Algebra & Number Theory

Volume 5

2011

No. 5

Density of rational points on isotrivial rational elliptic surfaces

Anthony Várilly-Alvarado

mathematical sciences publishers

ALGEBRA AND NUMBER THEORY 5:5(2011)

msp

Density of rational points on isotrivial rational elliptic surfaces

Anthony Várilly-Alvarado

For a large class of isotrivial rational elliptic surfaces (with section), we show that the set of rational points is dense for the Zariski topology, by carefully studying variations of root numbers among the fibers of these surfaces. We also prove that these surfaces satisfy a variant of weak-weak approximation. Our results are conditional on the finiteness of Tate–Shafarevich groups for elliptic curves over the field of rational numbers.

1. Introduction

1A. ***Del Pezzo surfaces of degree*** **1*: a sample result.*** Let X be a smooth projective geometrically integral surface over a number field k. Fix an algebraic closure $\bar{k}$ of k and assume that X is geometrically rational, i.e., the base extension $X_{\bar{k}} := X \times_k \bar{k}$ is birational to the projective plane $\mathbb{P}^2_{\bar{k}}$. A well-known result of Iskovskikh [1979] guarantees that X is k-birational to either a rational conic bundle or a del Pezzo surface.

Del Pezzo surfaces that are not geometrically isomorphic to $\mathbb{P}^1_{\bar{k}} \times \mathbb{P}^1_{\bar{k}}$ are classified by their *degree* $d := K_X^2$, an integer in the range $1 \leq d \leq 9$. Segre and Manin have shown that if X is a del Pezzo surface with $d \geq 2$, and if X contains a k-point not lying on an explicitly computable locus, then $X(k)$ is dense in the Zariski topology; moreover, X is k-unirational in this case [Manin and Hazewinkel 1974, Theorem 29.4]. Surfaces X with $d = 1$ come furnished with a rational point (the base point of the anticanonical linear system). Hence the question: is $X(k)$ dense for the Zariski topology? One of our goals in this paper is to shed some light on this question, in the case when $k = \mathbb{Q}$.

Theorem 1.1. *Let A, B be nonzero integers, and let X be the del Pezzo surface of degree* 1 *over $\mathbb{Q}$ given by*

$$w^2 = z^3 + Ax^6 + By^6 \tag{1}$$

MSC2000: primary 11G35; secondary 14G05, 11G05.

Keywords: rational elliptic surfaces, del Pezzo surfaces, root numbers.

in $\mathbb{P}_{\mathbb{Q}}(1,1,2,3)$. *Assume that Tate–Shafarevich groups of elliptic curves over* $\mathbb{Q}$ *with* j*-invariant* 0 *are finite. If* $3A/B$ *is not a rational square, or if* A *and* B *are relatively prime and* $9 \nmid AB$, *then the rational points of* X *are Zariski dense.*

See Section 2 for statements of our most general results.

Remarks 1.2. (i) Every del Pezzo surface of degree 1 is isomorphic to a *smooth* sextic hypersurface in $\mathbb{P}_k(1,1,2,3)$; conversely, a smooth sextic hypersurface in this weighted projective space is a del Pezzo surface of degree 1 [Kollár 1996, Theorem III.3.5].

(ii) Using explicit rational base changes, it is shown in [Ulas 2007, Corollary 4.4] that the conclusion of Theorem 1.1 holds *unconditionally* in the case $A = 1$.

(iii) The restriction in (1) that A and B are integers is not severe. If A and B are rational numbers, one can clear denominators and rescale the variables to obtain an equation of the form (1).

(iv) Using the methods in [Várilly-Alvarado 2008], we may compute $\operatorname{Pic} X$ for the surfaces (1). If $\operatorname{rk}\operatorname{Pic} X = 1$, then X is $\mathbb{Q}$-minimal, and is thus a "genuine" del Pezzo surface of degree 1, i.e., X is not the blow-up of a higher degree surface at closed $\mathbb{Q}$-points. This is the case, for example, if $A = B = p^3$, where $p > 3$ is a prime number; see Theorem 1.1 of that reference.

Blowing up the base point of the anticanonical linear system of a del Pezzo surface of degree 1, we obtain a rational elliptic surface. These are the main objects of study in our paper. However, we state our results in Section 2 in terms of hypersurfaces in $\mathbb{P}_{\mathbb{Q}}(1,1,2,3)$ to emphasize the connection with del Pezzo surfaces of degree 1.

1B. ***Rational elliptic surfaces.*** Let k be a number field, and let $(\mathscr{E}, \rho, \sigma)$ be an *elliptic surface with base* $\mathbb{P}^1_k$, i.e., a smooth surface $\mathscr{E}$ together with a morphism $\rho\colon \mathscr{E} \to \mathbb{P}^1_k$ that has a section $\sigma : \mathbb{P}^1_k \to \mathscr{E}$, such that ρ is a relatively minimal elliptic fibration and has at least one (geometric) singular fiber. We often write $\mathscr{E}$ instead of $(\mathscr{E}, \rho, \sigma)$, the morphisms ρ and σ being understood. Suppose that $\mathscr{E} \times_k \bar{k}$ is birational to $\mathbb{P}^2_{\bar{k}}$ (in which case we say that $\mathscr{E}$ is *rational*). Then the generic fiber of ρ is an elliptic curve $E/k(T)$ that can given by a Weierstrass equation of the form

$$Y^2 = X^3 + a(T)X + b(T), \quad a(T), b(T) \in k[T], \tag{2}$$

where

$$\deg a(T) \le 4, \quad \deg b(T) \le 6 \quad \text{and} \quad \Delta := 4a(T)^3 + 27b(T)^2 \notin k.$$

Conversely, any elliptic curve $E/k(T)$ of the form (2) uniquely extends to a rational elliptic surface with base $\mathbb{P}^1_k$ (the Kodaira–Néron model of E).

We associate to $\mathscr{E}$ a sextic hypersurface X in the weighted projective space $\mathbb{P}_k(1,1,2,3)$ as follows. Let $k[x,y,z,w]$ be the graded ring where the variables x,y,z,w have weights 1, 1, 2, 3, respectively. Set

$$\mathbb{P}_k(1,1,2,3) := \operatorname{Proj} k[x,y,z,w]$$

and let X be the sextic hypersurface

$$w^2 = z^3 + G(x,y)z + F(x,y), \tag{3}$$

where

$$G(x,y) = y^4 a(x/y) \quad \text{and} \quad F(x,y) = y^6 b(x/y).$$

The schemes X and $\mathscr{E}$ are birational: X can be obtained from $\mathscr{E}$ by contracting the image of the section σ as well as the components of the singular fibers of ρ that do not meet $\sigma(\mathbb{P}^1_k)$. In general, X will be a singular hypersurface.

We are interested in the qualitative distribution of the set $\mathscr{E}(k)$. In particular, we want to determine if the set $\mathscr{E}(k)$ (equivalently, the set $X(k)$) is dense for the Zariski topology. Our investigations rely heavily on the root numbers of the fibers of ρ, and for this reason we focus our attention on the case $k = \mathbb{Q}$.

To prove that $\mathscr{E}(\mathbb{Q})$ is Zariski dense, it suffices to show that for infinitely many $t \in \mathbb{P}^1(\mathbb{Q})$, the fiber $\mathscr{E}_t$ of ρ is an elliptic curve with positive Mordell–Weil rank. Assuming finiteness of Tate–Shafarevich groups, Nekovář, Dokchitser and Dokchitser have shown that the root number of an elliptic curve $E/\mathbb{Q}$ is $(-1)^{\operatorname{rank}(E)}$ (the parity conjecture; see [Nekovář 2001; Dokchitser and Dokchitser 2010]). We study the variation of root numbers among the smooth fibers of $\mathscr{E}$, hoping to find infinitely many fibers with negative root number.

Rohrlich [1993] pioneered the study of variations of root numbers on algebraic families of elliptic curves. Many authors followed suit; see, for example, [Manduchi 1995; Grant and Manduchi 1997; Grant and Manduchi 1998; Rizzo 2003; Conrad et al. 2005]. Some authors (see notably [Conrad et al. 2005, p. 686]) have observed that if the fibers of an elliptic surface lack "geometric variation," then often there are simple formulae that describe the root numbers of these fibers; see, for example [Rohrlich 1996, Corollary to Proposition 10]. For this reason, we restrict our attention to *isotrivial* rational elliptic surfaces, i.e., surfaces $\mathscr{E}$ as above for which the modular invariant $j(E)$ has no T-dependence. Such surfaces arise as families of (quadratic, cubic, quartic or sextic) twists of a fixed elliptic curve $E_0/\mathbb{Q}$:

(i) (quadratic twists) $Y^2 = X^3 + af(T)^2X + bf(T)^3$ with $a, b \in k$, $f(T) \in k[T]$ and $1 \leq \deg f(T) \leq 2$,

(ii) (cubic twists) $Y^2 = X^3 + f(T)^2$ with $f(T) \in k[T]$ and $1 \leq \deg f(T) \leq 3$,

(iii) (quartic twists) $Y^2 = X^3 + f(T)X$ with $f(T) \in k[T]$ and $1 \leq \deg f(T) \leq 4$,

(iv) (sextic twists) $Y^2 = X^3 + f(T)$ with $f(T) \in k[T] \backslash k[T]^2$ and $1 \leq \deg f(T) \leq 6$.

We use Rohrlich's formulae for local root numbers, together with those of Halberstadt [1998] and Rizzo [2003], to assemble root number formulae for quartic and sextic twists of elliptic curves over $\mathbb{Q}$ (see Propositions 4.8 and 4.4, respectively). We then combine our explicit formulae for root numbers with an adaptation of a sieve introduced by Gouvêa and Mazur [1991] and Greaves [1992]. The modified sieve allows us to search for infinitely many pairs of fibers on a surface that have *opposite* root numbers, which yields our density results (Theorems 2.1 and 2.3). For a similarly motivated idea, see [Manduchi 1995].

Outline of the paper. In Section 2, we state our density theorems (Theorems 2.1, 2.3 and 2.6), and we relate them to the literature, where many similar results can be found under the umbrella of Mazur's conjecture on the topology of rational points. In Section 3, we make precise the relation between isotrivial rational elliptic surfaces and del Pezzo surfaces of degree 1. In Section 4, we present formulae for the root numbers of elliptic curves $E_\alpha/\mathbb{Q}$ of the form $y^2 = x^3 + \alpha$ or $y^2 = x^3 + \alpha x$, where α is a nonzero integer. We use our formulae to give conditions on integers α and β under which E_α and E_β have opposite root numbers (Corollaries 4.5 and 4.9), a crucial input in the proof of our density results. In Section 5, we turn our attention to sieving, and present our modification of the squarefree sieve of Gouvêa, Mazur and Greaves. In Section 6, we use this sieve to locate infinite families of fibers on elliptic surfaces with *opposite* root number, and thus prove Theorems 2.1 and 2.3. In Section 7, we specialize to the case of "diagonal" del Pezzo surfaces of degree 1 over $\mathbb{Q}$. Finally, we prove Theorem 2.6 in Section 8.

2. Main results

Let $F(x, y) \in \mathbb{Z}[x, y]$ be a homogeneous binary form. We say that *F has a fixed prime divisor* if there is a prime number p such that $F(a, b) \in p\mathbb{Z}$ for all $a, b \in \mathbb{Z}$. Note that if the content of $F(x, y)$ is not divisible by p, then $F(x, y) \bmod p$ has at most $\deg F(x, y)$ zeroes in $\mathbb{P}^1(\mathbb{F}_p)$. Hence, if p is a fixed prime divisor of $F(x, y)$, then $p + 1 \leq \deg F(x, y)$.

