COMPOSITIO MATHEMATICA

DAVID E. ROHRLICH

Variation of the root number in families of elliptic curves

Compositio Mathematica, tome 87, n° 2 (1993), p. 119-151

<http://www.numdam.org/item?id=CM_1993__87_2_119_0>

Compositio Mathematica **87**: 119–151, 1993.

Variation of the root number in families of elliptic curves

DAVID E. ROHRLICH
Department of Mathematics, University of Maryland, College Park MD 20742, U.S.A.

Received 17 March 1992; accepted 7 July 1992

Let E be an elliptic curve over $\mathbb{Q}$, $L(E, s)$ its L-function, and $W(E)$ the associated root number, defined intrinsically as a product of local epsilon factors (Deligne [6]) and hypothetically as the sign ± 1 in the conjectural functional equation of $L(E, s)$:

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

($N(E)$ denotes the conductor of E). The Birch-Swinnerton-Dyer Conjecture implies that

$$W(E) = (-1)^{\text{rank } E(\mathbb{Q})}. \tag{0.1}$$

Over the years this conjectural formula has been a frequent source of insight in the study of elliptic curves. Here it will be used to study some elliptic surfaces.

Our project is inspired by some recent ideas of Mazur concerning the "topology of rational points" on an algebraic variety over $\mathbb{Q}$, and in particular by the case where the variety in question is an elliptic surface over $\mathbb{Q}$ with base the affine line. Given such a surface, consider the family of elliptic curves E_t over $\mathbb{Q}$ which arise as smooth fibers over rational points t in the base. Mazur conjectures that a sharp dichotomy governs the variation of the rank of $E_t(\mathbb{Q})$ with t: either there are only finitely many $t \in \mathbb{Q}$ such that the rank of $E_t(\mathbb{Q})$ is positive, or else the set of all such t is dense in $\mathbb{R}$. With this hypothesis in mind we shall look at a few examples, seeking evidence not only for Mazur's conjecture but also for the existence of a similar dichotomy in the variation of $W(E_t)$ with t.

The first example we shall consider is the family

$$E_j\colon y^2 + jxy = x^3 - \frac{j(j-1)}{4}x^2 - \frac{36j^2}{j-1728}x - \frac{j^3}{j-1728} \tag{0.2}$$

($j \in \mathbb{Q}, j \neq 0, 1728$). The modular invariant of E_j is j.

Research partially supported by NSF grant DMS-9114603.

THEOREM 1. *Given* $j \in \mathbb{Q}$, $j \neq 0$, 1728, *write*

$$j = \gamma \frac{c}{a} \quad \text{and} \quad j - 1728 = \beta \frac{b}{a}$$

with $\beta, \gamma \in \{\pm 1\}$ *and positive integers* a, b, c *such that* a *and* c (*hence also* a *and* b) *are coprime. If* a, b, *and* c *are square-free and relatively prime to* 6, *and* $\gamma ac \equiv 1 \pmod 4$, *then*

$$W(E_j) = -\left(\frac{-1}{a}\right)\left(\frac{-2}{b}\right)\left(\frac{-3}{c}\right).$$

The arguments of Gouvêa-Mazur [10] yield a corollary:

COROLLARY. *Put*

$$J^{\pm} = \{j \in \mathbb{Q}, j \neq 0, 1728: W(E_j) = \pm 1\}.$$

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

If we grant (0.1), then Mazur's conjecture for the family $\{E_j\}$ follows from the density of J^- in $\mathbb{R}$. I do not know whether the counterparts to J^+ and J^- are dense in $\mathbb{R}$ for an arbitrary family with nonconstant j-invariant. However, for families with constant j-invariant it can happen that neither set is dense, as we shall now explain.

Given an elliptic curve E over $\mathbb{Q}$ and a nonzero rational number d, let E^d denote the quadratic twist of E by d, so that if $y^2 = x^3 + ax + b$ is an equation for E then $dy^2 = x^3 + ax + b$ is an equation for E^d. Our second theorem concerns families of the form

$$E_t = E^{f(t)}$$

($t \in \mathbb{Q}$, $f(t) \neq 0$), where E is a given elliptic curve over $\mathbb{Q}$ and f is a nonzero polynomial with rational coefficients. Using a method of Waldspurger ([22], Prop. 16), we shall prove:

THEOREM 2. *Put*

$$T^{\pm} = \{t \in \mathbb{Q}, f(t) \neq 0: W(E^{f(t)}) = \pm 1\}.$$

One of two mutually exclusive alternatives holds: Either

(1) *the sets* T^+ *and* T^- *are both dense in* $\mathbb{R}$; *or,*

(2) *one of the sets* $T^{\pm}$ *is* $\{t \in \mathbb{Q}: f(t) > 0\}$ *and the other is* $\{t \in \mathbb{Q}: f(t) < 0\}$.

Furthermore, if E is given, then there exists f such that (2) *holds and such that the number of sign changes of f on* $\mathbb{R}$ *exceeds any preassigned value. On the other hand, there exists f such that* (1) *holds if and only if E does not acquire everywhere good reduction over any abelian extension of* $\mathbb{Q}$.

It is easy to give examples of elliptic curves over $\mathbb{Q}$ which do not acquire everywhere good reduction over any abelian extension of $\mathbb{Q}$: for example, any elliptic curve over $\mathbb{Q}$ with multiplicative reduction at some prime has this property. According to the theorem, for such elliptic curves we can realize both alternatives (1) and (2) by an appropriate choice of f. On the other hand, there exist elliptic curves over $\mathbb{Q}$ which do acquire everywhere good reduction over some abelian extension of $\mathbb{Q}$, and for these curves only the second alternative can occur. As examples of the latter class of elliptic curves we mention two curves of conductor 37^2: the curve

$$y^2 + 5y = x^3 + x^2 - 12x - 23, \tag{0.3}$$

which has invariant $j = 2^{12}$ and minimal discriminant $\Delta = 37^3$, and the curve

$$y^2 + 3xy = x^3 + 4x + 1, \tag{0.4}$$

which has invariant $j = 3^3 \times 37$ and minimal discriminant $\Delta = -37^2$. (The second example was also found by Masato Kuwata.) Other examples are given in [12], pp. 9–11, and in a forthcoming paper of Connell [5], who gives a complete characterization of such elliptic curves using congruences on the j-invariant. In addition, the list of elliptic curves in Edixhoven-De Groot-Top [7], although compiled for a different purpose, actually contains several curves with the property at issue here.

At first glance, the fact that the second alternative in Theorem 2 really does occur may appear to cast doubt on Mazur's conjecture. Suppose for example that E is either of the elliptic curves (0.3) and (0.4), and choose f to be any quadratic polynomial over $\mathbb{Q}$ with two distinct real zeros. Then Mazur's conjecture and (0.1) together imply that the set of $t \in \mathbb{Q}$ for which $E^{f(t)}(\mathbb{Q})$ has positive rank is dense in $\mathbb{R}$. This conclusion may appear implausible, because the function $t \mapsto W(E^{f(t)})$ is identically equal to 1 on one of the sets $\{t \in \mathbb{Q}: f(t) > 0\}$ and $\{t \in \mathbb{Q}: f(t) < 0\}$. Nevertheless, in the case at hand one can verify Mazur's conjecture directly by an elementary argument:

THEOREM 3. *Let E be an elliptic curve over* $\mathbb{Q}$ *and f a quadratic polynomial with rational coefficients. If there exists* $t \in \mathbb{Q}$ *for which* $f(t) \neq 0$ *and* $E^{f(t)}(\mathbb{Q})$ *has positive rank, then the set of all such t is dense in* $\mathbb{R}$.

So far we have made no reference to the group of sections of an elliptic surface

or to the interplay between the rank of the group of sections and the rank of the individual fibers. We shall end the paper by touching on this theme at least briefly. In [4], Cassels and Schinzel consider the family

$$E_t\colon 7(1+t^4)y^2 = x^3 - x. \tag{0.5}$$

Using the root number calculations of Birch-Stephens [1] and granting (0.1) (or using the descent calculations of Cassels [2] and granting Selmer's conjecture; see [3], p. 276, and [13]) they observe that each member of the family (0.5) has positive Mordell-Weil rank while the group of $\mathbb{Q}$-rational sections has rank 0. We shall present a class of examples in the same spirit, still contingent on (0.1), in which the curve $y^2 = x^3 - x$ is replaced by any elliptic curve over $\mathbb{Q}$ and the polynomial $7(1+t^4)$ by some other suitably chosen polynomial, which can always be taken to be of degree four. Assuming (0.1) we shall also give examples of families for which the group of $\mathbb{Q}$-rational sections has rank 0 while the individual members E_t have Mordell-Weil rank $\geqslant 2$ for a dense set of $t \in \mathbb{Q}$. These applications appear as Proposition 9 in Section 9.

1. Root numbers

Let E be an elliptic curve over $\mathbb{Q}$. As we have already mentioned in the introduction, the root number of E has an intrinsic definition, independent of any conjectures, as a product of local factors

$$W(E) = \prod_{p \leqslant \infty} W_p(E), \tag{1.1}$$

where p runs over the prime numbers and infinity, $W_p(E) = \pm 1$ for all p, and $W_p(E) = 1$ for all but finitely many p. The local factor $W_p(E)$ is an invariant of the isomorphism class of E as an elliptic curve over $\mathbb{Q}_p$. It is defined by the formula

$$W_p(E) = \frac{\varepsilon(\sigma'_{E,p}, \psi, dx)}{|\varepsilon(\sigma'_{E,p}, \psi, dx)|}, \tag{1.2}$$

where ψ is any nontrivial unitary character of $\mathbb{Q}_p$, dx is any Haar measure on $\mathbb{Q}_p$, $\sigma'_{E,p}$ is a certain representation of the Weil-Deligne group of $\mathbb{Q}_p$ (here denoted $\mathscr{W}'(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$), and $\varepsilon(\sigma'_{E,p}, \psi, dx)$ is the corresponding epsilon factor as in Deligne [6] and Tate [19]. That the right-hand side of (1.2) is independent of the choice of dx and ψ follows from formulas (3.4.3), (3.4.4), and (4.1.6) of [19]; in the case of ψ we must also use the fact that $\det \sigma_{E,p}$ is real-valued and positive. Here we should explain that we are thinking of $\sigma'_{E,p}$ as a pair $(\sigma_{E,p}, N_{E,p})$, where $\sigma_{E,p}$ is

a continuous representation of the ordinary Weil group $\mathcal{W}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ on a two-dimensional complex vector space V, and $N_{E,p}$ is a nilpotent endomorphism of V satisfying a certain compatibility with $\sigma_{E,p}$. The precise definition of $\sigma'_{E,p}$ will be recalled in stages as needed, but we mention at the outset that it breaks up into three cases: the case where $p = \infty$, the case where $p < \infty$ and E has potential good reduction at p, and the case where $p < \infty$ and E has potential multiplicative reduction at p. It is only in the last case that the nilpotent endomorphism $N_{E,p}$ comes into play; in the other two cases we simply set $N_{E,p} = 0$ and identify $\sigma'_{E,p}$ with $\sigma_{E,p}$. Corresponding to the three cases just enumerated, there are three types of formulas for $W_p(E)$ which are needed for the proof of Theorem 1. The first of these allows us to rewrite (1.1) in the form

$$W(E) = -\prod_{p<\infty} W_p(E). \tag{1.3}$$

PROPOSITION 1. $W_\infty(E) = -1$.

