve $E_t : y^2 = x^3 + t$. We denote by $W_2(t)$ and $W_3(t)$ its local root numbers at 2 and 3. Put $t_{(2)}$ and $t_{(3)}$ the integers such that $t = 2^{v_2(t)}t_{(2)} = 3^{v_3(t)}t_{(3)}$.*

Then

$$W_2(t) = \begin{cases} -1 & \textit{if } v_2(t) \equiv 0 \textit{ or } 2 \mod 6; \\ & \textit{or if } v_2(t) \equiv 1,3,4 \textit{ or } 5 \mod 6 \textit{ and } t_{(2)} \equiv 3 \mod 4; \\ +1, & \textit{otherwise.} \end{cases}$$

$$W_3(t) = \begin{cases} -1 & \textit{if } v_3(t) \equiv 1 \textit{ or } 2 \mod 6 \textit{ and } t_{(3)} \equiv 1 \mod 3; \\ & \textit{or if } v_3(t) \equiv 4 \textit{ or } 5 \mod 6 \textit{ and } t_{(3)} \equiv 2 \mod 3; \\ & \textit{or if } v_3(t) \equiv 0 \mod 6 \textit{ and } t_{(3)} \equiv 5 \textit{ or } 7 \mod 9; \\ & \textit{or if } v_3(t) \equiv 3 \mod 6 \textit{ and } t_{(3)} \equiv 2 \textit{ or } 4 \mod 9; \\ +1, & \textit{otherwise.} \end{cases}$$

We may reformulate this theorem as follows:

Lemma 3.12. *The function of the local root number at 2 defined as $t \mapsto W_2(\mathscr{E}_t)$ is 2^6-periodic on $\mathscr{F}_6$ and it takes the value $+1$ if and only if $t \in [2^k a]$ the congruence class mod 2^6, where $k \in \{1,3,4,5\}$ and $a \equiv 3 \mod 4$.*

Lemma 3.13. *The function of the local root number at 3 defined as $t \mapsto W_3(\mathscr{E}_t)$ is 3^6-periodic on $\mathscr{F}_6$ and it takes the values -1 if and only if $t \in [3^k a]$ the congruence class mod 3^6, where $k \in \{1,2\}$ and $a \equiv 1 \mod 3 \mod 4$; $k \in \{4,5\}$ and $a \equiv 2 \mod 3 \mod 4$; $k = 0$ and $a \equiv 5,7 \mod 3 \mod 4$; or $k \in \{1,2\}$ and $a \equiv 2,4 \mod 3 \mod 4$.*

4. Proof of the main theorem

4.1. Families of quadratic twists.

Theorem 4.1. *Let E be an elliptic curve such that $j(E) \neq 0, 1728$. Define $\mathscr{F}_2$ to be the set of squarefree integers. Then*

(1) *the function $t \mapsto W(\mathscr{E}_t)$ is periodic on $\mathscr{F}_2$,*
(2) *the root number $W(\mathscr{E}_t)$ is not constant when t runs through $\mathbb{Z} \setminus \{0\}$.*

The proof of this theorem is based on the following lemma of independent interest.

Lemma 4.2. *Let E be an elliptic curve.*

Suppose that for all positive squarefree integer $t \in \mathbb{N}$ one has $W(E_t) = W(E)$. This happens if and only if the elliptic curve E has the following properties:

(a) *there is no finite place of multiplicative reduction except possibly at 2 or 3;*
(b) *for all t non-zero squarefree integers one has $W_2(E_t) = W_2(E) \cdot \operatorname{sgn}(t) \cdot \left(\frac{-1}{|t_{(2)}|}\right)$;*
(c) *for all t non-zero squarefree integers one has $W_3(E_t) = W_3(E) \cdot (-1)^{v_3(t)}$;*

(d) *if there exists* $p \mid \Delta_{(6)}$ *then:*
   (i) *if the reduction of* E *at* p *has type III or III*, then* $p \equiv 1 \mod 4$*;*
   (ii) *if the reduction of* E *at* p *has type II, II*, IV or IV*, then* $p \equiv 1 \mod 6$*;*
   (iii) *the reduction at* p *is not additive potentially multiplicative.*

Remark 4.3. The elliptic curves E with property (b) or (c) are respectively given by Lemma 3.4 or 3.6.