2A. ***Sextic twists and del Pezzo surfaces of degree* 1.** Let

$$\rho\colon \mathscr{E} \to \mathbb{P}^1_{\mathbb{Q}}$$

be an isotrivial rational elliptic surface whose associated sextic hypersurface

$$X \subseteq \mathbb{P}_{\mathbb{Q}}(1, 1, 2, 3)$$

is smooth (hence a del Pezzo surface of degree 1). We show in Section 3 that X must be isomorphic to a sextic of the form

$$w^2 = z^3 + F(x, y),$$

where $F(x, y)$ is a squarefree homogeneous form of degree 6. The generic fiber $E/\mathbb{Q}(T)$ of $\mathscr{E}$ is isomorphic to

$$Y^2 = X^3 + b(T), \quad \text{where } b(T) = F(T, 1) \text{ or } F(1, T),$$

and can be thought of family of sextic twists. We prove the following density result for this class of surfaces.

Theorem 2.1. *Let $F(x, y) \in \mathbb{Z}[x, y]$ be a homogeneous binary form of degree 6; assume that the coefficients of x^6 and y^6 are nonzero. Let X be the del Pezzo surface of degree 1 over $\mathbb{Q}$ given by*

$$w^2 = z^3 + F(x, y) \tag{4}$$

in $\mathbb{P}_{\mathbb{Q}}(1, 1, 2, 3)$. Let c be the content of F and write $F(x, y) = cF_1(x, y)$ for some $F_1(x, y) \in \mathbb{Z}[x, y]$. Suppose that F_1 has no fixed prime divisors and that $F_1 = \prod_i f_i$, where the $f_i \in \mathbb{Z}[x, y]$ are irreducible homogeneous forms. Assume further that

$$\mu_3 \not\subseteq \mathbb{Q}[t]/f_i(t, 1) \quad \textit{for some } i, \tag{5}$$

where μ_3 is the group of third roots of unity. Finally, assume that Tate–Shafarevich groups of elliptic curves over $\mathbb{Q}$ with j-invariant 0 are finite. Then the rational points of X are dense for the Zariski topology.

Remark 2.2. The restriction that $F(x, y) \in \mathbb{Z}[x, y]$ in Theorem 2.1 is not severe; see Remark 1.2(i). Also, the assumption that the coefficients of x^6 and y^6 are nonzero is not a restriction: it can be achieved with a suitable linear transformation, without so changing the isomorphism class of X.

We use Theorem 2.1 to deduce Theorem 1.1, which addresses the question of Zariski density of rational points for "diagonal" del Pezzo surfaces of degree 1 over $\mathbb{Q}$. We believe that the extraneous-looking hypotheses in Theorem 1.1, such as "$3A/B$ is not a rational square" or "$9 \nmid AB$," are not necessary. Our method of proof, however, breaks down without them. For example, if $(A, B) = (27, 16)$ then *all* the nonsingular fibers of the corresponding elliptic surface $\rho\colon \mathscr{E} \to \mathbb{P}^1_{\mathbb{Q}}$ have *positive* root number, and thus (conjecturally) even rank. In this particular example one can even show that all but finitely many fibers have rank at least 2, whence Zariski density of rational points on X is still true. However, if, for example, $(A, B) = (243, 16)$, then again all associated root numbers are positive, but we are unable to show rational points on X are Zariski dense (see Example 7.1 and Remark 7.4).

2B. ***Quartic twists and (mildly singular) del Pezzo surfaces of degree* 1.** Let $\rho\colon \mathscr{E} \to \mathbb{P}^1_{\mathbb{Q}}$ be an isotrivial rational elliptic surface and suppose that its generic fiber is of the form

$$Y^2 = X^3 + a(T)X, \quad a(T) \in \mathbb{Q}[t],\ \deg a(T) \leq 4,$$

which can be thought of as a family of quartic twists over $\mathbb{Q}$. The associated hypersurface $X \subseteq \mathbb{P}_{\mathbb{Q}}(1, 1, 2, 3)$, given by

$$w^2 = z^3 + G(x, y)z, \quad G(x, y) := y^4 a(x/y),$$

is not smooth (and hence not a del Pezzo surface of degree 1). However, X is not too far from being smooth: for example, when G is squarefree, its singular locus consists of four A_2-singularities ($w = z = G(x, y) = 0$). We prove the following density result for this class of surfaces.

Theorem 2.3. *Let $G[x, y] \in \mathbb{Z}[x, y]$ be a squarefree homogeneous binary form of degree* 4; *assume that the coefficients of x^4 and y^4 are nonzero. Let X be the hypersurface given by*

$$w^2 = z^3 + G(x, y)z \tag{6}$$

in $\mathbb{P}_{\mathbb{Q}}(1, 1, 2, 3)$. Let c be the content of G and write $G(x, y) = cG_1(x, y)$ for some $G_1(x, y) \in \mathbb{Z}[x, y]$. Suppose that G_1 has no fixed prime divisors and that $G_1 = \prod_i g_i$, where the $g_i \in \mathbb{Z}[x, y]$ are irreducible homogeneous forms. Assume further that

$$\mu_4 \not\subseteq \mathbb{Q}[t]/g_i(t, 1) \quad \textit{for some } i, \tag{7}$$

where μ_4 is the group of fourth roots of unity. Finally, assume that Tate–Shafarevich groups of elliptic curves over $\mathbb{Q}$ with j-invariant 1728 *are finite. Then the rational points of X are dense for the Zariski topology.*

Remark 2.4. The assumption that the coefficients of x^4 and y^4 are nonzero is not a restriction: it can be achieved with a suitable linear transformation, without so changing the isomorphism class of X.

Remark 2.5. Ulas [2007; 2008] studied the question of Zariski density of rational points on certain del Pezzo surfaces of degree 1 over $\mathbb{Q}$ by looking at explicit rational base-changes of their associated elliptic surfaces. His results do not depend on arithmetic conjectures and are thus stronger than ours, whenever there is an overlap — compare our Theorem 2.1 with Theorems 2.1 and 2.2 of [Ulas 2007] and our Theorem 2.3 with Theorems 3.1 and 3.2 of the same reference.

2C. ***Toward weak-weak approximation.*** Write Ω_k for the set of places of a number field k, and let k_v be the completion of k at $v \in \Omega_k$. Recall that a geometrically integral variety X over k satisfies *weak-weak approximation* if there exists a finite set $T \subseteq \Omega_k$ such that for every other finite set $S \subseteq \Omega_k$ with $S \cap T = \varnothing$, the image of the embedding

$$X(k) \hookrightarrow \prod_{v \in S} X(k_v)$$

is dense for the product topology of the v-adic topologies. We say that X satisfies *weak approximation* if we can take $T = \varnothing$.

It is known that del Pezzo surfaces of low degree need not satisfy weak approximation; see [Colliot-Thélène et al. 1987, Example 15.5; Swinnerton-Dyer 1962; Kresch and Tschinkel 2008, Example 2, Várilly-Alvarado 2008, Theorem 1.1] for counterexamples in degrees 4, 3, 2 and 1, respectively. It is believed, however, that these surfaces satisfy weak-weak approximation. More generally, a conjecture of Colliot-Thélène predicts that unirational varietes satisfy weak-weak approximation (the conjecture implies a positive solution to the inverse Galois problem over number fields); see [Serre 2008, p. 30]. Following a suggestion of Colliot-Thélène, we use our modified squarefree sieve to show that the surfaces of Theorems 2.1 and 2.3 satisfy a "surrogate" property that would be easily implied by weak-weak approximation. For analogous results in this direction on certain elliptic surfaces without section, see [Colliot-Thélène et al. 1998a], and for more general fibrations over the projective line, see [Colliot-Thélène et al. 1998b].

Theorem 2.6. *Let $\rho\colon \mathscr{E} \to \mathbb{P}^1_{\mathbb{Q}}$ be an elliptic surface associated to one of the hypersurfaces considered in either Theorem 2.1 or 2.3. Let $\mathscr{R}$ be the set of points $x \in \mathbb{P}^1(\mathbb{Q})$ such that the fiber $\mathscr{E}_x = \rho^{-1}(x)$ is an elliptic curve of positive Mordell–Weil rank. Assume that Tate–Shafarevich groups of elliptic curves over $\mathbb{Q}$ with j-invariant* 0 *or* 1728 *are finite. Then there exists a finite set of primes P_0, containing the infinite prime, such that for every finite set of primes P with $P \cap P_0 = \varnothing$, the image of the embedding*

$$\mathscr{R} \hookrightarrow \prod_{p \in P} \mathbb{P}^1(\mathbb{Q}_p)$$

is dense for the product topology of the p-adic topologies.

Remark 2.7. The set P_0 in Theorem 2.6 is effectively computed in the proof of the theorem.

2D. *Mazur's conjecture and related work.*

Mazur has made a series of conjectures on the topology of rational points on varieties, including the following.

Conjecture 2.8 [Mazur 1992, Conjecture 4]. Let $\mathscr{E} \to \mathbb{P}^1_{\mathbb{Q}}$ be an elliptic surface with base $\mathbb{P}^1_{\mathbb{Q}}$. Then one of the following two conditions hold:

(1) for all but finitely many $t \in \mathbb{P}^1(\mathbb{Q})$, the fiber $\mathscr{E}_t$ is an elliptic curve with Mordell–Weil rank equal to zero,

(2) the set of $t \in \mathbb{P}^1(\mathbb{Q})$ such that $\mathscr{E}_t$ is an elliptic curve with positive Mordell–Weil rank is dense in $\mathbb{P}^1(\mathbb{R})$.

Many authors have shown since that (2) holds for a range of elliptic surfaces. In particular, the set $\mathscr{E}(\mathbb{Q})$ is dense in the Zariski topology for these surfaces. For example, in [Rohrlich 1993, Theorem 3] Rohrlich shows, unconditionally and using elementary methods, that if $f(t) \in \mathbb{Q}[t]$ is a quadratic polynomial, then the Kodaira–Néron model $\mathscr{E}$ of the elliptic curve over $\mathbb{Q}(T)$ given by

$$Y^2 = X^3 + af(T)^2X + bf(T)^3 \quad a, b \in \mathbb{Q}$$

satisfies part (2) of Conjecture 2.8, provided that there exists $t \in \mathbb{Q}$ such that $f(t) \neq 0$ and that $\mathscr{E}_t$ has positive Mordell–Weil rank. Munshi has recently extended this result to rational elliptic surfaces over real number fields, provided there are at least two fibers of positive rank and one fiber with a 2-torsion point defined over the ground field [Munshi 2010, Theorem 2].

Kuwata and Wang have a similar result to Rohrlich's for quadratic twists by cubic polynomials [Kuwata and Wang 1993]. The resulting isotrivial elliptic surfaces, however, are not rational; they are $K3$ surfaces. Munshi [2007] examined Conjecture 2.8 for many kinds of isotrivial rational elliptic surfaces, including cubic twists, by studying "horizontal" elliptic or conic bundle structures on these surfaces. There is surprisingly little overlap between Munshi's and our investigations; in fact, our methods cannot yield density results for cubic twists (the squarefreeness of $F(x, y)$ in (4) is central to our sieving argument). We have conditionally addressed the question of Zariski density of rational points on some of the isotrivial cases left open in [Munshi 2007, §7].

Assuming the parity conjecture, Manduchi has shown that conclusion (2) of Conjecture 2.8 holds for large families of *nonisotrivial* elliptic surfaces with base $\mathbb{P}^1_{\mathbb{Q}}$; see [Manduchi 1995]. Over a general number field, and assuming the Birch–Swinnerton-Dyer conjecture, as well as a conjecture of Deligne and Gross, Grant and Manduchi have shown that rational points are *potentially dense* for nonisotrivial elliptic surfaces over a rational or elliptic base; see [Grant and Manduchi 1997; 1998]. Ulas [2007, Theorems 5.1 and 5.3] has obtained density results on extensive families of rational nonisotrivial elliptic surfaces by studying explicit rational base changes (see Remark 2.5 as well). Helfgott [2004] has also obtained density results for elliptic surfaces through his study of average root numbers in families. His results depend on classical arithmetical conjectures.

Elkies (private communication, 2009) has suggested that Conjecture 2.8 is false; he has a heuristic which indicates that certain families of quadratic twists by a polynomial of high degree should yield counterexamples.

Colliot-Thélène, Swinnerton-Dyer and Skorobogatov study in [Colliot-Thélène et al. 1998a] the vertical Brauer–Manin obstruction of a large class of elliptic surfaces *without section*. In particular, they show that the set of rational points of the elliptic surfaces they study is dense for the Zariski topology as soon as it is nonempty. Their results are conditional on the finiteness of Tate–Shafarevich groups and Schinzel's hypothesis (a wild generalization of the twin primes conjecture).