Proof. This is completely standard, but for the sake of completeness we say a few words. At the infinite prime the Weil-Deligne group is simply the Weil group $\mathcal{W}(\mathbb{C}/\mathbb{R})$, defined by

$$\mathcal{W}(\mathbb{C}/\mathbb{R}) = \mathbb{C}^\times \cup J\mathbb{C}^\times,$$

where $J^2 = -1$ and $JzJ^{-1} = \bar{z}$ for $z \in \mathbb{C}^\times$. The representation $\sigma'_{E,\infty} = \sigma_{E,\infty}$ is canonically associated to the Hodge decomposition of $H^1(E(\mathbb{C}))$ and can be described as follows: if we write $\mathcal{W}(\mathbb{C}/\mathbb{C})$ for the subgroup $\mathbb{C}^\times$ of $\mathcal{W}(\mathbb{C}/\mathbb{R})$, then $\sigma_{E,\infty}$ is the induced representation

$$\sigma_{E,\infty} = \mathrm{ind}_{\mathcal{W}(\mathbb{C}/\mathbb{C})}^{\mathcal{W}(\mathbb{C}/\mathbb{R})}\varphi,$$

where $\varphi: \mathbb{C}^\times (= \mathcal{W}(\mathbb{C}/\mathbb{C})) \to \mathbb{C}^\times$ is the character $z \mapsto z^{-1}$. To compute the associated root number, put $\psi_{\mathbb{R}}(x) = e^{2\pi i x}$ and $\psi_{\mathbb{C}}(z) = \psi_{\mathbb{R}}(\mathrm{tr}_{\mathbb{C}/\mathbb{R}}(z))$, and let dx and dz denote respectively Lebesgue measure on $\mathbb{R}$ and twice Lebesgue measure on $\mathbb{C}$. Also let $1_{\mathbb{R}}$ and $1_{\mathbb{C}}$ denote the trivial representations of $\mathcal{W}(\mathbb{C}/\mathbb{R})$ and $\mathcal{W}(\mathbb{C}/\mathbb{C})$ respectively, and let "sign" denote the nontrivial character of $\mathcal{W}(\mathbb{C}/\mathbb{R})$ with kernel $\mathcal{W}(\mathbb{C}/\mathbb{C})$. Inductivity of the epsilon factor in degree 0 gives

$$\varepsilon(\sigma_{E,\infty}, \psi_{\mathbb{R}}, dx) = \frac{\varepsilon(\varphi, \psi_{\mathbb{C}}, dz)}{\varepsilon(1_{\mathbb{C}}, \psi_{\mathbb{C}}, dz)}\, \varepsilon(\mathrm{ind}_{\mathcal{W}(\mathbb{C}/\mathbb{C})}^{\mathcal{W}(\mathbb{C}/\mathbb{R})} 1_{\mathbb{C}}, \psi_{\mathbb{R}}, dx), \tag{1.4}$$

while

$$\varepsilon(\mathrm{ind}_{\mathcal{W}(\mathbb{C}/\mathbb{C})}^{\mathcal{W}(\mathbb{C}/\mathbb{R})} 1_{\mathbb{C}}, \psi_{\mathbb{R}}, dx) = \varepsilon(1_{\mathbb{R}}, \psi_{\mathbb{R}}, dx)\varepsilon(\mathrm{sign}, \psi_{\mathbb{R}}, dx) \tag{1.5}$$

by additivity. Hence the proposition follows from formulas (3.2.4) and (3.2.5) of [19].

2. The case of potential good reduction

Let p be a prime and let $\bar{\mathbb{Q}}_p$ denote a fixed algebraic closure of $\mathbb{Q}_p$. We recall that the Weil group $\mathscr{W}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ is the subgroup of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ consisting of those elements which induce an integral power of the Frobenius automorphism $x \mapsto x^p$ on the residue class field of $\bar{\mathbb{Q}}_p$. By its very definition, $\mathscr{W}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ comes equipped with a homomorphism

$$\omega\colon \mathscr{W}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \to \{p^n\colon n \in \mathbb{Z}\}$$

such that $\omega(\sigma) = p^n$ if σ induces the n-th power of the map $x \mapsto x^p$ on the residue class field of $\bar{\mathbb{Q}}_p$. By an inverse Frobenius element of $\mathscr{W}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ we shall mean any element Φ such that $\omega(\Phi) = p^{-1}$.

Let I denote the inertia subgroup of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$. Then I is contained in $\mathscr{W}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ and is in fact the kernel of ω. We make $\mathscr{W}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ into a topological group by requiring that I be open in $\mathscr{W}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ and that it retain the topology it inherits as a subgroup of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$.

Now let E be an elliptic curve over $\mathbb{Q}_p$ with potential good reduction. We write $\mathbb{Q}_{p,\mathrm{unr}}$ for the maximal unramified extension of $\mathbb{Q}_p$ in $\bar{\mathbb{Q}}_p$ and L for the minimal extension of $\mathbb{Q}_{p,\mathrm{unr}}$ over which E acquires good reduction. If $m \geqslant 3$ is an integer prime to p, then it is known ([15], p. 498, Cor. 3) that

$$L = \mathbb{Q}_{p,\mathrm{unr}}(E[m]), \tag{2.1}$$

where $E[m]$ denotes the group of points on E of order dividing m. Furthermore, putting

$$\Lambda = \mathrm{Gal}(L/\mathbb{Q}_{p,\mathrm{unr}})$$

we have exactly four possibilities for Λ:

(a) $\Lambda \cong \mathbb{Z}/e\mathbb{Z}$, with $e = 1, 2, 3, 4$, or 6.
(b) $p = 3$ and $\Lambda \cong \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$, where the semidirect product is taken with respect to the unique nontrivial action of $\mathbb{Z}/4\mathbb{Z}$ on $\mathbb{Z}/3\mathbb{Z}$.
(c) $p = 2$ and $\Lambda \cong H_8$, the quaternion group of order 8.
(d) $p = 2$ and $\Lambda \cong \mathrm{SL}(2, \mathbb{Z}/3\mathbb{Z})$.

Cf. [14], p. 312. The classification follows from the argument used to prove [15], Thm. 1 together with the list of possible automorphism groups of elliptic curves

over finite fields, as in [17], pp. 325–329. Note in particular that Λ is abelian only in case (a).

Let $\mathscr{W}(L/\mathbb{Q}_p)$ denote the subgroup of $\mathrm{Gal}(L/\mathbb{Q}_p)$ consisting of elements which induce an integral power of the map $x \mapsto x^p$ on the residue class field of L. The natural identification

$$\mathscr{W}(L/\mathbb{Q}_p) \cong \mathscr{W}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)/\mathrm{Gal}(\bar{\mathbb{Q}}_p/L)$$

endows $\mathscr{W}(L/\mathbb{Q}_p)$ with the discrete topology, because $\mathrm{Gal}(\bar{\mathbb{Q}}_p/L)$ is open in $\mathscr{W}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$. If Φ is any inverse Frobenius element of $\mathscr{W}(L/\mathbb{Q}_p)$ (i.e. the image in $\mathscr{W}(L/\mathbb{Q}_p)$ of any inverse Frobenius element of $\mathscr{W}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$) then we have an isomorphism

$$\mathscr{W}(L/\mathbb{Q}_p) \cong \Lambda \rtimes \langle \Phi \rangle,$$

where $\langle \Phi \rangle$ denotes the infinite cyclic group generated by Φ.

Now choose a prime $l \neq p$, and fix an embedding of $\mathbb{Q}_l$ in $\mathbb{C}$ as well as a $\mathbb{Z}_l$-basis for the Tate module $T_l(E)$. These choices determine a representation

$$\mathscr{W}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{Aut}(T_l(E)) \cong \mathrm{GL}(2, \mathbb{Z}_l) \subset \mathrm{GL}(2, \mathbb{C}), \tag{2.2}$$

where the first arrow represents the natural action of $\mathscr{W}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ on $T_l(E)$. The isomorphism class of this representation is independent of the choices made to define it by virtue of [15], Thm. 2 and Cor. to Thm. 3. We define $\sigma_{E,p}$ to be the *contragredient* of (2.2). Note that with this definition we have

$$\det \sigma_{E,p} = \omega^{-1}, \tag{2.3}$$

because $\bigwedge^2 T_l(E)$ is isomorphic as a $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$-module to the Tate module of the group of l-power roots of unity. It follows from (2.3) that the kernel of $\sigma_{E,p}$ is contained in I. In fact by taking $m = l^n$ in (2.1) with n arbitrarily large, we see that the kernel of $\sigma_{E,p}$ is precisely $\mathrm{Gal}(\bar{\mathbb{Q}}_p/L)$, so that $\sigma_{E,p}$ may be viewed as a faithful representation of $\mathscr{W}(L/\mathbb{Q}_p)$.

Our assumption that E has potential good reduction means that there is a finite extension of $\mathbb{Q}_p$ over which E acquires good reduction. Part (ii) of the following proposition specifies conditions under which we can choose this extension to be *abelian* over $\mathbb{Q}_p$. Parts (iii) and (iv) give formulas for $W_p(E)$ in this special case. Part (v) gives a formula in the general case, but only for $p > 3$. Part (i) merely recalls a well-known fact.

PROPOSITION 2. (i) *The representation $\sigma_{E,p}$ is semisimple.*

(ii) *The following are equivalent:*

(1) *E acquires good reduction over some finite abelian extension of* $\mathbb{Q}_p$
(2) $\mathscr{W}(L/\mathbb{Q}_p)$ *is abelian.*
(3) $\sigma_{E,p}$ *is reducible.*
(4) *E acquires good reduction over some totally ramified cyclic extension of* $\mathbb{Q}_p$ *of degree* $|\Lambda|$.

Furthermore, if $p > 3$, *then the preceding conditions are equivalent to*

(5) $(p-1)ord_p\Delta \equiv 0 \pmod{12}$,

where Δ *is the discriminant of any generalized Weierstrass equation for E over* $\mathbb{Q}_p$.

(iii) *Suppose that the equivalent conditions in* (ii) *hold, and let K be any totally ramified cyclic extension of* $\mathbb{Q}_p$ *of degree* $e = |\Lambda|$ *such that E has good reduction over K. Let* μ *be any character of* $\mathbb{Q}_p^\times$ *of order e which is trivial on* $N_{K/\mathbb{Q}_p}(K^\times)$. *Then*

$$W_p(E) = \mu(-1).$$

(iv) *If E has good reduction over* $\mathbb{Q}_p$, *then* $W_p(E) = 1$.

(v) *Suppose that* $p > 3$. *Put* $e = |\Lambda|$ *and let* $\Delta \in \mathbb{Q}_p^\times$ *be the discriminant of any generalized Weierstrass equation for E over* $\mathbb{Q}_p$. *Then*

$$e = \frac{12}{\gcd(\mathrm{ord}_p\Delta, 12)} = 1, 2, 3, 4, \text{ or } 6,$$

and

$$W_p(E) = \begin{cases} 1, & \text{if } e = 1 \\ \left(\dfrac{-1}{p}\right), & \text{if } e = 2 \text{ or } 6 \\ \left(\dfrac{-3}{p}\right), & \text{if } e = 3 \\ \left(\dfrac{-2}{p}\right), & \text{if } e = 4 \end{cases}.$$

Proof. (i) The endomorphism ring of an elliptic curve over a finite field is an order in an imaginary quadratic field or in a quaternion algebra, and as such it contains no nilpotent elements. The semisimplicity of the matrix $\sigma_{E,p}(\Phi)$ is a consequence of this fact. The semisimplicity of $\sigma_{E,p}$ as a representation follows because $\langle\Phi\rangle$ has finite index in $\mathscr{W}(L/\mathbb{Q}_p)$ (cf. [19], p. 20).

(ii) We begin with a general remark. Let K be any finite extension of $\mathbb{Q}_p$. By the criterion of Néron-Ogg-Shafarevich,

E has good reduction over $K \Leftrightarrow \mathrm{Gal}(\bar{\mathbb{Q}}_p/K) \cap I \subset \ker \sigma_{E,p}$.