Example 4.4. Let $E_{+1} : y^2 = x^3 - 91x + 182$ and $E_{-1} : y^2 = x^3 - 91 - 182$. For any $t \in \mathbb{N}$, the quadratic twist of E_{+1} by t has root number $+1$ and the quadratic twist of E_{-1} has root number -1. Indeed, the discriminant of these elliptic curves is $\Delta = 2^{12}7^2 13^2$. So we have:

(a) The only finite place of multiplicative reduction is in 2.
(b) By Lemma 3.4, $W_2(E_t) = W_2(E) \cdot \operatorname{sgn}(t)\left(\frac{-1}{|t_{(2)}|}\right)$ because the associated triple of a minimal model of E_t is $(v_2(c_4), v_2(c_6), v_2(\Delta)) = (0, 0, 0)$.
(c) By Lemma 3.6, $W_3(E_t) = W_3(E) \cdot (-1)^{v_3(t)}$ because the associated triple of a minimal model of E_t is $(v_2(c_4), v_2(c_6), v_2(\Delta)) = (1, 3, 0)$ and $a_{(3)} \equiv 2 \mod 3$.
(d) The only prime dividing $\Delta_{(6)}$ are 7 and 13, for both of them the reduction has type *II* and that $p \equiv 1 \mod 6$

Proof of Theorem 4.1. Let E_t be the elliptic curve obtained by the twist by $t \in \mathbb{Z}$ of the elliptic curve $E : y^2 = x^3 + ax + b$ with integer coefficients $a, b \in \mathbb{Z}$. Put $\Delta = \Delta(E) = 2^{v_2(\Delta)}3^{v_3(\Delta)}\Delta_{(6)}$ the discriminant of E that we suppose minimal.

The root number can be written as

$$W(E_t) = -W_2(E_t)W_3(E_t) \prod_{p|t; p\nmid 6\Delta} W_p(E_t) \prod_{p|\Delta_{(6)}} W_p(E_t).$$

The places at $p \mid t$ such that $p \nmid \Delta$ have reduction type I_0^* on E_t, and thus by Proposition 3.1 one has $W_p(E_t) = \left(\frac{-1}{p}\right)$.

$$W(E_t) = -W_2(E_t)W_3(E_t)\left(\frac{-1}{|t_{(6\Delta)}|}\right)\left(\prod_{p|\Delta_{(6)}} W_p(E_t)\right).$$

We have $\Delta(E_t) = \Delta t^6$. Since t is assumed squarefree, the equation of the twist E_t is minimal unless $\gcd(\Delta, t) \neq 1$.

Proof of the first property. For each prime p, Lemma 3.2 proves that there exists an integer α_p such that $W_p(E_t) = W_p(E_{t'})$ for all $t \equiv t' \mod p^{\alpha_p}$. Put $N = 2^{\alpha_2}3^{\alpha_3}\prod_{p|\Delta_{(6)}} p^{\alpha_p}$. The global root number is the same for t and t', squarefree integers in the same congruence class modulo N.

Proof of the second property. It is now left to show that this partition is not trivial, in other words that there exists at least one congruence class $[t_+]$ with root number $+1$ and one class $[t_-]$ with root number -1.

By Lemma 4.2, we know that if E does not satisfy one or more of the properties (a) to (d), then there exists such $t_+, t_- \in \mathbb{N}$. Suppose then that E satisfies the properties (a) to (d). Then by Lemma 4.2, $W(E_t) = W(E)$ for any squarefree positive $t \in \mathbb{N}$. We compare the twists $E_1(= E)$ and E_{-1}, then by Proposition 3.3 combined with the fact that E has no multiplicative reduction, for $p \neq 2, 3$ we have $W_p(E_{-1}) = W_p(E)$. The global root numbers are thus related as follows:

$$W(E_{-1}) = -W_2(E_{-1})W(E_{-1}) \prod_p W_p(E_1)$$

Observe that by assumption of property b),

$$W_2(E_{-1}) = W_2(E) \cdot \operatorname{sgn}(-1) \left(\frac{-1}{|-1|} \right) = -W_2(E)$$

