Root number of twists of an elliptic curve

Julie DESJARDINS

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 $W_p(E) \in \{-1, 1\}$:

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

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 $W_p$, have the property that $W_p(E) = 1$ for all but finitely many $p$. Rohrlich [Roh96] explains in details by Rohrlich in [Roh96], have the property that $W_p(E) = 1$ for all but finitely many $p$. Rohrlich [Roh96] 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 [Hal98] (see also Rizzo [Riz03]).

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

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

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

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

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 $t$, $E_t : y^2 = x^3 + A(t)x + B(t)$, is an elliptic curve. In this paper we consider the case where the family is isotrivial, i.e. when its $j$-invariant function $t \mapsto j(E_t) = \frac{4A(t)^3}{\Delta(t)}$ is constant. In that case, the curves $E_t$ are twists of one another, and $E$ can be seen as a sub-family of the families of all twists of $E_1$:

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

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

In a previous article [Des18], the author proves that the function $t \mapsto W(E_t)$ defined by the root number on a non-isotrivial family $E$ is never periodic (i.e. constant on a congruence class of
1.2 Main results

Elliptic curves, that is, to say in the fibres of an isotrivial elliptic surface.

A function \( \alpha \) where \( i \) ranges on \( \mathbb{E} \)

Incidentally, \( \alpha \) has constant root number +1.

We will denote by \( \alpha \) over every extension of \( K \).

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 [Hua18] and in [VA11, Example 7.1]. By the time the present article was published, the author and B. Naskrεcki [De19] released a preprint presenting a simple algorithm to find the Zariski-density of the rational points associated to a smooth \( \mathcal{E} \) curve.

It is not possible that all quadratic twists have the same root number, as observed by Dokchitser and Dokchitser [DD09]. However, they proved that the elliptic curve

\[
y^2 = x^3 + x^2 - 12x - \frac{67}{4}
\]

has root number +1 over every extension of \( K = \mathbb{Q}(\sqrt{-37}) \). 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 \( \leq 2 \) [Des19 Theorem 4.2].

In this article, we describe for which elliptic curves \( \mathcal{E} \) the root number of a twist by \( t \in \mathbb{Z} \) only depends on the sign of \( t \) (Lemma 1.2). Moreover, for general elliptic curves \( \mathcal{E} \) we describe the behaviour of the root number (Theorem 1.1).

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

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

Similiarly, we define \( \alpha_{(d)} \) with \( d = \prod_{i} p_i^{e_i} \in \mathbb{N} \) 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 \( \alpha \) 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 \( \text{sgn}(\alpha) \) the sign of \( \alpha \).

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

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

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

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

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

where \( sq(t) = \prod_{i=0} \text{even } p_i \) and \( sq(t') = \prod_{i=0} \text{even } q_i \).

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 Weierstrass 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 Weierstrass equation:

1. \( E_1 : y^2 = x^3 + at^2 x + bt^3 \) if \( j(E) \neq 0, 1728 \) (i.e. \( ab \neq 0 \)),
2. \( E_2 : y^2 = x^3 + ax \) if \( j(E) = 1728 \) (i.e. \( b = 0 \)),
3. \( E_3 : y^2 = x^3 + bt \) 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 \( j(E) = 1728 \), \( E_{t^2} \cong E \) 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 \( E_{t^2} \) for \( t' = q^2 \) if \( ab \neq 0 \); \( t' = pq \) if \( b = 0 \); \( t' = pq^2 \) 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 1.1.** 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 \( \mathcal{F}_2 \) to be the set of square-free integers, and \( \mathcal{F}_2^+ \) (respectively \( \mathcal{F}_2^- \)) the subset of \( t \in \mathcal{F}_2 \) with \( \text{sgn}(t) = +1 \) (resp. \( \text{sgn}(t) = -1 \)). Then

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

\[
W(E_t) = -W_2(E_t) W_3(E_t) \left( \frac{-1}{[t(6)]} \right) \left( \prod_{p|\Delta(E)} W_p(E_t) \right),
\]

where \( (\cdot) \) is the Jacobi symbol.

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

(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 \( \mathcal{F}_4 \) to be the set of fourth-powerfree integers, and \( \mathcal{F}_4^+ \) (respectively \( \mathcal{F}_4^- \)) the subset of \( t \in \mathcal{F}_4 \) with \( \text{sgn}(t) = +1 \) (resp. \( \text{sgn}(t) = -1 \)). 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 \( \mathcal{F}_4^\pm \).

(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 \( \mathcal{F}_6 \) to be the set of sixth-powerfree integers, and \( \mathcal{F}_6^+ \) (respectively \( \mathcal{F}_6^- \)) the subset of \( t \in \mathcal{F}_6 \) with \( \text{sgn}(t) = +1 \) (resp. \( \text{sgn}(t) = -1 \)). 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 \( \mathcal{F}_6^\pm \).

(c) The root number \( W(E_t) \) is not constant when \( t \) runs through \( \mathbb{Z} \setminus \{ 0 \} \).

The article is organized 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 \( j \in \mathbb{Q} \setminus \{ 0, 1728 \} \). 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 1.1 in each of the three cases.
1.3 Recollection on Rohrlich’s results

Theorem 1.1 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 1.2.** [Roh93] 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

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

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 \( E \):
   a. there exists \( f \) such that the second assertion holds and such that the number of change of the sign of \( f \) over \( \mathbb{R} \) is greater than any given value.
   b. if \( E \) has good reduction on an abelian extension of \( \mathbb{Q} \), then the second assertion holds.