Since $I = \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_{p,\mathrm{unr}})$ and $\ker \sigma_{E,p} = \mathrm{Gal}(\bar{\mathbb{Q}}_p/L)$, this equivalence amounts to:

$$E \text{ has good reduction over } K \Leftrightarrow K\mathbb{Q}_{p,\mathrm{unr}} \supset L. \tag{2.4}$$

Suppose now that the left-hand side of (2.4) holds with K abelian over $\mathbb{Q}_p$. Then L is contained in the compositum of two abelian extensions of $\mathbb{Q}_p$ and so is itself abelian over $\mathbb{Q}_p$. Hence (1) implies (2).

Next suppose that $\mathscr{W}(L/\mathbb{Q}_p)$ is abelian. Then Λ is abelian and the action of $\langle\Phi\rangle$ on Λ is trivial. Recalling the four possibilities for Λ, we see that $\Lambda \cong \mathbb{Z}/e\mathbb{Z}$ (with $e = 1, 2, 3, 4$ or 6) and that $\mathscr{W}(L/\mathbb{Q}_p) \cong \mathbb{Z}/e\mathbb{Z} \times \langle\Phi\rangle$. Let K be the subfield of L fixed by $\langle\Phi\rangle$ (i.e. fixed by the closure of $\langle\Phi\rangle$ in $\mathrm{Gal}(L/\mathbb{Q}_p)$). Then K is a totally ramified cyclic extension of $\mathbb{Q}_p$ of degree e, and E has good reduction over K by (2.4). Therefore (2) implies (4). Since (4) trivially implies (1) we see in fact that (1), (2), and (4) are equivalent. Now a faithful two-dimensional semisimple complex representation of a group is reducible if and only if the group is abelian. This gives the equivalence of (2) and (3). Finally, the equivalence of conditions (4) and (5) when $p > 3$ will be verified in the course of proving (v).

(iii) By assumption, E has good reduction over the extension $K\mathbb{Q}_{p,\mathrm{unr}}$. Since L is the minimal extension of $\mathbb{Q}_{p,\mathrm{unr}}$ with this property, L is contained in $K\mathbb{Q}_{p,\mathrm{unr}}$. On the other hand, since K is totally ramified over $\mathbb{Q}_p$, we have

$$[K\mathbb{Q}_{p,\mathrm{unr}}\colon \mathbb{Q}_{p,\mathrm{unr}}] = [K\colon \mathbb{Q}_p] = e = [L\colon \mathbb{Q}_{p,\mathrm{unr}}],$$

and therefore $L = K\mathbb{Q}_{p,\mathrm{unr}}$. Thus $\mathrm{Gal}(L/\mathbb{Q}_{p,\mathrm{unr}})$ is isomorphic to $\mathrm{Gal}(K/\mathbb{Q}_p)$, and the Artin map affords identifications

$$\mathrm{Gal}(L/\mathbb{Q}_{p,\mathrm{unr}}) \cong \mathbb{Q}_p^\times / N_{K/\mathbb{Q}_p}(K^\times) \cong \mathbb{Z}_p^\times / (\mathbb{Z}_p^\times \cap N_{K/\mathbb{Q}_p}(K^\times)), \tag{2.5}$$

the second isomorphism being an expression of the fact that K is totally ramified over $\mathbb{Q}_p$.

Since $\sigma_{E,p}$ is a reducible semisimple representation of $\mathscr{W}(L/\mathbb{Q}_p)$ of determinant ω^{-1} (cf. (2.3)), we have

$$\sigma_{E,p} \cong \nu \oplus \omega^{-1}\nu^{-1} \tag{2.6}$$

for some one-dimensional representation ν of $\mathscr{W}(L/\mathbb{Q}_p)$. Furthermore, since the restriction of ω to $\mathrm{Gal}(L/\mathbb{Q}_{p,\mathrm{unr}})$ is trivial while $\sigma_{E,p}$ is faithful we see that the

restriction of v to $\mathrm{Gal}(L/\mathbb{Q}_{p,\mathrm{unr}})$ is also faithful. Hence if v is regarded as a character of $\mathbb{Q}_p^\times$ using (2.5), then

$$v|\mathbb{Z}_p^\times = \mu^k|\mathbb{Z}_p^\times$$

for some $k \in (\mathbb{Z}/e\mathbb{Z})^\times$. In particular,

$$v(-1) = \mu(-1). \tag{2.7}$$

Now let ψ be a nontrivial unitary character of $\mathbb{Q}_p$ and dx a Haar measure on $\mathbb{Q}_p$. By (2.6) we can write

$$\varepsilon(\sigma_{E,p}, \psi, dx) = \varepsilon(v, \psi, dx)\varepsilon(\omega^{-1}v^{-1}, \psi, dx).$$

Dividing both sides by their absolute values and applying formulas (3.4.4), (3.4.5), and (3.4.7) of [19], we obtain $W_p(E) = v(-1)$, whence the desired formula follows from (2.7).

(iv) This is a special case of (iii) (and a well-known fact).

(v) If $p > 3$ then the only possibility for Λ is $\mathbb{Z}/e\mathbb{Z}$, with $e = 1, 2, 3, 4$ or 6. Furthermore, since E has potential good reduction and $p > 3$, we can apply a well-known criterion to decide whether E has good reduction over a given algebraic extension K of $\mathbb{Q}_p$: E has good reduction over K if and only if the order of Δ with respect to a uniformizer of K is divisible by 12 (cf. [17], p. 186, Ex. 7.2). In particular, let d be an arbitrary positive divisor of e, and let K be the unique extension of $\mathbb{Q}_{p,\mathrm{unr}}$ of degree d contained in L. Then E has good reduction over K if and only if

$$d \operatorname{ord}_p \Delta \equiv 0 \pmod{12}.$$

On the other hand, L was chosen to be the minimal extension of $\mathbb{Q}_{p,\mathrm{unr}}$ over which E acquires good reduction. Hence the preceding congruence holds if and only if $d = e$, so that

$$e = \frac{12}{\gcd(\operatorname{ord}_p \Delta, 12)}. \tag{2.8}$$

Before proving the formula for $W_p(E)$ let us complete the proof of (ii) by verifying that for $p > 3$, conditions (4) and (5) in (ii) are equivalent. On the one hand, (5) amounts to the congruence $p \equiv 1 \pmod{e}$, and by local class field theory, this congruence holds if and only if $\mathbb{Q}_p$ has a totally ramified cyclic extension of degree e. Hence (4) implies (5). On the other hand, if $p \equiv 1 \pmod{e}$,

and if K is a totally ramified cyclic extension of $\mathbb{Q}_p$ of degree e, then the valuation of Δ relative to a uniformizer of K is congruent to 0 modulo 12, by (2.8). Then E has good reduction over K. Therefore (5) implies (4).

To prove the formula for $W_p(E)$ we consider two cases, according as the equivalent conditions in (ii) do or do not hold. First suppose that these conditions do hold, so that $p \equiv 1 \pmod{e}$. Let μ be as in (iii). Then $W_p(E) = \mu(-1)$, and the restriction of μ to $\mathbb{Z}_p^\times$ has order e. Hence if $e = 1$ or 3 then $W_p(E) = 1$. This conclusion is in agreement with the stated formula, because if $e = 3$ then our assumption that $p \equiv 1 \pmod{e}$ implies that $(-3/p) = 1$. Now if $e = 2$ or 6 then $\mu|\mathbb{Z}_p^\times$ is the Legendre symbol at p times a character of order 1 or 3 respectively. Hence $\mu(-1) = (-1/p)$, as claimed. Finally, suppose that $e = 4$. Then $p \equiv 1 \pmod{4}$, and $\mu(-1)$ is 1 or -1 according as -1 is or is not a quartic residue modulo p. In other words, $\mu(-1) = (-2/p)$, as claimed.

Next suppose that the equivalent conditions in (ii) are not satisfied, so that $\sigma_{E,p}$ is irreducible and $p \not\equiv 1 \pmod{e}$. Then $e = 3, 4$, or 6, and $\mathcal{W}(L/\mathbb{Q}_p)$ is isomorphic to $\mathbb{Z}/e\mathbb{Z} \rtimes \langle\Phi\rangle$, with the unique nontrivial action of $\langle\Phi\rangle$ on $\mathbb{Z}/e\mathbb{Z}$. Now the group $\mathbb{Z}/e\mathbb{Z} \rtimes \langle\Phi\rangle$ contains $\mathbb{Z}/e\mathbb{Z} \times \langle\Phi^2\rangle$ as an abelian normal subgroup. Hence if we view $\sigma_{E,p}$ as a representation of the former group, then $\sigma_{E,p}$ is induced from a one-dimensional representation of the latter group. Stated more intrinsically,

$$\sigma_{E,p} = \operatorname{ind}_{\mathcal{W}(L/H)}^{\mathcal{W}(L/\mathbb{Q}_p)} \varphi,$$

where H is the unique unramified quadratic extension of $\mathbb{Q}_p$ and φ is a one-dimensional representation of $\mathcal{W}(L/H) (= \mathcal{W}(L/\mathbb{Q}_p) \cap \operatorname{Gal}(L/H))$. Let $\mathcal{O}_H$ denote the ring of integers of H. Via the Artin isomorphism we may identify φ with a quasicharacter of $H^\times$, and since $\sigma_{E,p}$ is faithful we know that $\varphi|\mathcal{O}_H^\times$ has order e.

Now choose a nontrivial unitary character $\psi: \mathbb{Q}_p \to \mathbb{C}^\times$ as well as Haar measures dx and dy on $\mathbb{Q}_p$ and H respectively. Let η denote the unramified quadratic character of $\mathbb{Q}_p^\times$ and write $1_{\mathbb{Q}_p}$ and 1_H for the trivial characters of $\mathbb{Q}_p^\times$ and $H^\times$. As in (1.4) and (1.5), the inductivity of the epsilon factor in degree 0 gives

$$\varepsilon(\sigma_{E,p}, \psi, dx) = \frac{\varepsilon(\varphi, \psi \circ \operatorname{tr}_{H/\mathbb{Q}_p}, dy)}{\varepsilon(1_H, \psi \circ \operatorname{tr}_{H/\mathbb{Q}_p}, dy)} \varepsilon(\eta, \psi, dx)\varepsilon(1_{\mathbb{Q}_p}, \psi, dx).$$

Dividing each side of this equation by its absolute value, and applying [19], formula (3.2.6.1), we obtain

$$W_p(E) = (-1)^n W(\varphi, \psi \circ \operatorname{tr}_{H/\mathbb{Q}_p}), \tag{2.9}$$

where n is the largest integer such that $\psi(p^{-n}\mathbb{Z}_p) = 1$ and

$$W(*, \psi \circ \mathrm{tr}_{H/\mathbb{Q}_p}) = \frac{\varepsilon(*, \psi \circ \mathrm{tr}_{H/\mathbb{Q}_p}, dy)}{|\varepsilon(*, \psi \circ \mathrm{tr}_{H/\mathbb{Q}_p}, dy)|}$$

(the asterisk denotes an arbitrary character of $H^\times$).

Write $H = \mathbb{Q}_p(u)$, with $u^2 \in \mathbb{Z}_p^\times$. We claim that

$$W(\varphi, \psi \circ \mathrm{tr}_{H/\mathbb{Q}_p}) = \varphi(u)(-1)^{n+1}, \tag{2.10}$$

whence

$$W_p(E) = -\varphi(u) \tag{2.11}$$

after substitution in (2.9).

