COMPOSITIO MATHEMATICA

ELISABETTA MANDUCHI

Root numbers of fibers of elliptic surfaces

Compositio Mathematica, tome 99, nº 1 (1995), p. 33-58
<http://www.numdam.org/item?id=CM_1995__99_1_33_0>

Compositio Mathematica **99**: 33–58, 1995.

Root numbers of fibers of elliptic surfaces

ELISABETTA MANDUCHI
Department of Mathematics, University of Maryland, College Park, MD 20742

Received 3 May 1994; accepted in final form 29 July 1994

Abstract. The variation of the root number on fibers of elliptic surfaces over the rationals with base the projective line is studied. It is proved that for a large class of such surfaces the sets of rational t's such that the fiber over t is an elliptic curve with root number 1 and -1 respectively are both dense in the set of real numbers. This result provides some evidence for a recent conjecture of B. Mazur. A similar result and some applications are also discussed.

Introduction

This paper deals with elliptic surfaces over $\mathbb{Q}$. We are interested in how the root number of their fibers varies. (Here the root number is defined as product of local factors, as in [9]). If $\mathcal{E}$ is an elliptic surface over $\mathbb{Q}$ with base $\mathbb{P}^1$, denote by E_t the fiber over t. If $t \in \mathbb{Q}$ is such that E_t is an elliptic curve, denote by $W(t)$ the root number of E_t. Let

$$T^{\pm} = \{t \in \mathbb{Q}\colon\ E_t \text{ is an elliptic curve and } W(t) = \pm 1\}.$$

We study the sets T^+ and T^-. The motivation for studying these sets comes in part from a recent conjecture of B. Mazur ([8], Conjecture 4, Section 6). He conjectured that one of the following occurs:

(1) $\operatorname{rank}(E_t(\mathbb{Q})) > 0$ for only finitely many $t \in \mathbb{Q}$, or

(2) $\operatorname{rank}(E_t(\mathbb{Q})) > 0$ for a set of rational t's which is dense in $\mathbb{R}$.

Now, let $\mathcal{R} = \{t \in \mathbb{Q}\colon\ E_t \text{ is an elliptic curve with positive rank}\}$. The conjectural functional equation of $L(E_t, s)$ and the Birch-Swinnerton-Dyer Conjecture imply that

$$W(t) = (-1)^{\operatorname{rank}(E_t(\mathbb{Q}))}. \tag{$*$}$$

Thus if we grant $(*)$, then T^- is contained in $\mathcal{R}$. In particular, if T^- is dense in $\mathbb{R}$, then so is $\mathcal{R}$.

If $\mathcal{E}$ is an elliptic surface over $\mathbb{Q}$ with base $\mathbb{P}^1$, then we can think of $\mathcal{E}$ as an elliptic curve over $\mathbb{Q}(t)$. Let $j(t) \in \mathbb{Q}(t)$ be the j-invariant of such a curve and let $c_4(t)$ and $c_6(t) \in \mathbb{Q}(t)$ be its covariants, determined respectively up to a fourth and a sixth power in $\mathbb{Q}(t)^{\times}$. If $j \neq 0, 1728$, then $j(t)$, $c_4(t)$ (mod $(\mathbb{Q}(t)^{\times})^4$) and $c_6(t)$ (mod $(\mathbb{Q}(t)^{\times})^6$) determine $\mathcal{E}$ as an elliptic curve over $\mathbb{Q}(t)$, up to $\mathbb{Q}(t)$-isomorphisms. In his recent paper ([9], Theorems 1 and 2), Rohrlich studies elliptic surfaces with constant j-invariant and the elliptic surface with j-invariant $j(t) = t$ and covariants $c_4(t) = t^3/(t - 1728)$ and $c_6(t) = -t^4/(t - 1728)$. In this paper more general cases of elliptic surfaces with non-constant j-invariant are studied. The main result is

THEOREM 1. *Let $\mathcal{E}$ be an elliptic surface over $\mathbb{Q}$ with base $\mathbb{P}^1$ and non-constant j-invariant $j(t) \in \mathbb{Q}(t)$. Let $c_4(t)$ and $c_6(t) \in \mathbb{Q}(t)$ be the covariants of $\mathcal{E}$, defined respectively up to a fourth and a sixth power in $\mathbb{Q}(t)^{\times}$.*

Assume the following:

(1) *The irreducible factors over* $\mathbb{Z}$ *of the numerators and denominators of* $j(t)$ *and* $j(t) - 1728$ *have degrees less than or equal to* 6.

(2) *If* $x \in \mathbb{P}^1(\mathbb{C})$ *is a pole of* $j(t)$, *then* $\text{ord}_x c_4 \not\equiv \text{ord}_x c_6 \pmod 2$.

Then T^+ *and* T^- *are both dense in* $\mathbb{R}$.

There are three main ingredients in the proof of this theorem. The first is the computation of local root numbers using Rohrlich's formulas ([9]). The second is the application of square-free sieve techniques, obtained by modifying some results of Hooley ([5]), Gouvêa–Mazur ([3]), Greaves ([4]), and Rohrlich ([9]). The third and crucial ingredient is the construction of a number $W_{\mathcal{P},P} \in \{\pm 1\}$ for each finite set of primes $\mathcal{P}$ containing 2 and 3 and for each $P = (x_0, x_1) \in \mathbb{Z}^2$ (see Notation 2.8). The root number $W(x_1/x_0)$ can be expressed in terms of $W_{\mathcal{P},P}$ provided that the value at P of a certain binary form F (see Notation 2.5) is not divisible by the square of any prime not in $\mathcal{P}$. It is shown that there is a $P_0 \in \mathbb{Z}^2$ and two finite sets of primes $\mathcal{P}^+$ and $\mathcal{P}^-$ – with $\mathcal{P}^+$ and $\mathcal{P}^-$ differing only by a single prime p_0 – such that $W_{\mathcal{P}^+,P_0} = 1$ and $W_{\mathcal{P}^-,P_0} = -1$ (see Corollary 2.1). The key point is to exploit the existence of fibers of the elliptic surface which have split multiplicative reduction at p_0. This is the only step in the proof of Theorem 1 where having multiplicative reduction at some prime turns out to be an advantage, rather than an occurrence to be avoided.

We can also prove a weaker statement under a slightly different set of hypotheses (precisely, strenghtening hypothesis (1) and weakening hypothesis (2)).

THEOREM 2. *Let* $\mathcal{E}$ *be an elliptic surface over* $\mathbb{Q}$ *with base* $\mathbb{P}^1$ *and non-constant j-invariant* $j(t) \in \mathbb{Q}(t)$. *Let* $c_4(t)$ *and* $c_6(t) \in \mathbb{Q}(t)$ *be the covariants of* $\mathcal{E}$, *defined respectively up to a fourth and sixth power in* $\mathbb{Q}(t)^\times$.

Assume the following:

(1) *The irreducible factors over* $\mathbb{Z}$ *of the numerators and denominators of* $j(t)$ *and* $j(t) - 1728$ *have degrees less than or equal to* 3.

(2) *There is at most one* $x \in \mathbb{P}^1(\mathbb{C})$ *such that* x *is a pole of* $j(t)$ *and* $ord_x c_4 \equiv ord_x c_6 \pmod 2$.

Then T^+ *and* T^- *are both infinite.*

The constraints given in hypotheses (1) and (2) of these two theorems come from some important number-theoretic obstructions. Precisely, the constraints in (1) are square-free sieve constraints, in the sense that the relevant square-free sieves have been proved only for polynomials whose irreducible factors over $\mathbb{Z}$ have "small" degrees. The constraint in (2) is connected to the problem of controlling the parity of the cardinality of the set of primes dividing an integer n when n varies in a certain set.

As an application of Theorem 1, one can look at the elliptic surface given by

$$y^2 = x^3 - 12t(t-1)^2 x + 16t(t-1)^3.$$

This has j-invariant $j(t) = 2^6 3^3 t/(t-1)$ and covariants $c_4(t) = 2^6 3^2 t(t-1)^2$ and $c_6(t) = -2^9 3^3 t(t-1)^3$. Thus it satisfies the hypotheses of Theorem 1, so T^+ and T^- are dense in $\mathbb{R}$. Moreover one can see that its group of rational sections has rank one (using [2], Equation 5, p. 28. See also [11], (10.2), (10.4)). This appears to be the first example of elliptic surface with the following properties:

(1) $\mathcal{E}$ has non constant j-invariant.
(2) $\mathcal{E}$ has positive Mordell–Weil rank over $\mathbb{Q}(t)$.
(3) For a dense set of $t \in \mathbb{Q}$, $W(t) = 1$.

Using Silverman's Specialization Theorem ([13], Chapter 3, Theorem 11.4) and granting $(*)$, we can replace (3) by

(3′) For a dense set of $t \in \mathbb{Q}$, the group of rational points of the fiber over t has rank greater than or equal to 2 (hence greater than the Mordell–Weil rank of the elliptic surface $\mathcal{E}$).

This paper is organized as follows. Section 1 contains the proofs of some slight generalizations of results of Hooley ([5]), Gouvêa–Mazur ([3]), Greaves ([4]), and Rohrlich ([9]) on square-free sieves. Sections 2 and 3 are devoted to the proofs of Theorem 1 and 2 respectively. In Section 4 some applications of Theorem 1 are discussed.

1. Square-free sieves

In this section we are going to generalize some results on square-free sieves by Hooley ([5]), Gouvêa–Mazur ([3]), Greaves ([4]), and Rohrlich ([9]). In [3], Gouvêa and Mazur – using also some results of Hooley ([5], Chapter 4) – obtain asymptotic estimates for the number of pairs of integers (a, b) – satisfying certain congruences and lying in a given interval – which give square-free values for a binary form $F(x_0, x_1) \in \mathbb{Z}[x_0, x_1]$ whose irreducible factors over $\mathbb{Z}$ have degree less than or equal to 3. In [4], Greaves generalizes the results of Gouvêa and Mazur to forms whose irreducible factors over $\mathbb{Z}$ have degree less than or equal to 6. In [9], Rohrlich redoes the Gouvêa–Mazur result in the easiest case, namely the case in which all irreducible factors over $\mathbb{Z}$ have degree 1, but he allows the integers plugged in for x_0 and x_1 to vary over independent intervals. The purpose of the following proposition is to obtain Greaves's result (i.e. the degrees of the irreducible factors over $\mathbb{Z}$ can be as big as 6), allowing the integers plugged in for x_0 and x_1 to vary over independent intervals as in Rohrlich. In addition we are interested in values which are not exactly square-free, but "almost" square-free, in the sense that they are not divisible by the square of any prime outside of a finite set.

PROPOSITION 1.1. *Let $F(x_0, x_1) \in \mathbb{Z}[x_0, x_1]$ be a binary form with no non-constant square factor and all of whose irreducible factors over $\mathbb{Z}$ have degree less than or equal to 6. Let M be a positive integer, let $(a_0, b_0) \in \mathbb{Z}^2$, and let $\mathcal{P}$ be a finite set of primes. Denote by $N_{\mathcal{P}}(x, y)$ the number of pairs $(a, b) \in \mathbb{Z}^2$ such that $0 < a \leqslant x$, $0 < b \leqslant y$, $(a, b) \equiv (a_0, b_0) \pmod M$, and such that $p^2 \nmid F(a, b)$ for all $p \notin \mathcal{P}$. Then, for $x, y \to \infty$ with $x \ll y \ll x$, we have*

$$N_{\mathcal{P}}(x, y) = A^{\mathcal{P}} xy + \mathrm{O}(x^2 / \log^{1/3} x), \tag{1.1}$$

where

$$A^{\mathcal{P}} = M^{-2} \prod_{p \notin \mathcal{P}} A_p$$

with A_p defined as in [3] *Section* 9.

Note. We will discuss below (see Remark 1.1) conditions under which $A^{\mathcal{P}} \neq 0$.