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 1.1 is necessary. Here is how to proceed:

(1) Find \( N \) the smallest integer such that for each \( t, t' \in \mathcal{F}_2 \) the congruence \( t \equiv t' \mod \mathcal{N} \) implies \( W(E_t) = W(E_{t'}) \), or in other terms the smallest \( N \) for which the root number function \( t \rightarrow W(E_t) \) is \( N \)-periodic. The existence of this \( N \) is given by Theorem 1.1. The value of \( N \) depends on the coefficients of a Weierstrass equation of \( E \) and can be found with the help of Corollary 1.3.

(2) Then determine in which of the equivalence classes modulo \( N \) are the values of the squarefree factors of \( f(t) \). Take representatives \( t_1, \ldots, t_n \) 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.** 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 \( \Delta(E) = -2^3 \cdot 7^2 \cdot 17^2 \cdot 173 \).

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). Then by Corollary 1.3 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:

\[
w_p(t) = \begin{cases} 
\text{sgn}(t)D_2 \left( \frac{-1}{p(t)} \right) W_2(E) & \text{for } p = 2 \\
(-1)^{v_2(t)}D_3 W_3(E) & \text{for } p = 3 \\
D_p \left( \frac{-1}{t} \right) W_p(E) & \text{for } p = 7, 17 \\
\left( \frac{t^{173}}{173} \right) D_p W_p(E) & \text{for } p = 173,
\end{cases}
\]

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 5.4, 5.5 and 5.7. Although an appropriate \( D_p \) is not always given by Lemma 5.4 or 5.6 for \( p = 2, 3 \) in the case of a general elliptic curve, as is the case in this example. Example 3 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 3.3, \(w_2(t)\) 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 \((v_2(a) + 1, v_2(b) + 3, v_2(\Delta)) = (1, 3, 0)\). According to Lemma 3.3, \(w_3\) 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 5.3 gives the value of \(D_p\).

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

\[
   w_p(t) = \begin{cases} \left(\frac{2}{p}\right) \left(\frac{-1}{p}\right) W_p(E) & \text{if } p \mid t \\ W_p(E) & \text{if } p \nmid t. \end{cases}
\]

Since \(7 \equiv 1 \mod 6\) we have \(w_7(t) = W_7(E) = -1\) for all \(t\) square-free 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

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

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 \(f(t) = t^{30} + 14\) takes the values among \{13, 14, 15\} mod 173. Thus we have \(w_{173}(f(t)) = \left(\frac{f(t)}{173}\right)\). This Jacobi symbol is equal to +1 for all squarefree \(t\) since \(\left(\frac{13}{173}\right) = \left(\frac{14}{173}\right) = \left(\frac{15}{173}\right) = +1\).

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 \(w_7(f(t)) = +1\).

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 2.** If we twist \(E: y^2 = x^3 + 238x + 952\) by the polynomial \(g(t) = t^{86} + 1\) instead: we have \(W(E_0) = W(E) = 1\) and \(W(E_1) = W(E_2) = -1\) so the root number is not constant on the family \(E_g\). (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 3.** 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 \(h(t) = 8t^{30} + 5\):

\[
   E_h(t): y^2 = x^3 + 34(8t^{30} + 5)^2x + 68(8t^{30} + 5)^3.
\]

The discriminant of \(E'\) is \(\Delta(E') = -2^817^261\), so the reduction of \(E'\) at 17 has type II and the reduction at 61 is II. The root number can be written as

\[
   W(E'_h) = \prod_{p=2,3,17,61} w_p(t),
\]

with \(w_p(t)\) as in Corollary 1.3. 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 \(E_2\). Some additional work must be done here with Rizzo’s table III [Riz03]. From there we extract the formula (for odd \(t\)):

\[
   W_2(E'_h) = \begin{cases} +1 & \text{if } 6 \cdot 17t^2 + 27 \cdot 17t^3 \equiv 1 \mod 8 \text{ or } 27 \cdot 17t^3 \equiv 5 \mod 8 \\ -1 & \text{otherwise.} \end{cases}
\]
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 $w_4(h(t)) = \text{sgn}(h(t)) \left( \frac{-1}{h(t)} \right) D_2 W_2(E'') = -1$ for all $t \in \mathbb{Z}$.

By Lemma 4.5, $w_3(t) = +1$ for all $t$.

Similarly as in Example 1, 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 [BS66] 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 $y^2 = x^3 - 432A^2$). Livierance [Liv95] 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 5a and 5b of Theorem 4.1 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 [VA11] Prop. 4.4 and 4.8.

Connell [Con94] computer-implemented the root number formulae from Rohrlich [Roh93]. Livierance [Liv95], Birch and Stephens [BS66].