To verify (2.10), we first observe that

$$\varphi|\mathbb{Q}_p^\times = \omega^{-1}\eta. \tag{2.12}$$

Indeed the formula for the determinant of an induced representation ([9]; or see [6], p. 508) gives

$$\det \sigma_{E,p} = \eta(\varphi|\mathbb{Q}_p^\times),$$

whence (2.12) follows from (2.3). Now let θ be the unramified character of $H^\times$ such that $\theta(p) = -p^{-1}$. Following the convention of [6] and [19] for the reciprocity law map, we have $\omega(p) = \omega(\Phi) = p^{-1} = \eta\theta(p)$, so that $\varphi\theta|\mathbb{Q}_p^\times$ is trivial, by (2.12). Hence the result of Fröhlich-Queyrut ([8], Thm. 3) gives

$$W(\varphi\theta, \psi \circ \mathrm{tr}_{H/\mathbb{Q}_p}) = \varphi(u). \tag{2.13}$$

(In applying [8], note that the left-hand side of (2.13) is *a priori* independent of the choice of ψ by virtue of formula (3.4.4) of [19] and the fact that $\varphi\theta|\mathbb{Q}_p^\times$ is trivial.) On the other hand, θ is unramified, and since $p \nmid e$ the conductor-exponent of φ is 1. Hence formula (3.2.6.3) of [19] gives

$$\begin{aligned} W(\varphi\theta, \psi \circ \mathrm{tr}_{H/\mathbb{Q}_p}) &= \left(\frac{\theta(p)}{|\theta(p)|}\right)^{n+1} W(\varphi, \psi \circ \mathrm{tr}_{H/\mathbb{Q}_p}) \\ &= (-1)^{n+1} W(\varphi, \psi \circ \mathrm{tr}_{H/\mathbb{Q}_p}) \end{aligned} \tag{2.14}$$

Together, (2.13) and (2.14) yield (2.10) and therefore (2.11).

It remains to check that (2.11) coincides with the stated formulas for $W_p(E)$ in terms of Legendre symbols. If $e = 3$ then our assumption that $p \not\equiv 1 \pmod{e}$ implies that $(-3/p) = -1$. This value coincides with (2.11), because $\varphi(u)$ is equal *a priori* to a cube root of unity and by (2.11) to ± 1, hence to 1. If $e = 4$ then $p \equiv 3 \pmod 4$, and $u^2 \in -1\mathbb{Z}_p^{\times 2}$. Thus the order of the subgroup of $(\mathcal{O}_H/p\mathcal{O}_H)^\times$ generated by the image of u is divisible by 4 but not by 8, and $\varphi(u)$ is 1 or -1 according as $p^2 - 1$ is or is not divisible by 16. Therefore $\varphi(u) = -(-2/p)$, as desired. A similar argument for $e = 6$ completes the proof.

3. The case of potential multiplicative reduction

Let E be an elliptic curve over $\mathbb{Q}_p$ with potential multiplicative reduction. The distinction between $\mathcal{W}'(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ and $\mathcal{W}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ now becomes important; the l-adic representations afforded by E are not trivial on an open subgroup of I and hence do not define continuous *complex* representations of $\mathcal{W}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$. In compensation for this, one exploits the correspondence between l-adic representations of $\mathcal{W}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ and certain complex representations of $\mathcal{W}'(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ ([19], (4.2.1)), associating to E a representation $\sigma'_{E,p} = (\sigma_{E,p}, N_{E,p})$ of $\mathcal{W}'(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ which must now be made explicit.

Since E has potential multiplicative reduction, there is a unique Tate curve E_{Tate} over $\mathbb{Q}_p$, together with an element $d \in \mathbb{Q}_p^\times$, uniquely determined modulo $\mathbb{Q}_p^{\times 2}$, such that E is isomorphic over $\mathbb{Q}_p$ to the twist of E_{Tate} by d:

$$E = E_{\text{Tate}}^d.$$

Let $\chi = \chi_{d,p}$ be the character of $\mathbb{Q}_p^\times$ (quadratic or trivial) determined by the extension $\mathbb{Q}_p(\sqrt{d})/\mathbb{Q}_p$, and define a continuous homomorphism

$$\sigma_{E,p}: \mathcal{W}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{GL}(2, \mathbb{C})$$

by

$$w \mapsto \begin{pmatrix} \chi\omega^{-1}(w) & 0 \\ 0 & \chi(w) \end{pmatrix}.$$

The matrix

$$N_{E,p} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

satisfies the compatibility relation

$$\sigma_{E,p}(w)N_{E,p}\sigma_{E,p}(w)^{-1} = \omega(w)N_{E,p},$$

and so fixing a basis $\{e_1, e_2\}$ for $\mathbb{C}^2$ we may view the pair $(\sigma_{E,p}, N_{E,p})$ as giving a representation of $\mathscr{W}'(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ on $\mathbb{C}^2$. This is $\sigma'_{E,p}$.

Put $V = \mathbb{C}^2$ and let V_N denote the kernel of $N_{E,p}$. We write V^I for the subspace of V fixed by $\sigma_{E,p}(I)$ and V_N^I for $V^I \cap V_N$.

PROPOSITION 3. (i) *The representation $\sigma'_{E,p}$ is reducible but indecomposable.* (ii) *The following are equivalent:*

(1) *E has additive reduction over $\mathbb{Q}_p$.*
(2) *$\chi_{d,p}$ is ramified.*
(3) $V^I = V_N^I = \{0\}$.

If these equivalent conditions hold, then $W_p(E) = \chi_{d,p}(-1)$. In particular, if p is odd, then

$$W_p(E) = \left(\frac{-1}{p}\right).$$

(iii) *The following are equivalent*:

(1) *E has multiplicative reduction over $\mathbb{Q}_p$.*
(2) *$\chi_{d,p}$ is unramified.*
(3) $V^I = V$ *and* $V_N^I = V_N = \mathbb{C}e_2$.

If these equivalent conditions hold, then

$$W_p(E) = \begin{cases} -1, & \text{if } E/\mathbb{Q}_p \text{ has split multiplicative reduction} \\ 1, & \text{if } E/\mathbb{Q}_p \text{ has nonsplit multiplicative reduction.} \end{cases}$$

Proof. Part (i) and the equivalence of conditions (1), (2), and (3) in parts (ii) and (iii) are immediate consequences of the definitions and the theory of Tate curves. The formulas for $W_p(E)$ are also well known, but we say a few words for the sake of completeness.

If ψ is a nontrivial unitary character of $\mathbb{Q}_p$, dx a Haar measure on $\mathbb{Q}_p$, and $\Phi \in \mathscr{W}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ an inverse Frobenius element, then

$$\varepsilon(\sigma'_{E,p}, \psi, dx) = \varepsilon(\sigma_{E,p}, \psi, dx)\det(-\Phi|V^I/V_N^I)$$

([19], (4.1.6)), and therefore

$$\varepsilon(\sigma'_{E,p}, \psi, dx) = \varepsilon(\chi\omega^{-1}, \psi, dx)\varepsilon(\chi, \psi, dx)\det(-\Phi|V^I/V_N^I)$$

by additivity. Dividing each side by its absolute value we find

$$W_p(E) = \chi(-1)\frac{\det(-\Phi|V^I/V_N^I)}{|\det(-\Phi|V^I/V_N^I)|} \tag{3.1}$$

by formulas (3.4.5) and (3.4.7) of [19]. Now under the equivalent conditions in (ii) we have $V^I/V_N^I = \{0\}$, so that the determinant in (3.1) is 1 and $W_p(E) = \chi(-1)$. On the other hand, in the situation of (iii) we have $\chi(-1) = 1$ but

$$\frac{\det(-\Phi|V^I/V_N^I)}{|\det(-\Phi|V^I/V_N^I)|} = \frac{-\chi\omega^{-1}(p)}{|\chi\omega^{-1}(p)|} = -\chi(p),$$

so that $W_p(E)$ is -1 or 1 according as χ is trivial or nontrivial.

4. Proof of Theorem 1

Let a, b, and c be square-free positive integers satisfying $1728a + \beta b - \gamma c = 0$, with $\beta, \gamma \in \{\pm 1\}$. We assume that a, b, c are relatively prime to 6 and to each other and that $\gamma ac \equiv 1 \pmod 4$. Put $j = \gamma c/a$ and let E_j be as in (0.2). We shall compute $W(E_j)$.

The curve E_j is the quadratic twist by j of the curve on p. 52 of [17] or on p. 38 of [18]. Using the formulas on p. 38 of [18] (but noting a sign error in the formula for c_6), one sees directly that the covariants c_4, c_6, and Δ associated to the equation (0.2) are

$$c_4 = \frac{j^3}{j - 1728},$$

$$c_6 = -\frac{j^4}{j - 1728},$$

and

$$\Delta = \frac{j^8}{(j - 1728)^3}.$$

If p is a prime not dividing abc, then the coefficients of the equation (0.2) are p-integral and Δ is a p-unit. (The congruence $\gamma ac \equiv 1 \pmod 4$ ensures that the coefficient of x^2 in (0.2) is p-integral even for $p = 2$.) It follows that E_j has good reduction at p, whence

$$W_p(E_j) = 1 \qquad (p \nmid abc) \tag{4.1}$$

by part (iv) of Proposition 2.

If p is a prime dividing a, then $\mathrm{ord}_p j = -1 < 0$. Hence E has potential multiplicative reduction at p. From the theory of Tate curves we see that over $\mathbb{Q}_p$, E is isomorphic to E^d_{Tate}, with $d = -c_6/c_4$ (notation as in Section 3). On the other hand, since $-c_6/c_4 = j$ and $\mathrm{ord}_p j = -1$, the extension $\mathbb{Q}_p(\sqrt{-c_6/c_4})/\mathbb{Q}_p$ is ramified. Therefore

$$W_p(E_j) = \left(\frac{-1}{p}\right) \qquad (p|a) \tag{4.2}$$

by part (ii) of Proposition 3.

Next suppose that p divides either b or c. Then j is p-integral; E_j has potential good reduction at p. Furthermore, $\mathrm{ord}_p \Delta = -3$ if p divides b and $\mathrm{ord}_p \Delta = 8$ if p divides c. Hence part (v) of Proposition 2 gives

$$W_p(E_j) = \left(\frac{-2}{p}\right) \qquad (p|b) \tag{4.3}$$

and

$$W_p(E_j) = \left(\frac{-3}{p}\right) \qquad (p|c). \tag{4.4}$$

Substituting formulas (4.1) through (4.4) into (1.3), we obtain

$$W(E_j) = -\left(\frac{-1}{a}\right)\left(\frac{-2}{b}\right)\left(\frac{-3}{c}\right), \tag{4.5}$$

proving Theorem 1.

For later reference, we note that the formula for $W(E_j)$ can also be written as

$$W(E_j) = -\gamma\left(\frac{-6}{b}\right). \tag{4.6}$$

Indeed, since $\gamma c = 1728a + \beta b$, we have $c \equiv \gamma\beta b \pmod{24}$. In particular, we have the congruence $c \equiv \gamma\beta b \pmod 3$, and also, since $a \equiv \gamma c \pmod 4$, the congruence $a \equiv \beta b \pmod 4$. It follows that

$$\left(\frac{-3}{c}\right) = \gamma\beta\left(\frac{-3}{b}\right)$$

and that

$$\left(\frac{-1}{a}\right) = \beta\left(\frac{-1}{b}\right).$$

Making these substitutions in (4.5) we obtain (4.6).

5. The square-free sieve

We shall formulate a variant of a result of Gouvêa-Mazur ([10], Thm. 3) which will be used in Section 6 to derive the corollary to Theorem 1. In principle, Proposition 4 below is much weaker than the original result, because we consider only forms which factor into linear factors, rather than into factors of degree $\leqslant 3$ as in [10]. However, the key point for us is that in Proposition 4, a and b are allowed to vary over independent intervals.

Let $F(u, v) \in \mathbb{Z}[u, v]$ be a product of homogeneous linear forms with coefficients in $\mathbb{Z}$, and assume that $F(u, v)$ is not divisible by the square of any nonunit of $\mathbb{Z}[u, v]$. Let M be a positive integer, let a_0 and b_0 be integers relatively prime to M, and let $N(x, y)$ denote the number of integers (a, b) such that $0 \leqslant a \leqslant x$, $0 \leqslant b \leqslant y$, $a \equiv a_0 \pmod{M}$, $b \equiv b_0 \pmod{M}$, and $F(a, b)$ is square-free. For a positive integer m put $\delta(m) = \gcd(m, M)$ and let $\rho(m)$ denote the number of pairs of integers (a, b) satisfying $0 \leqslant a, b \leqslant m - 1$, $F(a, b) \equiv 0 \pmod{m}$, $a \equiv a_0 \pmod{\delta(m)}$, and $b \equiv b_0 \pmod{\delta(m)}$. Also put $r(m) = \delta(m)^2 \rho(m)$.