Proof. The proof of this proposition follows line by line the argument in Section 5 of [9], with of course the necessary adaptations (which are in some cases straightforward, in others rely on results of [4]). Let $\xi = \frac{1}{3}\log x$ and let $N'_{\mathcal{P}}(x,y)$ be the number of pairs $(a,b) \in \mathbb{Z}^2$ such that $0 < a \leqslant x$, $0 < b \leqslant y$, $(a,b) \equiv (a_0,b_0) \pmod{M}$, and such that $p^2 \nmid F(a,b)$ for all p with $p \leqslant \xi$ and $p \notin \mathcal{P}$. Clearly $N'_{\mathcal{P}}(x,y) \geqslant N_{\mathcal{P}}(x,y)$. So it suffices to prove that, for $x, y \to \infty$ with $x \ll y \ll x$,

$$N'_{\mathcal{P}}(x,y) = A^{\mathcal{P}}xy + \mathrm{O}(x^2/\log x), \tag{1.2}$$

and

$$N'_{\mathcal{P}}(x,y) - N_{\mathcal{P}}(x,y) = \mathrm{O}(x^2/\log^{1/3} x). \tag{1.3}$$

For $m \in \mathbb{N}_{>0}$, let $N_m(x,y)$ be the number of pairs $(a,b) \in \mathbb{Z}^2$ such that $0 < a \leqslant x$, $0 < b \leqslant y$, $(a,b) \equiv (a_0,b_0) \pmod{M}$, and $F(a,b) \equiv 0 \pmod{m}$, as in [9] Section 5. By the inclusion–exclusion principle we have

$$N'_{\mathcal{P}}(x,y) = \sum_{\ell} \mu(\ell) N_{\ell^2}(x,y)$$

where ℓ runs over 1 and the square-free integers whose prime divisors are less than or equal to ξ and do not belong to $\mathcal{P}$. Now, using (5.4) in [9], we can argue in a similar fashion to the proof of Lemma 8 in [3], keeping in mind that in our case the prime divisors of ℓ do not belong to $\mathcal{P}$. This leads to (1.2).

Let $F(x_0,x_1) = \prod_{i=1}^{t} f_i(x_0,x_1)$ where, for all i, $f_i(x_0,x_1)$ is an irreducible form in $\mathbb{Z}[x_0,x_1]$ of degree $\nu_i \leqslant 6$. Let

$$E(x,y) = \sum_{i=1}^{t} E_i(x,y)$$

where $E_0(x,y)$ is the number of pairs $(a,b) \in \mathbb{Z}^2$ such that $0 < a \leqslant x$, $0 < b \leqslant y$, and such that there exists a prime $p > \xi$ with $p \mid a$ and $p \mid b$. For all $i \in \{1,2,\ldots,t\}$ such that $f_i(x_0,x_1) \neq x_0, x_1$, $E_i(x,y)$ is the number of pairs $(a,b) \in \mathbb{Z}^2$ such that $0 < a \leqslant x$, $0 < b \leqslant y$, and such that there exists a prime $p > \xi$ with $p \nmid ab$ and $p^2 | f_i(a,b)$. For $i \in \{1,2,\ldots,t\}$ such that $f_i(x_0,x_1) = x_0$ or x_1, $E_i(x,y)$ is the number of pairs $(a,b) \in \mathbb{Z}^2$ such that $0 < a \leqslant x$, $0 < b \leqslant y$, and such that there exists a prime $p > \xi$ with $p^2 | f_i(a,b)$. By an argument analogous to those in the proofs of Proposition 2 in [3] and Theorem 1 in [4], one sees that

$$N'_{\mathcal{P}}(x,y) - N_{\mathcal{P}}(x,y) \leqslant E(x,y)$$

for x (and hence y) big enough. To be precise, both Gouvêa and Mazur and Greaves exclude the possibility that either x_0 or x_1 is a factor of $F(x_0,x_1)$. But an analogous argument works even in this case. Now, for $i = 0$ and for $i \in \{1,2,\ldots,t\}$ such that $f_i(x_0,x_1) = x_0$ or x_1,

$$E_i(x,y) = \mathrm{O}(x^2/\log x) \tag{1.4}$$

arguing as in [9] end of Section 5. Moreover, for all $i \in \{1,2,\ldots,t\}$ such that $f_i(x_0,x_1) \neq x_0, x_1$, we have

$$E_i(x,y) = \mathrm{O}(x^2/\log x), \text{ if } \nu_i < 6, \tag{1.5}$$

and

$$E_i(x,y) = \mathrm{O}(x^2/\log^{1/3} x), \text{ if } \nu_i = 6. \tag{1.6}$$

To prove this observe that, by hypothesis, $y \leqslant cx$ for some $c > 1$. Now – as in [4] – denote by $E_i(x)$ the number of pairs $(a,b) \in \mathbb{Z}^2$ such that $0 < a \leqslant x$, $0 < b \leqslant x$, and such that there exists a prime $p > \xi$ with $p \nmid ab$ and $p^2 | f_i(a,b)$. Then clearly

$$E_i(x,y) \leqslant E_i(cx). \tag{1.7}$$

But (see [4]) we have that

$$E_i(cx) = \mathrm{O}(x^2/\log x), \quad \text{if } \nu_i < 6 \tag{1.8}$$

and

$$E_i(cx) = \mathrm{O}(x^2/\log^{1/3} x), \quad \text{if } \nu_i = 6. \tag{1.9}$$

(1.5) and (1.6) then follow from (1.7)–(1.9). So

$$E(x,y) = \sum_{i=0}^{t} E_i(x,y) = \mathrm{O}\big(x^2/\log^{1/3} x\big)$$

and this concludes the proof. □

Remark 1.1. From Proposition 5 in [3] we have

(1) $A^{\mathcal{P}} = 0$ if and only if $A_p = 0$ for some $p \notin \mathcal{P}$.

(2) If p^2 divides all the coefficients of $F(x_0, x_1)$, then $A_p = 0$.

(3) If p does not divide some coefficient of $F(x_0, x_1)$, $p \nmid M$, and $p > \deg(F)$, then $A_p \neq 0$.

In [5] Chapter 4, Hooley studies square-free values of polynomials in $\mathbb{Z}[x]$ whose irreducible factors over $\mathbb{Z}$ have degree less than or equal to 3. The purpose of the following proposition is to obtain Hooley's result for "almost" square-free values, in the sense explained above. Moreover we want to plug in integers satisfying certain congruence conditions. In what follows, given $F(t) \in \mathbb{Z}[t]$, $n_0 \in \mathbb{Z}$, and $M \in \mathbb{N}_{>0}$, we denote by $A_{1,p}$ the quantity $A_{1,p} = 1 - r_1(p^2)/p^2$, where for each integer $m \geqslant 1$ we define $r_1(m) = \text{g.c.d.}(m, M)\rho_1(m)$. Here $\rho_1(1) = 1$ and $\rho_1(m)$ equals the number of solutions – noncongruent (mod m) – of $F(n) \equiv 0 \pmod m$ in integers n such that $n \equiv n_0 \pmod M$, if $m \in \mathbb{N}$, $m > 1$.

PROPOSITION 1.2. *Let $F(t) \in \mathbb{Z}[t]$ be a polynomial with no non-trivial square factors and all whose irreducible factors over $\mathbb{Z}$ have degree less than or equal to 3. Let M be a positive integer, n_0 be an integer, and $\mathcal{P}$ be a finite set of primes. Denote by $N_{\mathcal{P}}(x)$ the number of integers n such that $0 \leqslant n \leqslant x$, $n \equiv n_0 \pmod M$, and such that $p^2 \nmid F(n)$ for all $p \notin \mathcal{P}$. Then, for $x \to \infty$, we have*

$$N_{\mathcal{P}}(x) = A_1^{\mathcal{P}} x + \mathrm{O}(x/\log^{1/2} x) \tag{1.10}$$

where

$$A_1^{\mathcal{P}} = M^{-1} \prod_{p \notin \mathcal{P}} A_{1,p}.$$

Note. We will discuss below (see Remark 1.2) conditions under which $A_1^{\mathcal{P}} \neq 0$.

Proof. The proof of this proposition is a slight variation of the arguments in [5] Section 4 (the only difference being that we are imposing some congruence conditions and we are discarding a finite set of primes $\mathcal{P}$) and is quite similar to that of Proposition 1.1, so it is left to the reader.

Remark 1.2. Reasoning as in Proposition 5 of [3], we have
(1) $A_1^{\mathcal{P}} = 0$ if and only if $A_{1,p} = 0$ for some $p \notin \mathcal{P}$.
(2) If p^2 divides all coefficient of $F(t)$, then $A_{1,p} = 0$.
(3) If p does not divide some coefficient of $F(t)$, $p \nmid M$, and $p > \deg F$, then $A_{1,p} \neq 0$.

2. Density of $T^{\pm}$

In this section we will prove Theorem 1 stated in the Introduction. Given any elliptic surface $\mathcal{E}$ defined over $\mathbb{Q}$ with base $\mathbb{P}^1$, let's denote by $\mathcal{E}$ also its associated elliptic curve over $\mathbb{Q}(t)$ which is unique up to $\mathbb{Q}(t)$-isomorphisms. If the j-invariant of $\mathcal{E}$ is different from 0 and 1728, then $\mathcal{E}$ is determined (up to $\mathbb{Q}(t)$-isomorphisms) by its j-invariant $j(t) \in \mathbb{Q}(t)$ and by the quantity $[-c_4(t)/c_6(t)] \in \mathbb{Q}(t)^\times/(\mathbb{Q}(t)^\times)^2$, where we write $[*]$ for the class of $*$ in $\mathbb{Q}(t)^\times/(\mathbb{Q}(t)^\times)^2$. Now, let $j(t) \in \mathbb{Q}(t) \setminus \{0, 1728\}$ and let $d(t) \in \mathbb{Z}[t] \setminus \{0\}$. Consider the elliptic curve over $\mathbb{Q}(t)$ with equation

$$y^2 = x^3 + \frac{j(t)d(t)}{4} x^2 - \frac{36 j(t)^2 d(t)^2}{j(t) - 1728} x - \frac{j(t)^3 d(t)^3}{j(t) - 1728} \tag{2.1}$$

This curve has j-invariant $j(t)$, and covariants

$$c_4(t) = \frac{j(t)^3 d(t)^2}{j(t) - 1728} \quad \text{and} \quad c_6(t) = -\frac{j(t)^4 d(t)^3}{j(t) - 1728}, \tag{2.2}$$

so

$$\left(-\frac{c_4}{c_6}\right)(t) := -\frac{c_4(t)}{c_6(t)} = \frac{1}{j(t)d(t)}. \tag{2.3}$$

Moreover, it has discriminant

$$\Delta(t) = \frac{j(t)^8 d(t)^6}{(j(t) - 1728)^3}. \tag{2.4}$$

If $\mathcal{E}$ is any elliptic curve over $\mathbb{Q}(t)$ with j-invariant $j(t) \neq 0, 1728$, and covariants $c_4(t)$ and $c_6(t)$, then $\mathcal{E}$ is isomorphic over $\mathbb{Q}(t)$ to the curve given by Equation (2.1) for $j(t)$ equal to the j-invariant of $\mathcal{E}$ and $d(t) \in [-c_6(t)/j(t)c_4(t)]$. We are interested in studying the variation of the root number on fibers of elliptic surfaces with non-constant j-invariant. So in what follows we will assume that $\mathcal{E}$ is given by (2.1), where $j(t) \in \mathbb{Q}(t) \setminus \mathbb{Q}$ and $d(t) \in \mathbb{Z}[t] \setminus \{0\}$.

Let's start by setting up some notations which we will use to restate and prove Theorem 1 of the Introduction.

Notation 2.1. For each $t \in \mathbb{P}^1$, we denote by E_t the fiber of $\mathcal{E}$ over t. If $t \in \mathbb{Q}$ and E_t is an elliptic curve, we write $W(t)$ for the root number of E_t and, for each prime p, we write $W_p(t)$ for the local root number of E_t at p. We have

$$T^{\pm} = \{t \in \mathbb{Q}\colon j(t) \text{ is defined, } j(t) \neq 0, 1728, d(t) \neq 0, \text{ and } W(t) = \pm 1\}.$$

Notation 2.2. For any $\varphi(t) \in \mathbb{Q}(t)$, we denote by φ_0 and φ_1 forms in $\mathbb{Z}[x_0, x_1]$ – having the same degree and no common factors – such that

$$\varphi\left(\frac{x_1}{x_0}\right) = \frac{\varphi_1(x_0, x_1)}{\varphi_0(x_0, x_1)}.$$

Convention 2.1. For each pair of associate irreducible elements $\{\varphi, -\varphi\}$ of $\mathbb{Z}[x_0, x_1]$, fix a choice of one or the other element, so that we can speak of "the" irreducible factors of a non-zero element of $\mathbb{Z}[x_0, x_1]$. We make the convention that for the pair $\{x_0, -x_0\}$ we choose x_0.