3. Isotrivial elliptic surfaces and del Pezzo surfaces of degree 1

Let k be a number field, and let $(\mathscr{E}, \rho, \sigma)$ be an isotrivial rational elliptic surface with base $\mathbb{P}^1_k$. The generic fiber $E/k(T)$ of $\mathscr{E}$ is isomorphic to a curve in the list (i)–(iv) on page 661. Suppose that the sextic hypersurface $X \subseteq \mathbb{P}_k(1, 1, 2, 3)$ associated to $\mathscr{E}$ is smooth (and hence a del Pezzo surface of degree 1). Then a straightforward (albeit tedious) application of the Jacobian criterion shows that $E/k(T)$ must be a family of sextic twists (iv), with $f(T)$ squarefree. Alternatively, we may argue as follows. Since $X_{\bar{k}}$ is isomorphic to $\mathbb{P}^2_{\bar{k}}$ blown-up at 9 distinct points in general position [Manin and Hazewinkel 1974], it follows from [Shioda 1990, Theorem 10.11] that the Mordell–Weil lattice of $E_{\bar{k}(T)}$ has rank 8. From the Shioda–Tate formula [Shioda 1990, Corollary 5.3], we deduce that $\mathscr{E}_{\bar{k}}$ has no reducible fibers, i.e., the singular fibers of $\rho_{\bar{k}} : \mathscr{E}_{\bar{k}} \to \mathbb{P}^1_{\bar{k}}$ must be of type I_0 or II, in Kodaira's notation. The isotriviality of $\mathscr{E}$ precludes singular fibers of type I_0 (because these fibers are semistable). Looking at Persson's classification [1990] of rational elliptic surfaces, we conclude that $\mathscr{E}_{\bar{k}}$ must have six singular fibers of type II. A quick application of Tate's algorithm to the Kodaira–Néron models of the possible generic fibers from the list leaves (iv) as the only possibility, under the additional hypothesis that $f(T)$ is squarefree. We have thus shown:

Proposition 3.1. *Let k be a number field and let $(\mathscr{E}, \rho, \sigma)$ be an isotrivial rational elliptic surface with base $\mathbb{P}^1_k$. Suppose that the sextic hypersurface $X \subseteq \mathbb{P}^1_k(1, 1, 2, 3)$ associated to $\mathscr{E}$ is smooth. Then X is isomorphic to a hypersurface of the form*

$$w^2 = z^3 + F(x, y),$$

where $F(x, y)$ is a squarefree homogeneous form. □

4. Root numbers and flipping

Let E be an elliptic curve over $\mathbb{Q}$. The *root number* $W(E)$ of E is defined as a product of local factors

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

where p runs over the rational prime numbers and infinity, $W_p(E) \in \{\pm 1\}$ and $W_p(E) = +1$ for all but finitely many p. The *local root number* $W_p(E)$ of E at p is defined in terms of epsilon factors of Weil–Deligne representations of $\mathbb{Q}_p$; it is an invariant of the isomorphism class of the base extension $E_{\mathbb{Q}_p}$ of E. For a definition of these local factors see [Deligne 1973; Tate 1979]. If p is a prime of good reduction for E then $W_p(E) = +1$; furthermore, $W_\infty(E) = -1$ (see [Rohrlich 1993]). The computation of $W_p(E)$ for primes of bad reduction in terms of data associated to a Weierstrass model of E has been studied by various authors; see particularly [Rohrlich 1993; Halberstadt 1998; Rizzo 2003]. In this section, we build on their work to give formulae for the root numbers of elliptic curves over $\mathbb{Q}$ of the form

$$y^2 = x^3 + \alpha \quad \text{and} \quad y^2 = x^3 + \alpha x \quad (\alpha \neq 0).$$

Our formula for the root number of $y^2 = x^3 + \alpha$ has a flavor different from that found in [Liverance 1995]; in particular, it is visibly insensitive to primes $p \geq 5$ whose *square* does not divide α.

Conjecturally, the root number $W(E)$ of an elliptic curve is the sign in the functional equation for the L-series $L(E, s)$ of E:

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

where N is the conductor of E, and $\Gamma(s)$ is the usual gamma function. According to the Birch–Swinnerton-Dyer conjecture,

$$W(E) = (-1)^{\operatorname{rank}(E)}. \tag{8}$$

Equality (8) is itself known as the *parity conjecture*. By [Nekovář 2001] and [Dokchitser and Dokchitser 2010] the finiteness of Tate–Shafarevich groups is enough to prove the parity conjecture.

Notation. In addition to the notation introduced above, we use the following conventions. Throughout, for a prime $p \in \mathbb{Z}$ we denote the corresponding p-adic valuation by v_p. If a is a nonzero integer then $\left(\frac{a}{p}\right)$ will denote the usual Legendre symbol; if m is an odd positive integer, $\left(\frac{a}{m}\right)$ will denote the usual Jacobi symbol.

4A. *The root number of $E_\alpha : y^2 = x^3 + \alpha$.*

Let α be a nonzero integer. We give a closed formula for the root number of the elliptic curve $E_\alpha/\mathbb{Q} : y^2 = x^3 + \alpha$, in terms of α. Throughout, we write $W(\alpha)$ for this root number and $W_p(\alpha)$ for the local root number of E_α at p. We begin by determining $W_2(\alpha)$ and $W_3(\alpha)$.

Lemma 4.1. *Let α be a nonzero integer. Define α_2 and α_3 by*

$$\alpha = 2^{v_2(\alpha)}\alpha_2 = 3^{v_3(\alpha)}\alpha_3.$$

Then

$$W_2(\alpha) = \begin{cases} -1 & \textit{if } v_2(\alpha) \equiv 0 \textit{ or } 2 \bmod 6 \\ & \textit{or if } v_2(\alpha) \equiv 1, 3, 4 \textit{ or } 5 \bmod 6 \textit{ and } \alpha_2 \equiv 3 \bmod 4, \\ +1 & \textit{otherwise} \end{cases}$$

and

$$W_3(\alpha) = \begin{cases} -1 & \textit{if } v_3(\alpha) \equiv 1 \textit{ or } 2 \bmod 6 \textit{ and } \alpha_3 \equiv 1 \bmod 3, \\ & \textit{or if } v_3(\alpha) \equiv 4 \textit{ or } 5 \bmod 6 \textit{ and } \alpha_3 \equiv 2 \bmod 3, \\ & \textit{or if } v_3(\alpha) \equiv 0 \bmod 6 \textit{ and } \alpha_3 \equiv 5 \textit{ or } 7 \bmod 9 \\ & \textit{or if } v_3(\alpha) \equiv 3 \bmod 6 \textit{ and } \alpha_3 \equiv 2 \textit{ or } 4 \bmod 9, \\ +1 & \textit{otherwise.} \end{cases}$$

Proof. According to [Rizzo 2003, §1.1], to determine the local root number at p of an elliptic curve given in Weierstrass form, we must find the smallest vector with nonnegative entries

$$(a, b, c) := (v_p(c_4), v_p(c_6), v_p(\Delta)) + k(4, 6, 12) \tag{9}$$

for $k \in \mathbb{Z}$, where c_4, c_6 and Δ are the usual quantities associated to a Weierstrass equation (see [Silverman 1992, Chapter III]). For the curves in question we have

$$c_4 = 0, \quad c_6 = -2^5 \cdot 3^3 \cdot \alpha, \quad \text{and} \quad \Delta = -2^4 \cdot 3^3 \cdot \alpha^2,$$

whence

$$(v_p(c_4), v_p(c_6), v_p(\Delta)) = (\infty, v_p(\alpha), 2v_p(\alpha)) + \begin{cases} (0, 5, 4) & \text{if } p = 2, \\ (0, 3, 3) & \text{if } p = 3, \end{cases}$$

Now it is a simple matter of using the tables in [Rizzo 2003, §1.1] to compute local root numbers. We illustrate the computation of $W_2(\alpha)$ in one example. Suppose that $v_2(\alpha) \equiv 4 \bmod 6$. Then $(a, b, c) = (\infty, 3, 0)$, and according to the entries under $(\geq 4, 3, 0)$ in Rizzo's Table III, we have $W_2(\alpha) = -1$ if and only if $c_6' := c_6/2^{v_2(c_6)} \equiv 3 \bmod 4$, i.e., if and only if $\alpha_2 \equiv 3 \bmod 4$. All other local root number computations are similar and we omit the details. □

Remark 4.2. We take the opportunity to note that the entry $(\geq 5, 6, 9)$ in Table II of [Rizzo 2003] has a typo. The "special condition" should read $c_6' \not\equiv \pm 4 \bmod 9$.

The elliptic curve E_α has potential good reduction at every nonarchimedean place. We will use the following proposition, due to Rohrlich, which gives a formula for the local root numbers of an elliptic curve at primes $p \geq 5$ of potential good reduction.

Proposition 4.3 [Rohrlich 1993, Proposition 2]. *Let $p \geq 5$ be a rational prime, and let $E/\mathbb{Q}_p$ be an elliptic curve with potential good reduction. Write $\Delta \in \mathbb{Q}_p^*$ for the discriminant of any generalized Weierstrass equation for E over $\mathbb{Q}_p$. Let*

$$e := \frac{12}{\gcd(v_p(\Delta), 12)}.$$

Then

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

Proposition 4.4 (Root numbers for $y^2 = x^3 + \alpha$). *Let α be a nonzero integer, and let*

$$R(\alpha) = W_2(\alpha)\left(\frac{-1}{\alpha_2}\right)W_3(\alpha)(-1)^{v_3(\alpha)}. \tag{10}$$

Then

$$W(\alpha) = -R(\alpha)\prod_{\substack{p^2 \mid \alpha \\ p \geq 5}} \begin{cases} 1 & \textit{if } v_p(\alpha) \equiv 0, 1, 3, 5 \bmod 6, \\ \left(\frac{-3}{p}\right) & \textit{if } v_p(\alpha) \equiv 2, 4 \bmod 6. \end{cases} \tag{11}$$

Let β be another nonzero integer, and suppose that $\alpha \equiv \beta \bmod 2^{v_2(\alpha)+2} \cdot 3^{v_3(\alpha)+2}$. Then $R(\alpha) = R(\beta)$.

Proof. Since $\Delta(E_\alpha) = -2^4 3^3 \alpha^2$, applying Proposition 4.3 we obtain

$$W(\alpha) = -W_2(\alpha)W_3(\alpha)\prod_{\substack{p \mid \alpha \\ p \geq 5}} \begin{cases} 1 & \text{if } v_p(\alpha) \equiv 0 \bmod 6, \\ \left(\frac{-1}{p}\right) & \text{if } v_p(\alpha) \equiv 1, 3, 5 \bmod 6, \\ \left(\frac{-3}{p}\right) & \text{if } v_p(\alpha) \equiv 2, 4 \bmod 6. \end{cases} \tag{12}$$

Let r be the product of the primes $p \geq 5$ such that $v_p(\alpha) = 1$, let $b = \alpha/r$ and set

$$\alpha_2 := \frac{\alpha}{2^{v_2(\alpha)}}, \quad b_2 := \frac{b}{2^{v_2(b)}}.$$

Note that $r = \alpha_2/b_2 = \alpha/b$. We may rewrite (12) as

$$W(\alpha) = -W_2(\alpha)W_3(\alpha)\left(\frac{-1}{r}\right)\prod_{\substack{p \mid b \\ p \geq 5}} \begin{cases} 1 & \text{if } v_p(\alpha) \equiv 0 \bmod 6, \\ \left(\frac{-1}{p}\right) & \text{if } v_p(\alpha) \equiv 1, 3, 5 \bmod 6, \\ \left(\frac{-3}{p}\right) & \text{if } v_p(\alpha) \equiv 2, 4 \bmod 6. \end{cases} \tag{13}$$

On the other hand, we have

$$\left(\frac{-1}{r}\right) = \left(\frac{-1}{\alpha_2/b_2}\right) = \left(\frac{-1}{\alpha_2}\right)\cdot\left(\frac{-1}{b_2}\right) = \left(\frac{-1}{\alpha_2}\right)\cdot\left(\frac{-1}{3}\right)^{v_3(\alpha)}\cdot\prod_{\substack{p \mid b \\ p \geq 5}}\left(\frac{-1}{p}\right)^{v_p(\alpha)},$$

so we can write (13) as

$$W(\alpha)=$$

$$-W_2(\alpha)\Big(\frac{-1}{\alpha_2}\Big)W_3(\alpha)(-1)^{v_3(\alpha)}\prod_{\substack{p\,|\,b\\ p\geq 5}}\begin{cases}\Big(\frac{-1}{p}\Big)^{v_p(\alpha)} & \text{if } v_p(\alpha)\equiv 0 \bmod 6,\\ \Big(\frac{-1}{p}\Big)^{1+v_p(\alpha)} & \text{if } v_p(\alpha)\equiv 1,3,5 \bmod 6,\\ \Big(\frac{-3}{p}\Big)\Big(\frac{-1}{p}\Big)^{v_p(\alpha)} & \text{if } v_p(\alpha)\equiv 2,4 \bmod 6.\end{cases}$$

This reduces to

$$W(\alpha)=-R(\alpha)\prod_{\substack{p^2\,|\,\alpha\\ p\geq 5}}\begin{cases}1 & \text{if } v_p(\alpha)\equiv 0,1,3,5 \bmod 6,\\ \Big(\frac{-3}{p}\Big) & \text{if } v_p(\alpha)\equiv 2,4 \bmod 6.\end{cases}$$

as desired, because, for $p\geq 5$, we have $p\,|\,b \iff p^2\,|\,\alpha$.