PROPOSITION 4. *For $x, y \to \infty$ with $x \gg y \gg x$, we have*

$$N(x, y) = Axy + O(x^2/\log x),$$

where

$$A = (1/M^2) \prod_p (1 - r(p^2)/p^4)$$

(p runs over all prime numbers).

Proof. Since the argument in [10] goes through virtually without change, we shall be brief.

Put $\xi = (1/3)\log x$ and let $N'(x, y)$ denote the number of pairs of integers (a, b) satisfying $0 \leqslant a \leqslant x$, $0 \leqslant b \leqslant y$, $a \equiv a_0 \pmod{M}$, and $b \equiv b_0 \pmod{M}$, and such that $F(a, b)$ is not divisible by the square of any prime $\leqslant \xi$. Clearly $N'(x, y) \geqslant N(x, y)$. It suffices to prove that

$$N'(x, y) = Axy + O(x^2/\log x) \tag{5.1}$$

and that

$$N'(x, y) - N(x, y) = O(x^2/\log x). \tag{5.2}$$

For a positive integer n, let $N_n(x, y)$ denote the number of pairs of integers (a, b) satisfying $0 \leqslant a \leqslant x$, $0 \leqslant b \leqslant y$, $a \equiv a_0 \pmod{M}$, and $b \equiv b_0 \pmod{M}$, and such that $F(a, b)$ is divisible by n. The inclusion-exclusion principle gives

$$N'(x, y) = \sum_l \mu(l) N_{l^2}(x, y), \tag{5.3}$$

where l runs over square-free integers divisible only by primes $\leqslant \xi$. On the other hand, reasoning as in the second paragraph on p. 16 of [10], but recalling that by definition $\delta(l^2) = \gcd(l^2, M)$, we find

$$N_{l^2}(x, y) = \rho(l^2)\{\delta(l^2)^2 xy/(l^4 M^2) + O(x/l^2)\}. \tag{5.4}$$

(The key point to keep in mind is that $x = O(y)$ and $y = O(x)$.) Substituting (5.4) in (5.3) and arguing as in the remainder of the proof of Lemma 8 of [10], we obtain (5.1).

Now write

$$F(u, v) = \prod_{i=1}^{t} f_i(u, v),$$

where the f_i are homogeneous linear forms with integer coefficients. For $1 \leqslant i \leqslant t$, let $E_i'(x, y)$ be the number of pairs of integers (a, b) such that $0 \leqslant a \leqslant x$, $0 \leqslant b \leqslant y$, and $f_i(a, b) = 0$, and let $E_i''(x, y)$ be the number of pairs of integers (a, b) such that $0 \leqslant a \leqslant x$, $0 \leqslant b \leqslant y$, and $f_i(a, b)$ is nonzero but divisible by the square of some prime $> \xi$. Put $E_i(x, y) = E_i'(x, y) + E_i''(x, y)$. Also let $E_0(x, y)$ denote the number of pairs of integers (a, b) satisfying $0 \leqslant a \leqslant x$ and $0 \leqslant b \leqslant y$ such that there is a prime $p > \xi$ which divides both a and b. Finally, let

$$E(x, y) = \sum_{i=0}^{t} E_i(x, y).$$

Reasoning as in the proof of [10], Proposition 2, we see that

$$N'(x, y) - N(x, y) \leqslant E(x, y) \tag{5.5}$$

if x (and hence y) is sufficiently large.

We have

$$E_0(x, y) = O(x^2/\log x) \tag{5.6}$$

just as in Lemma 9 of [10]. Also $E_i'(x, y) = O(x)$ for $1 \leqslant i \leqslant t$ because the zeros of f_i lie on a line. As for $E_i''(x, y)$, observe that if $0 \leqslant a \leqslant x$ and $0 \leqslant b \leqslant y$, then $|f_i(a, b)| \ll x$. Hence if p^2 divides $f_i(a, b)$ and $f_i(a, b) \neq 0$, then $p^2 \ll x$. We may now argue as in [10] to conclude that $E_i''(x, y) = O(x^2/\log x)$, whence

$$E_i(x, y) = O(x^2/\log x) \tag{5.7}$$

for $1 \leqslant i \leqslant t$. Combining (5.5), (5.6), and (5.7), we obtain (5.2).

6. Proof of the corollary

We apply Proposition 4 with $M = 24$ and $F(u, v) = uv(1728u + \beta v)$, where $\beta \in \{\pm 1\}$. Integers a_0 and b_0 relatively prime to M will be chosen later. We claim that $A \neq 0$. To see this we refer to [10], Proposition 5. According to part (1) of the result cited, it suffices to check that for each prime $p, r(p^2) \neq p^4$. This condition is satisfied for $p > 3$ by part (4) of the proposition, and for $p = 2$ and $p = 3$ by part (3). Thus $A \neq 0$. Now let r be a fixed positive real number, let n be a large positive integer, and put $x = n$, $y = rn$, $\Delta = n/(\log n)^{1/3}$. Then Proposition 4 gives

$$N(x+\Delta, y+\Delta) - N(x+\Delta, y) - N(x, y+\Delta) + N(x, y) = A\Delta^2 + O\left(\frac{x^2}{\log x}\right),$$

and the right-hand side is simply

$$A\frac{n^2}{(\log n)^{2/3}} + O\left(\frac{n^2}{\log n}\right).$$

We conclude that if n is sufficiently large, then there is a pair of integers (a_n, b_n) satisfying $n < a_n \leqslant n + n/(\log n)^{1/3}$, $rn < b_n \leqslant rn + n/(\log n)^{1/3}$, $a_n \equiv a_0 \pmod{24}$, and $b_n \equiv b_0 \pmod{24}$, and such that $a_n b_n(1728a_n + \beta b_n)$ is square-free. Note that

$$\lim_{n\to\infty} \frac{b_n}{a_n} = r.$$

Now suppose that $j_0 \in \mathbb{R}\backslash\{0, 1728\}$ and $\varepsilon \in \{\pm 1\}$ are given. Put

$$\beta = \begin{cases} 1, & \text{if } j_0 > 1728 \\ -1, & \text{if } j_0 < 1728, \end{cases}$$

$$\gamma = \begin{cases} 1, & \text{if } j_0 > 0 \\ -1, & \text{if } j_0 < 0, \end{cases}$$

and

$$r = \beta(j_0 - 1728).$$

Then $r > 0$. Choose integers a_0 and b_0 relatively prime to 24 such that

$$\left(\frac{-6}{b_0}\right) = -\gamma\varepsilon \tag{6.1}$$

and

$$a_0 \equiv \beta b_0 \pmod 4. \tag{6.2}$$

Let (a_n, b_n) be the sequence of pairs of positive integers constructed in the previous paragraph, and define

$$c_n = \gamma(1728a_n + \beta b_n), \tag{6.3}$$

$$j_n = \gamma\frac{c_n}{a_n} = 1728 + \beta\frac{b_n}{a_n}. \tag{6.4}$$

The second expression for j_n in (6.4) gives

$$\lim_{n\to\infty} j_n = 1728 + \beta r = j_0. \tag{6.5}$$

Since this is also the limit of $\gamma c_n/a_n$, we see that for n sufficiently large, $\gamma c_n/a_n$ has the same sign as j_0. In fact since a_n is positive and γ has the same sign as j_0, we see that c_n is positive for large n, whence a_n, b_n, and c_n are square-free positive integers relatively prime to 6 and to each other such that

$$1728a_n + \beta b_n - \gamma c_n = 0. \tag{6.6}$$

Furthermore,

$$\gamma a_n c_n \equiv 1 \pmod 4,$$

because $a_n \equiv \beta b_n \pmod 4$ by (6.2) and $\beta b_n \equiv \gamma c_n \pmod 4$ by (6.6). Consequently, the rational number j_n satisfies the hypotheses of Theorem 1, and using (4.6) and (6.1) we find

$$W(E_{j_n}) = -\gamma\left(\frac{-6}{b_n}\right) = \varepsilon. \tag{6.7}$$

Since $j_0 \in \mathbb{R}\backslash\{0, 1728\}$ and $\varepsilon \in \{\pm 1\}$ were arbitrary, (6.5) and (6.7) together imply that the closure of $J^{\pm}$ contains $\mathbb{R}\backslash\{0, 1728\}$ and therefore equals $\mathbb{R}$. This completes the proof of the corollary.

7. Proof of Theorem 2

We shall prove three propositions (Propositions 6, 7, and 9 below) which together contain all of the assertions of Theorem 2. The proofs are a straightforward application of Waldspurger's results on local epsilon factors, encapsulated here in Propositions 5 and 8.

Let E be an elliptic curve over $\mathbb{Q}$. For each prime p we may regard E as an elliptic curve over $\mathbb{Q}_p$ and form the quadratic twist E^d over $\mathbb{Q}_p$ by an element $d \in \mathbb{Q}_p$. We let $D_{E,p}^{+}$ denote the set of all $d \in \mathbb{Q}_p^{\times}$ such that

$$W_p(E^d) = \chi_{d,p}(-1) W_p(E),$$

where $\chi_{d,p}: \mathbb{Q}_p^{\times} \to \{\pm 1\}$ is the character (quadratic or trivial) associated to the extension $\mathbb{Q}_p(\sqrt{d})/\mathbb{Q}_p$. We also let $D_{E,p}^{-}$ denote the complement of $D_{E,p}^{+}$ in $\mathbb{Q}_p^{\times}$, and we define $\delta_{E,p}: \mathbb{Q}_p^{\times} \to \{\pm 1\}$ by

$$\delta_{E,p}(d) = \begin{cases} 1, & \text{if } d \in D_{E,p}^{+} \\ -1, & \text{if } d \in D_{E,p}^{-}. \end{cases}$$

Then for all $d \in \mathbb{Q}_p^{\times}$ we have

$$W_p(E^d) = \delta_{E,p}(d) \chi_{d,p}(-1) W_p(E). \tag{7.1}$$

Note that $D_{E,p}^{+}$ contains $\mathbb{Q}_p^{\times 2}$ and is in fact a union of cosets of $\mathbb{Q}_p^{\times 2}$. Hence $D_{E,p}^{+}$ is both open and closed in $\mathbb{Q}_p^{\times}$, and $\delta_{E,p}$ is continuous.

Now suppose that $d \in \mathbb{Q}^{\times}$. For all but finitely many p, the factors $W_p(E^d)$, $\chi_{d,p}(-1)$, and $W_p(E)$ are equal to 1, hence the same is true for $\delta_{E,p}(d)$. Using Proposition 1 we may write

$$\begin{aligned} W(E^d) &= -\prod_{p<\infty} W_p(E^d) \\ &= \left(\prod_{p<\infty} \delta_{E,p}(d)\right)\left(\prod_{p<\infty} \chi_{d,p}(-1)\right)\left(-\prod_{p<\infty} W_p(E)\right). \end{aligned}$$

The last of these three products is $W(E)$, by Proposition 1, and the second is $\chi_{d,\infty}(-1)$, by global reciprocity. Hence

$$W(E^d) = \operatorname{sign}(d) W(E) \prod_{p<\infty} \delta_{E,p}(d), \tag{7.2}$$

where we put sign $x = x/|x|$ for a nonzero real number x.

To make use of this formula we need some information about the functions $\delta_{E,p}$.

PROPOSITION 5. (i) *If E acquires good reduction over some abelian extension of $\mathbb{Q}_p$ then $D^+_{E,p} = \mathbb{Q}_p^\times$, i.e. $\delta_{E,p}$ is identically* 1.