With notation as in Notation 2.2, look at the forms $j_0(x_0, x_1)$, $j_1(x_0, x_1)$, and $j_1(x_0, x_1) - 1728 j_0(x_0, x_1)$ associated to the j-invariant of $\mathcal{E}$. Let's denote by $\mathcal{F}$ the union of the set of irreducible factors over $\mathbb{Z}$ with positive degree of these three forms and the set $\{x_0\}$. Let $\mathcal{J}_0$, $\mathcal{J}_1$, and $\mathcal{J}_{1728}$ denote the collections of those forms in $\mathcal{F}$ which are factors of $j_0(x_0, x_1)$, $j_1(x_0, x_1)$, and $j_1(x_0, x_1) - 1728 j_0(x_0, x_1)$ respectively. $\mathcal{J}_0$, $\mathcal{J}_1$, and $\mathcal{J}_{1728}$ are pairwise disjoint, since $j_0(x_0, x_1)$ and $j_1(x_0, x_1)$ are relatively prime over $\mathbb{Z}$. Let's denote by $c(x_0, x_1)$ the primitive form obtained by taking the product of all irreducible factors over $\mathbb{Z}$ of $d_1(x_0, x_1)$ of positive degree which do not belong to $\mathcal{F}$. Finally, note that $d_0(x_0, x_1) = x_0^{\deg d}$. Theorem 1 of the Introduction can be restated as follows:

THEOREM 2.1. *Let $j(t) \in \mathbb{Q}(t) \setminus \mathbb{Q}$, $d(t) \in \mathbb{Z}[t] \setminus \{0\}$, and let $\mathcal{E}$ be given by Equation* (2.1). *With notations as above, assume the following:*

(1) *Each $f \in \mathcal{F}$ has degree less than or equal to* 6.

(2) *If $x \in \mathbb{P}^1(\mathbb{C})$ is a pole of j, then* $\operatorname{ord}_x j \not\equiv \operatorname{ord}_x d \pmod 2$.

Then T^+ and T^- are both dense in $\mathbb{R}$.

In order to prove this theorem we need to set up more notation and to prove some preliminary lemmas.

Notation 2.3. If $q \in \mathbb{Z}[t]$ (or $q \in \mathbb{Z}[x_0, x_1]$) is irreducible of positive degree and $r \in \mathbb{Q}(t)$ (or $r \in \mathbb{Q}(x_0, x_1)$), we denote the multiplicity of q in r by $\operatorname{ord}_q r$.

Notation 2.4. Let $\Delta(x_0, x_1) \in \mathbb{Q}(x_0, x_1)$ be obtained by homogenizing the discriminant $\Delta(t)$ of $\mathcal{E}$, given by formula (2.4). So

$$\Delta(x_0, x_1) = \frac{j_1(x_0, x_1)^8 d_1(x_0, x_1)^6}{x_0^{6 \deg d} j_0(x_0, x_1)^5 (j_1(x_0, x_1) - 1728 j_0(x_0, x_1))^3}.$$

Let's write $\Delta(x_0, x_1)$ as

$$\Delta(x_0, x_1) = AB^{-1}c(x_0, x_1)^6 J_0(x_0, x_1)\left[\prod_{i\in\{1,2,3,4,6\}} F_i(x_0, x_1)\right] \tag{2.5}$$

where $A, B \in \mathbb{Z} \setminus \{0\}$,

$$J_0(x_0, x_1) = \prod_{f\in\mathcal{J}_0} f(x_0, x_1)^{\mathrm{ord}_f \Delta}$$

and, for $i = 1, 2, 3, 4, 6$,

$$F_i(x_0, x_1) = \prod_{f\in\mathcal{F}_i} f(x_0, x_1)^{\mathrm{ord}_f \Delta}$$

with $\mathcal{F}_i = \{f \in \mathcal{F} \setminus \mathcal{J}_0\colon \text{g.c.d.}(\mathrm{ord}_f\Delta, 12) = 12/i\}$. Note that $\mathcal{F} \setminus \mathcal{J}_0 = \coprod_i \mathcal{F}_i$, where $\coprod$ denotes disjoint union. Finally, let

$$\mathcal{L} = \{c(x_0, x_1)\} \cup (\mathcal{F} \setminus \mathcal{F}_1)$$

Notation 2.5. Let

$$F(x_0, x_1) = x_1^{\alpha}\left[\prod_{f\in\mathcal{F}} f(x_0, x_1)\right]$$

where $\alpha \in \{0, 1\}$ is chosen so that x_1 appears in $F(x_0, x_1)$ with multiplicity 1. $F(x_0, x_1)$ is a primitive form, since it is a product of primitive forms. Moreover, it has no multiple factors over $\mathbb{C}$.

Notation 2.6. If $\mathcal{P}$ is a finite set of primes and $z \in \mathbb{Z}$, we write $z = z_{\mathcal{P}} z'_{\mathcal{P}}$ where $z_{\mathcal{P}} = \prod_{p\in\mathcal{P}} p^{\mathrm{ord}_p z}$. So $z'_{\mathcal{P}}$ is the "non-$\mathcal{P}$-part" of z.

Notation 2.7. We use the standard notation for the Kronecker symbols, i.e. if $z \in \mathbb{Z}$ and g.c.d.$(z,\ 6) = 1$, we set

$$\left(\frac{-1}{z}\right) = \begin{cases} +1, & \text{if } z \equiv +1 \pmod 4 \\ -1, & \text{if } z \equiv -1 \pmod 4 \end{cases}$$

$$\left(\frac{-2}{z}\right) = \begin{cases} +1, & \text{if } z \equiv 1 \text{ or } -5 \pmod 8 \\ -1, & \text{if } z \equiv 5 \text{ or } -1 \pmod 8 \end{cases}$$

$$\left(\frac{-3}{z}\right) = \begin{cases} +1, & \text{if } z \equiv +1 \pmod 3 \\ -1, & \text{if } z \equiv -1 \pmod 3 \end{cases}$$

LEMMA 2.1. *With notations as above, there exists a finite set of primes $\mathcal{P}_1$, containing* 2 *and* 3, *such that the following holds. Let $\mathcal{P}$ be a finite set of primes containing $\mathcal{P}_1$, let $\gamma \in \{\pm 1\}$ and let $(a, b) \in \mathbb{N}_{>0} \times \mathbb{N}$ be such that $j(\gamma b/a)$ is defined, $j(\gamma b/a) \neq 0, 1728$, and $d(\gamma b/a) \neq 0$. Let $P = (a, \gamma b)$. Assume*

(1) *For each* $p \notin \mathcal{P}$, $p^2 \nmid F(P)$.

(2) *If* $x \in \mathbb{P}^1(\mathbb{C})$ *is a pole of* j, *then* $\mathrm{ord}_x j \not\equiv \mathrm{ord}_x d \pmod 2$.

Then

$$W\left(\gamma\frac{b}{a}\right) = -\mathrm{sign}\left(\prod_{f\in\mathcal{L}} f(P)\right)\left[\prod_{p\in\mathcal{P}} W_p\left(\gamma\frac{b}{a}\right)\right]\left[\prod_{f\in\mathcal{L}}\left(\frac{-\beta_f}{(f(P))'_{\mathcal{P}}}\right)\right] \tag{2.6}$$

where, for each $f \in \mathcal{L}$,

$$\beta_f = \begin{cases} 1, & \text{if } f \in \mathcal{L}\setminus(\mathcal{F}_3 \cup \mathcal{F}_4),\\ 3, & \text{if } f \in \mathcal{F}_3,\\ 2, & \text{if } f \in \mathcal{F}_4.\end{cases}$$

Proof. Since $c(x_0, x_1)$ and $e(x_0, x_1) := \prod_{f\in\mathcal{F}} f(x_0, x_1)$ are relatively prime over $\mathbb{Q}$, there exist forms $m(x_0, x_1)$, $n(x_0, x_1) \in \mathbb{Z}[x_0, x_1]$ such that

$$m(x_0, x_1)c(x_0, x_1) + n(x_0, x_1)e(x_0, x_1) = l_0 x_0^L$$

for some $l_0 \in \mathbb{N}_{>0}$ and some $L \in \mathbb{N}$. Let

$$\mathcal{P}_1 = \{p \text{ prime: } p \mid 2\cdot 3\cdot A\cdot B\} \cup \{p \text{ prime: } p \mid l_0\} \cup \{p \text{ prime: } p \mid c_0\},$$

where c_0 is the coefficient of the term not containing the variable x_0 in $c(x_0, x_1)$ (recall that $x_0 \nmid c(x_0, x_1)$ by definition of $c(x_0, x_1)$ and the fact that $x_0 \in \mathcal{F}$) and let $\mathcal{P}$ be a finite set of primes containing $\mathcal{P}_1$.

First of all let's observe that if $p \notin \mathcal{P}$ and $p \mid f(P)$ for some $f \in \mathcal{F}$, then $p \nmid c(P)$. To prove this, we distinguish two cases: (i) $p \nmid a$ and (ii) $p \mid a$.

(i) If $p \nmid a$, then $p \mid f(P)$ and $p \mid c(P)$ would imply $p \mid l_0$, which is impossible since $p \notin \mathcal{P}_1$.

(ii) If $p \mid a$, then $p \nmid b$ by hypothesis (1) because $x_0 x_1 \mid F(x_0, x_1)$, and $p \nmid c_0$ since $p \notin \mathcal{P}_1$. Now, $x_0 \nmid c(x_0, x_1)$. Since p divides a but not b or c_0, it follows that p does not divide $c(P)$.

Now, let $p \notin \mathcal{P}$. By (1) and by the previous observation, we have that p can divide at most one element in the set $\{c(P)\} \cup \{f(P)\colon f \in \mathcal{F}\}$. So, since $\mathcal{F} = \mathcal{J}_0 \coprod (\coprod_i \mathcal{F}_i)$, exactly one of the following occurs:

(I) $p \nmid c(P)\left[\prod_{f\in\mathcal{F}} f(P)\right]$,

(II) $p \mid c(P)$,

(III) $p \mid f(P)$ for some $f \in \mathcal{F}_1$,

(IV) $p \mid f(P)$ for some $f \in \mathcal{F}_2$,

(V) $p \mid f(P)$ for some $f \in \mathcal{F}_3$,

(VI) $p \mid f(P)$ for some $f \in \mathcal{F}_4$,

(VII) $p \mid f(P)$ for some $f \in \mathcal{F}_6$,

(VIII) $p \mid f(P)$ for some $f \in \mathcal{J}_0$.

Since $j_0(x_0, x_1)$ is an integer constant times a product of powers of elements of $\mathcal{J}_0$, we have that in case (VIII) $E_{\gamma \frac{b}{a}}$ has potential multiplicative reduction at p, while in all the other cases $E_{\gamma \frac{b}{a}}$ has potential good reduction at p. By formula (2.5), we have that

$$\Delta\left(\gamma \frac{b}{a}\right) = AB^{-1}c(P)^6 J_0(P)\left[\prod_{i\in\{1,2,3,4,6\}} F_i(P)\right]. \tag{2.7}$$

Moreover, by formula (2.3), we have

$$-\frac{c_4}{c_6}\left(\gamma \frac{b}{a}\right) = \frac{a^{\deg d} j_0(P)}{d_1(P) j_1(P)}. \tag{2.8}$$

Then, using (2.7) and (2.8), and the fact that – by hypothesis (1) – if p divides $f(P)$ for some $f \in \mathcal{F}$, then it does so with multiplicity 1, we get the following:

(I) If $p \nmid c(P)\left[\prod_{f\in\mathcal{F}} f(P)\right]$, then $E_{\gamma \frac{b}{a}}$ has good reduction at p and $W_p(\gamma b/a) = 1$.

(II) If $p \mid c(P)$, then $E_{\gamma \frac{b}{a}}$ has potential good reduction at p and $\operatorname{ord}_p\Delta(\gamma b/a) = 6 \operatorname{ord}_p c(P)$. Thus

$$W_p\left(\gamma \frac{b}{a}\right) = \begin{cases} 1 = \left(\frac{-1}{p}\right)^2, & \text{if } \operatorname{ord}_p c(P) \text{ is even,} \\ \left(\frac{-1}{p}\right), & \text{if } \operatorname{ord}_p c(P) \text{ is odd} \end{cases}$$

by [9] Proposition 2(v).

(III)–(VII) If $i \in \{1,2,3,4,6\}$ and $p \mid f(P)$ for some $f \in \mathcal{F}_i$, then $E_{\gamma \frac{b}{a}}$ has potential good reduction at p and g.c.d.$(\operatorname{ord}_p\Delta(\gamma b/a), 12) =$ g.c.d.$(\operatorname{ord}_f\Delta, 12) = 12/i$, so

$$W_p\left(\gamma \frac{b}{a}\right) = \begin{cases} 1, & \text{if } i = 1 \\ \left(\frac{-1}{p}\right), & \text{if } i = 2,6 \\ \left(\frac{-2}{p}\right), & \text{if } i = 4 \\ \left(\frac{-3}{p}\right), & \text{if } i = 3 \end{cases}$$

by [9] Proposition 2(v).