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 $\Delta$ 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 \( I_0, III, I_0^* \) if \( v_p(\Delta) \equiv 0, 1, 2, 3 \mod 4 \) 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 \( \Delta(E_t) = -2^4 3^4 b^2 t^2 \). 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.** ([Roh93, 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

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

However, it is not as simple when \( p = 2 \) or \( 3 \). According to [Riz03, 1.1], to determine the local root number at \( p = 2, 3 \) of an elliptic curve, we must find the smallest vector \((\alpha, \beta, \gamma)\) with nonnegative entries such that

\[
(\alpha, \beta, \gamma) = (v_p(c_4), v_p(c_6), v_p(\Delta)) + k(4, 6, 12)
\]

for \( k \in \mathbb{Z} \), where \( c_4, c_6 \) and \( \Delta \) are the usual quantities associated to a Weierstrass equation (as in [Sil94, Chap. III]).

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

\[
E_t : y^2 = x^3 + t a x^2 + b t^3,
\]

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

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

The root number is given by the entry of Rizzo’s Table II (if \( p = 3 \)) or Table III (if \( p = 2 \)) corresponding to \((\alpha, \beta, \gamma)\).

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 \( t = t_0(\Delta) \) be a decomposition such that \( t_0 \) is a product of prime factors of \( \Delta \) (the discriminant of \( E \)) and \( t(\Delta) \) is an integer coprime with \( \Delta \). 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 \( v_p(\Delta_{E_t}) = v_p(\Delta) + 12v_p(t(\Delta)) \). 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 [Hal98] depend only of the 2-adic and 3-adic valuation of \( c_4 \) and \( c_6 \) as well as the remainder of \( c_{1,2}, c_{4,3}, c_{6,2}, c_{6,3} \) modulo a certain power of 2 or 3.

### 3.1.2 Variation of the local root number at \( p \geq 5 \) 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 \( W_p(E) = D_pW_p(E_t) \). 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 \( p \mid t \)

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

**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

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

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 \( E_{p|t} \) has type \( I_0 \). The local root number at \( p \) changes from \( \left(\frac{1}{p}\right) \) to +1. We have \( D_p = \left(\frac{2}{p}\right) \).

(b) If \( E \) has type \( II \), then \( E_t \) has type \( IV^* \). Conversely, if \( E_t \) has type \( IV^* \), then \( E_{p|t} \) has type \( II \). The local root number at \( p \) changes from \( \left(\frac{1}{p}\right) \) to \( \left(\frac{2}{p}\right) \). We have \( D_p = \left(\frac{2}{p}\right) \).

(c) If \( E \) has type \( III \), then \( E_t \) has type \( III^* \) and conversely. The local root number at \( p \) changes from \( \left(\frac{2}{p}\right) \) to \( \left(\frac{3}{p}\right) \). 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 \( \left(\frac{-1}{p}\right) \) to \( \left(\frac{-6b_{t(p)}t(p)}{p}\right) \). We have \( D_p = -\left(\frac{-6b_{t(p)}t(p)}{p}\right) \).

| Type of \( E \) | Type of \( E_t \) | Local root number at \( p \) | Formula |
|-----------------|-----------------|------------------|--------|
| \( I_0 \leftrightarrow I_0^* \) | \( \left(\frac{1}{p}\right) \leftrightarrow +1 \) | \( D_p = \left(\frac{2}{p}\right) \) |
| \( II \leftrightarrow IV^* \) | \( \left(\frac{2}{p}\right) \leftrightarrow \left(\frac{3}{p}\right) \) | \( D_p = \left(\frac{2}{p}\right) \) |
| \( III \leftrightarrow III^* \) | \( \left(\frac{-2}{p}\right) \leftrightarrow \left(\frac{-1}{p}\right) \) | \( D_p = \left(\frac{-6b_{t(p)}t(p)}{p}\right) \) |
| \( I_m^* \leftrightarrow I_m \) | \( \left(\frac{-1}{p}\right) \leftrightarrow \left(\frac{-6b_{t(p)}t(p)}{p}\right) \) | \( D_p = -\left(\frac{-6b_{t(p)}t(p)}{p}\right) \) |
3.1.3 Local root number at $p = 2$

Lemma 3.4. We have $W_2(E_t) = \epsilon_2 \cdot \text{sgn}(t) \left( \frac{-1}{(t,2)} \right)$ (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

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

where $D_2$ is the integer depending on $t$ such that $W_2(E_t) = D_2W_2(E)$. In particular, we have $D_2 = \epsilon_2 \cdot \text{sgn}(t) \left( \frac{-1}{(t,2)} \right)$ and so the function $w_2$ defined in Corollary 4.3 is constant and $w_2(t) = \epsilon_2$.

Proof. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve and let $\Delta$ 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 $\Delta$ for the root number at 2 of the fibres $E_t$ to be $W_2(E_t) = \text{sgn}(t) \left( \frac{-1}{(t,2)} \right)$ for all positive $t$ and $- \left( \frac{-1}{(t,2)} \right)$ for all negative $t$. We can classify the curves $E$ by their triple $(v_2(a) + 4, v_2(b) + 5, v_2(\Delta))$: a formula for their local root number at 2 is given by the table of Rizzo [Riz03, Table III]. (In Rizzo, the notation with the $c$-invariants is preferred. Note that $(c_0,2) = 3b(2)$ and that $(c_4,2) = 3^2a(2)$.) The first step is to select the surfaces such that $W_2(E_t) = \epsilon \cdot \text{sgn}(t) \left( \frac{-1}{|t|} \right)$ when $2 \| t$, 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 $W_2(E_t) = +1 \iff t \equiv 1 \mod 4$, 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

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

In any case of $a(2) \mod 4$ and $b(2) \mod 8$, there will be values of $t \mod 8$ such that $W_2(E_t) \neq \text{sgn}(t) \left( \frac{-1}{|t|} \right)$. 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 $t \equiv 5 \mod 8$.