To prove the last claim of the proposition, note that if

$$\alpha\equiv\beta \bmod 2^{v_2(\alpha)+2}\cdot 3^{v_3(\alpha)+2}$$

then $v_2(\alpha)=v_2(\beta)$ and $v_3(\alpha)=v_3(\beta)$; thus we have

$$\frac{\alpha}{2^{v_2(\alpha)}}\equiv\frac{\beta}{2^{v_2(\beta)}} \bmod 4 \quad\text{and}\quad \frac{\alpha}{3^{v_3(\alpha)}}\equiv\frac{\beta}{3^{v_3(\beta)}} \bmod 9.$$

The claim now follows from Lemma 4.1 □

The following corollary describes conditions on two nonzero integers α and β which guarantee that the elliptic curves $y^2=x^3+\alpha$ and $y^2=x^3+\beta$ have *opposite* root numbers. This is one of the key inputs to the proof of Theorem 2.1. This corollary is similar in spirit to [Manduchi 1995, Corollary 2.1].

Corollary 4.5 (Flipping I). *Let α, β be nonzero integers such that*

(1) $\alpha\equiv\beta \bmod 2^{v_2(\alpha)+2}\cdot 3^{v_3(\alpha)+2}$,

(2) $\alpha=c\ell$, *where ℓ is squarefree and* $\gcd(c,\ell)=1$,

(3) $\beta=cq^{2+6k}\eta$, *where η is square free*, $\gcd(c,\eta)=\gcd(q,c\eta)=1$, $k\geq 0$, $q\geq 5$ *is prime and $q\equiv 2 \bmod 3$.*

Then $W(\alpha)=-W(\beta)$.

Proof. The first condition ensures that $R(\alpha)=R(\beta)$. Since ℓ is squarefree and $\gcd(c,\ell)=1$, the only primes greater than 3 contributing to $W(\alpha)$ are those whose square divides c. Similarly, since η is squarefree and $\gcd(c,\eta)=\gcd(q,\eta)=1$, the only primes greater than 3 contributing to $W(\beta)$ are those whose square divides c, and q. Since $\gcd(q, c) = 1$, $q \geq 5$ and $q \equiv 2 \bmod 3$, we have

$$W(\beta) = \left(\frac{-3}{q}\right) W(\alpha) = -W(\alpha) \qquad \square$$

Remark 4.6. To prove Zariski density of rational points on the elliptic surface $\mathscr{E} \to \mathbb{P}^1_{\mathbb{Q}}$ associated to a del Pezzo of degree 1 as in Theorem 2.1, it is enough to do the following. First, prove that there exist infinite sets $\mathscr{F}_1$ and $\mathscr{F}_2$ of coprime pairs of integers such that whenever $(m_1, n_1) \in \mathscr{F}_1$ and $(m_2, n_2) \in \mathscr{F}_2$ then

(1) $\alpha := F(m_1, n_1)$ and $\beta := F(m_2, n_2)$ are nonzero integers, and

(2) the integers α and β satisfy the hypotheses of Corollary 4.5.

Then, by Corollary 4.5, we know that either

$$W(F(m, n)) = -1 \text{ for all } (m, n) \in \mathscr{F}_1,$$

or

$$W(F(m, n)) = -1 \text{ for all } (m, n) \in \mathscr{F}_2.$$

Hence, there are infinitely many closed fibers of $\mathscr{E} \to \mathbb{P}^1_{\mathbb{Q}}$ with negative root number. Assuming the parity conjecture, this gives an infinite number of closed fibers with infinitely many points, and hence a Zariski dense set of rational points on $\mathscr{E}$.

4B. ***The root number of $E_\alpha : y^2 = x^3 + \alpha x$.*** Next, we give a closed formula for the root number of the elliptic curve $E_\alpha/\mathbb{Q} : y^2 = x^3 + \alpha x$, in terms of the nonzero integer α. The proofs mirror those of Section 4A, and thus we have omitted them. Throughout this section, we write $W(\alpha)$ for the root number of E_α and $W_p(\alpha)$ for the local root number at p of E_α.

Lemma 4.7. *Let α be a nonzero integer. Define α_2 and α_3 by $\alpha = 2^{v_2(\alpha)}\alpha_2 = 3^{v_3(\alpha)}\alpha_3$. Then*

$$W_2(\alpha) = \begin{cases} -1 & \textit{if } v_2(\alpha) \equiv 1 \textit{ or } 3 \bmod 4 \textit{ and } \alpha_2 \equiv 1 \textit{ or } 3 \bmod 8 \\ & \textit{or if } v_2(\alpha) \equiv 0 \bmod 4 \textit{ and } \alpha_2 \equiv 1, 5, 9, 11, 13 \textit{ or } 15 \bmod 16 \\ & \textit{or if } v_2(\alpha) \equiv 2 \bmod 4 \textit{ and } \alpha_2 \equiv 1, 3, 5, 7, 11 \textit{ or } 15 \bmod 16, \\ +1 & \textit{otherwise}; \end{cases}$$

$$W_3(\alpha) = \begin{cases} -1 & \textit{if } v_3(\alpha) \equiv 2 \bmod 4, \\ +1 & \textit{otherwise.} \end{cases}$$

Proof. Proceed as in the proof of Lemma 4.1, using the quantities

$$c_4 = -2^4 \cdot 3 \cdot \alpha, \quad c_6 = 0, \quad \text{and} \quad \Delta = -2^6 \cdot \alpha^3. \qquad \square$$

Proposition 4.8 (Root numbers for $y^2 = x^3 + \alpha x$). *Let α be a nonzero integer, and let*

$$R(\alpha) = W_2(\alpha)\Big(\frac{-1}{\alpha_2}\Big) W_3(\alpha)(-1)^{v_3(\alpha)}. \tag{14}$$

Then

$$W(\alpha) = -R(\alpha) \prod_{\substack{p^2 \mid \alpha \\ p \geq 5}} \begin{cases} \Big(\dfrac{-1}{p}\Big) & \text{if } v_p(\alpha) \equiv 2 \bmod 4, \\ \Big(\dfrac{2}{p}\Big) & \text{if } v_p(\alpha) \equiv 3 \bmod 4. \end{cases}$$

Let β be another nonzero free integer, and suppose that $\alpha \equiv \beta \bmod 2^{v_2(\alpha)+4} \cdot 3^{v_3(\alpha)}$. Then $R(\alpha) = R(\beta)$. □

The following corollary, which parallels Corollary 4.5, describes conditions on two nonzero integers α and β that guarantee that the elliptic curves $y^2 = x^3 + \alpha x$ and $y^2 = x^3 + \beta x$ have *opposite* root numbers. This is one of the key inputs to the proof of Theorem 2.3.

Corollary 4.9 (Flipping II). *Let α, β be nonzero integers such that*

(1) $\alpha \equiv \beta \bmod 2^{v_2(\alpha)+4} \cdot 3^{v_3(\alpha)}$,

(2) $\alpha = c\ell$, *where ℓ is squarefree and* $\gcd(c, \ell) = 1$,

(3) $\beta = cq^{2+4k}\eta$, *where η is square free*, $\gcd(c, \eta) = \gcd(q, c\eta) = 1$, $k \geq 0$, $q \geq 5$ *is prime and* $q \equiv 3 \bmod 4$; *or* $\beta = cp^{3+4k}\eta$, *where η is square free*, $\gcd(c, \eta) = \gcd(q, c\eta) = 1$, $k \geq 0$, $q \geq 5$ *is prime and* $q \equiv 3$ *or* $5 \bmod 8$.

Then $W(\alpha) = -W(\beta)$. □

Remark 4.10. To prove Zariski density of rational points on the elliptic surface $\mathscr{E} \to \mathbb{P}^1_{\mathbb{Q}}$ associated to a sextic hypersurface as in Theorem 2.3, it is enough to do the following. First, prove that there exist infinite sets $\mathscr{F}_1$ and $\mathscr{F}_2$ of coprime pairs of integers such that whenever $(m_1, n_1) \in \mathscr{F}_1$ and $(m_2, n_2) \in \mathscr{F}_2$ then

(1) $\alpha := G(m_1, n_1)$ and $\beta := G(m_2, n_2)$ are nonzero integers.

(2) The integers α and β satisfy the hypotheses of Corollary 4.9.

Then, arguing as in Remark 4.6 (using Corollary 4.9) we find infinitely many closed fibers of $\mathscr{E} \to \mathbb{P}^1_{\mathbb{Q}}$ with negative root number. This gives a Zariski dense set of rational point for $\mathscr{E}$, assuming the parity conjecture.

5. The modified square-free sieve

In this section we present a variation of a squarefree sieve by Gouvêa and Mazur [1991] and Greaves [1992]. It is the tool that allows us to identify families of fibers with negative root numbers on certain elliptic surfaces.

Let $F(m, n) \in \mathbb{Z}[m, n]$ be a binary homogeneous form of degree d, not divisible by the square of a nonunit in $\mathbb{Z}[m, n]$. Write $F = \prod_{i=1}^{t} f_i$, where the

$f_i(m,n) \in \mathbb{Z}[m,n]$ are irreducible, and assume that $\deg f_i \le 6$ for all i. Applying a unimodular transformation we may (and do) assume that the coefficients of m^d and n^d in $F(m,n)$ are nonzero. Call their respective coefficients a_d and a_0. Write $F(m,n) = a_d \prod(m - \theta_i n)$, where the θ_i are algebraic numbers and $1 \le i \le d$. Let

$$\Delta(F) = \left| a_0 a_d^{2d-1} \prod_{i \ne j} (\theta_i - \theta_j) \right|;$$

this is essentially the discriminant of the form F. It is nonzero if and only if F contains no square factors.

Fix a positive integer M, as well as a subset $\mathcal{S}$ of $(\mathbb{Z}/M\mathbb{Z})^2$. Our goal is to count pairs of integers (m,n) such that $(m \bmod M, n \bmod M) \in \mathcal{S}$ and $F(m,n)$ is not divisible by p^2 for any prime number p such that $p \nmid M$. This will allow us to give an asymptotic formula for the number of pairs of integers (m,n) with $0 \le m, n \le x$ such that

$$F(m,n) = \nu \cdot \ell,$$

where ν is a *fixed* integer and ℓ is a squarefree integer such that $\gcd(\nu, \ell) = 1$. The case $\nu = 1$ is handled in [Gouvêa and Mazur 1991] under the additional assumption that $\deg f_i \le 3$, and extended in [Greaves 1992] to the case $\deg f_i \le 6$. We build upon their work to prove an asymptotic formula when $\nu > 1$.