(VIII) If $p \mid f(P)$ for some $f \in \mathcal{J}_0$, then $E_{\gamma \frac{b}{a}}$ has potential multiplicative reduction at p and

$$\operatorname{ord}_p\left[-\frac{c_4}{c_6}\left(\gamma \frac{b}{a}\right)\right] = \operatorname{ord}_f\left(\frac{1}{jd}\right).$$

The right-hand side is odd by hypothesis (1). Thus $E_{\gamma \frac{b}{a}}$ has additive reduction at p and $W_p(\gamma b/a) = \left(\frac{-1}{p}\right)$, by [9] Proposition 3(ii).

From the considerations above we have that

$$\prod_{p\notin\mathcal{P}} W_p\left(\gamma\frac{b}{a}\right) = \left[\prod_{\substack{p\notin\mathcal{P}\\ p|c(P)}} W_p\left(\gamma\frac{b}{a}\right)\right]\left[\prod_{f\in\mathcal{F}\setminus\mathcal{F}_1}\prod_{\substack{p\notin\mathcal{P}\\ p|f(P)}} W_p\left(\gamma\frac{b}{a}\right)\right], \tag{2.9}$$

where

$$\prod_{\substack{p\notin\mathcal{P}\\ p|c(P)}} W_p\left(\gamma\frac{b}{a}\right) = \left[\prod_{\substack{p\notin\mathcal{P}\\ p|c(P)\\ \mathrm{ord}_p c(P)\mathrm{even}}}\left(\frac{-1}{p}\right)^2\right]\left[\prod_{\substack{p\notin\mathcal{P}\\ p|c(P)\\ \mathrm{ord}_p c(P)\mathrm{odd}}}\left(\frac{-1}{p}\right)\right],$$

so

$$\prod_{\substack{p\notin\mathcal{P}\\ p|c(P)}} W_p\left(\gamma\frac{b}{a}\right) = \left(\frac{-1}{|(c(P))'_{\mathcal{P}}|}\right).$$

Hence

$$\prod_{\substack{p\notin\mathcal{P}\\ p|c(P)}} W_p\left(\gamma\frac{b}{a}\right) = \mathrm{sign}(c(P))\left(\frac{-1}{(c(P))'_{\mathcal{P}}}\right). \tag{2.10}$$

Moreover, for all $f\in\mathcal{F}\setminus\mathcal{F}_1$, we have

$$\prod_{\substack{p\notin\mathcal{P}\\ p|f(P)}} W_p\left(\gamma\frac{b}{a}\right) = \prod_{\substack{p\notin\mathcal{P}\\ p|f(P)}}\left(\frac{-\beta_f}{p}\right) = \left(\frac{-\beta_f}{|(f(P))'_{\mathcal{P}}|}\right)$$

where

$$\beta_f = \begin{cases} 1, & \text{if } f\in\mathcal{F}_2\cup\mathcal{F}_6\cup\mathcal{J}_0,\\ 3, & \text{if } f\in\mathcal{F}_3,\\ 2, & \text{if } f\in\mathcal{F}_4.\end{cases}$$

Hence, for all $f\in\mathcal{F}\setminus\mathcal{F}_1$, we have

$$\prod_{\substack{p\notin\mathcal{P}\\ p|f(P)}} W_p\left(\gamma\frac{b}{a}\right) = \mathrm{sign}(f(P))\left(\frac{-\beta_f}{(f(P))'_{\mathcal{P}}}\right). \tag{2.11}$$

Plugging (2.10) and (2.11) in (2.9) we get

$$\prod_{p\notin\mathcal{P}} W_p\left(\gamma\frac{b}{a}\right) = \mathrm{sign}\left(\prod_{f\in\mathcal{L}} f(P)\right)\left[\prod_{f\in\mathcal{L}}\left(\frac{-\beta_f}{(f(P))'_{\mathcal{P}}}\right)\right]. \tag{2.12}$$

From this (2.6) follows in view of the fact that

$$W\left(\gamma\frac{b}{a}\right) = -\prod_{p<\infty} W_p\left(\gamma\frac{b}{a}\right)$$
$$= -\left[\prod_{p\in\mathcal{P}} W_p\left(\gamma\frac{b}{a}\right)\right]\left[\prod_{p\notin\mathcal{P}} W_p\left(\gamma\frac{b}{a}\right)\right] .$$

(see [9] formula (1.3)). □

LEMMA 2.2. *Let* $\gamma \in \{\pm 1\}$ *and* $(a_0, b_0) \in \mathbb{N}_{>0} \times \mathbb{N}$ *be such that* $j(\gamma b_0/a_0)$ *is defined,* $j(\gamma b_0/a_0) \neq 0, 1728$, *and* $d(\gamma b_0/a_0) \neq 0$. *Let* p *be a prime. Then, if* $N_p \in \mathbb{N}$ *is big enough, for each* $(a, b) \in \mathbb{N}_{>0}\times\mathbb{N}$ *with* $(a, b) \equiv (a_0, b_0) \pmod{p^{N_p}}$, *we have* $W_p(\gamma b/a) = W_p(\gamma b_0/a_0)$.

Note. For N_p big enough we have that if $(a, b) \in \mathbb{N}_{>0}\times\mathbb{N}$ is such that $(a, b) \equiv (a_0, b_0)$ $\pmod{p^{N_p}}$, then $j(\gamma b/a)$ is defined, $j(\gamma b/a) \neq 0, 1728$, and $d(\gamma b/a) \neq 0$. So it makes sense to talk about $W_p(\gamma b/a)$.

Proof. See Appendix.

The following is just a result about polynomials.

LEMMA 2.3. *Let* $r(x)$ *and* $s(x) \in \mathbb{Z}[x]$ *with* $r(x)$ *non-constant. Let* $R = \mathrm{Res}(r, s)$ *be the resultant of* r *and* s *and let* Δ_r *be the discriminant of* r. *Assume* R, $\Delta_r \neq 0$. *Then, if* $\mathcal{P}_0$ *is any finite set of primes, there exists a prime* $p_0 \notin \mathcal{P}_0$ *and a positive integer* n_0 *such that* $p_0^2 \mid r(n_0)$ *and* $p_0^{-2}r(n_0)s(n_0) \equiv 1 \pmod{p_0}$. *In particular,* $p_0^2 \| r(n_0)$ *and* $p_0 \nmid s(n_0)$.

Proof. Since $r(x)$ is non-constant, there are infinitely many primes p such that the equation $r(x) \equiv 0 \pmod{p}$ has a solution. Choose such a prime p_0 with $p_0 \notin \mathcal{P}_0$, $p_0 \nmid R$, and $\mathrm{ord}_{p_0}\Delta_r = 0$. Let $n_{0,0}$ be a positive integer such that $r(n_{0,0}) \equiv 0 \pmod{p_0}$. Since $\mathrm{ord}_{p_0}\Delta_r = 0$, by Hensel's Lemma, we can lift $n_{0,0}$ to a root $\tilde{n}_0$ of $r(x)$ in $\mathbb{Z}_p$. Write $\tilde{n}_0 = n_{0,0} + n_{0,1}p_0 + n_{0,2}p_0^2 + \dots$. Let $\bar{n}_0 = n_{0,0} + n_{0,1}p_0 + n_{0,2}p_0^2$, so $r(\bar{n}_0) \equiv 0 \pmod{p_0^3}$. Note that $r'(\bar{n}_0) \not\equiv 0 \pmod{p_0}$, since $\mathrm{ord}_{p_0}\Delta_r = 0$, and $s(\bar{n}_0) \equiv s(n_{0,0}) \not\equiv 0 \pmod{p_0}$, since $p_0 \nmid R$ so r and s have no common roots $\pmod{p_0}$. Let

$$m \equiv \frac{s(\bar{n}_0)^{-1} - r(\bar{n}_0)p_0^{-2}}{r'(\bar{n}_0)} \pmod{p_0}$$

and let $n_0 = \bar{n}_0 + mp_0^2$. Then we have

$$r(n_0) \equiv r(\bar{n}_0) \equiv 0 \pmod{p_0^2}$$

and

$$r(n_0) = r(\bar{n}_0 + mp_0^2) = r(\bar{n}_0) + r'(\bar{n}_0)mp_0^2 + \sum_{n\geqslant 2} a_n(mp_0^2)^n,$$

where $a_n \in \mathbb{Z}$ for all n and $a_n = 0$ for n sufficiently large. Thus

$$p_0^{-2}r(n_0)s(n_0) \equiv p_0^{-2}r(\bar{n}_0)s(\bar{n}_0) + r'(\bar{n}_0)ms(\bar{n}_0) \equiv 1 \pmod{p_0}$$

by the choice of m, and we are done. □

Notation 2.8. Let $\mathcal{P}$ be a finite set of primes containing 2 and 3. Let $\gamma \in \{\pm 1\}$ and $(a, b) \in \mathbb{N}_{>0} \times \mathbb{N}$ be such that $j(\gamma b/a)$ is defined, $j(\gamma b/a) \neq 0, 1728$, and $d(\gamma b/a) \neq 0$. Let $P = (a, \gamma b)$. We denote by $W_{\mathcal{P},P}$ the quantity

$$W_{\mathcal{P},P} = -\left[\prod_{p \in \mathcal{P}} W_p\left(\gamma \frac{b}{a}\right)\right]\left[\prod_{f \in \mathcal{L}}\left(\frac{-\beta_f}{(f(P))'_{\mathcal{P}}}\right)\right].$$

So, if j, d, $\mathcal{P}$, and P satisfy the hypotheses of Lemma 2.1, we have

$$W_{\mathcal{P},P} = \operatorname{sign}\left(\prod_{f \in \mathcal{L}} f(P)\right) W\left(\gamma \frac{b}{a}\right).$$

COROLLARY 2.1. *With notation as above, assume that j is non-constant and that hypothesis* (2) *of Lemma* 2.1 *is satisfied. Let $\gamma \in \{\pm 1\}$ and let $\mathcal{P}_0$ be a finite set of primes containing* 2 *and* 3. *Then there exist a prime $p_0 \notin \mathcal{P}_0$ and a pair $(a_0, b_0) \in \mathbb{N}^2_{>0}$ with $j(\gamma b_0/a_0)$ defined, $j(\gamma b_0/a_0) \neq$ 0,1728, and $d(\gamma b_0/a_0) \neq$ 0, such that $W_{\mathcal{P}_0,P_0} = -W_{\mathcal{P}_0 \cup \{p_0\},P_0}$, where $P_0 = (a_0, \gamma b_0)$.*

Note. With the notation as in the Introduction, we choose one of the sets $\mathcal{P}^+$ and $\mathcal{P}^-$ to be $\mathcal{P}_0$ and the other $\mathcal{P}_0 \cup \{p_0\}$.

Proof. Since j is non-constant, $\mathcal{J}_0$ is non-empty. Fix any $\bar{f} \in \mathcal{J}_0$. Then $\bar{f}(x_0, x_1)$ has positive degree, so either $\bar{f}(1, \gamma x)$ has positive degree or otherwise $\bar{f}(x, \gamma) = x$.