Proceeding 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 $\text{sgn}(t) \left( \frac{-1}{|t|} \right)$. We obtain the list given in Table III. We have double checked every computation with the computation software MAGMA.

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 $W_2(E_{2t}) = \epsilon \cdot \text{sgn}(t) \left( \frac{-1}{|t|} \right)$ (for the same $\epsilon$). A list of the monodromy of the triples, as well as whether or not those pairs figure in Table III. 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 $b(2)$).
| \((v_2(a) + 4, v_2(b) + 5, v_2(\Delta))\) (of a minimal model) | Special conditions | \(\epsilon\), such that \(W_2 = \epsilon \cdot \text{sgn}(t) \left(\frac{-1}{|t|}\right)\) |
|---|---|---|
| \((0, 0, 0)\) | \(b_{(2)} \equiv 1 \mod 4\) \(\quad b_{(2)} \equiv 3 \mod 4\) | +1 \(-1\) |
| \((\geq 4, 3, 0)\) | \(b_{(2)} \equiv 1 \mod 4\) \(\quad b_{(2)} \equiv 3 \mod 4\) | +1 \(-1\) |
| \((2, 3, \geq 4)\) | \(b_{(2)} \equiv 1 \mod 4\) \(\quad b_{(2)} \equiv 3 \mod 4\) | -1 \(+1\) |
| \((\geq 4, 4, 2)\) | \(b_{(2)} \equiv 1 \mod 4\) \(\quad b_{(2)} \equiv 3 \mod 4\) | +1 \(-1\) |
| \((3, 5, 3)\) | \(a_{(2)} \equiv 3, 5 \mod 8 \text{ and } b_{(2)} \equiv 3 \mod 4;\) \(\quad a_{(2)} \equiv 1, 7 \mod 16 \text{ and } b_{(2)} \equiv 1 \mod 4;\) \(\quad a_{(2)} \equiv 3, 5 \mod 8 \text{ and } b_{(2)} \equiv 1 \mod 4;\) \(\quad a_{(2)} \equiv 1, 7 \mod 16 \text{ and } b_{(2)} \equiv 3 \mod 4;\) | -1 \(+1\) |
| \((5, 8, 9)\) | \(a_{(2)} \equiv 5, 7 \mod 8 \text{ and } b_{(2)} \equiv 3 \mod 4;\) \(\quad a_{(2)} \equiv 1, 3 \mod 16 \text{ and } b_{(2)} \equiv 1 \mod 4;\) \(\quad a_{(2)} \equiv 5, 7 \mod 8 \text{ and } b_{(2)} \equiv 1 \mod 4;\) \(\quad a_{(2)} \equiv 1, 3 \mod 16 \text{ and } b_{(2)} \equiv 3 \mod 4;\) | +1 \(-1\) |
| \((\geq 6, 6, 6)\) | \(b_{(2)} \equiv 1 \mod 4\) \(\quad b_{(2)} \equiv 3 \mod 4;\) | +1 \(-1\) |
| \((4, 6, 7)\) | \(b_{(2)} \equiv 3 \mod 4 \text{ and } a_{(2)} \equiv 7 \mod 8;\) \(\quad b_{(2)} \equiv 1 \mod 4 \text{ and } a_{(2)} \equiv 7 \mod 8;\) | +1 \(-1\) |
| \((\geq 7, 7, 8)\) | \(b_{(2)} \equiv 1 \mod 4\) \(\quad b_{(2)} \equiv 3 \mod 4;\) | +1 \(-1\) |
| \((6, 8, 10)\) | \(a_{(2)} b_{(2)} \equiv 3 \mod 4;\) \(\quad a_{(2)} b_{(2)} \equiv 1 \mod 4;\) | +1 \(-1\) |
| \((\geq 7, 8, 10)\) | \(b_{(2)} \equiv 1 \mod 4\) \(\quad b_{(2)} \equiv 3 \mod 4;\) | +1 \(-1\) |

Table 1 – Cases where \(W_2(E_t) = \epsilon \cdot \text{sgn}(t) \cdot \left(\frac{-1}{|t|}\right)\) for every odd squarefree \(t \in \mathbb{Z} - 0\).