(by convention, $(\frac{-1}{1}) = 1$). Moreover by assumption of property c),

$$W_3(E_{-1}) = (-1)^{v_3(-1)} W_3(E) = W_3(E).$$

Thus

$$W(E_{-1}) = -W_2(E)W_3(E) \prod_{p \neq 2,3} W_p(E) = W(E). \qquad \square$$

Proof of Lemma 4.2. By Theorem 4.1's first property, the root number is periodic on the squarefree integers. In other words there exists a positive integer N such that for $t \equiv t' \mod N$ we have $W(E_t) = W(E_{t'})$. Hence in particular any $t \equiv 1 \mod N$ will have the same global root number as $W(E)$.

We look for a congruence class $[t_-] \mod N$ such that $W(E_{t_-}) = -W(E)$.

Let t be a non-zero squarefree integer. For each prime p, let $D_p \in \{+1, -1\}$ be the integer depending on t such that $W_p(E_t) = D_p W_p(E)$. In Proposition 3.3, we already computed the values of D_p (for $p \neq 2, 3$) according to the reduction of E at p and to whether p divides t.

One has

$$W(E_t) = - \prod_{p | \Delta t} (D_p W_p(E)) = \left(\prod_{p|\Delta t} D_p \right) W(E),$$

which we can split the following way:

$$W(E_t) = D_2D_3\left(\prod_{p\mid\Delta_{(6)};p\nmid t} D_p\right)\left(\prod_{p\mid t} D_p\right)W(E)$$

$$= D_2D_3\left(\prod_{\substack{p\nmid 6t\\ p\text{ mult.}}} D_p\right)\left(\prod_{\substack{p\nmid 6t\\ p\text{ add.}}} D_p\right)\left(\prod_{\substack{p\mid t\\ p\text{ is }I_0}} D_p\right)\left(\prod_{\substack{p\mid t\\ p\text{ not }I_0}} D_p\right)W(E)$$

and Proposition 3.3 gives

$$= D_2D_3\left(\prod_{\substack{p\nmid 6t\\ p\text{ mult.}}} \left(\frac{t}{p}\right)\right)\left(\prod_{\substack{p\mid t\\ p\text{ is }I_0}} \left(\frac{-1}{p}\right)\right)\left(\prod_{\substack{p\mid t\\ p\text{ not }I_0}} D_p\right)W(E)$$

so that

$$W(E_t) = D_2D_3\left(\frac{t}{\Delta_M}\right)\left(\frac{-1}{|t_{(6\Delta)}|}\right)\left(\prod_{\substack{p\mid t\\ E\text{ has bad red.}}} D_{p_0}\right)W(E_t),$$

where Δ_M is the product of the prime numbers $p \neq 2,3$ at which the reduction of E has multiplicative reduction. Let $t_{(6\Delta)'}$ be the integer such that

$$t = \operatorname{sgn}(t)\cdot 2^{v_2(t)}3^{v_3(t)}t_{(6\Delta)'}t_{(6\Delta)},$$

that is to say $t_{(6\Delta)'} = \prod_{p\mid\Delta_{(6)}} p^{v_p(t)}$. We can write

$$\left(\frac{-1}{|t_{(6\Delta)}|}\right) = \operatorname{sgn}(t)\left(\frac{-1}{|t_{(2)}|}\right)(-1)^{v_3(t)}\left(\frac{-1}{|t_{(6\Delta)'}|}\right).$$

Let

$$C_2 = \operatorname{sgn}(t)\cdot D_2\left(\frac{-1}{|t_{(2)}|}\right),\quad C_3 = D_3(-1)^{v_3(t)},\quad C_M = \left(\frac{t}{\Delta_M}\right),$$

$$C_0 = \prod_{\substack{p\mid t\\ E\text{ has add. red.}}} D_p,\quad C_\Delta = \left(\frac{-1}{t_{(6\Delta)'}}\right)$$

so that

$$C = C_2C_3C_MC_0C_\Delta,$$

is the integer depending on t such that $W(E_t) = C\cdot W(E)$. In the remainder of the proof, we study in more detail the variation of each component in dependance of t.