Case A. $\bar{f}(1, \gamma x)$ has positive degree.
Apply Lemma 2.3 to $\mathcal{P}_0$ and to the polynomials $r(x) = \bar{f}(1, \gamma x)$ and $s(x) = D(1, \gamma x)$ $\bar{f}(1, \gamma x)^{-\mathrm{ord}_{\bar{f}} D}$, where we take

$$\begin{aligned} D(x_0, x_1) &= j_0(x_0, x_1) j_1(x_0, x_1) x_0^{\deg d} d_1(x_0, x_1) \\ &\quad \times \left(j_1(x_0, x_1) - 1728 j_0(x_0, x_1)\right)^2, \end{aligned}$$

so that $D(x_0, x_1)$ and $-\frac{c_4}{c_6}\left(\frac{x_1}{x_0}\right)$ differ by the square of some element of $\mathbb{Q}(x_0, x_1)^\times$. Note that $R = \mathrm{Res}(r, s) \neq 0$ since r and s are relatively prime polynomials, and $\Delta_r \neq 0$ since r is irreducible over $\mathbb{Q}$. Let p_0 and n_0 be as in Lemma 2.3 and take $a_0 = 1$ and $b_0 = n_0$. After replacing b_0 by $b_0 + np_0^3$ for some $n \in \mathbb{N}$, we can assume that $j(\gamma b_0/a_0)$ is defined, $j(\gamma b_0/a_0) \neq$ 0,1728, and $d(\gamma b_0/a_0) \neq 0$. Since $p_0 \nmid s(b_0) = s(n_0)$ by construction, and since, for each $f \in \mathcal{L} \setminus \{\bar{f}\}$, $f(1, \gamma x)$ divides $s(x)$, we have

$$(f(P_0))'_{\mathcal{P}_0} = (f(P_0))'_{\mathcal{P}_0 \cup \{p_0\}}, \quad \text{for all } f \in \mathcal{L} \setminus \{\bar{f}\},$$

thus

$$\left(\frac{-\beta_f}{(f(P_0))'_{\mathcal{P}_0}}\right) = \left(\frac{-\beta_f}{(f(P_0))'_{\mathcal{P}_0 \cup \{p_0\}}}\right), \quad \text{for all } f \in \mathcal{L} \setminus \{\bar{f}\}.$$

Moreover, since $p_0^2 \| \bar{f}(P_0)$ by construction, we have

$$(\bar{f}(P_0))'_{\mathcal{P}_0} = p_0^2(\bar{f}(P_0))'_{\mathcal{P}_0 \cup \{p_0\}}$$

so

$$\left(\frac{-\beta_{\bar{f}}}{(\bar{f}(P_0))'_{\mathcal{P}_0}}\right) = \left(\frac{-\beta_{\bar{f}}}{(\bar{f}(P_0))'_{\mathcal{P}_0 \cup \{p_0\}}}\right)$$

(of course $\beta_{\bar{f}} = 1$). Thus

$$\prod_{f \in \mathcal{L}} \left(\frac{-\beta_f}{(f(P_0))'_{\mathcal{P}_0}}\right) = \prod_{f \in \mathcal{L}} \left(\frac{-\beta_f}{(f(P_0))'_{\mathcal{P}_0 \cup \{p_0\}}}\right).$$

To finish the proof it is enough to show that $W_{p_0}(\gamma b_0/a_0) = -1$. By the choice of (a_0, b_0), we have that $\mathrm{ord}_{p_0} j(\gamma b/a) = -2 \,\mathrm{ord}_{\bar{f}} j_0 < 0$ and $\mathrm{ord}_{p_0} D(P_0) = 2 \,\mathrm{ord}_{\bar{f}} D$ is even. So $E_{\gamma \frac{b_0}{a_0}}$ has multiplicative reduction at p_0. Moreover, since hypothesis (2) of Lemma 2.1 is satisfied, we have that $\mathrm{ord}_{\bar{f}} D = \mathrm{ord}_{\bar{f}} j_0 + \mathrm{ord}_{\bar{f}} d_1$ is odd, so

$$(D(P_0))'_{\{p_0\}} = (\text{square}) p_0^{-2} r(n_0) s(n_0) \equiv (\text{square}) \cdot 1 \pmod{p_0}.$$

Thus $E_{\gamma \frac{b_0}{a_0}}$ has split multiplicative reduction at p_0 and $W_{p_0}(\gamma b_0/a_0) = -1$, by [9] Proposition 3(iii).

Case B. $\bar{f}(x, \gamma) = x$.
Proceed in a fashion similar to what was done in case A, applying Lemma 2.3 to $\mathcal{P}_0$ and to the polynomials $r(x) = \bar{f}(x, \gamma) = x$ and $s(x) = D(x, \gamma)\bar{f}(x, \gamma)^{-\mathrm{ord}_{\bar{f}} D}$, where $D(x_0, x_1)$ is defined as in case A, and taking p_0 as in Lemma 2.3, and $a_0 = n_0$ and $b_0 = 1$. □

We can finally proceed to the proof of Theorem 2.1.

Proof of Theorem 2.1. Fix $\epsilon \in \{\pm 1\}$. Fix $\bar{t} \in \mathbb{R}$ with $j(\bar{t})$ defined, $j(\bar{t}) \neq 0, 1728$, and $d(\bar{t}) \neq 0$. In particular, $\prod_{f \in \mathcal{L}} f(1, \bar{t}) \neq 0$, where $\mathcal{L}$ is as in Notations 2.4. Let $\gamma = \mathrm{sign}(\bar{t})$, $r = \gamma \bar{t} = |\bar{t}| > 0$, $\epsilon' = \epsilon \cdot \mathrm{sign}\left(\prod_{f \in \mathcal{L}} f(1, \bar{t})\right)$. Let

$$\mathcal{P}_0 = \mathcal{P}_1 \cup \{p \text{ prime: } p \leqslant \deg F(x_0, x_1)\}$$

where $\mathcal{P}_1$ is as in Lemma 2.1. Apply Corollary 2.1 to these choices for γ and $\mathcal{P}_0$ and let p_0, (a_0, b_0), and $P_0 = (a_0, \gamma b_0)$ be as in Corollary 2.1. Let

$$\mathcal{P} = \begin{cases} \mathcal{P}_0, & \text{if } W_{\mathcal{P}_0, P_0} = \epsilon' \\ \mathcal{P}_0 \cup \{p_0\}, & \text{otherwise.} \end{cases}$$

Thus $W_{\mathcal{P}, P_0} = \epsilon'$.

For each $p \in \mathcal{P}$, choose N_p big enough so that Lemma 2.2 holds. Also take N_p bigger than $2 + \max\{\mathrm{ord}_p f(P_0) \colon f \in \mathcal{L}\}$. Let $M = \prod_{p \in \mathcal{P}} p^{N_p}$ and apply Proposition 1.1 to

$F(x_0, \gamma x_1)$, M, (a_0, b_0), and $\mathcal{P}$. For $(a, b) \in \mathbb{N}^2$, write $P = (a, \gamma b)$. Then with notation as in Proposition 1.1, for $x, y \to \infty$ with $x \ll y \ll x$, we have

$$N_{\mathcal{P}}(x, y) = A^{\mathcal{P}} xy + \mathrm{O}\big(x^2/\log^{1/3} x\big).$$

If $p \notin \mathcal{P}$, then p does not divide some coefficient of F (since F is primitive), $p \nmid M$, and $p > \deg F$. Thus $A^{\mathcal{P}} \neq 0$ by Remark 1.1.

Let n be a large positive integer. Set $x_n = n$, $y_n = rn$, and $\Delta_n = n/\log^{1/7} n$ and proceed as in [9] Section 6. We get that $N_{\mathcal{P}}(x_n + \Delta_n, y_n + \Delta_n) - N_{\mathcal{P}}(x_n + \Delta_n, y_n) - N_{\mathcal{P}}(x_n, y_n + \Delta_n) + N_{\mathcal{P}}(x_n, y_n) = A^{\mathcal{P}} n^2/\log^{2/7} n + \mathrm{O}(n^2/\log^{1/3} n)$. So, for $n \gg 0$, there exists $(a_n, b_n) \in \mathbb{N}^2$ such that $x_n < a_n \leqslant x_n + \Delta_n$, $y_n < b_n \leqslant y_n + \Delta_n$, $(a_n, b_n) \equiv (a_0, b_0) \pmod{M}$, and $p^2 \nmid F(P_n)$ for all $p \notin \mathcal{P}$, where $P_n = (a_n, \gamma b_n)$. Note that $\lim_{n\to\infty} b_n/a_n = r = |\bar{t}|$, so $\lim_{n\to\infty} \gamma b_n/a_n = \bar{t}$. Thus, for $n \gg 0$, a_n and b_n are positive integers such that $j(\gamma b_n/a_n)$ is defined, $j(\gamma b_n/a_n) \neq 0, 1728$, and $d(\gamma b_n/a_n) \neq 0$. Moreover, j, d, $\mathcal{P}$, and P_n satisfy hypotheses (1) and (2) of Lemma 2.1, so $W(\gamma b_n/a_n)$ is given by formula (2.6) with P_n in place of P. Now, for each $p \in \mathcal{P}$, we have $(a_n, b_n) \equiv (a_0, b_0) \pmod{p^{N_p}}$, so $W_p(\gamma b_n/a_n) = W_p(\gamma b_0/a_0)$ by Lemma 2.2. Moreover, by the choice of the N_p's, we have that for each $f \in \mathcal{L}$

$$\mathrm{ord}_p f(P_n) = \mathrm{ord}_p f(P_0), \quad \text{for all } p \in \mathcal{P},$$

and

$$(f(P_n))'_{\mathcal{P}} \equiv (f(P_0))'_{\mathcal{P}} \pmod{24}.$$

Thus, for each $f \in \mathcal{L}$,

$$\left(\frac{-\beta_f}{(f(P_n))'_{\mathcal{P}}}\right) = \left(\frac{-\beta_f}{(f(P_0))'_{\mathcal{P}}}\right).$$

Finally, since $\lim_{n\to\infty} \gamma b_n/a_n = \bar{t}$, for $n \gg 0$ we have

$$\begin{aligned}\mathrm{sign}\Bigg(\prod_{f\in\mathcal{L}} f(P_n)\Bigg) &= \mathrm{sign}\Bigg(\prod_{f\in\mathcal{L}} f\left(1, \gamma\frac{b_n}{a_n}\right)\Bigg)\\ &= \mathrm{sign}\Bigg(\prod_{f\in\mathcal{L}} f(1, \bar{t})\Bigg) = \epsilon\cdot\epsilon'.\end{aligned}$$

So, using (2.6), we get for $n \gg 0$

$$W\left(\gamma\frac{b_n}{a_n}\right) = \epsilon\cdot\epsilon' W_{\mathcal{P},P_0} = \epsilon(\epsilon')^2 = \epsilon.$$

Hence for all $\epsilon \in \{\pm 1\}$ and for all $\bar{t} \in \mathbb{R}\backslash$(finite set) we have that there exists a sequence $\{\gamma b_n/a_n\}_n \subseteq \mathbb{Q}$ converging to $\bar{t}$ and such that $W(\gamma b_n/a_n) = \epsilon$. This concludes the proof. □

3. More on $T^{\pm}$

In this section we will prove Theorem 2 stated in the Introduction. Let's start with a couple of observations which will allow us to reduce the statement of this theorem to a simpler one. Throughout this section we follow the notation introduced in Section 2.

Let $\mathcal{E}$ be given by Equation (2.1) and assume that it satisfies the hypotheses of Theorem 2 of the Introduction. Recall that condition (2) of this theorem, namely:

there is at most one $x \in \mathbb{P}^1(\mathbb{C})$ *such that* x *is a pole of* $j(t)$ *and* $\mathrm{ord}_x c_4 \equiv \mathrm{ord}_x c_6 \pmod 2$

is equivalent to:

there is at most one $x \in \mathbb{P}^1(\mathbb{C})$ *such that* x *is a pole of* $j(t)$ *and* $\mathrm{ord}_x j \equiv \mathrm{ord}_x d \pmod 2$.

Observation 3.1. If $t_0 \in \mathbb{P}^1(\mathbb{C})$ is a pole of j with $\mathrm{ord}_{t_0} j \equiv \mathrm{ord}_{t_0} d \pmod 2$, then $t_0 \in \mathbb{P}^1(\mathbb{Q})$. This is trivial if $t_0 = \infty$. If t_0 is in $\mathbb{C}$ and is a pole of j then, since $j(t) \in \mathbb{Q}(t)$ and $d(t) \in \mathbb{Z}[t]$, t_0 is algebraic and, for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $\sigma(t_0)$ is also a pole of j with $\mathrm{ord}_{\sigma(t_0)} j = \mathrm{ord}_{t_0} j$ and $\mathrm{ord}_{\sigma(t_0)} d = \mathrm{ord}_{t_0} d$. So we must have $t_0 \in \mathbb{Q}$.

Observation 3.2. If t_0 is as in Observation 3.1, after a change of parameter of the form $t' = \frac{\mu_1 t + \mu_0}{\nu_1 t + \nu_0}$ with $\mu_0, \mu_1, \nu_0, \nu_1 \in \mathbb{Z}$ and $\mu_1\nu_0 - \mu_0\nu_1 = \pm 1$, we may assume that $t_0 = \infty$ (so that $x_0 \in \mathcal{J}_0$).

In view of these observations, in order to prove Theorem 2 of the Introduction it is enough to prove the following:

THEOREM 3.1. *With notation as in Section 2, assume that* $x_0 \in \mathcal{J}_0$. *Moreover, assume the following:*

(1) *Each* $f \in \mathcal{F}$ *has degree less than or equal to* 3.

(2) *If* $x \in \mathbb{C}$ *is a pole of* j, *then* $\mathrm{ord}_x j \not\equiv \mathrm{ord}_x d \pmod 2$.

Then T^+ *and* T^- *are both infinite.*

In order to prove this theorem, we need some preliminary lemmas.

LEMMA 3.1. *With notation as in Section 2, assume that* $x_0 \in \mathcal{J}_0$. *There exists a finite set of primes* $\mathcal{P}_1$, *containing* 2 *and* 3, *such that the following holds. Let* $\mathcal{P}$ *be a finite set of primes containing* $\mathcal{P}_1$, *let* $\gamma \in \{\pm 1\}$ *and let* $(a, b) \in \mathbb{N}_{>0} \times \mathbb{N}$ *be such that* $j(\gamma b/a)$ *is defined,* $j(\gamma b/a) \neq 0{,}1728$, *and* $d(\gamma b/a) \neq 0$. *Let* $P = (a, \gamma b)$. *Assume*

(1) *For each* $p \notin \mathcal{P}$, $p^2 \nmid F(P)$.