Remark 5.1. The role of the set $\mathcal{S}$ above is to "decouple" the congruence conditions on (m,n) from the sieving process. This artifact, suggested to us by Bjorn Poonen after an initial reading of the manuscript, cleans up the analytic proofs in the main-term estimate for our sieve.

We make use of the following (mild variation of an) arithmetic function studied by Gouvêa and Mazur: put $\rho(1) = 1$, and for $k \ge 2$ let

$$\rho(k) = \#\{(m,n) \in \mathbb{Z}^2 : 0 \le m, n \le k-1,\ F(m,n) \equiv 0 \bmod k\}.$$

By the Chinese remainder theorem, the function ρ is multiplicative; i.e., if k_1 and k_2 are relatively prime positive integers then $\rho(k_1k_2) = \rho(k_1)\rho(k_2)$.

Lemma 5.2 [Gouvêa and Mazur 1991, Lemma 3(2)]. *For fixed F as above and squarefree ℓ, we have $\rho(\ell^2) = O(\ell^2 \cdot d_k(\ell))$ as $\ell \to \infty$, where $k = \deg(F) + 1$ and $d_k(\ell)$ denotes the number of ways in which ℓ can be expressed as a product of k factors. In particular, $\rho(p^2) = O(p^2)$ as $p \to \infty$.* □

We can now state the main result of this section.

Theorem 5.3. *Let $F(m,n) \in \mathbb{Z}[m,n]$ be a homogeneous binary form of degree d. Assume that no square of a nonunit in $\mathbb{Z}[m,n]$ divides $F(m,n)$, and that no irreducible factor of F has degree greater than 6. Fix a positive integer M, as well as a subset $\mathcal{S}$ of $(\mathbb{Z}/M\mathbb{Z})^2$. Let $N(x)$ be the number of pairs of integers (m,n) with*

$0 \le m, n \le x$ such that $(m \bmod M, n \bmod M) \in \mathcal{S}$ and $F(m,n)$ is not divisible by p^2 for any prime p such that $p \nmid M$. Then

$$N(x) = Cx^2 + O\left(\frac{x^2}{(\log x)^{1/3}}\right) \quad \text{as } x \to \infty,$$

where

$$C = \frac{|\mathcal{S}|}{M^2} \prod_{p \nmid M} \left(1 - \frac{\rho(p^2)}{p^4}\right).$$

Remark 5.4. By Lemma 5.2, $\rho(p^2) = O(p^2)$ as $p \to \infty$ for a fixed F, so the infinite product defining C converges.

Heuristically, the condition that $F(m,n)$ be squarefree outside a prescribed integer is well approximated by the condition that $F(m,n)$ not be divisible by the square of a prime that is "small relative to x." More precisely, let $\xi = \frac{1}{3}\log x$ and define the principal term

$$N'(x) = \big\{(m,n) \in \mathbb{Z}^2 :\ 0 \le m, n \le x,\ F(m,n) \not\equiv 0 \bmod p^2 \text{ for all } p \le \xi,\ p \nmid M \\ \text{and } (m \bmod M, n \bmod M) \in \mathcal{S}\big\}.$$

Let $F = \prod_{i=1}^{t} f_i$ be a factorization of F into irreducible binary forms. Define the partial i-th error term $E_i(x)$ by

$$E_0(x) = \#\big\{(m,n) \in \mathbb{Z}^2 : 0 \le m, n \le x,\ p \mid m \text{ and } p \mid n \text{ for some } p > \xi\big\},$$
$$E_i(x) = \#\big\{(m,n) \in \mathbb{Z}^2 : 0 \le m, n \le x,\ p^2 \mid f_i(m,n) \text{ for some } p > \xi\big\}.$$

The proof of [Gouvêa and Mazur 1991, Proposition 2], essentially unchanged, shows that $E(x) := \sum_{i=0}^{t} E_i(x)$ gives an upper bound for the error term of our approximation, as follows.

Proposition 5.5. *If $\xi > \max\{\Delta(F), M\}$ then*

$$N'(x) - E(x) \le N(x) \le N'(x). \qquad \square$$

The proposition implies that

$$N(x) = N'(x) + O(E(x)),$$

which is why we think of ξ as giving us the notion of "small prime relative to x." The choice of $\frac{1}{3}\log x$ is somewhat flexible (see [Gouvêa and Mazur 1991, §4]); what is important is that when ℓ is a squarefree integer divisible only by primes *smaller* than ξ then

$$\ell \le \prod_{p<\xi} p = \exp\left(\sum_{p<\xi} \log p\right) \le e^{2\xi} = x^{2/3}, \tag{15}$$

where the last inequality follows from the estimate

$$\sum_{p<\xi} \log p \leq \sum_{p<\xi} \log \xi = \pi(\xi) \log \xi < 2\xi,$$

with $\pi(x) = \#\{p \text{ prime} : p < x\}$; see [Stopple 2003, p. 105].

Greaves [1992] showed that

$$E(x) = O\left(\frac{x^2}{(\log x)^{1/3}}\right) \quad \text{as } x \to \infty.$$

His proof requires the hypothesis that no irreducible factor of F have degree greater than 6, which explains the presence of this hypothesis in Theorem 5.3. Thus Theorem 5.3 follows from the next lemma.

Lemma 5.6. *With C as in Theorem 5.3, we have*

$$N'(x) = Cx^2 + O\left(\frac{x^2}{\log x}\right) \quad \text{as } x \to \infty.$$

Proof. Let ℓ be a squarefree integer divisible only by primes smaller than ξ, and such that $\gcd(\ell, M) = 1$. Let

$$N_\ell(M, \mathcal{S}; x)$$

be the number of pairs of integers (m, n) such that

$$0 \leq m, n \leq x, \quad (m \bmod M, n \bmod M) \in \mathcal{S}, \quad \text{and} \quad F(m, n) \equiv 0 \bmod \ell^2.$$

For a fixed congruence class modulo ℓ^2 of solutions of $F(m_0, n_0) \equiv 0 \bmod \ell^2$, satisfying $(m_0 \bmod M, n_0 \bmod M) \in \mathcal{S}$, we count the number of representatives in the box $0 \leq m, n \leq x$, and obtain

$$N_\ell(M, \mathcal{S}; x) = \frac{x^2 \cdot |\mathcal{S}|}{M^2} \cdot \frac{\rho(\ell^2)}{\ell^4} + O\left(x \cdot \frac{\rho(\ell^2)}{\ell^2}\right),$$

where the implied constant depends on F, M and $\mathcal{S}$, but not on ℓ or x. By the inclusion-exclusion principle we have

$$N'(x) = \sum_{\ell} \mu(\ell) N_\ell(M, \mathcal{S}; x),$$

where μ denotes the usual Möbius function and the sum runs over squarefree integers that are divisible only by primes smaller than ξ and that are relatively prime to M. Thus, by (15),

$$\begin{aligned} N'(x) &= \frac{x^2 \cdot |\mathcal{S}|}{M^2} \sum_{\ell} \mu(\ell) \frac{\rho(\ell^2)}{\ell^4} + O\biggl(x \sum_{\ell \le x^{2/3}} \frac{\rho(\ell^2)}{\ell^2}\biggr) \\ &= \frac{x^2 \cdot |\mathcal{S}|}{M^2} \prod_{p<\xi,\ p \nmid M} \biggl(1 - \frac{\rho(p^2)}{p^4}\biggr) + O\biggl(x \sum_{\ell \le x^{2/3}} \frac{\rho(\ell^2)}{\ell^2}\biggr). \end{aligned}$$

Assume that x is large enough so that $\xi > M$. Then, by Lemma 5.2, we have

$$\begin{aligned} \prod_{p \ge \xi} \biggl(1 - \frac{\rho(p^2)}{p^4}\biggr) = \prod_{p \ge \xi} \biggl(1 - O\biggl(\frac{1}{p^2}\biggr)\biggr) &= 1 - \sum_{p \ge \xi} O\biggl(\frac{1}{p^2}\biggr) \\ = 1 - O\biggl(\int_{t \ge \xi} \frac{1}{t^2}\,dt\biggr) &= 1 - O\biggl(\frac{1}{\xi}\biggr). \end{aligned}$$

Hence

$$N'(x) = \frac{x^2 \cdot |\mathcal{S}|}{M^2} \prod_{p \nmid M} \biggl(1 - \frac{\rho(p^2)}{p^4}\biggr) + O\biggl(\frac{x^2}{\xi}\biggr) + O\biggl(x \sum_{\ell \le x^{2/3}} \frac{\rho(\ell^2)}{\ell^2}\biggr).$$

By Lemma 5.2, we have

$$O\biggl(x \sum_{\ell \le x^{2/3}} \frac{\rho(\ell^2)}{\ell^2}\biggr) = O\biggl(x \sum_{\ell \le x^{2/3}} d_k(\ell)\biggr) = O(x \cdot x^{2/3} \log^{k-1} x),$$

with $k = \deg F + 1$, where we have used the well-known fact that

$$\sum_{n \le x} d_k(n) = O(x \log^{k-1} x);$$

see, for example, [Iwaniec and Kowalski 2004, (1.80)]. Since $\xi = \frac{1}{3} \log x$, it follows that

$$\begin{aligned} N'(x) &= \frac{x^2 \cdot |\mathcal{S}|}{M^2} \prod_{p \nmid M} \biggl(1 - \frac{\rho(p^2)}{p^4}\biggr) + O\biggl(\frac{x^2}{\xi}\biggr) + O(x \cdot x^{2/3} \log^{k-1} x) \\ &= \frac{x^2 \cdot |\mathcal{S}|}{M^2} \prod_{p \nmid M} \biggl(1 - \frac{\rho(p^2)}{p^4}\biggr) + O\biggl(\frac{x^2}{\log x}\biggr), \end{aligned}$$

which concludes the proof. □

5A. ***Making sure that C does not vanish.*** In this section we explore the possibility that the constant C for the principal term of $N(x)$ is zero. This will depend on the particular binary form $F(m, n)$, the integer M and the set $\mathcal{S}$. For any prime

$p \nmid M$, let

$$C_p = \left(1 - \frac{\rho(p^2)}{p^4}\right),$$

so that

$$C = \frac{|\mathcal{S}|}{M^2} \prod_{p \nmid M} C_p.$$

For $p \nmid M$ we know that $\rho(p^2) = O(p^2)$ (see Lemma 5.2); hence C vanishes if and only if either $\mathcal{S} = \varnothing$, or one of the factors C_p vanishes.

Lemma 5.7. *With notation as above, if $p \nmid M$ and $p \geq \deg F$, then $C_p \neq 0$.*

Proof. If $p \nmid M$ then $C_p = 0$ if and only if $\rho(p^2) = p^4$, which happens if and only if all pairs of integers (m, n) modulo $\mathbb{Z}/p^2\mathbb{Z}$ are solutions to $F(m, n) \equiv 0 \bmod p^2$. But then *all* pairs of integers (m, n) give solutions to the given congruence equation. This can happen only if $p < \deg(F)$; see the beginning of Section 2. □

5B. *An application of the modified sieve.*

Corollary 5.8 (Pseudosquarefree sieve). *Let $F(m, n) \in \mathbb{Z}[m, n]$ be a homogeneous binary form of degree d. Assume that no square of a nonunit in $\mathbb{Z}[m, n]$ divides $F(m, n)$, and that no irreducible factor of F has degree greater than 6. Fix*

- *a sequence $S = (p_1, \ldots, p_r)$ of distinct prime numbers and*
- *a sequence $T = (t_1, \ldots, t_r)$ of nonnegative integers.*

Let M be an integer divisible by $p_1^{t_1+1} \cdots p_r^{t_r+1}$ and by p^2 for all primes $p < \deg F$. Suppose that there exist integers a, b such that

$$F(a, b) \not\equiv 0 \bmod p^2 \quad \textit{whenever } p \mid M \textit{ and } p \neq p_i \textit{ for any } i, \tag{16}$$

and such that

$$v_{p_i}(F(a, b)) = t_i \quad \textit{for all } i. \tag{17}$$

Then there are infinitely many pairs of integers (m, n) such that

$$m \equiv a \bmod M, \quad n \equiv b \bmod M, \tag{18}$$

and

$$F(m, n) = p_1^{t_1} \cdots p_r^{t_r} \cdot \ell,$$

where ℓ is squarefree and $v_{p_i}(\ell) = 0$ for all i.