Observe that it is always possible to find t such that $C_2 = +1$ (or $C_3 = +1$), a trivial example being $t = 1$. We now look at multiple ways to obtain $C = -1$ for a certain positive integer t, depending on the properties of E.

(a). Suppose E admits places of multiplicative reduction, i.e. $\Delta_M \neq 1$. Let t_0 be a prime number with the following properties:

- it does not divide $\Delta_{(6)}$, (so that $C_\Delta = C_0 = +1$)
- it is not a square modulo Δ_M (so that $C_M = -1$)
- and it is such that $C_2 = +1$ and $C_3 = +1$.

Such a prime exists by the Chinese Remainder Theorem. For this p_0, we have

$$W(E_{p_0}) = -W(E).$$

However, in case $\Delta_M = 1$, this construction is not possible, since one has $C_M = +1$ for any squarefree integer t. Suppose thus that E has no multiplicative reduction at any $p \neq 2, 3$ and let us look at what we can do instead.

Suppose that there exists a positive $t_0 \nmid \Delta_{(6)}$ such that for the twist E_{t_0} one has $C_2 = -1$, then by the Chinese Remainder Theorem we can choose a positive $t \nmid \Delta_6$ (in addition we may assume that it is squarefree) respecting $t \equiv t_0 \mod 2^{\alpha_2}$ and such that $C_3 = C_M = C_0 = +1$. For this t, one has $W(E_t) = -W(E)$. In a similar way, if there exists a positive $t'_0 \nmid \Delta$ such that $C_3 = -1$, then one can find a $t' \in \mathbb{N}$ such that $W(E'_t) = -W(E)$.

Thus it is necessary for the triple $(v_p(c_4), v_p(c_6), v_p(\Delta))$ to be among those listed in Lemma 3.4 when $p = 2$ and among those listed in the Lemma 3.6 when $p = 3$, so that they have the property that $C_2 = +1$ and $C_3 = +1$ for any squarefree $t \in \mathbb{N}$.

(d). In the following, we will assume that $C_2 = C_3 = C_M = +1$ for any quadratic twist of E. Let us look at E_{p_0} the twist at a prime $p_0 \neq 2, 3$ that divides Δ. According to the reduction at p_0, we have different a value of $C_0 = D_{p_0}$ given by Proposition 3.3. As for C_Δ, it is equal to $\left(\frac{-1}{p_0}\right)$.

(1) If the reduction is of type *III* or *III**, then $D_{p_0} = +1$ (i.e. $W_{p_0}(E_t) = W_{p_0}(E)$ if $p_0 \mid t$), so for E_{p_0} we have $C_0 = +1$ and $C_\Delta = \left(\frac{-1}{p_0}\right)$. Thus $W(E_{p_0}) = \left(\frac{-1}{p_0}\right) W(E)$ for all $t \in \mathbb{Z} \setminus \{0\}$. If $p_0 \equiv 3 \mod 4$, then $W(E_{p_0}) = -W(E)$, otherwise $W(E_{p_0}) = W(E)$.

(2) If the reduction has type *II*, *II**, *IV* or *IV** then $D_{p_0} = \left(\frac{3}{p_0}\right)$, and thus $W(E_{p_0}) = \left(\frac{3}{p_0}\right)\left(\frac{-1}{p_0}\right) W(E_t) = \left(\frac{-3}{p_0}\right) W(E_t)$ for all $t \in \mathbb{Z} \setminus \{0\}$. If $p_0 \equiv 5 \mod 6$, then $W(E_{p_0}) = -W(E)$, otherwise if $p_0 \equiv 1 \mod 6$, $W(E_{p_0}) = W(E)$.