(2) *If* $x \in \mathbb{C}$ *is a pole of* j, *then* $\mathrm{ord}_x j \not\equiv \mathrm{ord}_x d \pmod 2$.

Then

$$W\left(\gamma \frac{b}{a}\right) = -\mathrm{sign}\left(\prod_{f \in \mathcal{L}'} f(P)\right)\left[\prod_{p \in \mathcal{P}} W_p\left(\gamma \frac{b}{a}\right)\right] \times$$

$$\times w(P)\left[\prod_{f \in \mathcal{L}'}\left(\frac{-\beta_f}{(f(P))'_{\mathcal{P}}}\right)\right] \qquad (3.1)$$

where $\mathcal{L}$ *and* β_f *are as in Lemma* 2.1, $\mathcal{L}' = \mathcal{L} \setminus \{x_0\}$, *and*

$$w(x_0, x_1) = \begin{cases} \left(\frac{-1}{(x_0)'_{\mathcal{P}}}\right), & \textit{if } \operatorname{ord}_\infty j \not\equiv \operatorname{ord}_\infty d \ (\operatorname{mod} 2), \\ \prod_{p \in \mathcal{P}_{x_0,x_1}} (-1), & \textit{if } \operatorname{ord}_\infty j \equiv \operatorname{ord}_\infty d \ (\operatorname{mod} 2), \end{cases}$$

for $\mathcal{P}_{x_0,x_1}$ *equal to the set of primes p such that* $p|(x_0)'_{\mathcal{P}}$ *and* $\left(-\frac{c_4}{c_6}\left(\frac{x_1}{x_0}\right)\right)'_{\{p\}}$ *is a square* $(\operatorname{mod} p)$.

Proof. The proof is essentially the same as that of Lemma 2.1. The only difference is that here we allow the possibility of multiplicative reduction at those primes dividing a (hypothesis (2) here is weaker than hypothesis (2) of Lemma 2.1, because x is in $\mathbb{C}$, not in $\mathbb{P}^1(\mathbb{C})$). So everything is as in the proof of Lemma 2.1, except for the case $p \notin \mathcal{P}$ and $p \mid f(P)$ for $f(x_0, x_1) = x_0 \in \mathcal{J}_0$, i.e. the case $p|a$. In this case $E_{\gamma\frac{b}{a}}$ has potential multiplicative reduction at p, and

$$\operatorname{ord}_p \left(-\frac{c_4}{c_6}\left(\gamma\frac{b}{a}\right)\right) = \operatorname{ord}_{x_0} j_0 + \deg d = -\operatorname{ord}_\infty j - \operatorname{ord}_\infty d.$$

Thus – by [9] Proposition 3(ii) and (iii) –

$$W_p\left(\gamma\frac{b}{a}\right) = \begin{cases} \left(\frac{-1}{p}\right), & \text{if } \operatorname{ord}_\infty j \not\equiv \operatorname{ord}_\infty d \ (\operatorname{mod} 2) \\ +1, & \text{if } \operatorname{ord}_\infty j \equiv \operatorname{ord}_\infty d \ (\operatorname{mod} 2) \\ & \text{and } \left(-\frac{c_4}{c_6}\left(\gamma\frac{b}{a}\right)\right)'_{\{p\}} \not\equiv \square \\ -1, & \text{if } \operatorname{ord}_\infty j \equiv \operatorname{ord}_\infty d \ (\operatorname{mod} 2) \\ & \text{and } \left(-\frac{c_4}{c_6}\left(\gamma\frac{b}{a}\right)\right)'_{\{p\}} \equiv \square \end{cases}$$

where $\square$ denotes a square $(\operatorname{mod} p)$. So

$$\prod_{\substack{p \notin \mathcal{P} \\ p|a}} W_p\left(\gamma\frac{b}{a}\right) = w(P),$$

and we are done. $\square$

Notation 3.1. Let $\mathcal{P}$ be a finite set of primes containing 2 and 3. Let $\gamma \in \{\pm 1\}$ and $(a, b) \in \mathbb{N}_{>0} \times \mathbb{N}$ be such that $j(\gamma b/a)$ is defined, $j(\gamma b/a) \neq 0, 1728$, and $d(\gamma b/a) \neq 0$. Let $P = (a, \gamma b)$. We denote by $W_{\mathcal{P},P}$ the quantity

$$W_{\mathcal{P},P} = -\left[\prod_{p \in \mathcal{P}} W_p\left(\gamma\frac{b}{a}\right)\right] w(P) \left[\prod_{f \in \mathcal{L}'} \left(\frac{-\beta_f}{(f(P))'_{\mathcal{P}}}\right)\right].$$

So, if j, d, $\mathcal{P}$, and P satisfy the hypotheses of Lemma 3.1, we have

$$W_{\mathcal{P},P} = \operatorname{sign}\left(\prod_{f \in \mathcal{L}'} f(P)\right) W\left(\gamma\frac{b}{a}\right).$$

LEMMA 3.2. *With notation as in Section 2, assume $x_0 \in \mathcal{J}_0$. Let $\mathcal{P}_0$ be a finite set of primes containing 2 and 3. Then, for each $\gamma, \epsilon' \in \{\pm 1\}$, there exist a finite set of primes $\mathcal{P}$ containing $\mathcal{P}_0$ and a pair $(a_0, b_0) \in \mathbb{N}^2_{>0}$ such that*

(i) $a_0 = \prod_{p\in\mathcal{P}} p^{N_p}$, *for some positive integers N_p.*

(ii) g.c.d.$(b_0, p) = 1$ *for all $p \in \mathcal{P}$.*

(iii) $j(\gamma b_0/a_0)$ *is defined,* $j(\gamma b_0/a_0) \neq 0{,}1728$, *and* $d(\gamma b_0/a_0) \neq 0$.

(iv) $W_{\mathcal{P},P_0} = \epsilon'$, *for* $P_0 = (a_0, \gamma b_0)$.

Proof. Let d_0, $j_{0,0}$, $j_{1,0}$, and $j_{1728,0}$ be the leading coefficients of $d(t)$, $j_0(1,x)$, $j_1(1,x)$, and $j_1(1,x) - 1728 j_0(1,x)$ respectively, so $C := d_0 \cdot j_{0,0} \cdot j_{1,0} \cdot j_{1728,0} \neq 0$. Consider the polynomial

$$g(x) = -j_{0,0} + d_0 j_{1,0}\left(\gamma\left(\left(\prod_{p\in\mathcal{P}_0} p\right)x + 1\right)\right)^{-\mathrm{ord}_\infty j - \mathrm{ord}_\infty d}.$$

Since $-\mathrm{ord}_\infty j > 0$ by hypothesis, and $-\mathrm{ord}_\infty d \geqslant 0$ because d is a polynomial, we have that $g(x)$ is non-constant. Thus the set of primes p such that the equation $g(x) = 0$ has a solution modulo p is infinite. Let $p_0 \notin \mathcal{P}_0 \cup \{p \text{ prime: } p \mid C\}$ and $m_0 \in \mathbb{N}$ be such that

$$g(m_0) \equiv 0 \pmod{p_0},$$

and let

$$b_0 = \left(\prod_{p\in\mathcal{P}_0} p\right) m_0 + 1.$$

Then we have

$$d_0 j_{1,0} (\gamma b_0)^{-\mathrm{ord}_\infty j - \mathrm{ord}_\infty d} \equiv j_{0,0} \pmod{p_0}.$$

Moreover, we have g.c.d.$(b_0, p) = 1$ for all $p \in \mathcal{P}_0$ by construction, and $p_0 \nmid b_0$ since $p_0 \nmid C$.

For each $p \in \mathcal{P}_0$, fix N_p even with $N_p > 2 + \mathrm{ord}_p C$. Take $\mathcal{Q}_1 = \mathcal{P}_0$, $\mathcal{Q}_2 = \mathcal{Q}_1 \cup \{p_0\}$, $N_{p_0} = 2$, and $a_s = \prod_{p\in\mathcal{Q}_s} p^{N_p}$ for $s = 1, 2$. Up to changing N_p, we can assume that (a_s, b_0) satisfies (iii) for $s = 1, 2$. Let $P_s = (a_s, \gamma b_0)$, for $s = 1, 2$. We will prove that $W_{\mathcal{Q}_1,P_1} = -W_{\mathcal{Q}_2,P_2}$. So for all $\epsilon' \in \{\pm 1\}$, either $\mathcal{Q}_1$ and (a_1, b_0) or $\mathcal{Q}_2$ and (a_2, b_0) will do the job.

Since $(a_1)'_{\mathcal{Q}_1} = (a_2)'_{\mathcal{Q}_2} = 1$, we have that $w(P_1) = w(P_2)$.

Now, $\mathcal{Q}_1 \subset \mathcal{Q}_2$ and for all $p \in \mathcal{Q}_1$ we have, for $s = 1, 2$,

$$\begin{aligned}\mathrm{ord}_p j\left(\gamma\frac{b_0}{a_s}\right) &= \mathrm{ord}_p \frac{j_1(a_s, \gamma b_0)}{j_0(a_s, \gamma b_0)} \\ &= \mathrm{ord}_p j_{1,0} - N_p \mathrm{ord}_{x_0} j_0 - \mathrm{ord}_p j_{0,0} < 0,\end{aligned}$$

hence $E_{\gamma\frac{b_0}{a_s}}$ has potential multiplicative reduction at p. Moreover,

$$\begin{aligned}\mathrm{ord}_p\left[-\frac{c_4}{c_6}\left(\gamma\frac{b_0}{a_s}\right)\right] &= \mathrm{ord}_p j_{0,0} + (\mathrm{ord}_{x_0} j_0 + \deg d) N_p - \\ &\quad -\mathrm{ord}_p d_0 - \mathrm{ord}_p j_{1,0}\end{aligned}$$

and

$$\left(-\frac{c_4}{c_6}\left(\gamma\frac{b_0}{a_1}\right)\right)'_{\{p\}} \equiv p_0^{-2(\mathrm{ord}_{x_0}j_0+\deg d)}\left(-\frac{c_4}{c_6}\left(\gamma\frac{b_0}{a_2}\right)\right)'_{\{p\}} \pmod{p^3}.$$

By [9] Proposition 3(ii) and (iii), it follows that

$$W_p\left(\gamma\frac{b_0}{a_1}\right) = W_p\left(\gamma\frac{b_0}{a_2}\right), \quad \text{for all } p \in \mathcal{Q}_1.$$

For $\mathcal{Q}_2$ and (a_2, b_0), look at $W_{p_0}(\gamma b_0/a_2)$. Since $N_{p_0} = 2$, we have

$$\mathrm{ord}_{p_0}j\left(\gamma\frac{b_0}{a_2}\right) = -2\ \mathrm{ord}_{x_0}j_0 < 0$$

and

$$\mathrm{ord}_{p_0}\left(-\frac{c_4}{c_6}\left(\gamma\frac{b_0}{a_2}\right)\right) = 2(\mathrm{ord}_{x_0}j_0 + \deg d)$$

is even. So $E_{\gamma\frac{b_0}{a_2}}$ has multiplicative reduction at p_0. Furthermore, by the choice of b_0 and p_0, we have

$$\left(-\frac{c_4}{c_6}\left(\gamma\frac{b_0}{a_2}\right)\right)'_{\{p_0\}} \equiv \square\cdot\frac{j_{0,0}(\gamma b_0)^{\deg j_0-\mathrm{ord}_{x_0}j_0}}{d_0 j_{1,0}(\gamma b_0)^{\deg d+\deg j_1}} \equiv \square\cdot 1 \pmod{p_0},$$

where $\square$ denotes a non-zero square. So $E_{\gamma\frac{b_0}{a_2}}$ has split multiplicative reduction at p_0 and

$$W_{p_0}\left(\gamma\frac{b_0}{a_2}\right) = -1$$

by [9] Proposition 3(iii). Thus

$$\prod_{p\in\mathcal{Q}_1} W_p\left(\gamma\frac{b_0}{a_1}\right) = -\prod_{p\in\mathcal{Q}_2} W_p\left(\gamma\frac{b_0}{a_2}\right).$$

Now, by the choice of N_p, we have that for all $p \in \mathcal{Q}_1$

$$\mathrm{ord}_p f(P_1) = \mathrm{ord}_p f(P_2), \quad \text{for all } f \in \mathcal{L}'.$$

Moreover,

$$\mathrm{ord}_{p_0} f(P_2) = 0, \quad \text{for all } f \in \mathcal{L}'.$$

So, by the choice of N_2 and N_3, we get

$$(f(P_1))'_{\mathcal{Q}_1} \equiv (f(P_2))'_{\mathcal{Q}_2} \pmod{24}, \quad \text{for all } f \in \mathcal{L}'.$$

This concludes the proof. □

Let's now proceed to the proof of Theorem 3.1.