Proof. Let $\mathcal{S} = \{(a, b)\}$. By Theorem 5.3, there are infinitely many pairs of integers (m, n) such that

$$m \equiv a \bmod M, \qquad n \equiv b \bmod M, \qquad F(m, n) \not\equiv 0 \bmod p^2 \quad \text{whenever } p \nmid M.$$

(Note that $|\mathcal{S}| = 1$ and $C \neq 0$ by Lemma 5.7.) Condition (16) then guarantees that $F(m, n)$ is not divisible by the square of any prime outside the sequence S. We also have

$$m \equiv a \bmod p_i^{t_i+1}, \quad n \equiv b \bmod p_i^{t_i+1}, \quad \text{for all } i,$$

because $p_i^{t_i+1} \mid M$ for all i, and hence

$$F(m, n) = F(a, b) \bmod p_i^{t_i+1} \quad \text{for all } i.$$

Using condition (17), we conclude that

$$v_{p_i}(F(m, n)) = t_i. \qquad \square$$

6. Proof of Theorems 2.1 and 2.3

For a finite extension L/k of number fields, we let $S(L/k)$ denote the set of unramified prime ideals of k that have a degree 1 prime over k in L. Given two sets A and B, we write $A \doteq B$ if A and B differ by finitely many elements, and we write $A \sqsubseteq B$ if $x \in A \implies x \in B$ with finitely many exceptions.

Proposition 6.1 (Bauer; see [Neukirch 1999, p. 548]). *Let k be a number field, N/k a Galois extension of k and M/k an arbitrary finite extension of k. Then*

$$S(M/k) \sqsubseteq S(N/k) \iff M \supseteq N.$$

Lemma 6.2. *Let $f(t) \in \mathbb{Z}[t]$ be an irreducible nonconstant polynomial, and let $N = \mathbb{Q}[t]/f(t)$. Let μ_3 denote the group of third roots of unity, and suppose that $\mathbb{Q}(\mu_3) \not\subseteq N$. Then there are infinitely many rational primes p such that $p \equiv 2 \pmod 3$ and such that there exists a degree-1 prime $\mathfrak{p} \subseteq N$ lying over p.*

Proof. Since $\mathbb{F}_p^\times$ contains an element of order 3 if and only if $3 | (p-1)$, it follows that

$$S(\mathbb{Q}(\mu_3)/\mathbb{Q}) \doteq \{p \in \mathbb{Z} : p \text{ prime and } p \equiv 1 \bmod 3\}.$$

Suppose that the following implication holds (with possibly finitely many exceptions):

$$p \in \mathbb{Z} \text{ has a degree 1 prime in } N \implies p \equiv 1 \bmod 3.$$

Then

$$S(N/\mathbb{Q}) \sqsubseteq S(\mathbb{Q}(\mu_3)/\mathbb{Q}).$$

It follows from Proposition 6.1 that $\mathbb{Q}(\mu_3) \subseteq N$, a contradiction. $\square$

A similar argument proves the following entirely analogous lemma.

Lemma 6.3. *Let $g(t) \in \mathbb{Z}[t]$ be an irreducible nonconstant polynomial, and let $N = \mathbb{Q}[t]/g(t)$. Let μ_4 denote the group of fourth roots of unity, and suppose that $\mathbb{Q}(\mu_4) \not\subseteq N$. Then there are infinitely rational primes p such that $p \equiv 3 \pmod 4$ and such that there exists a degree-1 prime $\mathfrak{p} \subseteq N$ lying over p.* $\square$

Proof of Theorem 2.1. Since the surface in $\mathbb{P}_{\mathbb{Q}}(1, 1, 2, 3)$ given by an equation of the form (4) is smooth (by the definition of a del Pezzo surface), it follows that F_1 is a squarefree binary form of degree 6 (see Section 3). Blowing up the anticanonical point $[0:0:1:1]$ of X we obtain an elliptic surface $\rho\colon \mathscr{E} \to \mathbb{P}^1_{\mathbb{Q}}$ whose fiber above $[m:n] \in \mathbb{P}^1(\mathbb{Q})$ is isomorphic to a curve in $\mathbb{P}^2_{\mathbb{Q}}$ whose affine equation is given by

$$y^2 = x^3 + F(m, n). \tag{19}$$

This is an elliptic curve for almost all $[m:n]$.

Write $c = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, where the p_i are distinct primes. Let $S = (p_1, \dots, p_r)$, $T = (0, \dots, 0)$ and let

$$M = (2 \cdot 3 \cdot 5)^3 \cdot (p_1 \cdots p_r).$$

Since $F_1(m, n)$ has no fixed prime divisors, we know that for each prime $p \mid M$ with $p \neq p_i$ for all i there exist congruence classes a_p, b_p modulo p^2 such that

$$F_1(a_p, b_p) \not\equiv 0 \bmod p^2.$$

Similarly, for a prime p_i in the sequence S there exist congruence classes a_{p_i}, b_{p_i} modulo p_i such that

$$F_1(a_{p_i}, b_{p_i}) \not\equiv 0 \bmod p_i;$$

in other words, $v_{p_i}(F_1(a_{p_i}, b_{p_i})) = 0$. By the Chinese remainder theorem there exist congruence classes a, b modulo M such that

$$(a, b) \equiv \begin{cases} (a_p, b_p) \bmod p^2 & \text{for all primes } p \text{ such that } p \mid M,\ p \neq p_i \text{ for any } i, \\ (a_{p_i}, b_{p_i}) \bmod p_i & \text{for all primes } p_i \text{ in the sequence } S. \end{cases} \tag{20}$$

By Corollary 5.8, applied to F_1, S, T, M, a and b as above, there is an infinite set $\mathscr{F}_1$ of pairs $(m, n) \in \mathbb{Z}^2$ such that

$$F_1(m, n) = \ell,$$

where ℓ is a squarefree integer with $\gcd(c, \ell) = 1$, by our choice of S and T. Note that the elements m, n of each pair must be coprime since $F_1(m, n)$ is squarefree. Furthermore, the congruence class of ℓ modulo $2^3 \cdot 3^3$ is fixed (by our choice of M) and nonzero (because ℓ is squarefree). Thus, for $(m, n) \in \mathscr{F}_1$ we have

$$F(m, n) = c\ell \qquad \gcd(c, \ell) = 1,$$

and the congruence class of $c\ell/2^{v_2(c\ell)}3^{v_3(c\ell)}$ modulo $2^2 \cdot 3^2$ is fixed and nonzero.

By Lemma 6.2, applied to a number field $N := \mathbb{Q}[t]/f_i(t, 1)$ such that (5) holds, there is a rational prime $q \equiv 2 \bmod 3$ and a degree 1 prime $\mathfrak{q}$ in N lying over q. In fact, we may choose q so that $q > 5$, $\gcd(q, c) = 1$, and so that it does not divide the discriminant of $f_i(t, 1)$.

We apply Corollary 5.8 again to $F_1(m,n)$. This time we let $S=(p_1,\dots,p_r,q)$ and $T=(0,\dots,0,2+6k)$, where k is a large positive integer[1]. Let

$$M=(2\cdot 3\cdot 5)^3\cdot(p_1\cdots p_r)\cdot q^{3+6k}.$$

We claim that there exist integers m_q, n_q such that

$$v_q(F_1(m_q,n_q))=2+6k.$$

Indeed, since q has a prime $\mathfrak{q}$ of degree 1 in N and it does not divide the discriminant of $f_i(t,1)$, the equation

$$f_i(t,1)=0$$

has a simple root in $\mathbb{F}_q$. By Hensel's lemma, this solution lifts to a root in $\mathbb{Q}_q$. Hence $F_1(t,1)=0$ has a root in $\mathbb{Q}_q$. Approximating this solution by a rational number $r_q=m_q/n_q$ we can control $v_q(F_1(r_q,1))$ modulo 6; i.e., there exists a pair $(m_q,n_q)\in\mathbb{Z}^2$ of coprime integers such that $v_q(F_1(m_q,n_q))=2+6k$ for some (possibly very large) positive integer k. By the Chinese remainder theorem, there exists a pair of integers (a,b) simultaneously satisfying (20) and

$$a\equiv m_q \bmod q^{3+6k},\quad \text{and } b\equiv n_q \bmod q^{3+6k}. \tag{21}$$

By Corollary 5.8, applied to F_1, S, T, M, a and b as above, there is an infinite set $\mathcal{F}_2$ of pairs $(m,n)\in\mathbb{Z}^2$ such that

$$F_1(m,n)=q^{2+6k}\eta,$$

for some squarefree integer η with $\gcd(c,q\eta)=\gcd(q,\eta)=1$, by our choice of S and T. Suppose that $(m,n)\in\mathcal{F}_2$. Then

$$F(m,n)=cq^{2+6k}\eta\qquad \gcd(c,\eta)=\gcd(q,c\eta)=1.$$

Furthermore, we claim that $\gcd(m,n)=1$. To see this, note that since η is squarefree and F_1 is homogeneous of degree 6, then $\gcd(m,n)$ is some power of q; by (18), (21), and because $\gcd(m_q,n_q)=1$, this power of q must be 1. As before, the congruence class of $cq^{2+6k}\eta/2^{v_2(c\eta)}3^{v_3(c\eta)}$ mod $2^2\cdot 3^2$ is fixed, nonzero, and equal to that of $F_1(m,n)$ for $(m,n)\in\mathcal{F}_1$ (by our choice of a and b).

Whenever (19) is smooth, we write $W(F(m,n))$ for its root number. By Corollary 4.5, if $(m_1,n_1)\in\mathcal{F}_1$ and $(m_2,n_2)\in\mathcal{F}_2$ then

$$W(F(m_1,n_1))=-W(F(m_2,n_2)).$$

Zariski density of rational points on X now follows by arguing as in Remark 4.6.

□

[1] We will pick k large enough to ensure that $C\neq 0$ upon application of the pseudosquarefree sieve.

The proof of Theorem 2.3 is similar; we give enough details so that the interested reader can reconstruct it from the proof of Theorem 2.1.

Proof of Theorem 2.3. Blowing up the singular locus of X, as well as the base-point $[0:0:1:1]$ of $|-K_X|$, we obtain an elliptic surface $\rho\colon \mathscr{E} \to \mathbb{P}^1_{\mathbb{Q}}$ whose fiber above $[m:n] \in \mathbb{P}^1(\mathbb{Q})$ is isomorphic to a curve in $\mathbb{P}^2_{\mathbb{Q}}$ whose affine equation is given by

$$y^2 = x^3 + G(m,n)x, \tag{22}$$

which is an elliptic curve for almost all $[m:n]$.

We apply Corollary 5.8 twice, as in the proof of Theorem 2.1. First, we apply it to $G_1(m,n)$ by taking $S = (p_1, \dots, p_r)$, $T = (0, \dots, 0)$, where $c = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, and the p_i are distinct primes. We use

$$M = (2^2 \cdot 3)^3 \cdot (p_1 \cdots p_r).$$

This way we obtain an infinite set $\mathscr{F}_1$ of coprime pairs of integers (m,n) such that

$$G(m,n) = c\ell \quad \text{with} \quad \gcd(c,\ell) = 1,$$

and the congruence class of $c\ell/2^{v_2(c\ell)}3^{v_3(c\ell)}$ modulo $2^4 \cdot 3^2$ is fixed and nonzero.

By Lemma 6.3, applied to a number field $N := \mathbb{Q}[t]/g_i(t,1)$ such that (7) holds, there is a rational prime $q \equiv 3 \bmod 4$ and a degree 1 prime $\mathfrak{q}$ in N lying over q. In fact, we may choose q so that $q > 5$, $\gcd(q,c) = 1$, and so that it does not divide the discriminant of $g_i(t,1)$.