(ii) *If E does not acquire good reduction over any abelian extension of $\mathbb{Q}_p$, then $D^+_{E,p} \neq \mathbb{Q}_p^\times$, i.e. $\delta_{E,p}$ assumes both values* 1 *and* -1.

Proof. (i) If E acquires good reduction over some abelian extension of $\mathbb{Q}_p$, then $\sigma'_{E,p}$ $(=\sigma_{E,p})$ is a direct sum of two one-dimensional representations as in formula (2.6):

$$\sigma_{E,p} \cong \nu \oplus \omega^{-1}\nu^{-1}.$$

Furthermore, we have $W_p(E) = \nu(-1)$ by formula (2.7) and part (iii) of Proposition 2. In like manner, we have

$$\sigma_{E^d,p} \cong \sigma_{E,p} \otimes \chi_{d,p} \cong \nu\chi_{d,p} \oplus \omega^{-1}\nu^{-1}\chi_{d,p}$$

and $W_p(E^d) = \nu\chi_{d,p}(-1)$. Therefore $W_p(E^d) = \chi_{d,p}(-1)W_p(E)$ for all $d \in \mathbb{Q}_p^\times$, whence $\delta_{E,p}$ is identically 1.

(ii) Let $\omega_{1/2}$ denote the character of $\mathcal{W}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ given by $w \mapsto \omega(w)^{1/2}$, so that $\sigma_{E,p} \otimes \omega_{1/2}$ has trivial determinant. Following the usual conventions for a tensor product of representations of $\mathcal{W}'(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$, put

$$\sigma'_{E,p} \otimes \omega_{1/2} = (\sigma_{E,p} \otimes \omega_{1/2}, N_{E,p}),$$

and let π be the irreducible admissible representation of $\mathrm{PGL}(2, \mathbb{Q}_p)$ corresponding to $\sigma'_{E,p} \otimes \omega_{1/2}$ under the local Langlands correspondence. (For the cases of the local Langlands correspondence needed here see Tunnell [20], [21].) In terms of the epsilon factor $\varepsilon(\pi, s)$, defined as in [22], p. 225, the relation (7.1) takes the form

$$\varepsilon(\pi \otimes \chi_{d,p}, 1/2) = \delta_{E,p}(d)\chi_{d,p}(-1)\varepsilon(\pi, 1/2). \tag{7.3}$$

If E does not acquire good reduction over any abelian extension of $\mathbb{Q}_p$ then $\sigma'_{E,p}$ is either irreducible (Proposition 2, part (ii)) or else reducible but indecomposable (Proposition 3, part (i)). Hence π is a discrete series representation, and there exists $d \in \mathbb{Q}_p^\times$ such that

$$\varepsilon(\pi \otimes \chi_{d,p}, 1/2) = -\chi_{d,p}(-1)\varepsilon(\pi, 1/2)$$

([22], Prop. 16 b)). Referring to (7.3), we see that $\delta_{E,p}(d) = -1$ for this d, whence $D_{E,p}^{+} \neq \mathbb{Q}_p^{\times}$.

Let $M(E)$ be the product of all primes p such that E does not acquire good reduction over any abelian extension of $\mathbb{Q}_p$. In view of part (i) of Proposition 5 we can rewrite formula (7.2) as

$$W(E^d) = \operatorname{sign}(d) W(E) \prod_{p|M(E)} \delta_{E,p}(d). \tag{7.4}$$

Now consider a family of elliptic curves of the form $E_t = E^{f(t)} (t \in \mathbb{Q}, f(t) \neq 0)$, where E is a given elliptic curve over $\mathbb{Q}$ and f is a nonzero polynomial with rational coefficients. Put

$$T^{\pm} = \{t \in \mathbb{Q},\ f(t) \neq 0 \colon W(E^{f(t)}) = \pm 1\}.$$

The first assertion of Theorem 2 is contained in the following proposition:

PROPOSITION 6. (i) *If there exists a prime divisor p_0 of $M(E)$ such that the sets $f(\mathbb{Q}_{p_0}) \cap D_{E,p_0}^{+}$ and $f(\mathbb{Q}_{p_0}) \cap D_{E,p_0}^{-}$ are both nonempty, then T^{+} and T^{-} are both dense in $\mathbb{R}$.*

(ii) *Suppose on the other hand that for every prime divisor p of $M(E)$, one of the sets $f(\mathbb{Q}_p) \cap D_{E,p}^{+}$ and $f(\mathbb{Q}_p) \cap D_{E,p}^{-}$ is empty. Then one of the sets $T^{\pm}$ is $\{t \in \mathbb{Q} \colon f(t) > 0\}$ and the other is $\{t \in \mathbb{Q} \colon f(t) < 0\}$.*

Proof. (i) Let $U^{\pm}$ denote the nonempty open subset of $\mathbb{Q}_{p_0}$ consisting of $t \in \mathbb{Q}_{p_0}$ such that $f(t) \in D_{E,p_0}^{\pm}$. Let $r \in \mathbb{R}$ be given, and suppose that $f(r) \neq 0$. There exist rational numbers q^{+} and q^{-} arbitrarily close to r such that $q^{\pm} \in U^{\pm}$ and such that $q^{\pm} \in \mathbb{Q}_p^{\times 2}$ for every prime divisor p of $M(E)$ different from p_0. We have $\delta_{E,p_0}(f(q^{\pm})) = \pm 1$ and $\delta_{E,p}(f(q^{\pm})) = 1$ for $p \neq p_0$; also $\operatorname{sign}(f(q^{\pm})) = \operatorname{sign}(f(r))$ if q^{+} and q^{-} are sufficiently close to r. Hence (7.4) gives

$$W(E^{f(q^{\pm})}) = \pm \operatorname{sign}(f(r)) W(E),$$

so that one of q^{+} and q^{-} belongs to T^{+} and the other to T^{-}. Since $r \in \mathbb{R}$ was arbitrary except for the condition $f(r) \neq 0$, we conclude that T^{+} and T^{-} are both dense in $\mathbb{R}$.

(ii) Our hypothesis is now that for every prime divisor p of $M(E)$, the function $t \mapsto \delta_{E,p}(f(t))$ (with domain $\{t \in \mathbb{Q}_p \colon f(t) \neq 0\}$) is a constant function, say with constant value ε_p. Put

$$\varepsilon = W(E) \prod_{p|M(E)} \varepsilon_p.$$

Then (7.4) gives $T^{\pm} = \{t \in \mathbb{Q} \colon \pm \varepsilon f(t) > 0\}$.

The next proposition contains the third assertion in Theorem 2.

PROPOSITION 7. *The following are equivalent*:

(1) *E acquires everywhere good reduction over some abelian extension of* $\mathbb{Q}$.
(2) *For each prime p, E acquires good reduction over some abelian extension of* $\mathbb{Q}_p$.
(3) *We have* $W(E^d) = \mathrm{sign}(d)W(E)$ *for every* $d \in \mathbb{Q}^\times$.
(4) *For every nonzero polynomial f over* $\mathbb{Q}$, *one of the sets* $T^\pm$ *is* $\{t \in \mathbb{Q}: f(t) > 0\}$ *and the other is* $\{t \in \mathbb{Q}: f(t) < 0\}$.

Proof. Clearly (1) implies (2), and the converse implication holds because any finite set of local abelian extensions can be realized by a global abelian extension. That (2) implies (3) follows from (7.4), because (2) means that $M(E) = 1$. Furthermore, (4) is an immediate consequence of (3). Suppose now that (2) does not hold. Then by part (ii) of Proposition 5 there is a prime p_0 such that δ_{E,p_0} assumes both values 1 and -1. Since $\mathbb{Q}^\times$ is dense in $\mathbb{Q}_{p_0}^\times$, there exist $a, b \in \mathbb{Q}^\times$ such that $\delta_{E,p_0}(a) = 1$ and $\delta_{E,p_0}(b) = -1$. Choose a polynomial f over $\mathbb{Q}$ such that $a, b \in f(\mathbb{Q})$. For this f the first alternative in Proposition 6 is in force, and therefore (4) does not hold.

Using condition (5) in part (ii) of Proposition 2, one sees that the equivalent conditions of Proposition 7 are satisfied by the curves (0.3) and (0.4) of the introduction, because $37 - 1$ is divisible by 12.

It remains to prove the second assertion of Theorem 2. Before doing so, we prepare an ancillary result. Given an elliptic curve E over $\mathbb{Q}_p$, consider the following condition:

(§) There exists a subgroup C of index 2 in $\mathbb{Q}_p^\times$ and an element $b \in \mathbb{Q}_p^\times$ such that $\delta_{E,p}$ is constant on bC.

LEMMA. (i) *If p is odd then* (§) *is satisfied.*
(ii) *If* $p = 2$ *then* (§) *is satisfied under either of the following hypotheses:*

(1) *E acquires good reduction over some abelian extension of* $\mathbb{Q}_2$.
(2) *E has potential multiplicative reduction.*

(iii) *If* $p = 2$ *then* (§) *holds with the words "index 2" replaced by "index 4".*

Proof. (i) If p is odd then $\mathbb{Q}_p^{\times 2}$ has four cosets in $\mathbb{Q}_p^\times$, and the union of any two of them is a coset of some subgroup of $\mathbb{Q}_p^\times$ of index 2. Since $\delta_{E,p}$ has at most two values and is constant on cosets of $\mathbb{Q}_p^{\times 2}$, we can find two cosets on which $\delta_{E,p}$ takes the same value.

(ii) If E acquires good reduction over some abelian extension of $\mathbb{Q}_2$ then $\delta_{E,2}$ is identically 1 (Proposition 5, part (i)) and C and b may be chosen arbitrarily. If E has potential multiplicative reduction, then we can write $E = E_{\mathrm{Tate}}^{d_0}$ with a unique Tate curve E_{Tate} over $\mathbb{Q}_2$ and an element $d_0 \in \mathbb{Q}_2^\times$ uniquely determined modulo $\mathbb{Q}_2^{\times 2}$. Put

$$C = \{c \in \mathbb{Q}_2^\times: \chi_{c,2}(-1) = 1\}$$

and $b = -d_0$. Since $\chi_{-1,2}(-1) = -1$ we have

$$bC = \{d \in \mathbb{Q}_2^\times : \chi_{dd_0,2}(-1) = -1\}.$$

In particular, if $d \in bC$ then $\chi_{dd_0,2}$ is ramified. Referring to (7.1) and to part (ii) of Proposition 3, we see that for $d \in bC$,

$$\delta_{E,2}(d) = \frac{W_2(E^d)}{\chi_{d,2}(-1)W_2(E)} = \frac{W_2(E^{dd_0}_{\text{Tate}})}{\chi_{d,2}(-1)W_2(E)} = \frac{\chi_{d_0,2}(-1)}{W_2(E^{d_0}_{\text{Tate}})},$$

which is independent of d.

(iii) We argue as in (i): $\mathbb{Q}_2^{\times 2}$ has eight cosets in $\mathbb{Q}_2^\times$ and the union of any two of them is a coset of some subgroup of $\mathbb{Q}_2^\times$ of index 4.

REMARK. There exist elliptic curves over $\mathbb{Q}_2$ which do not satisfy either of the hypotheses in part (ii) of the lemma but nevertheless satisfy (§) for $p = 2$. However, (§) does not hold in all cases when $p = 2$: the curve $y^2 = x^3 - x$ is a counterexample.

Let us now prove the second assertion of Theorem 2. Given an arbitrary elliptic curve E over $\mathbb{Q}$ we must show that we can choose f so that the family $E_t = E^{f(t)}$ falls into the second case of Proposition 6, the number of sign changes of f on $\mathbb{R}$ being arbitrarily large. Recall that the zeros of an irreducible polynomial over $\mathbb{Q}$ are simple, whence such a polynomial changes sign at every real zero.