(3) If the reduction has type I_m^*, then in the summerizing table of Section 2 we find that $D_{p_0} = -\left(\frac{-6b_{(p_0)}}{p_0}\right)$. Put $r \in \{\pm 1\}$ to be the

remainder modulo 4 of p_0. Then take t such that $t \equiv -6b_{(p_0)}r \bmod p_0$ and prime to 6Δ. We have

$$\begin{aligned} W(E_{p_0}) &= \left(\frac{-1}{p_0}\right) D_0 W(E), \quad \text{since } C_2 = C_3 = C_M = +1 \\ &= \left(\frac{-1}{p_0}\right)\left(\frac{-6b_{(p_0)}t}{p_0}\right) W(E) = \left(\frac{-r}{p_0}\right)\left(\frac{(-6b_{(p_0)})^2}{p_0}\right) W(E) \\ &= -W(E). \end{aligned}$$

(4) If the reduction has type I_0^*, then $D_{p_0} = (\frac{-1}{p_0})$, and thus $W(E_{p_0}) = W(E)$ in any case.

Observe that if we take, rather than a prime, a (positive) squarefree product $t_0 = \prod p_0$ of primes p_0 dividing $\Delta_{(6)}$, then $C_0 = \prod_{p_0} D_{p_0}$ and $C_\Delta = \left(\frac{-1}{\prod p_0}\right)$. So if each of the condition described in (1), (2), (3) and (4) hold on the corresponding factor of t_0, the root number is $W(E_{t_0}) = W(E)$.

Suppose that the hypotheses (a), (b), (c) and (d) in the statement are verified. Let t be a positive integer. Then by hypotheses (a), $C_M = +1$, by (b) and (c), $w_2 = w_3 = +1$, and by (d), the contributions of a p_0 to C_0 and C_Δ (those are respectively equal to D_{p_0} and $(\frac{-1}{p_0})$) are compensating each other: $C_0 \cdot C_\Delta = +1$. Thus $W(E_t) = W(E)$. This prove Lemma 4.2. □

As a corollary of the proofs of Theorem 4.1 and of Lemma 4.2, we have the following decomposition that become handy in the computation of examples (see Examples 1.4 to 1.6):

Corollary 4.5. *Let E be an elliptic curve, and E_t the quadratic twist by $t \in \mathscr{F}$. Then the root number can be written as the following product:*

$$W(E_t) = -\prod_{p=2,3,\ p \text{ bad reduction}} w_p(t),$$

where $w_p(t)$ are "local contributions" at each p determined as follows:

$$w_p(t) = \begin{cases} \operatorname{sgn}(t) D_2 \left(\frac{-1}{|t_{(2)}|}\right) W_2(E) & \text{for } p = 2 \\ (-1)^{v_3(t)} D_3 W_3(E) & \text{for } p = 3 \\ D_p \left(\frac{-1}{p}\right)^{v_p(t)} W_p(E) & \text{for } p (\neq 2,3) \text{ of additive reduction} \\ \left(\frac{p}{t_{(p)}}\right) D_p W_p(E) & \text{for } p (\neq 2,3) \text{ of mult. reduction,} \end{cases}$$

where D_p are the integers such that $W_p(E_t) = D_p W_p(E)$ (they are given by Proposition 3.3 for $p \neq 2, 3$).

4.2. Families of sextic twists. For any $t \in \mathbb{Z} \setminus \{0\}$, put the curve $E_t : y^2 = x^3 + t$.

Theorem 4.6. *Let $t \in \mathscr{F}_6$ be a sixth-powerfree integer. Then the root number can be written as*

$$W(E_t) = -W_2(E_t)W_3(E_t)\left(\frac{-1}{|t_{(6)}|}\right)\left(\frac{sq(t)_{(6)}}{3}\right).$$

Moreover, it is $(2^6 3^6, 3)$-square periodic and there exist square-congruence classes of t such that $W(E_t) = +1$, and another such that $W(E_t) = -1$.

Proof. Let $E_t : y^2 = x^3 + t$ be a family of elliptic curve parametrized by the variable t.

Suppose t sixth-powerfree. The root number can be written as

$$W(E_t) = -W_2(E_t)W_3(E_t)\prod_{p|t,\ p\neq 2,3} W_p(E_t).$$

As previously, we simplify the notations by writting $W_p(t)$ rather that $W_p(E_t)$. The formulae for the local root number at 2 and 3 are given by [15, Lemme 4.1]. The local root number at 2 stays the same on a congruence class modulo 2^6 as proven in Lemma 3.12 and the local root number at 3 stays the same on a congruence class modulo 3^6 as proven in 3.13.