Proof of Theorem 3.1. Fix $\epsilon \in \{\pm 1\}$. We want to show that there are infinitely many $t \in \mathbb{Q}$ with $W(t) = \epsilon$. Let $\mathcal{P}_0$ be as in the proof of Theorem 2.1. Assume that, for $x \gg 0$,

$$\operatorname{sign}\left(\prod_{f\in\mathcal{L}'} f(1,x)\right) = \eta.$$

Apply Lemma 3.2 to $\gamma = 1$ and $\epsilon' = \epsilon\cdot\eta$ and let $\mathcal{P}$, (a_0, b_0) and P_0 be as this lemma, so that $W_{\mathcal{P},P_0} = \epsilon'$. For each $p \in \mathcal{P}$ let N_p be as in the proof of Lemma 3.2. Now, apply Proposition 1.2 to $F(x) = F(a_0, x)$, $M = a_0 = \prod_{p\in\mathcal{P}} p^{N_p}$, $n_0 = b_0$, and $\mathcal{P}$. Note that $F(x)$ has no non-constant square factors and all of its irreducible factors over $\mathbb{Z}$ have degree less than or equal to 3. Then, with notation as in Proposition 1.2, for $x \to \infty$ we have

$$N_{\mathcal{P}}(x) = A_1^{\mathcal{P}} x + \mathrm{O}(x/\log^{1/2} x).$$

If $p \notin \mathcal{P}$, then p does not divide some coefficient of $F(x)$, $p \nmid M$, and $p > \deg F$ (because $p \notin \mathcal{P}_0$). Thus $A_1^{\mathcal{P}} \neq 0$ by Remark 1.2.

Now, let $x_0 > 0$ be such that:

(i) for $n > x_0$, $\operatorname{sign}\left(\prod_{f\in\mathcal{L}'} f(a_0, n)\right) = \eta$, and

(ii) for $x > x_0$, $N_{\mathcal{P}}(x) = A_1^{\mathcal{P}} x + \mathrm{O}(x/\log^{1/2} x)$.

For $x > x_0$ we then have

$$N_{\mathcal{P}}(2x) - N_{\mathcal{P}}(x) = A_1^{\mathcal{P}} x + \mathrm{O}(x/\log^{1/2} x).$$

Thus, if $x \gg 0$, there exists $n_x \in \mathbb{N}$ with $x < n_x \leqslant 2x$, $n_x \equiv b_0 \pmod{M}$, and $p^2 \nmid F(n_x)$ for all $p \notin \mathcal{P}$. Note that $\lim_{x\to\infty} n_x = \infty$, so there exist infinitely many $n \in \mathbb{N}$, with $n > x_0$, $n \equiv b_0 \pmod{M}$, and $p^2 \nmid F(n)$ for all $p \notin \mathcal{P}$. For each such n, let $a_n = a_0$, $b_n = n$, and $P_n \equiv (a_n, b_n)$. Each such P_n satisfies the hypotheses of Lemma 3.1, so $W(\gamma b_n/a_n)$ is given by formula (3.1) with P_n in place of P.

For each $p \in \mathcal{P}$, $n \equiv b_0 \pmod{p^{N_p}}$, thus – by the choice of N_p – we get

$$\mathrm{ord}_p j(\gamma b_n/a_n) = \mathrm{ord}_p j(\gamma b_0/a_0) < 0,$$

$$\mathrm{ord}_p\left(-\frac{c_4}{c_6}\left(\gamma\frac{b_n}{a_n}\right)\right) = \mathrm{ord}_p\left(-\frac{c_4}{c_6}\left(\gamma\frac{b_0}{a_0}\right)\right),$$

and

$$\left(-\frac{c_4}{c_6}\left(\gamma\frac{b_n}{a_n}\right)\right)'_{\{p\}} \equiv \left(-\frac{c_4}{c_6}\left(\gamma\frac{b_0}{a_0}\right)\right)'_{\{p\}} \pmod{p^3},$$

so

$$W_p\left(\gamma\frac{b_n}{a_n}\right) = W_p\left(\gamma\frac{b_0}{a_0}\right)$$

by [9] Proposition 3(ii) and (iii).

Since $(a_n)'_{\mathcal{P}} = (a_0)'_{\mathcal{P}} = 1$, we have that

$$w(P_n) = w(P_0).$$

Finally we have that, for all $f \in \mathcal{L}'$,

$$\mathrm{ord}_p f(P_n) = \mathrm{ord}_p f(P_0) \text{ for all } p \in \mathcal{P}.$$

Moreover, by the choice of N_2 and N_3,

$$(f(P_n))'_{\mathcal{P}} \equiv (f(P_0))'_{\mathcal{P}} \pmod{24}.$$

Thus, using formula (3.1) and Lemma 3.2, for each such n we get

$$W\left(\gamma\frac{b_n}{a_n}\right) = \eta \cdot W_{\mathcal{P},\mathcal{P}_0} = \eta \cdot \epsilon' = \epsilon.$$

This concludes the proof. □

4. Applications

In this section we are going to apply Theorem 1 stated in the Introduction to give some examples illustrating the relationship between the rank of the group of rational sections of an elliptic surface over $\mathbb{Q}$ with base $\mathbb{P}^1$ and the rank of the groups of rational points of its smooth fibers.

Both Cassels and Schinzel ([1]) and Rohrlich ([9], Section 9) – granting $(*)$ of the Introduction – provided examples in this spirit. Cassels and Schinzel considered the elliptic surface $\mathcal{E}$ given by

$$7(1+t^4)y^2 = x^3 - x$$

and showed that the group of rational sections of $\mathcal{E}$ has rank 0, while each elliptic curve arising as a fiber of $\mathcal{E}$ over some $t \in \mathbb{Q}$ has positive Mordell–Weil rank. Rohrlich provided a class of examples of elliptic surfaces with the same property. In addition, he also provided a class of examples of elliptic surfaces whose group of rational sections has rank 0 and whose smooth fibers over rational points of the base have Mordell–Weil rank greater than or equal to 2 for a dense set of $t \in \mathbb{Q}$. Both the example of Cassels and Shinzel and those of Rohrlich have the property that the elliptic surfaces in question have constant j-invariant. Still granting $(*)$ of the Introduction, we will provide examples of the same sort but where the elliptic surfaces in question have non-constant j-invariant.

First of all let's recall the following lemma of Rohrlich ([9], lemma in Section 9).

LEMMA. *Let $\mathcal{E}$ be an elliptic curve over $\mathbb{Q}(t)$. Assume that $\mathcal{E}$ is not isomorphic to a constant elliptic curve. Then, for all but finitely many square-free integers m, the rank of $\mathcal{E}^m(\mathbb{Q}(t))$ is 0, where $\mathcal{E}^m$ is the quadratic twist of $\mathcal{E}$ by m.*

As an immediate corollary of this lemma and of Theorem 1 of the Introduction, we get that if $\mathcal{E}$ satisfies the hypotheses of this theorem (so, in particular, $\mathcal{E}$ is an elliptic curve over $\mathbb{Q}(t)$ with non-constant j-invariant, hence it is not isomorphic to a constant elliptic curve) then, for all but finitely many square-free integers m, the Mordell–Weil rank of $\mathcal{E}^m$ is 0. But – granting (*) of the Introduction – the fact that T_m^- is dense in $\mathbb{R}$ implies that the rank of $E_t^m(\mathbb{Q})$ is positive for a dense set of $t \in \mathbb{Q}$ such that E_t^m is an elliptic curve (here E_t^m denotes the fiber of $\mathcal{E}^m$ over t and T_m^- denotes the set of rational t's such that E_t^m is an elliptic curve with root number -1).

Let's now look at a perhaps more interesting example. Consider the elliptic surface $\mathcal{E}$ given by

$$y^2 = 4x^3 - 3t(t-1)^2x - t(t-1)^3. \tag{4.1}$$

A basis for the (torsion free) group of sections of $\mathcal{E}$ over $\mathbb{C}$ is given by

$$\left\{(t-1, 2i(t-1)^2), \left(-\frac{1}{2}(t-1), \frac{1}{\sqrt{2}}(t-1)^2\right)\right\}$$

(see [2], Equation 5, p. 28). The group of rational sections of $\mathcal{E}$ is 0, so let's consider the quadratic twist $\mathcal{E}^-$ of $\mathcal{E}$ by -1. This is given by

$$-y^2 = 4x^3 - 3t(t-1)^2x - t(t-1)^3. \tag{4.2}$$

$\mathcal{E}^-$ is isomorphic to $\mathcal{E}$ as an elliptic curve over $\mathbb{C}(t)$, so a basis for $\mathcal{E}^-(\mathbb{C}(t))$ is given by

$$\left\{P_1 = (t-1, 2(t-1)^2), P_2 = \left(-\frac{1}{2}(t-1), \frac{i}{\sqrt{2}}(t-1)^2\right)\right\}.$$

The rank of $\mathcal{E}^-(\mathbb{Q}(t))$ (i.e. the rank of the group of rational sections of $\mathcal{E}^-$) is 1. In fact $\mathcal{E}^-(\mathbb{Q}(t)) = \langle P_1 \rangle$, the cyclic group generated by P_1. Since $\mathcal{E}^-(\mathbb{C}(t)) = \mathcal{E}^-(\bar{\mathbb{Q}}(t)) = \mathcal{E}^-(\mathbb{Q}(\sqrt{2}, i)(t))$, $\mathcal{E}^-(\mathbb{Q}(t))$ consists of those points $P \in \mathcal{E}^-(\mathbb{C}(t))$ fixed by the action of $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$ on $\mathcal{E}^-$. Now, $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}) = \langle \sigma_{-1}, \sigma_2 \rangle$ where $\sigma_{-1}(i) = -i$, $\sigma_{-1}(\sqrt{2}) = \sqrt{2}$, $\sigma_2(i) = i$, and $\sigma_2(\sqrt{2}) = -\sqrt{2}$. Thus a point $P \in \mathcal{E}^-(\mathbb{C}(t))$ is in $\mathcal{E}^-(\mathbb{Q}(t))$ if and only if $\sigma_{-1}(P) = P$ and $\sigma_2(P) = P$. From this it follows that $P \in \mathcal{E}^-(\mathbb{Q}(t)) \Leftrightarrow P \in \langle P_1 \rangle$. So $\mathcal{E}^-(\mathbb{Q}(t)) = \langle P_1 \rangle$. Now, Silverman's Specialization Theorem ([13], Chapter 3. Theorem 11.4) implies that for all but finitely many $t \in \mathbb{Q}$, $\mathrm{rank}(E_t^-(\mathbb{Q})) \geqslant 1$, where we denote by E_t^- the fiber of $\mathcal{E}^-$ over t.

Let's show that $\mathcal{E}^-$ satisfies the hypotheses of Theorem 1 of the Introduction. A Weierstrass equation for $\mathcal{E}^-$ is

$$y^2 = x^3 - 12t(t-1)^2x + 16t(t-1)^3. \tag{4.3}$$

So, the j-invariant of $\mathcal{E}^-$ is

$$j(t) = \frac{1728t}{t-1}$$

and its covariants are

$$c_4(t) = 2^6 3^2 t(t-1)^2 \quad \text{and} \quad c_6(t) = -2^9 3^3 t(t-1)^3.$$

The only pole of $j(t)$ is 1, and we have $\mathrm{ord}_1 c_4 = 2$ and $\mathrm{ord}_1 c_6 = 3$. So $\mathcal{E}^-$ satisfies the hypotheses of Theorem 1 of the Introduction. Therefore T^+ and T^- are both dense in $\mathbb{R}$.

Summarizing, $\mathcal{E}^-$ has the following properties:

(1) it has non-constant j-invariant,

(2) its group of rational sections has rank 1 (hence for all but finitely many $t \in \mathbb{Q}$, $\mathrm{rank}(E_t^-(\mathbb{Q})) \geqslant 1$),

(3) T^+ is dense in $\mathbb{R}$.

Granting $(*)$ of the Introduction, we then get that for a dense set of $t \in \mathbb{Q}$, $\mathrm{rank}(E_t^-(\mathbb{Q})) \geqslant 2$, which is strictly greater than the Mordell–Weil rank of $\mathcal{E}^-$.

Appendix

This appendix is devoted to the proof of Lemma 2.2. In order to prove this lemma, we distinguish two cases:

(1) $E_{\gamma\frac{b_0}{a_0}}$ has potential multiplicative reduction at p,

(2) $E_{\gamma\frac{b_0}{a_0}}$ has potential good reduction at p.