PROPOSITION 8. *Let E be an elliptic curve over $\mathbb{Q}$, let n be a positive even integer, let m be an even integer satisfying $0 \leqslant m \leqslant n$, and let $\varepsilon \in \{\pm 1\}$. If E does not satisfy* (§) *for $p = 2$ then we assume that n is divisible by 4. There exists an irreducible polynomial f over $\mathbb{Q}$ of degree n, with exactly m real zeros $r_1 < r_2 < \cdots < r_m$, such that $W(E^{f(t)}) = \varepsilon(-1)^k$ for $t \in \mathbb{Q} \cap (r_k, r_{k+1})$, $0 \leqslant k \leqslant m$. Here we put $r_0 = -\infty$ and $r_{m+1} = \infty$.*

Proof. If $M(E) = 1$ then we choose f to be any irreducible polynomial over $\mathbb{Q}$ of degree n with exactly m real zeros such that $\lim_{|t|\to\infty} \operatorname{sign}(f(t)) = \varepsilon W(E)$. The formula for $W(E^{f(t)})$ then follows from (7.4). Henceforth we assume that $M(E) > 1$.

For each prime p dividing $M(E)$, choose a subgroup C_p of $\mathbb{Q}_p^\times$ and an element $b_p \in \mathbb{Q}_p^\times$ such that $\delta_{E,p}$ is constant on b_pC_p, with C_p of index 2 or 4 in $\mathbb{Q}_p^\times$ according as (§) is or is not satisfied. Let K_p be the unique abelian extension of $\mathbb{Q}_p$ such that $N_{K_p/\mathbb{Q}_p}(K_p^\times) = C_p$, and let L_p be any extension of K_p of degree $n/[\mathbb{Q}_p^\times : C_p]$. Thus L_p is an extension of $\mathbb{Q}_p$ of degree n. Choose a primitive element of L_p over $\mathbb{Q}_p$ and let

$$g_p(x) = x^n + \sum_{k=0}^{n-1} a_{k,p}x^k$$

be its irreducible monic polynomial over $\mathbb{Q}_p$. Also choose a monic polynomial

$$g_\infty(x) = x^n + \sum_{k=0}^{n-1} a_{k,\infty} x^k$$

of degree n with real coefficients and exactly m real zeros, all of them simple. Finally, let $\varepsilon_p \in \{\pm 1\}$ be the constant value of $\delta_{E,p}$ on $b_p C_p$ for p dividing $M(E)$, and define ε_∞ by the requirement

$$\varepsilon_\infty \prod_{p|M(E)} \varepsilon_p = \varepsilon W(E). \tag{7.5}$$

Now choose a monic polynomial

$$g(x) = x^n + \sum_{k=0}^{n-1} a_k x^k$$

with rational coefficients such that for $p|M(E)$ and $p = \infty$ the coefficient a_k approximates $a_{k,p}$ very closely. Our precise requirements are as follows:

- For each p dividing $M(E)$, g is irreducible over $\mathbb{Q}_p$, and one of its zeros in $\bar{\mathbb{Q}}_p$ generates L_p over $\mathbb{Q}_p$.
- g has exactly m real zeros, all of them simple.

We also choose a rational number b such that $b \in b_p C_p$ for $p|M(E)$ and such that $\operatorname{sign} b = \varepsilon_\infty$. We claim that the polynomial $f = bg$ has the desired properties.

By assumption, $M(E)$ has at least one prime divisor p_0, and since g is irreducible over $\mathbb{Q}_{p_0}$ we see that f is irreducible over $\mathbb{Q}$. By construction, f has exactly m real zeros and

$$\lim_{|t| \to \infty} \operatorname{sign}(f(t)) = \operatorname{sign} b = \varepsilon_\infty. \tag{7.6}$$

We claim that for $p|M(E)$ we have $f(\mathbb{Q}) \subset b_p C_p$, so that

$$\delta_{E,p}(f(t)) = \varepsilon_p \tag{7.7}$$

for $t \in \mathbb{Q}$. Indeed, let α_p be a zero of g in $\bar{\mathbb{Q}}_p$ which generates L_p over $\mathbb{Q}_p$. Given $t \in \mathbb{Q}$ we have

$$\begin{aligned} f(t) &= bg(t) = bN_{L_p/\mathbb{Q}_p}(t - \alpha_p) \\ &= bN_{K_p/\mathbb{Q}_p}(N_{L_p/K_p}(t - \alpha_p)) \in bN_{K_p/\mathbb{Q}_p}(K_p^\times), \end{aligned}$$

and the last term is equal to $b_p C_p$ by construction. Combining (7.4), (7.5), and (7.7), we find

$$W(E^{f(t)}) = \operatorname{sign}(f(t))\varepsilon_\infty \varepsilon,$$

and then (7.6) gives $W(E^{f(t)}) = \varepsilon(-1)^k$ for $t \in \mathbb{Q} \cap (r_k, r_{k+1})$.

8. Proof of Theorem 3

Next we specialize to the case of a family of the form $E_t = E^{f(t)}$ with f quadratic. We assume that there exists a value of $t \in \mathbb{Q}$ such that $f(t) \neq 0$ and $E_t(\mathbb{Q})$ has positive rank, and we must prove that the set of all such t is dense in $\mathbb{R}$. After completing the square in f and replacing the parameter t by a translate of t, we may assume that f has the form $f(t) = ct^2 + e$ with $c, e \in \mathbb{Q}$ and $c \neq 0$. We may also assume that $e \neq 0$, for otherwise the family is a constant family and the assertion to be proved is trivial.

Let $y^2 = x^3 + ax + b$ be an equation for E over $\mathbb{Q}$. Then

$$(ct^2 + e)y^2 = x^3 + ax + b \tag{8.1}$$

is an equation for E_t. Let n be a positive integer divisible by the denominators of a, b, c, and e. After multiplying (8.1) by n^3 and replacing the variables x and y by nx and ny, we may assume that $a, b, c, e \in \mathbb{Z}$.

The principle of the proof is simply this: the surface defined by equation (8.1) can be realized as an elliptic fibration of the affine line in two different ways. First, the map $(x, y, t) \mapsto t$ gives an elliptic fibration of the t-line, and second, the map $(x, y, t) \mapsto y$ gives an elliptic fibration of the y-line. Now suppose that some fiber of the first fibration has a point of infinite order. This point belongs to some fiber of the second fibration, and if we arrange things properly then it is even a point of infinite order on that fiber. By projecting the group it generates onto the base of the first fibration, we shall obtain a dense subset of the t-line where the fibers have positive rank. (The referee has informed me that this type of argument is well known and occurs for example in Elkies' proof that the rational locus of $x^4 + y^4 + z^4 = 1$ is dense in the real locus.)

Let us now put this prescription into practice. By assumption, there exists $s \in \mathbb{Q}$ such that $f(s) \neq 0$ and $E_s(\mathbb{Q})$ has positive rank. Since $cef(s) \neq 0$, the equation $cx^2 + e = f(s)y^2$ defines a smooth curve of genus 0 over $\mathbb{Q}$ with a rational point $(x, y) = (s, 1)$. Hence this curve has infinitely many rational points. Now if (u, v) is any such rational point, then $E_s \cong E_u$. Hence after replacing s by some u if necessary, we may assume that $s \neq 0$.

By assumption, $E_s(\mathbb{Q}) \cap E_s(\mathbb{R})^\circ$ is dense in $E_s(\mathbb{R})^\circ$, where the circle denotes identity component. Since the map $E_s(\mathbb{R})^\circ \setminus \{O\} \to \mathbb{R}$ sending a point to its y-coordinate relative to equation (8.1) is surjective, the restriction of this map to $E_s(\mathbb{Q}) \cap (E_s(\mathbb{R})^\circ \setminus \{O\})$ has dense image. Thus $E_s(\mathbb{Q})$ contains points of infinite order of the form $(q, k/l)$, with $q \in \mathbb{Q}$ and relatively prime positive integers k and l which are greater than any prescribed bound. In particular, we can choose such a point with

$$l > 27e^2 \tag{8.2}$$

and

$$k > ch|4a^3 + 27b^2|^{1/2}. \tag{8.3}$$

Here $h > 0$ denotes the denominator of s.

Consider the curve

$$E' : y^2 = x^3 + Ax + B, \tag{8.4}$$

where

$$A = ac^2l^4$$

and

$$B = c^3l^4(bl^2 - ek^2).$$

We have

$$\frac{4A^3 + 27B^2}{c^6l^8} \equiv 27e^2k^4 \pmod{l}, \tag{8.5}$$

and k is relatively prime to l. From (8.2) we conclude that the left-hand side of (8.5) is not congruent to 0 modulo l and hence is not equal to 0. Therefore E' is an elliptic curve.

By direct calculation, (cl^2q, c^2kl^2s) is a point on E'. We claim that it is a point of infinite order. If not, then it is a torsion point of order > 2, because $ckls \neq 0$. Hence the Lutz-Nagell Theorem implies that $c^2kl^2s \in \mathbb{Z}$ and that $(c^2kl^2s)^2$ divides $4A^3 + 27B^2$. Recalling that h is the denominator of s, we see that k^2 divides $h^2(4A^3 + 27B^2)/(c^4l^4)$, whence k^2 divides $c^2l^8h^2(4a^3 + 27b^2)$. Since k and l are relatively prime and $c^2h^2(4a^3 + 27b^2) \neq 0$, we have a contradiction to (8.3). Thus (cl^2q, c^2kl^2s) is a point of infinite order on E'.

It follows that $E'(\mathbb{Q}) \cap E'(\mathbb{R})^\circ$ is dense in $E'(\mathbb{R})^\circ$. Hence the set of y-coordinates (relative to the equation (8.4)) of points in $E'(\mathbb{Q})\backslash\{O\}$ is dense in $\mathbb{R}$. For $(u, v) \in E'(\mathbb{Q})\backslash\{O\}$ put $t(u, v) = v/(c^2kl^2)$. Then the set

$$\{t(u, v)\colon (u, v) \in E'(\mathbb{Q}),\ (u, v) \neq O\}$$

is the set of all multiples of y-coordinates of points in $E'(\mathbb{Q})\backslash\{O\}$ by the nonzero constant $1/(c^2kl^2)$. Hence this set is also dense in $\mathbb{R}$. On the other hand, putting $x(u, v) = u/(cl^2)$ and $y(u, v) = k/l$, we see by direct calculation that for $(u, v) \in E'(\mathbb{Q})\backslash\{O\}$ we have $(x(u, v), y(u, v)) \in E_{t(u,v)}(\mathbb{Q})$. Thus it suffices to show that for all but finitely many (u, v), the point $(x(u, v), y(u, v))$ has infinite order. This is a consequence of the following lemma, because the map $(u, v) \mapsto x(u, v)$ is finite-to-one:

LEMMA. *Let E be an elliptic curve over $\mathbb{Q}$. Fix an equation*

$$y^2 = x^3 + ax + b$$

for E over $\mathbb{Q}$, so that

$$dy^2 = x^3 + ax + b \qquad (\#)$$

is an equation for E^d over $\mathbb{Q}$ for every $d \in \mathbb{Q}^\times$. Let X be the set of all rational numbers which occur as the x-coordinate (relative to $(\#)$) of some rational torsion point of order >1 on some E^d. Then X is finite.

Proof. By [11] (or see Prop. 1 of [10]) there are only finitely many square-free integers d such that $E^d(\mathbb{Q})$ has a torsion point of order > 2. Let $\{d_1, d_2, \ldots, d_v\}$ be the set of such square-free integers, and for $1 \leqslant i \leqslant v$, let X_i be the finite set consisting of the x-coordinates of rational torsion points of order >1 on E^{d_i}. We claim that

$$X = \bigcup_{i=1}^{v} X_i.$$

Indeed, suppose that $(\xi, \eta) \in E^d(\mathbb{Q})$ is a torsion point of order >1 for some $d \in \mathbb{Q}^\times$. If (ξ, η) has order 2 then $\eta = 0$ and ξ belongs to all of the X_i. If (ξ, η) has order >2, then we can write $d = d_i w^2$ with $w \in \mathbb{Q}^\times$ and $1 \leqslant i \leqslant v$, and $(\xi, w\eta)$ is a torsion point of order >2 in $E^{d_i}(\mathbb{Q})$. Hence $\xi \in X_i$. This proves the claim.