Now look at the product in the root number formula, i.e. the quantity

$$\mathscr{P}(t) := \prod_{p|t,\ p\neq 2,3} W_p(E_t).$$

By [13, Proposition 2] (reported in Proposition 3.1), we have

$$\mathscr{P}(t) = \prod_{p|t, p\neq 2,3} \begin{cases} +1 & \text{si } v_p(t) \equiv 0 \mod 6; \\ \left(\frac{-1}{p}\right) & \text{si } v_p(t) \equiv 1,3,5 \mod 6; \\ \left(\frac{-3}{p}\right) & \text{si } v_p(t) \equiv 2,4 \mod 6. \end{cases}$$

Since t is assumed sixth-powerfree, we can write it as $t = 2^\alpha 3^\beta t_1 t_2^2 t_3^3 t_4^4 t_5^5$ where t_i are pairwise prime and neither divisible by 2 nor 3. Note that $|t_{(6)}| = t_1 t_2^2 t_3^3 t_4^4 t_5^5$ and $\mathrm{sq}(t)_{(6)} = t_2 t_4$.

Then we split $\mathscr{P}(t)$ in two parts, according to whether $p \mid \tau_1 (:= t_1 t_3 t_5)$ or $p \mid \tau_2 (:= t_2 t_4)$.

$$\begin{aligned} \mathscr{P}(t) &= \prod_{p|\tau_1} W_p(E_t) \prod_{p|\tau_2} W_p(E_t) \\ &= \prod_{p|\tau_1}\left(\frac{-1}{p}\right)\prod_{p|\tau_2}\left(\frac{-3}{p}\right) \\ &= \left(\frac{-1}{\tau_1}\right)\left(\frac{-3}{\tau_2}\right) = \left(\frac{-1}{\tau_1}\right)\left(\frac{\tau_2}{3}\right) \end{aligned}$$

We obtain that the root number is

$$W(E_t) = -W_2(E_t)W_3(E_t)\left(\frac{-1}{\tau_1}\right)\left(\frac{\tau_2}{3}\right).$$

The root number depends of the remainders of t modulo $2^7 3^7$ and of τ_2 modulo 3. Note that it is possible to find a pair of congruence classes $[t_+]$ and $[t_-]$ such that $W(E_{t_+} = -W(E_{t_-})$. Indeed, if we take $t_+ \equiv C \mod 2^7 3^7$, we can (by replacing τ_2 by an integer τ_2' prime to $6\tau_1$ and such that $\tau_2' \equiv -\tau_2 \mod 3$) define $t_- = 2^\alpha 3^\beta t_1 \tau_2'$ whose root number is opposite to the root number of t_+. □

Remark 4.7. In [15], Várilly-Alvarado proved that the root number varies on a surface of the form $y^2 = x^3 + AT^6 + B$ except possibly if $3A/B$ is a rational square. In [5] the author explicit the conditions on A and B for the elliptic surfaces on which the root number is constant along the fibration. In particular, we give here an example that was previously found by Várilly-Alvarado [15]:

$$y^2 = x^3 + 27t^6 + 16. \tag{4.1}$$

Consider the elliptic surface given by (4.1). Every fibre E_t at $t = \frac{m}{n} \in \mathbb{Q}$ is $\mathbb{Q}$-isomorphic to the curve:

$$E_{m,n} : y^2 = x^3 + 27m^6 + 16n^6.$$

Remark that $-3 \equiv (4m^3/3n^3)^2 \mod p$ and thus $\left(\frac{-3}{p}\right) = 1$ for all $p|f(t)$. The formula becomes

$$W(E_t) = -W_2(E_t)W_3(E_t)\left(\frac{-1}{(27m^6 + 16n^6)_{(2)}}\right).$$

Moreover, for every value of t, the remainder modulo 3 of $27m^6 + 16n^6$ is 1. The minimal value of M_2 stays 3. It is possible to find a value of M_1 lower that the one given by the theorem (which is $M_1 = 2^7 3^7$). This new value is $M_1' = 2^4 3^0 = 16$. Observe that $27m^6 + 16n^6$ falls in the congruence classes $1, 11 \mod 16$. These values correspond to a root number $+1$. However, the generic rank can be proven to be equal to 2 on this elliptic surface, so the set of rational points is Zariski-dense.