Notation. As usual in what follows we set $P_0 = (a_0, \gamma b_0)$ and $P = (a, \gamma b)$.

Case (1).

Proof of Lemma 2.2 in case (1). Take any $N_p \in \mathbb{N}$ with

$$N_p > 2 + \mathrm{ord}_p(a_0^{\deg d} d_1(P_0) j_0(P_0) j_1(P_0)).$$

Then, if $(a, b) \in \mathbb{N}_{>0} \times \mathbb{N}$ is such that $j(\gamma b/a)$ is defined, $j(\gamma b/a) \neq 0{,}1728$, $d(\gamma b/a) \neq 0$, and $(a, b) \equiv (a_0, b_0) \pmod{p^{N_p}}$, we have:

$$\mathrm{ord}_p j\left(\gamma \frac{b}{a}\right) = \mathrm{ord}_p j\left(\gamma \frac{b_0}{a_0}\right),$$

$$\mathrm{ord}_p \left(-\frac{c_4}{c_6}\left(\gamma \frac{b}{a}\right)\right) = \mathrm{ord}_p \left(-\frac{c_4}{c_6}\left(\gamma \frac{b_0}{a_0}\right)\right), \text{ and}$$

$$\left(-\frac{c_4}{c_6}\left(\gamma \frac{b}{a}\right)\right)'_{\{p\}} \equiv \left(-\frac{c_4}{c_6}\left(\gamma \frac{b_0}{a_0}\right)\right)'_{\{p\}} \pmod{p^3}.$$

Thus $E_{\gamma\frac{b}{a}}$ has also potential multiplicative reduction at p and $W_p\left(\gamma \frac{b}{a}\right) = W_p\left(\gamma \frac{b_0}{a_0}\right)$, by [9] Proposition 3(ii) and (iii). □

Case (2). If $p \neq 2, 3$, one could prove Lemma 2.2 with an argument analogous to that used in case (1). In what follows however, we are going to give a proof which holds for any prime p of potential good reduction, including $p = 2, 3$. We need two sublemmas.

SUBLEMMA 1. *Let K be a non-archimedean local field. Let $q(x) \in K[x]$ be a monic polynomial of degree n, and let L be the splitting field of $q(x)$ over K. If $r(x) \in K[x]$ is another monic polynomial of degree n with coefficients sufficiently close to those of*

$q(x)$, then the splitting field M of $r(x)$ over K contains L. Moreover, if $q(x)$ has no multiple roots, then $L = M$.

This is just a version of Krasner's Lemma. The statement and the proof are as in [6] p. 43–44, except that here we do not assume that $q(x)$ is irreducible. The assumption in the second part of the statement that $q(x)$ has no multiple roots is enough to conclude that $L = M$.

SUBLEMMA 2. *Let E be an elliptic curve over $\mathbb{Q}$ with Weierstrass coefficients $a_1, \ldots, a_6$. Let p be a prime, and assume that E has potential good reduction at p. Let L be the minimal extension of $\mathbb{Q}_{p,\text{ unr}}$ over which E acquires good reduction. If E' is another elliptic curve over $\mathbb{Q}$ with Weierstrass coefficients $a'_1, \ldots, a'_6$ sufficiently close to those of E with respect to the p-adic norm, then E' has potential good reduction at p and $L' = L$, where L' is the minimal extension of $\mathbb{Q}_{p,\text{ unr}}$ over which E' acquires good reduction.*

Proof. If the a'_i's are sufficiently close to the a_i's, we can put the equations of E and E' in the forms

$$E\colon\ y^2 = x^3 + Ax + B$$

and

$$E'\colon\ y^2 = x^3 + A'x + B'$$

with $A, B, A, B' \in \mathbb{Q} \cap \mathbb{Z}_p$ and $|A - A'|_p$ and $|B - B'|_p$ small. Let $j(E)$ and $j(E')$ denote the j-invariants of E and E' respectively. For (A', B') close enough to (A, B), we have $\text{ord}_p j(E') = \text{ord}_p j(E)$ if $j(E) \neq 0$, and $\text{ord}_p j(E') > 0$ if $j(E) = 0$. So E' has potential good reduction at p.

Now, (see [10], p. 498, Corollary 3), $L = \mathbb{Q}_{p,\text{ unr}}(E[m])$ and $L' = \mathbb{Q}_{p,\text{ unr}}(E'[m])$, where we can take $m = 3$ if $p = 2$, and $m = 4$ if $p > 2$. First of all let's show that, if (A', B') is close to (A, B), then $L_1 = L'_1$, where L_1 and L'_1 are obtained by adjoining to $\mathbb{Q}_{p,\text{ unr}}$ the x-coordinates of the non-trivial m-division points of E and E' respectively.

(I) For $p = 2$, we have that L_1 is the splitting field of

$$q(x) = x^4 + 2Ax^2 + 4Bx - A^2/3$$

over $\mathbb{Q}_{p,\text{ unr}}$, and L'_1 is the splitting field of

$$r(x) = x^4 + 2A'x^2 + 4B'x - (A')^2/3$$

over $\mathbb{Q}_{p,\text{ unr}}$. We have that $q(x)$ has no multiple roots, because $q'(x) = 4(x^3 + Ax + B)$, and any root of $q'(x)$ corresponds to a 2-division point of E. Thus, by Sublemma 1, $L_1 = L'_1$.

(II) For $p > 2$, recall that if $Q = (x_0, y_0)$ is a point of exact order 4 on E, then $2Q$ is a non-zero 2-division point of E, so $2Q = (\alpha, 0)$, with α a root of $x^3 + Ax + B$. Moreover, $x_0 = \alpha + \beta$ and $y_0^2 = \beta^2(3\alpha + 2\beta)$, where $\beta^2 = 3\alpha^2 + A$ (see [7], p. 218). Let M_1 be the splitting field of

$$q_1(x) = x^3 + Ax + B$$

over $\mathbb{Q}_{p,\text{ unr}}$. Then L_1 is the splitting field of

$$q_2(x) = \prod_{\eta}(x^2 - \eta)$$

over M_1, where η runs over the set

$$\{3\alpha^2 + A : \alpha \text{ is a root of } q_1(x)\}.$$

Note that neither $q_1(x)$ nor $q_2(x)$ has multiple roots (the latter since $3\alpha^2 + A \neq 0$, because α is a simple root for $q_1(x)$ and $3x^2 + A = q_1'(x)$). Similarly, let M_1' be the splitting field of

$$r_1(x) = x^3 + A'x + B'$$

over $\mathbb{Q}_{p,\text{ unr}}$. Then L_1' is the splitting field of

$$r_2(x) = \prod_{\eta'}(x^2 - \eta')$$

over M_1', where η' runs over the set

$$\{3(\alpha')^2 + A\text{: } \alpha' \text{is a root of } r_1(x)\}.$$

By Sublemma 1, we have that if (A', B') is close to (A, B), then $M_1 = M_1'$ and $L_1 = L_1'$.

Now, L is the splitting field of

$$\prod_{\xi}(y^2 - \xi)$$

over L_1, where ξ runs over the set of elements of the form $x_0^3 + Ax_0 + B$ where x_0 is the x-coordinate of some m-division point of E which is not a 2-torsion point. Similarly L' is the splitting field of

$$\prod_{\xi'}(y^2 - \xi')$$

over L_1, where ξ' runs over the set of elements of the form $(x_0')^3 + Ax_0' + B$ where x_0' is the x-coordinate of some m-division point of E' which is not a 2-torsion point. By Sublemma 1, we are done. □

We can now finish the proof of Lemma 2.2.

Proof of Lemma 2.2 in case (2). Take $E = E_{\gamma\frac{b_0}{a_0}}$ and $E' = E_{\gamma\frac{b}{a}}$. Then, for N_p big enough, E' is "close" to E with respect to the p-adic norm. Below, we follow the notation of [9]. It is enough to show that the representations $\sigma_{E,p}$ and $\sigma_{E',p}$ are equivalent for E' "close" to E with respect to the p-adic norm.

By Sublemma 2, we have that both E and E' have good reduction over $L = \mathbb{Q}_{p,\text{ unr}}(E[m])$. Both $\sigma_{E,p}$ and $\sigma_{E',p}$ can be viewed as faithful representations of $\mathcal{W}(L/\mathbb{Q}_p)$. Since $\sigma_{E,p}$ and $\sigma_{E',p}$ are semisimple, to check that they are equivalent, it is enough to check that they have the same character. So, let $g \in \mathcal{W}(L/\mathbb{Q}_p) \simeq \Lambda \rtimes \langle\Phi\rangle$, where $\Lambda = \text{Gal}(L/\mathbb{Q}_{p,\text{ unr}})$ and Φ is an inverse Frobenius element. If $g \in \Lambda$, let $\widetilde{E}_L$ and $\widetilde{E}'_L$ be the reductions of E and E' over L. If E' is sufficiently "close" to E, then $\widetilde{E}_L = \widetilde{E}'_L$. The fact that $\sigma_{E,p}(g)$ and $\sigma_{E',p}(g)$ have the same trace then follows from the commutativity of the diagram

$$\begin{array}{ccc} \Lambda & \longrightarrow & \mathrm{Aut}(\widetilde{E}_L) \\ \downarrow & & \downarrow \\ \mathrm{Aut}(T_\ell(E)) & \xrightarrow{\sim} & \mathrm{Aut}(T_\ell(\widetilde{E}_L)) \end{array}$$

where ℓ is any prime different from p (see [10], Section 2). If $g \in \Phi^n\Lambda$ for some integer $n > 0$, then g is an inverse Frobenius element of $\mathcal{W}(L/F)$, where F is the unramified extension of $\mathbb{Q}_p$ of degree n. So we may assume that $g = \Phi$. Let K be the subfield of L fixed by $\langle\Phi\rangle$. Then both E and E' have good reduction over K. Moreover, if $\widetilde{E}_K$ and $\widetilde{E}'_K$ are the reductions of E and E' over K, then $\widetilde{E}_K = \widetilde{E}'_K$ if E' is sufficiently "close" to E. From this and from the results in [10], Section 2, it follows that $\sigma_{E,p}(\Phi)$ and $\sigma_{E',p}(\Phi)$ have the same characteristic polynomial, so in particular they have the same trace. If $g \in \Phi^n\Lambda$ for some integer $n < 0$, the fact that $\sigma_{E,p}(g)$ and $\sigma_{E',p}(g)$ have the same trace follows from the case $n > 0$ discussed above and from the fact that for any invertible 2×2 matrix X, we have $\mathrm{tr}(X^{-1}) = \mathrm{tr}(X)/\det(X)$. This concludes the proof. □

Acknowledgements

This paper has been extracted from the author's PhD dissertation. The author would like to express her gratitude to her advisor David Rohrlich for his teachings, for his careful guidance, and for his valuable pieces of advice. The author would also like to thank Larry Washington for his interesting comments and Greg Grant for many mathematical discussions. Finally the author wishes to thank the referee for his/her careful review of the manuscript, and Joseph Silverman for letting her have a preprint of the chapter on elliptic surfaces in his book "Advanced Topics in the Arithmetic of Elliptic Curves".

References

1. Cassels, J. W. S. and Schinzel, A.: Selmer's conjecture and families of elliptic curves, *Bull. London Math. Soc.* **14** (1982), 345–348.
2. Cox, D. A. and Zucker, S.: Intersection numbers of sections of elliptic surfaces, *Invent. Math.* **53** (1979), 1–44.
3. Gouvêa, F. and Mazur, B.: The square-free sieve and the rank of elliptic curves, *J. Amer. Math. Soc.* **4** (1991), 1–23.
4. Greaves, G.: Power-free values of binary forms, *Quart. J. Math. Oxford* **43**(2) (1992), 45–65.
5. Hooley, C.: *Applications of Sieve Methods to the Theory of Numbers*, Cambridge University Press, Cambridge, 1976.
6. Lang, S.: *Algebraic Number Theory*, Springer-Verlag, New York, 1986.
7. Lang, S. and Trotter, H.: *Frobenius Distributions in* GL_2*-Extensions*, Lecture Notes in Math. 504, Springer-Verlag, New York, 1976.
8. Mazur, B.: The topology of rational points, *J. Experimental Math.* **1** (1992), 35–45.
9. Rohrlich, D. E.: Variation of the root number in families of elliptic curves, *Compos. Math.* **87** (1993), 119–151.
10. Serre, J-P. and Tate, J.: Good reduction of abelian varieties, *Ann. Math.* **88** (1968), 492–517.
11. Shioda, T.: On the Mordell-Weil lattices, *Comment. Math. Univ. Sancti Pauli* **39** (1990), 211–240.
12. Silverman, J. H.: *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1985.
13. Silverman, J. H.: *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1994.