9. Applications

For the formulation and proof of the following lemma, it is convenient to alter our point of view slightly. Instead of referring to an algebraic family of elliptic

curves $\{E_t\}$ over $\mathbb{Q}$, we shall speak instead of an elliptic curve $\mathscr{E}$ over the rational function field $\mathbb{Q}(t)$. If $\mathscr{E}$ corresponds to the family $\{E_t\}$ then the group of $\mathbb{Q}$-rational sections of $\{E_t\}$ is identified with the Mordell-Weil group $\mathscr{E}(\mathbb{Q}(t))$. Given $d \in \mathbb{Q}^\times$, we let $\mathscr{E}^d$ denote as usual the quadratic twist of $\mathscr{E}$ by d.

LEMMA. *Assume that $\mathscr{E}$ is not isomorphic to a constant elliptic curve. Then for all but finitely many square-free integers d, the rank of $\mathscr{E}^d(\mathbb{Q}(t))$ is 0.*

Proof. Put

$$V = \mathbb{C} \otimes_{\mathbb{Z}} \mathscr{E}(\bar{\mathbb{Q}}(t)).$$

We consider the representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on V which is afforded by the natural action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on $\mathscr{E}(\bar{\mathbb{Q}}(t))$. Since $\mathscr{E}$ is not isomorphic to a constant elliptic curve, V is finite-dimensional. In particular, only finitely many irreducible representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ occur in V. But if $d \in \mathbb{Q}^\times$ and χ_d is the character of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ (quadratic or trivial) corresponding to the extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, then χ_d occurs in V if and only if $\mathscr{E}^d(\mathbb{Q}(t))$ has positive rank. From this the lemma follows.

Recall that in Section 7 we have introduced a condition denoted (§) on an elliptic curve E over $\mathbb{Q}_p$. If p is odd then (§) is always satisfied. If $p = 2$ then (§) is satisfied provided that E has potential multiplicative reduction or acquires good reduction over an abelian extension of $\mathbb{Q}_2$.

PROPOSITION 9. *Let E be an elliptic curve over $\mathbb{Q}$.*

(i) *Let n be a positive even integer. If E does not satisfy (§) for $p = 2$ then we assume that n is divisible by 4. There exists an irreducible polynomial f^- over $\mathbb{Q}$ of degree n such that:*

(1) *The group of $\mathbb{Q}$-rational sections of the family $E_t = E^{f^-(t)}$ has rank 0.*
(2) *$W(E^{f^-(t)}) = -1$ for all $t \in \mathbb{Q}$. Hence if we grant (0.1), then $E^{f^-(t)}(\mathbb{Q})$ has rank $\geqslant 1$ for all $t \in \mathbb{Q}$.*

(ii) *Assume that E satisfies (§) for $p = 2$. There exists an irreducible quadratic polynomial f^+ over $\mathbb{Q}$ such that:*

(1) *The group of $\mathbb{Q}$-rational sections of the family $E_t = E^{f^+(t)}$ has rank 0.*
(2) *$E^{f^+(t)}(\mathbb{Q})$ has rank > 0 for a dense set of $t \in \mathbb{Q}$.*
(3) *$W(E^{f^+(t)}) = 1$ for all $t \in \mathbb{Q}$. Hence if we grant (0.1), then $E^{f^+(t)}(\mathbb{Q})$ has rank $\geqslant 2$ for a dense set of $t \in \mathbb{Q}$.*

Proof. (i) We apply Proposition 8 with $m = 0$ and $\varepsilon = -1$. Let f be as in the conclusion of Proposition 8. Since f is irreducible, the family $E_t = E^{f(t)}$ is not isomorphic to a constant family. Hence the lemma implies that there is a positive integer d such that $d \in \mathbb{Q}_p^{\times 2}$ for every p dividing $M(E)$ and such that the group of $\mathbb{Q}$-rational sections of the family $E_t = E^{df(t)}$ has rank 0. We put $f^- = df$. Then (1)

holds. As for (2), we have $\operatorname{sign}(f^{-}(t)) = \operatorname{sign}(f(t))$ and also $\delta_{E,p}(f^{-}(t)) = \delta_{E,p}(f(t))$ for p dividing $M(E)$, because $\delta_{E,p}$ is constant on cosets of $\mathbb{Q}_p^{\times 2}$. Therefore (7.4) gives $W(E^{f^{-}(t)}) = W(E^{f(t)})$ for all $t \in \mathbb{Q}$, and (2) follows.

(ii) We apply Proposition 8 with $n = 2$, $m = 0$, and $\varepsilon = 1$, obtaining an irreducible polynomial f as in the conclusion of Proposition 8. Let $y^2 = x^3 + ax + b$ be an equation for E over $\mathbb{Q}$, and for each prime p dividing $M(E)$ let $(x_p, y_p) \in E^{f(1)}(\mathbb{Q}_p)$ be any point of order >2 (coordinates are taken relative to the equation $f(1)y^2 = x^3 + ax + b$ for $E^{f(1)}$). Let X be as in the lemma at the end of Section 8, so that X is the set of x-coordinates of torsion points on curves of the form $dy^2 = x^3 + ax + b$ with $d \in \mathbb{Q}^{\times}$. Choose a rational number $x_0 \notin X$ such that

$$\operatorname{sign}(x_0^3 + ax_0 + b) = \operatorname{sign}(f(1))$$

and such that for $p | M(E)$,

$$x_0^3 + ax_0 + b \in f(1)\mathbb{Q}_p^{\times 2}.$$

This is possible because the set

$$(x_p^3 + ax_p + b)\mathbb{Q}_p^{\times 2} = f(1)\mathbb{Q}_p^{\times 2}$$

is an open neighborhood of $x_p^3 + ax_p + b$ and therefore contains $x_0^3 + ax_0 + b$ if x_0 is close to x_p.

Put

$$f^{+} = \frac{x_0^3 + ax_0 + b}{f(1)} f.$$

Since $x_0 \notin X$, the point $(x_0, 1) \in E^{f^{+}(1)}(\mathbb{Q})$ has infinite order. Therefore (2) holds by Theorem 3. Regarding (3), we have $\operatorname{sign}(f^{+}(t)) = \operatorname{sign}(f(t))$ and $f^{+}(t) \in f(t)\mathbb{Q}_p^{\times 2}$ for p dividing $M(E)$, so that $W(E^{f^{+}(t)}) = W(E^{f(t)})$ for all $t \in \mathbb{Q}$ by (7.4). Hence (3) holds.

Finally, as pointed out to me by Masato Kuwata and the referee, one can use Shioda's formula ([16], (10.2) and (10.14)) to compute the rank of the elliptic surface $f(t)y^2 = x^3 + ax + b$ over $\mathbb{C}$. There are exactly two singular fibers, corresponding to the two complex zeros of f, and applying case (6.1) of Tate's algorithm ([18], p. 35), one sees that both fibers are of type I_0^*. Therefore the group of $\mathbb{C}$-rational sections has rank 0, and *a fortiori* (1) holds.

The referee has also supplied the following direct argument: Suppose that $(x(t), y(t))$ is a nonzero section of $f(t)y^2 = x^3 + ax + b$ over $\mathbb{C}$. Let $\sqrt{f(t)}$ denote

a fixed square root of $f(t)$ in $\overline{\mathbb{C}(t)}$. Then $(x(t), \sqrt{f(t)}y(t))$ is a point on E defined over the rational function field $\mathbb{C}\left(t, \sqrt{f(t)}\right)$ and so corresponds to a morphism $\mathbf{P}^1 \to E$. But any such morphism is constant. Therefore $x(t)$ and $y(t)$ are constant functions, and if $y(t)$ is nonzero then $f(t)$ is also constant, a contradiction. It follows that any section of $f(t)y^2 = x^3 + ax + b$ has order at most 2.

Acknowledgments

It is a pleasure to thank the referee for an exceptionally careful reading of the manuscript. I am also grateful to Barry Mazur for providing me with a preliminary version of his paper *The topology of rational points* and for some stimulating correspondence and conversations. A special case of Proposition 9 was first pointed out to me by Masato Kuwata in a remark concerning a previous work [12], and I am indebted both to Kuwata and to the referee for the geometric arguments used in the proof of part (ii) of the proposition, which made it possible to eliminate an unnecessary hypothesis. Finally, I would like to express may appreciation to Wenyun Gao, Elisabetta Manduchi, Joe Silverman, Lan Wang, and Larry Washington for a variety of comments and corrections.

References

1. B. J. Birch and N. M. Stephens, The parity of the rank of the Mordell-Weil group, *Topology* 5 (1966), 295–299.
2. J. W. S. Cassels, Arithmetic on curves of genus 1. VIII, *J. reine angew. Math.* 217 (1965), 180–199.
3. J. W. S. Cassels, Diophantine equations with special reference to elliptic curves, *J. London Math. Soc.* 41 (1966), 193–291.
4. J. W. S. Cassels and A. Schinzel, Selmer's conjecture and families of elliptic curves, *Bull. London Math. Soc.* 14 (1982), 345–348.
5. I. Connell, Good reduction of elliptic curves in abelian extensions, *J. reine angew. Math.* (to appear).
6. P. Deligne, Les constantes des équations fonctionelles des fonctions L, *Modular Functions of One Variable, II*, *SLN* 349, Springer-Verlag, New York, 1973, pp. 501–595.
7. B. Edixhoven, A. De Groot, and J. Top, Elliptic curves over the rationals with bad reduction at only one prime, *Math. of Comp.* 54 (1990), 413–419.
8. A. Fröhlich and J. Queyrut, On the functional equation of the Artin L-function for characters of real representations, *Invent. Math.* 20 (1973), 125–138.
9. P. X. Gallagher, Determinants of representations of finite groups, *Abh. Math. Sem. Univ. Hamburg* 28 (1965), 162–167.
10. F. Gouvêa and B. Mazur, The square-free sieve and the rank of elliptic curves, *J. Amer. Math. Soc.* 4 (1991), 1–23.
11. L. D. Olson, Torsion points on elliptic curves with given j-invariant, *Manuscripta Math.* 16 (1975), 145–150.
12. D. E. Rohrlich, Nonvanishing of L-functions and structure of Mordell-Weil groups, *J. reine angew. Math.* 417 (1991), 1–26.

13. E. S. Selmer, A conjecture concerning rational points on cubic curves, *Math. Scand.* 2 (1954), 49–54.
14. J-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* 15 (1972), 259–331.
15. J-P. Serre and J. Tate, Good reduction of abelian varieties, *Ann. Math.* 68 (1968), 492–517.
16. T. Shioda, On the Mordell-Weil lattices, *Comment. Math. Univ. Sancti Pauli* 39 (1990), 211–240.
17. J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1985.
18. J. Tate, Algorithm for finding the type of a singular fiber in an elliptic pencil, *Modular Functions of One Variable IV, Lect. Notes Math.* 476, Springer-Verlag, 1975, pp. 33–52.
19. J. Tate, Number theoretic background, *Automorphic Forms, Representations, and L-Functions, Proc. Symp. Pure Math.* Vol. 33 – Part 2, *Amer. Math. Soc.*, Providence, 1979, pp. 3–26.
20. J. Tunnell, On the local Langlands conjecture for GL(2), *Invent. Math.* 46 (1978), 179–200.
21. J. Tunnell, Report on the local Langlands conjecture for GL(2), *Automorphic Forms, Representations, and L-Functions, Proc. Symp. Pure Math.* Vol. 33 – Part 2, *Amer. Math. Soc.*, Providence, 1979.
22. J.-L. Waldspurger, Correspondances de Shimura et quaternions, *Forum Math.* 3 (1991), 219–307.