| Monodromy of \((v_2(a) + 4, v_2(b) + 5, v_2(\Delta))\) | Are triples in Table[1] |
|---|---|
| \((0, 0, 0) \leftrightarrow (2, 3, 6)\) | yes, yes |
| \((0, 0, > 0) \leftrightarrow (2, 3, > 6)\) | no, no |
| \((3, 3, 0) \leftrightarrow (5, 5, 6)\) | no, no |
| \((\geq 4, 3, 0) \leftrightarrow (\geq 6, 6, 6)\) | yes, yes |
| \((2, 4, 0) \leftrightarrow (4, 7, 6)\) | no, no |
| \((2, \geq 5, 0) \leftrightarrow (4, \geq 8, 6)\) | no, no |
| \((2, 3, 1) \leftrightarrow (4, 6, 7)\) | no, no |
| \((2, 3, 2) \leftrightarrow (4, 6, 8)\) | no, no |
| \((2, 3, 3) \leftrightarrow (4, 6, 7)\) | no, no |
| \((2, 3, \geq 4) \leftrightarrow (4, 6, \geq 8)\) | yes, no |
| \((3, 4, 2) \leftrightarrow (5, 7, 8)\) | no, no |
| \((3, 5, 3) \leftrightarrow (5, 8, 9)\) | yes, yes |
| \((4, 4, 2) \leftrightarrow (6, 7, 8)\) | yes, no |
| \((\geq 5, 4, 2) \leftrightarrow (\geq 7, 7, 8)\) | yes, no |
| \((4, 5, 4) \leftrightarrow (6, 8, 10)\) | no, yes |
| \((\geq 5, 5, 4) \leftrightarrow (\geq 7, 8, 10)\) | no, yes |

Table 2
$$\begin{array}{|c|c|c|}
\hline
(v_3(a) + 1, v_3(b) + 3, v_3(\Delta)) & \text{Special conditions} & \epsilon_3, \text{ such that } W_3 = \epsilon_3 \\
\hline
(0, 0, 0) & & +1 \\
(1, \geq 3, 0) & & +1 \\
(1, 2, 0) & & +1 \\
(2, \geq 5, 3) & & +1, \\
(2, 3, 3) & \text{if } a_{(3)} \equiv 1 \mod 3 \text{ and } b_{(3)} \equiv 4, 5 \mod 9 & +1, \\
(2, 3, 4) & & +1, \\
(2, 3, 6) & & -1, \\
(2, 3, \geq 7) & & -1, \\
(2, 3, 4) & & +1, \\
(2, \geq 5, 3) & & +1, \\
(\geq 3, 3, 3) & b_{(2)} \equiv 1, 8 \mod 9 & +1 \\
(3, 5, 6) & \text{if } a_{(3)} \equiv 1 \mod 3 & +1, \\
 & a_{(3)} \equiv 2 \mod 3 & -1 \\
(3, \geq 6, 9) & & -1, \\
(4, 6, 9) & \text{if } a_{(3)} \equiv 1 \mod 3 \text{ and } b_{(3)} \equiv 4, 5 \mod 9 & +1, \\
(4, \geq 8, 9) & & +1, \\
(\geq 5, 6, 9) & b_{(2)} \equiv 1, 8 \mod 9 & +1 \\
\hline
\end{array}$$

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

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

**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 $W_3(E_t) = D_3W_3(E)$) and so the function $w_3$ defined in Example 2.2 or Corollary 4.3 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 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.

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 (these facts are listed in Table 3) and comparing the values of $\epsilon_3$. We retain only $(0, 0, 0), (2, 3, 6), (1, \geq 3, 0) \geq 6, 6, \text{ and finally } (1, 2, 0) \text{ and } (3, 5, 6)$ with the additional condition that $a_{(3)} \equiv 2 \mod 3$. It is important to notice that in the following cases, although the triple $(v_3(a) + 1, v_3(b) + 3, v_3(\Delta))$ and the triple of a quadratic twist by 3 are both in Table 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 means that the triple is in Table 3 but under special conditions. If there is no special condition to take account of, then the table tells the value of the function $W_3(E_t)$.

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

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

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

We may reformulate this theorem as follows:

**Lemma 3.10.** The function of the local root number at 3 on the fourth-powerfree integers, defined as \( t \mapsto W_3(t_{(3)}) \), is \( 3^{v_3(t)} \)-periodic on \( \mathcal{F}_4 \) and it takes the value \(-1\) if and only if \( t \in [3^2 a] \) the congruence class \( \mod 3^4 \), where \( k = 1, 3 \mod 4 \) and \( a = 1, 3 \mod 8 \); or \( k = 0 \) and \( a = 1, 5, 9, 11, 13, 15 \mod 16 \); or \( k = 2 \) and \( a = 1, 3, 5, 7, 11, 15 \mod 16 \).

### 3.3 Root number of a sextic twist

**Lemma 3.11.** [VATI, Lemma 4.1] Let \( t \) be a non-zero integer and the elliptic curve \( E_t : y^2 = x^3 + tx \). 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

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

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

We may reformulate this theorem as follows:
Lemma 3.12. The function of the local root number at 2 defined as $t \mapsto W_2(\mathcal{E}_t)$ is $2^6$-periodic on $\mathcal{F}_6$ 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 $a \equiv 3 \pmod{4}$.

Lemma 3.13. The function of the local root number at 3 defined as $t \mapsto W_3(\mathcal{E}_t)$ is $3^6$-periodic on $\mathcal{F}_6$ 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 $a \equiv 1 \pmod{3} \pmod{4}$; $k \in \{4, 5\}$ and $a \equiv 2 \pmod{3} \pmod{4}$; $k = 0$ and $a \equiv 5, 7 \pmod{3} \pmod{4}$; or $k \in \{1, 2\}$ and $a \equiv 2, 4 \pmod{3} \pmod{4}$.