We apply Corollary 5.8 again to $G_1(m,n)$ with $S = (p_1, \dots, p_r, q)$ and $T = (0, \dots, 0, 2+4k)$, where k is a large positive integer, and

$$M = (2^2 \cdot 3)^3 \cdot (p_1 \cdots p_r) \cdot q^{3+4k}$$

Using Hensel's lemma as in the proof of Theorem 2.1, we obtain a different infinite set $\mathscr{F}_2$ of coprime pairs integers (m,n) such that

$$G(m,n) = cq^{2+4k}\eta \quad \text{with} \quad \gcd(c,\eta) = \gcd(q, c\eta) = 1,$$

where η is a squarefree integer. As before, the congruence class of

$$cq^{2+4k}\eta/2^{v_2(c\eta)}3^{v_3(c\eta)}$$

modulo $2^4 \cdot 3^2$ is fixed, nonzero, and equal to that of $G_1(m,n)$ for $(m,n) \in \mathscr{F}_1$ (by our choice of a and b).

Whenever (22) is smooth, we write $W(G(m,n))$ for its root number. By Corollary 4.9, if $(m_1,n_1) \in \mathscr{F}_1$ and $(m_2,n_2) \in \mathscr{F}_2$ then

$$W(G(m_1,n_1)) = -W(G(m_2,n_2)).$$

Zariski density of rational points on X now follows by arguing as in Remark 4.10. □

7. Diagonal del Pezzo surfaces of degree 1

We begin this section with two examples of del Pezzo surfaces of degree 1 that show how the sieving technique used in the proof of Theorems 2.1 and 2.3 can fail. In one case, however, we can show that rational points are Zariski dense, by exhibiting explicit nontorsion sections of the associated elliptic surfaces.

Example 7.1. Consider the del Pezzo surface of degree 1 given by

$$w^2 = z^3 + 27x^6 + 16y^6$$

in $\mathbb{P}_{\mathbb{Q}}(1, 1, 2, 3)$. Let $\rho\colon \mathscr{E} \to \mathbb{P}^1_{\mathbb{Q}}$ be its associated elliptic fibration. The elliptic curve $E_{m,n}$ above the point $[m : n] \in \mathbb{P}^1(\mathbb{Q})$ is given by

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

We claim that $W(E_{m,n}) = +1$ *for all* $[m : n] \in \mathbb{P}^1(\mathbb{Q})$. We may assume that $\gcd(m, n) = 1$. Let $\alpha = 27m^6 + 16n^6$, and suppose that $p \geq 5$ divides α (in particular, $p \nmid m$). Then

$$-3 \equiv (4n^3/3m^3)^2 \bmod p,$$

and thus $\left(\frac{-3}{p}\right) = 1$; hence the product over $p^2 \mid \alpha$ in (11) is equal to 1. In the notation of Proposition 4.4, it remains to see that $R(\alpha) = -1$. Since $\gcd(m, n) = 1$, we have $v_2(\alpha) = 4$ or 0, according to whether $2 \mid m$ or not. In either case, using Lemma 4.1, we see that

$$W_2(\alpha) \cdot \left(\frac{-1}{\alpha_2}\right) = 1 \quad \text{for all } \alpha.$$

Similarly, $v_3(\alpha) = 0$ or 3 according to whether $3 \nmid n$ or not. By Lemma 4.1 it also follows that

$$W_3(\alpha) \cdot (-1)^{v_3(\alpha)} = -1 \quad \text{for all } \alpha,$$

and hence $R(\alpha) = -1$, as desired.

The flipping technique of Corollary 4.5 thus cannot possibly work! Furthermore, assuming the parity conjecture, it follows that $E_{m,n}$ has even Mordell–Weil rank for all $[m : n] \in \mathbb{P}^1(\mathbb{Q})$. In fact, we claim that *all but finitely many* fibers have even rank ≥ 2. To see this note the family contains the points

$$(-3m^2, 4n^3) \quad \text{and} \quad \left(\frac{9m^4}{4n^2}, \frac{27m^6}{8n^3} + 4n^3\right).$$

We can check that these points are independent on the fiber above $[m : n] = [1 : 1]$, and thus they are independent as points on the generic fiber of $\mathscr{E}$. Then Silverman's specialization theorem [1994, Theorem 11.4] shows that the points are independent for all but finitely many pairs (m, n). Hence, rational points are Zariski dense on the original del Pezzo surface[2].

Example 7.2. Consider the del Pezzo surface of degree 1 given by

$$w^2 = z^3 + 6(27x^6 + y^6)$$

in $\mathbb{P}_{\mathbb{Q}}(1, 1, 2, 3)$. The elliptic curve $E_{m,n}$ above a point $[m : n] \subseteq \mathbb{P}^1(\mathbb{Q})$ of the associated elliptic surface $\mathscr{E} \to \mathbb{P}^1_{\mathbb{Q}}$ is given by

$$E_{m,n}: \quad y^2 = x^3 + 6(27m^6 + n^6).$$

As in Example 7.1 we can show that $W(E_{m,n}) = +1$ for all $[m : n] \in \mathbb{P}^1(\mathbb{Q})$. However, we cannot find readily available sections; Zariski density of rational points on this surface remains an open question.

The key point behind both of examples above is that condition (5) on the form $F_1(m, n)$ fails. The following lemma gives a necessary condition for the failure of (5) to occur, and suggests how to find the above examples.

Lemma 7.3. *Let* $F_1(m, n) = Am^6 + Bn^6 \in \mathbb{Z}[m, n]$, *and assume that* $\gcd(A, B) = 1$. *Write* $F_1 = \prod_i f_i$, *where the* $f_i \in \mathbb{Z}[m, n]$ *are irreducible homogeneous forms. Let* μ_3 *denote the group of third roots of unity. Then*

$$\mu_3 \subseteq \mathbb{Q}[t]/f_i(t, 1) \text{ for all } i \implies 3A/B \text{ is a rational square.} \tag{23}$$

Proof. The proof is an exercise in Galois theory. We will prove the case where F_1 is irreducible to illustrate the method. Choose a sixth root ξ of $-B/A$ and an isomorphism $\mathbb{Q}[t]/(At^6 + B) \xrightarrow{\sim} \mathbb{Q}(\xi)$. Suppose that $\mathbb{Q}(\mu_3) \subseteq \mathbb{Q}(\xi)$, so that $\mathbb{Q}(\xi)/\mathbb{Q}$ is a Galois extension of degree 6. Its unique quadratic subextension is $\mathbb{Q}(\mu_3) = \mathbb{Q}(\sqrt{-3})$, hence

$$\xi^3 = a + b\sqrt{-3} \quad \text{for some } a, b \in \mathbb{Q}.$$

Squaring both sides of the above equation and rearranging we obtain

$$-B/A - a^2 + 3b^2 = 2ab\sqrt{-3}$$

so that $ab = 0$. Since $\xi^3 \notin \mathbb{Q}$, it follows that $a = 0$ and $B/A = 3b^2$. □

If $3A/B$ is a rational square, it is often the case that not all fibers of the associated elliptic surface have positive root number: the 2-adic and 3-adic part of $Am^6 + Bn^6$ may vary enough to guarantee the existence of infinitely many fibers with root number -1. This idea, together with Theorem 2.1, are the necessary ingredients in the proof of Theorem 1.1.

[2] In fact, this surface is not minimal. The two nontorsion sections of $\mathscr{E} \to \mathbb{P}^1_{\mathbb{Q}}$ correspond to exceptional curves on X that are defined over $\mathbb{Q}$. Contracting these curves gives a del Pezzo surface of degree 3 with a rational point. This surface is unirational by the Segre–Manin Theorem.

Proof of Theorem 1.1. Let $F(x, y) = Ax^6 + By^6$ and put $c = \gcd(A, B)$. Write $F_1(x, y) = A_1x^6 + B_1y^6$, where $cA_1 = A$ and $cB_1 = B$. One easily checks that F_1 has no fixed prime factors. Write $F_1 = \prod_i f_i$, where the $f_i \in \mathbb{Z}[x, y]$ are irreducible homogeneous forms. If $3A/B$ is not a rational square then it follows from Lemma 7.3 that

$$\mu_3 \not\subseteq \mathbb{Q}[t]/f_i(t, 1) \quad \text{for some } i,$$

so by Theorem 2.1, $X(\mathbb{Q})$ is Zariski dense in X.

If, on the other hand, $3A/B$ is a rational square, then by assumption $c = 1$ and $9 \nmid AB$. After possibly interchanging A and B, we may write $A = 3a^2$ and $B = b^2$ for some relatively prime $a, b \in \mathbb{Z}$ not divisible by 3. A smooth fiber above $[m : n] \in \mathbb{P}^1(\mathbb{Q})$ of the elliptic surface $\mathscr{E} \to \mathbb{P}^1_{\mathbb{Q}}$ associated to X is the plane curve

$$E_\alpha : \quad y^2 = x^3 + \alpha,$$

where $\alpha = 3a^2m^6 + b^2n^6$. Arguing as in Example 7.1 we see that the product over $p^2 \mid \alpha$ in (11) is equal to 1.

To conclude the proof, it suffices to show that there are infinitely many pairs (m, n) of relatively prime integers such that $R(\alpha) = 1$ (see Proposition 4.4 for the definition of $R(\alpha)$). To construct such pairs (m, n), first suppose that $3 \mid n$ (whence $3 \nmid m$). Then $v_3(\alpha) = 1$ and $\alpha_3 \equiv 1 \bmod 3$, so by Lemma 4.1

$$W_3(\alpha) \cdot (-1)^{v_3(\alpha)} = (-1) \cdot (-1) = 1.$$

Next, we compute the product

$$w_2 := W_2(\alpha)\Big(\frac{-1}{\alpha_2}\Big).$$

We proceed by analyzing two cases, according to the 2-adic valuation of b, which we may assume is either 0, 1 or 2. We use Lemma 4.1 to compute the local root number at 2:

(1) $v_2(b) = 0$: choose n even. Then, regardless of the value of $v_2(a)$ (which we may also assume is 0, 1 or 2), we obtain $v_2(\alpha)$ even and $\alpha_2 \equiv 3 \bmod 4$, whence $w_2 = 1$.

(2) $v_2(b) = 1$ or 2: choose m odd, so that $v_2(\alpha) = 0$ and $\alpha_2 \equiv 3 \bmod 4$, whence $w_2 = 1$.

In any case, there are infinitely many pairs $(m, n) \in \mathbb{Z}^2$ with $R(3a^2m^6 + b^2n^6) = 1$, as desired. □

Remark 7.4. If $3A/B$ is a rational square, and either $\gcd(A, B) \neq 1$ or $9 \mid AB$, then it can happen that all the elliptic curves that are fibers of the rational surface associated to X have root number $+1$ (see Examples 7.1 and 7.2). Even when $9 \mid AB$ there are examples of surfaces, such as

$$w^2 = z^3 + 3^5x^6 + 2^4y^6,$$

where we were not able to find nontorsion sections.

8. Proof of Theorem 2.6

We carry out the details for the case of a surface X as in Theorem 2.1, the other case being similar. The fiber of ρ above $[m : n] \in \mathbb{P}^1(\mathbb{Q})$ is isomorphic to the plane curve

$$y^2 = x^3 + F(m, n) \tag{24}$$

which is an elliptic curve for almost all $[m : n]$. As in Theorem 2.1, we write c for the content of F and $F_1(m, n) := (1/c)F(m, n)$. By Lemma 6.2, applied to a number field $N := \mathbb{Q}[t]/f_i(t, 1)$ such that (5) holds, there is a rational prime $q \equiv 2 \bmod 3$ and a prime $\mathfrak{q}$ in N lying over q of degree 1 over $\mathbb{Q}$. We may assume that $q > 5$, $\gcd(c, q) = 1$, and that q does not divide the discriminant of $f_i(t, 1)$. Write $c = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, where the p_i are distinct primes. Let $P_0 = \{2, 3, 5, p_1, \cdots, p_r, q, \infty\}$.