4.3. Families of quartic twists. For every $t \in \mathbb{Z}\setminus\{0\}$, let E be the curve $E_t : y^2 = x^3 + tx$.

Theorem 4.8. *Let $t \in \mathscr{F}_4$ be a fourth-powerfree integer. Then the root number $E_t : y^2 = x^3$ can be written as*

$$W(E_t) = -W_2(E_t)W_3(E_t)\left(\frac{-2}{|t_{(6)}|}\right)\left(\frac{-1}{sq(t)_{(6)}}\right).$$

Moreover, the function $t \mapsto W(E_t)$ is $(2^4, 4)$-square periodic and there exists classes for which $W(E_t) = +1$, and other such that $W(E_t) = -1$.

Proof. Let $t \in \mathscr{F}_4$ and define the elliptic curve $E_t : y^2 = x^3 + tx$. The root number of E_t can be written as

$$W(E_t) = -W_2(E_t)W_3(E_t) \prod_{p|t,\ p\neq 2,3} W_p(E_t).$$

By Lemmas 3.9 and 3.10, the local root number at 2 and 3 are periodic. Look now at the remaining part of the root number, namely

$$\prod_{p|t,p\neq 2,3} W_p(E_t). \tag{4.2}$$

By [13, Proposition 2], we have

$$\prod_{p|t,p\neq 2,3} W_p(E_t) = \prod_{p|t,p\neq 2,3} \begin{cases} +1 & \text{if } v_p(t) \equiv 0 \mod 4; \\ (\frac{-1}{p}) & \text{si } v_p(t) \equiv 2 \mod 4 \\ (\frac{-2}{p}) & \text{si } v_p(t) \equiv 1,3 \mod 4. \end{cases}$$

Since t is assumed fourth-powerfree, we can write it as $t = 2^\alpha 3^\beta t_1 t_2^2 t_3^3$, where t_i are pairwise coprime and not divisible by 2 nor 3. Note that $|t_{(6)}| = t_1 t_2^2 t_3^3$ and that $\text{sq}(t) = t_2$. We split (4.2) in two parts according to whether $p \mid t_1 t_3$ or $p|t_2$.

$$\begin{aligned}\prod_{p|t} W_p(E_t) &= \prod_{p|t_1t_3} W_p(E_t) \prod_{p|t_2} W_p(E_t) \\ &= \prod_{p|\tau_1} \left(\frac{-2}{p}\right) \prod_{p|t_2} \left(\frac{-1}{p}\right) \\ &= \left(\frac{-2}{t_1t_3}\right)\left(\frac{-1}{t_2}\right). \\ &= \left(\frac{-2}{|t_{(6)}|}\right)\left(\frac{-1}{\text{sq}(t)_{(6)}}\right).\end{aligned}$$

This implies that the root number can be written as

$$W(E_t) = -W_2(E_t)W_3(E_t)\left(\frac{-2}{|t_{(6)}|}\right)\left(\frac{-1}{\text{sq}(t)_{(6)}}\right).$$

Its value depends on the remainder of τ_1 modulo $2^6 3^4$ and t_2 modulo 4. □

Remark 4.9. In [2], Cassels and Schinzel show that the elliptic surfaces given by the equations

$$y^2 = x(x^2 - (1 + t^4)^2) \tag{4.3}$$

and

$$y^2 = x(x^2 - 49(1 + t^4)^2) \tag{4.4}$$

are such that every fibre at $t \in \mathbb{Q}$ have the same root number. On (4.3), the root number is always $+1$ and on (4.4), always -1.

Remark that it is possible to find a N_1 lower than the one given by Theorem 4.8 such that the function $t \to W(E_{f(t)})$ is N_1-periodic. This value is $N_1 = 2^4 3^2 = 144$.