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 $\mathcal{F}_2$ to be the set of squarefree integers. Then

1. the function $t \mapsto W(\mathcal{E}_t)$ is periodic on $\mathcal{F}_2$,
2. the root number $W(\mathcal{E}_t)$ 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 $W_2(E_t) = W_2(E) \cdot \text{sgn}(t) \cdot \left(\frac{1}{\prod_{l|\Delta}}\right)$;
(c) for all $t$ non-zero squarefree integers one has $W_3(E_t) = W_3(E) \cdot (-1)^{\text{sgn}(t)}$;
(d) if there exists $p | \Delta(6)$ then:
   i. if the reduction of $E$ at $p$ has type III or III*, then $p \equiv 1 \pmod{4}$;
   ii. if the reduction of $E$ at $p$ has type II, II*, IV or IV*, then $p \equiv 1 \pmod{6}$;
   iii. the reduction at $p$ is not additive potentially multiplicative.

Remark 1. The elliptic curves $E$ with property (b) or (c) are respectively given by Lemma 3.4 or 3.6.

Example 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 $\Delta = 2^4 7^2 13^2$. So we have:

(a) The only finite place of multiplicative reduction is in 2.
(b) By Lemma 3.4, $W_2(E_t) = W_2(E) \cdot \text{sgn}(t) \left(\frac{1}{\prod_{l|\Delta}}\right)$ because the associated triple of a minimal model of $E_t$ is $(v_2(c_1), v_2(c_6), v_2(\Delta)) = (0, 0, 0)$.
(c) By Lemma 3.6, $W_3(E_t) = W_3(E) \cdot (-1)^{\text{sgn}(t)}$ because the associated triple of a minimal model of $E_t$ is $(v_2(c_1), v_2(c_6), v_2(\Delta)) = (1, 3, 0)$ and $a_{(3)} \equiv 2 \pmod{3}$.
(d) The only prime dividing $\Delta(6)$ are 7 and 13, for both of them the reduction has type II and that $p \equiv 1 \pmod{6}$.

Proof of Theorem 4.7. 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 $\Delta = \Delta(E) = 2^{a_2(\Delta)} 3^{a_3(\Delta)} \Delta(6)$ the discriminant of $E$ that we suppose minimal.

The root number can be written as

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

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

$$W(E_t) = -W_2(E_t)W_3(E_t) \left(\frac{-1}{\prod_{l|\Delta}}\right) \left(\prod_{p|\Delta(6)} W_p(E_t)\right).$$
We have $\Delta(E_t) = \Delta t^6$. Since $t$ is assumed squarefree, the equation of $E_t$ is minimal unless $\gcd(\Delta, t) \neq 1$.

Proof of the first property.

For each prime $p$, Lemma 3.3 proves that there exists an integer $\alpha_p$ such that $W_p(E_t) = W_p(E_{t'})$ for all $t \equiv t' \mod p^{\alpha_p}$. Put $N = 2^{2x_3^\alpha} \prod_{p|\Delta(t)} p^{\alpha_p}$. 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 3.2 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 3.2 $W(E_t) = W(E)$ 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:

$$W(E_{-1}) = -W_2(E_{-1})W(E_{-1}) \prod_{p \neq 2, 3} W_p(E_1)$$

Observe that by assumption of property b), $W_2(E_{-1}) = W_2(E) \cdot \text{sgn}(1) \left(\frac{-1}{-1}\right) = -W_2(E)$ (by convention, $\left(\frac{-1}{-1}\right) = 1$). Moreover by assumption of property c), $W_3(E_{-1}) = (-1)^3(1)W_3(E) = W_3(E)$. Thus

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

Proof of Lemma 4.2. By Theorem 4.2’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 $W(E_t)$. 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 $W_p(E_t) = D_pW_p(E)$. 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

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

which we can split the following way:

$$W(E_t) = D_2D_3\left(\prod_{p|\Delta(t)} D_p\right) \left(\prod_{p|t} D_p\right) W(E)$$

$$= D_2D_3\left(\prod_{p|\Delta(t)} D_p\right) \left(\prod_{p|t} D_p\right) W(E)$$

and Proposition 3.3 gives

$$= D_2D_3\left(\prod_{p|\Delta(t)} \left(\frac{t}{p}\right)\right) \left(\prod_{p|t} \left(-\frac{1}{p}\right)\right) \left(\prod_{p|\Delta(t)} D_p\right) W(E)$$

so that

$$W(E_t) = D_2D_3\left(\frac{t}{\Delta(t)}\right) \left(-\frac{1}{t(\Delta(t))}\right) \left(\prod_{p|t} D_p\right) W(E).$$
where $\Delta_M$ 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

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

that is to say $t(6\Delta)' = \prod_{p | (6\Delta_0)} p^s(t)$. We can write

$$\left( -\frac{1}{t(6\Delta)} \right) = \text{sgn}(t) \left( -\frac{1}{t(2)} \right) \left( -1 \right)^{v_2(t)} \left( -\frac{1}{t(6\Delta)} \right).$$