The only remainder values of $-(1+t^4)^2 \mod 16$ are -1 and -4, and the only remainder value modulo 9 is -1. By the Chinese Remainder Theorem, we find a small set of possible remainders modulo 144 for $-(1+t^4)^2$, and the associated root number on the congruence class they define is $+1$. It is not possible to conclude anything on the density of the rational points from the root number of the fibre of surface (4.3). On the surface (4.4), the root number is -1 for every possible remainder of $-7^2(1+t^4)^2$. Assuming the parity conjecture, the rational points of the surface (4.4) are dense.

In [10] Huang presents a geometric method that proves the density of rational points for elliptic surfaces defined by the equation $y^2 = x^3 - d^2(1+t^4)^2 x$, for infinitely many squarefree values of d including $d = 1$ and 7.

Acknowledments. This article is based on results obtained by the author in her PhD thesis [4]. She is grateful to Marc Hindry for his excellent supervision. She thanks David Rohrlich for carefully reading a previous version of this work. She also wishes to thank Samuele Anni, Vladimir Dokchitser, Anthony Várilly-Alvarado and Adam Morgan for helpful conversations, and the anonymous referee for useful suggestions.

References

[1] B. J. BIRCH & N. M. STEPHENS, "The parity of the rank of the Mordell–Weil group", *Topology* **5** (1966), p. 295-299.

[2] J. W. S. CASSELS & A. SCHINZEL, "Selmer's conjecture and families of elliptic curves", *Bull. Lond. Math. Soc.* **14** (1982), no. 4, p. 345-348.

[3] I. CONNELL, "Calculating root numbers of elliptic curves over $\mathbb{Q}$", *Manuscr. Math.* **82** (1994), no. 1, p. 93-104.

[4] J. DESJARDINS, "Densité des points rationnels sur les surfaces elliptiques et les surfaces de del Pezzo de degré 1", PhD Thesis, Université Paris-Diderot - Paris VII (France), 2016, `http://www.theses.fr/2016USPCC229`.

[5] ———, "On the density of rational points on rational elliptic surfaces", *Acta Arith.* **189** (2019), no. 2, p. 109-146.

[6] ———, "On the variation of the root number of the fibers of families of elliptic curves", *J. Lond. Math. Soc.* **99** (2019), no. 2, p. 295-331.

[7] J. DESJARDINS & B. NASKRĘCKI, "Geometry of del Pezzo surfaces of the form $y^2 = x^3 + Am^6 + Bn^6$", `https://arxiv.org/abs/1911.02684`, 2019.

[8] T. DOKCHITSER & V. DOKCHITSER, "Elliptic curves with all quadratic twists of positive rank", *Acta Arith.* **137** (2009), no. 2, p. 193-197.

[9] E. HALBERSTADT, "Signes locaux des courbes elliptiques en 2 et 3", *C. R. Math. Acad. Sci. Paris* **326** (1998), no. 9, p. 1047-1052.

[10] Z. HUANG, "Rational points on elliptic $K3$ surfaces of quadratic twist type", `https://arxiv.org/abs/1806.07869`, 2018.

[11] E. LIVERANCE, "A formula for the root number of a family of elliptic curves", *J. Number Theory* **51** (1995), no. 2, p. 288-305.

[12] O. G. Rizzo, "Average root numbers for a nonconstant family of elliptic curves", *Compos. Math.* **136** (2003), no. 1, p. 1-23.
[13] D. E. Rohrlich, "Variation of the root number in families of elliptic curves", *Compos. Math.* **87** (1993), no. 2, p. 119-151.
[14] ———, "Galois theory, elliptic curves, and root numbers", *Compos. Math.* **100** (1996), no. 3, p. 311-349.
[15] A. Várilly-Alvarado, "Density of rational points on isotrivial rational elliptic surfaces", *Algebra Number Theory* **5** (2011), no. 5, p. 659-690.

Julie Desjardins
DH-3062, University of Toronto Mississauga
3359 Mississauga Road
Mississauga, ON L5L 1C6, Canada
E-mail: `julie.desjardins@utoronto.ca`
URL: `https://sites.google.com/view/juliedesjardins/accueil`