Let

$$C_2 = \text{sgn}(t) \cdot D_2 \left( -\frac{1}{t(2)} \right), \quad C_3 = D_3(-1)^{v_3(t)} \cdot \frac{t}{\Delta_M}, \quad C_0 = \prod_{E \text{ has add. red.}} D_p, \quad C_\Delta = \left( -\frac{1}{t(6\Delta)} \right)$$

so that

$$C = C_2 C_3 C_0 C_\Delta,$$

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 dependence 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 $\Delta_0$, (so that $C_\Delta = C_0 = +1$)
— it is not a square modulo $\Delta_M$ (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 $t_0 \nmid \Delta_0$ such that for the twist $E_{t_0}$ one has $C_2 = -1$, then by the Chinese Remainder Theorem we can choose a positive $t \nmid \Delta_0$ (in addition we may assume that it is squarefree) respecting $t \equiv t_0 \pmod{2^{v_2}}$ 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 $(v_p(c_1), v_p(c_2), v_p(\Delta))$ 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 $C_2 = -1 = C_M = +1$ 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 $\Delta$. 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 $C_\Delta$, it is equal to $\left( -\frac{1}{p_0} \right)$.

i. 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 $p_0 \equiv 3 \pmod{4}$, then $W(E_{p_0}) = -W(E)$, otherwise $W(E_{p_0}) = W(E)$.

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

iii. If the reduction has type $I_m^*$, then in the sumerizing table of Section 2 we find that $D_{p_0} = -\left( -\frac{6d(p_0)}{p_0} \right)$. Put $r \in \{\pm 1\}$ to be the remainder modulo 4 of $p_0$. Then take $t$ such that
where integer. Then by hypotheses a),

tions of a

number can be written as the following product:

\[ W(E_{p_0}) = \left( -\frac{1}{p_0} \right) D_{p_0} W(E), \]

\[ = \left( -\frac{1}{p_0} \right) \left( -\frac{6b_{(p_0)} t}{p_0} \right) W(E) = \left( -\frac{t}{p_0} \right) \left( -\frac{6b_{(p_0)}}{p_0} \right)^2 W(E) \]

\[ = -W(E). \]

iv. If the reduction has type \( I_0^6 \), then \( D_{p_0} = \left( \frac{1}{p_0} \right) \), 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 \( C_{\Delta} = \left( \prod p_0 \right) \). So if each of the condition described in i. ii. iii. and iv. 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 \( C_{\Delta} \) (those are respectively equal to \( D_{p_0} \) and \( \left( \frac{1}{p_0} \right) \)) 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 11 to 31):

**Corollary 4.3.** Let \( E \) be an elliptic curve, and \( E_t \) the quadratic twist by \( t \in \mathbb{F} \). 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:

\[ w_p(t) = \begin{cases} 
\text{sgn}(t)D_2 \left( \frac{-1}{(t,2)} \right) W_2(E) & \text{for } p = 2 \\
(-1)^{\rho(t)} D_3 W_3(E) & \text{for } p = 3 \\
D_p \left( \frac{-1}{p} \right) v_p(t) W_p(E) & \text{for } p(\neq 2,3) \text{ of additive reduction} \\
\left( \frac{t}{p} \right) D_p W_p(E) & \text{for } p(\neq 2,3) \text{ of multiplicative reduction},
\end{cases} \]

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 4.4.** Let \( t \in \mathbb{F}_6 \) be a sixth-powerfree integer. Then the root number can be written as

\[ W(E_t) = -W_2(E_t)W_3(E_t) \left( \frac{-1}{|t|} \right) \left( \frac{\text{sgn}(t)_6}{3} \right). \]

Moreover, it is \((2^63^6,3)\)-square periodic and there exists 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 writing \( W_p(t) \) rather than \( W_p(E_t) \). The formulae for the local root number at 2 and 3 are given by [Vati] 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

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

By [Roh93 Prop. 2] (reported in Proposition 3.1), we have

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

Since $t$ is assumed sixth-powerfree, we can write it as $t = 2^a 3^b t_1^2 t_2^2 t_3^2 t_4^6 t_5^6$ where $t_i$ are pairwise prime and neither divisible by $2$ nor $3$. Note that $|t(0)| = t_1 t_2^2 t_3 t_4 t_5$ and $\sqrt{q(t(t))} = t_2 t_4$.

Then we split $\mathcal{P}(t)$ in two parts, according to whether $p \mid \tau_1$ or $p \mid \tau_2$.

$$\mathcal{P}(t) = \prod_{p \mid \tau_1} W_p(E_t) \prod_{p \mid \tau_2} W_p(E_t)$$

$$= \prod_{p \mid \tau_1} \left(\frac{-1}{p}\right) \prod_{p \mid \tau_2} \left(\frac{-3}{p}\right)$$

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 $\tau_2$ modulo $3$. Note that it is possible to find a pair of congruence classes $[t+]$ and $[t-]$ such that $W(\hat{E}_{t+}) = -W(\hat{E}_{t-})$. Indeed, if we take $t_+ \equiv C \mod 2^7 3^7$, we can (by replacing $\tau_2$ by an integer $\tau_2'$ prime to $6 \tau_1$ and such that $\tau_2' \equiv -\tau_2 \mod 3$) define $t_- = 2^a 3^b t_1 t_2'$ whose root number is opposite to the root number of $t_+$. \qed

**Remark 2.** In [VAI1], 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 [Des19] the author explicit the conditions on $A$ and $B$ for the elliptic surfaces on which the root number is constant along the fibrations. In particular, we give here an example that was previously found by Várilly-Alvarado [VAI1]:

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

Consider the elliptic surface given by (2). 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 $p \mid f(t)$. 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 $M_1 = 2^3 3^5$). This new value is $M_1 = 2^3 3^5 = 16$. 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 4.5.** Let $t \in \mathcal{P}_4$ be a fourth-powerfree integer. Then the root number $E_t : y^2 = x^3$ can be written as

$$W(E_t) = -W_2(E_t)W_3(E_t) \left( \frac{-2}{|t(0)|} \right) \left( \frac{-1}{\text{sq}(t)(6)} \right).$$

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 $t \in \mathcal{P}_4$ 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

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

By [Roh93] Prop. 2, we have

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

Since $t$ is assumed fourth-powerfree, we can write it as $t = 2^a 3^b t_1^2 t_2^2$, where $t_i$ are pairwise coprime and not divisible by 2 nor 3. Note that $|t(0)| = t_1 t_2^2 t_3^3$ and that $\text{sq}(t) = t_2$. We split (3) in two parts according to whether $p | t_1 t_3$ or $p | t_2$.

$$\prod_{p | t} W_p(E_t) = \prod_{p | t_3} W_p(E_t) \prod_{p | t_2} W_p(E_t)$$

$$= \prod_{p \mid t_3} \left( \frac{-2}{p} \right) \prod_{p \mid t_2} \left( \frac{-1}{p} \right)$$

$$= \left( \frac{-2}{t_1 t_3} \right) \left( \frac{-1}{t_2} \right)$$

$$= \left( \frac{-2}{|t(0)|} \right) \left( \frac{-1}{\text{sq}(t)(6)} \right).$$

This implies that the root number can be written as

$$W(E_t) = -W_2(E_t)W_3(E_t) \left( \frac{-2}{|t(0)|} \right) \left( \frac{-1}{\text{sq}(t)(6)} \right).$$

Its value depends on the remainder of $t_1$ modulo $2^6 3^4$ and $t_2$ modulo 4.

**Remark 3.** In [CSS2], Cassels and Schinzel show that the elliptic surfaces given by the equations

$$y^2 = x(x^2 - (1 + t^4)^2) \quad (4)$$

and

$$y^2 = x(x^2 - 49(1 + t^4)^2) \quad (5)$$

are such that every fibre at $t \in \mathbb{Q}$ have the same root number. On (4), the root number is always $+1$ and on (5), always $-1$.

Remark that it is possible to find a $N_1$ lower than the one given by Theorem 4.5 such that the function $t \mapsto W(E_f(t))$ 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 \([4]\). On the surface \([5]\), 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 \([4]\) are dense.

In \([Hua18]\) Huang presents a geometric method that proves the density of rational points for elliptic surfaces defined by the equation \(y^2 = x^3 - d^2(1 + t^4)^2x\), for infinitely many squarefree values of \(d\) including \(d = 1\) and 7.

Acknowledgment

This article is based on results obtained by the author in her PhD thesis \([Des16]\). 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. The author was supported by the Max Planck Institut für Mathematik in Bonn.

References

[BS66] B. J. Birch and N. M. Stephens. The parity of the rank of the Mordell-Weil group. Topology, 5:295–299, 1966.
[Con94] I. Connell. Calculating root number of elliptic curves over \(\mathbb{Q}\). Manuscripta Math., 82:93–104, 1994.
[CS82] J. W. S. Cassels and A. Schinzel. Selmer’s conjecture and families of elliptic curves. Bull. London Math. Soc., 14(4):345–348, 1982.
[DD09] T. Dokchitser and V. Dokchitser. Elliptic curves with all quadratic twists of positive rank. Acta Arith., 137(1):193–197, 2009.
[De19] J. Desjardins and B. Naskręcki. Geometry of del Pezzo surfaces of the form \(y^2 = x^3 + am^6 + bn^6\). arXiv:1911.02684, 2019.
[Des16] 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, November 2016.
[Des18] J. Desjardins. On the variation of the root number of the fibers of families of elliptic curves. J. London Math. Soc., 00(2):1–37, 2018.
[Des19] J. Desjardins. On the density of rational points on rational elliptic surfaces. Acta Arith., 189(2):109–146, 2019.
[Hal98] E. Halberstadt. Signes locaux des courbes elliptiques en 2 et 3. C. R. Acad. Sci. Paris Sér. I Math., 326(9):1047–1052, 1998.
[Hua18] Z. Huang. Rational points on elliptic K3 surfaces of quadratic twist type. arXiv:1806.07869, 2018.
[Liv95] E. Liverance. A formula for the root number of a family of elliptic curves. J. Number Theory, 51(2):288–305, 1995.
[Riz03] O. G. Rizzo. Average root numbers for a nonconstant family of elliptic curves. Compositio Math., 136(1):1–23, 2003.
[Roh93] D. E. Rohrlich. Variation of the root number in families of elliptic curves. Compositio Math., 87(2):119–151, 1993.
[Roh96] D. E. Rohrlich. Galois theory, elliptic curves, and root numbers. Compositio Math., 100(3):311–349, 1996.
[Sil94] J. H. Silverman. The Arithmetic of Elliptic Curves, volume 106. Springer-Verlag, New-York, 1994.
[VA11] A. Várilly-Alvarado. Density of rational points on isotrivial rational elliptic surfaces. Algebra & Number Theory, 5:659–690, 2011.