Fix a finite set of distinct primes $P = \{q_1 \ldots, q_s\}$ such that $P \cap P_0 = \varnothing$, as well as a point $[m_p : n_p] \in \mathbb{P}^1(\mathbb{Q}_p)$ for each $p \in P$. We may assume that $m_p, n_p \in \mathbb{Z}_p$, and without loss of generality[3] we will further assume that $n_p \in \mathbb{Z}_p^\times$ for every $p \in P$. Let $\epsilon > 0$ be given and choose an integer N large so that

$$1/p^N < \epsilon \quad \text{and} \quad v_p(F_1(m_p, n_p)) < N \quad \text{for every } p \in P. \tag{25}$$

Let

$$\begin{aligned} S &= (p_1, \ldots, p_r, q_1, \ldots, q_s), \\ T &= \big(0, \ldots, 0, v_{q_1}(F_1(m_{q_1}, n_{q_1})), \ldots, v_{q_s}(F_1(m_{q_s}, n_{q_s}))\big), \end{aligned}$$

and let

$$M = (2 \cdot 3 \cdot 5)^3 \cdot (p_1 \cdots p_r) \cdot (q_1 \cdots q_s)^N.$$

Since $F_1(m, n)$ has no fixed prime factors, for any prime $p \mid M$ such that $p \neq p_i$ for all i and $p \notin P$, there exist congruence classes a_p, b_p modulo p^2 such that

$$F_1(a_p, b_p) \not\equiv 0 \bmod p^2.$$

Similarly, for a prime p_i with $1 \leq i \leq r$, there exist congruence classes a_{p_i}, b_{p_i} modulo p_i such that

$$F_1(a_{p_i}, b_{p_i}) \not\equiv 0 \bmod p_i.$$

[3] In fact, we may only really assume that either $m_p \in \mathbb{Z}_p^\times$ or $n_p \in \mathbb{Z}_p^\times$. We can interchange the roles of m_p and n_p in any one step of the proof without much difficulty, so the assumption that $n_p \in \mathbb{Z}_p^\times$ is an artifact to clean up the details of the proof.

By the Chinese remainder theorem there exist congruence classes a, b modulo M such that

$$(a,b) \equiv \begin{cases} (a_p, b_p) \bmod p^2 & \text{for primes } p \text{ such that } p \mid M,\ p \notin P, \text{ and} \\ & \qquad\qquad\qquad\qquad\quad p \neq p_i \text{ for all } i, \\ (a_{p_i}, b_{p_i}) \bmod p_i & \text{for primes } p_i \text{ with } 1 \leq i \leq r, \\ (m_p, n_p) \bmod p^N & \text{for primes } p \in P. \end{cases} \tag{26}$$

By construction,

$$F_1(a,b) \equiv F_1(m_p, n_p) \bmod p^N \quad \text{for all } p \in P.$$

It follows from (25) that

$$v_p(F_1(a,b)) = v_p(F_1(m_p, n_p)) \quad \text{for all } p \in P.$$

By Corollary 5.8, applied to F_1, S, T, M, a, b as above, there is an infinite set $\mathcal{F}_1$ of pairs $(m,n) \in \mathbb{Z}^2$ such that

$$F_1(m,n) = \ell,$$

where ℓ is a squarefree integer with $\gcd(c, \ell) = 1$, by our choice of S and T. Furthermore, the congruence class of ℓ modulo $2^3 \cdot 3^3$ is fixed (by our choice of M) and nonzero (because ℓ is squarefree). Thus, for $(m,n) \in \mathcal{F}_1$ we have

$$F(m,n) = c\ell \quad \gcd(c, \ell) = 1,$$

and the congruence class of $c\ell/2^{v_2(c\ell)}3^{v_3(c\ell)}$ modulo $2^2 \cdot 3^2$ is fixed and nonzero.

We apply Corollary 5.8 again to $F_1(m,n)$. This time we let

$$S = (p_1, \dots, p_r, q_1, \dots, q_s, q),$$
$$T = \big(0, \dots, 0, v_{q_1}(F_1(m_{q_1}, n_{q_1})), \dots, v_{q_s}(F_1(m_{q_s}, n_{q_s})), 2 + 6k\big),$$

where k is a large positive integer (large enough to ensure that $C \neq 0$ upon application of the sieve), and we let

$$M = (2 \cdot 3 \cdot 5)^3 \cdot (p_1 \cdots p_r) \cdot (q_1 \cdots q_s)^N \cdot q^{3+6k}.$$

Arguing as in the proof of Theorem 2.1, using Hensel's lemma and Lemma 6.2, we can show that there exist integers a_q, b_q such that

$$v_q(F_1(a_q, b_q)) = 2 + 6k$$

for some large positive integer k. By the Chinese remainder theorem, there exist congruence classes a, b modulo M such that (26) holds, and in addition

$$a \equiv a_q \bmod q^{3+6k} \quad \text{and} \quad b \equiv b_q \bmod q^{3+6k}.$$

By Corollary 5.8 there is an infinite set $\mathcal{F}_2$ of pairs $(m, n) \in \mathbb{Z}^2$ such that

$$F_1(m, n) = q^{2+6k}\eta, \tag{27}$$

where η is a squarefree integer such that $\gcd(c, \eta) = \gcd(q, c\eta) = 1$ (by the choice of S and T). In summary, for $(m, n) \in \mathcal{F}_2$, we have

$$F(m, n) = cq^{2+6k}\eta \quad \text{with} \quad \gcd(c, \eta) = \gcd(q, c\eta) = 1,$$

and the congruence class of $cq^{2+6k}\eta/2^{v_2(c\eta)} \bmod 2^2 \cdot 3^2$ is fixed, nonzero, and equal to that of $F_1(m, n)$ for $(m, n) \in \mathcal{F}_1$.

Whenever (24) is smooth, we write $W(F(m, n))$ for its root number. By Corollary 4.5, if $(m_1, n_1) \in \mathcal{F}_1$ and $(m_2, n_2) \in \mathcal{F}_2$, then

$$W(F(m_1, n_1)) = -W(F(m_2, n_2)).$$

Hence, there exists a pair $(m_0, n_0) \in \mathcal{F}_1 \cup \mathcal{F}_2$ such that $W(F(m_0, n_0)) = -1$. By the assumption that Tate–Shafarevich groups are finite we conclude that the fiber of ρ above $[m_0 : n_0]$ has positive Mordell–Weil rank, i.e., $[m_0 : n_0] \in \mathcal{R}$. By construction, $n_0 \neq 0$, and

$$m_0 \equiv m_p \bmod p^N, \quad \text{and} \quad n_0 \equiv n_p \bmod p^N \quad \text{for all } p \in P.$$

Hence

$$\left| \frac{m_p}{n_p} - \frac{m_0}{n_0} \right|_p = |m_p n_0 - m_0 n_p|_p \leq \frac{1}{p^N} < \epsilon \quad \text{for all } p \in P,$$

and $[m_0 : n_0]$ is arbitrarily close to $[m_p : n_p]$ for all $p \in P$. This concludes the proof of the theorem. □

Acknowledgements

I thank my thesis advisor, Bjorn Poonen, for numerous helpful conversations and for suggestions following a careful reading of the manuscript. I thank David Zywina for useful conversations on sieves. I thank Brendan Hassett and Cecilia Salgado for helpful conversations on elliptic surfaces. I thank Jean-Louis Colliot-Thélène for suggesting that I use the methods in this paper to prove Theorem 2.6. Finally, I thank the anonymous referee for several useful suggestions.

References

[Colliot-Thélène et al. 1987] J.-L. Colliot-Thélène, J.-J. Sansuc, and P. Swinnerton-Dyer, "Intersections of two quadrics and Châtelet surfaces, II", *J. Reine Angew. Math.* **374** (1987), 72–168. MR 88m:11045b Zbl 0622.14030

[Colliot-Thélène et al. 1998a] J.-L. Colliot-Thélène, A. N. Skorobogatov, and P. Swinnerton-Dyer, "Hasse principle for pencils of curves of genus one whose Jacobians have rational 2-division points", *Invent. Math.* **134**:3 (1998), 579–650. MR 99k:11095 Zbl 0924.14011

[Colliot-Thélène et al. 1998b] J.-L. Colliot-Thélène, A. N. Skorobogatov, and P. Swinnerton-Dyer, "Rational points and zero-cycles on fibred varieties: Schinzel's hypothesis and Salberger's device", *J. Reine Angew. Math.* **495** (1998), 1–28. MR 99i:14027 Zbl 0883.11029

[Conrad et al. 2005] B. Conrad, K. Conrad, and H. Helfgott, "Root numbers and ranks in positive characteristic", *Adv. Math.* **198**:2 (2005), 684–731. MR 2006m:11080 Zbl 1113.11033

[Deligne 1973] P. Deligne, "Les constantes des équations fonctionnelles des fonctions L", pp. 501–597 in *Modular functions of one variable, II* (Antwerp, 1972), edited by P. Deligne and W. Kuyk, Lecture Notes in Math. **349**, Springer, Berlin, 1973. MR 50 #2128 Zbl 0271.14011

[Dokchitser and Dokchitser 2010] T. Dokchitser and V. Dokchitser, "On the Birch–Swinnerton-Dyer quotients modulo squares", *Ann. of Math.* (2) **172**:1 (2010), 567–596. MR 2011h:11069 Zbl 1223.11079

[Gouvêa and Mazur 1991] F. Gouvêa and B. Mazur, "The square-free sieve and the rank of elliptic curves", *J. Amer. Math. Soc.* **4**:1 (1991), 1–23. MR 92b:11039 Zbl 0725.11027

[Grant and Manduchi 1997] G. R. Grant and E. Manduchi, "Root numbers and algebraic points on elliptic surfaces with base $\mathbf{P}^1$", *Duke Math. J.* **89**:3 (1997), 413–422. MR 99a:14028 Zbl 0907.14012

[Grant and Manduchi 1998] G. R. Grant and E. Manduchi, "Root numbers and algebraic points on elliptic surfaces with elliptic base", *Duke Math. J.* **93**:3 (1998), 479–486. MR 99m:11071 Zbl 1029.11028

[Greaves 1992] G. Greaves, "Power-free values of binary forms", *Quart. J. Math. Oxford Ser.* (2) **43**:169 (1992), 45–65. MR 92m:11098 Zbl 0768.11034

[Halberstadt 1998] E. Halberstadt, "Signes locaux des courbes elliptiques en 2 et 3", *C. R. Acad. Sci. Paris Sér. I Math.* **326**:9 (1998), 1047–1052. MR 99k:11082 Zbl 0933.11030

[Helfgott 2004] H. A. Helfgott, "On the behaviour of root numbers in families of elliptic curves", preprint, 2004. arXiv math/0408141

[Iskovskih 1979] V. A. Iskovskih, "Minimal models of rational surfaces over arbitrary fields", *Izv. Akad. Nauk SSSR Ser. Mat.* **43**:1 (1979), 19–43, 237. In Russian; translated in *Math. USSR Izv.* **14**:1 (1980), 17–39. MR 80m:14021

[Iwaniec and Kowalski 2004] H. Iwaniec and E. Kowalski, *Analytic number theory*, AMS Colloquium Publications **53**, American Mathematical Society, Providence, RI, 2004. MR 2005h:11005 Zbl 1059.11001

[Kollár 1996] J. Kollár, *Rational curves on algebraic varieties*, Ergebnisse der Math. **32**, Springer, Berlin, 1996. MR 98c:14001 Zbl 0877.14012

[Kresch and Tschinkel 2008] A. Kresch and Y. Tschinkel, "Two examples of Brauer–Manin obstruction to integral points", *Bull. Lond. Math. Soc.* **40**:6 (2008), 995–1001. MR 2009k:14039 Zbl 1161.14019

[Kuwata and Wang 1993] M. Kuwata and L. Wang, "Topology of rational points on isotrivial elliptic surfaces", *Internat. Math. Res. Notices* **1993**:4 (1993), 113–123. MR 94a:11079 Zbl 0804.14008

[Liverance 1995] E. Liverance, "A formula for the root number of a family of elliptic curves", *J. Number Theory* **51**:2 (1995), 288–305. MR 96e:11086 Zbl 0831.14012

[Manduchi 1995] E. Manduchi, "Root numbers of fibers of elliptic surfaces", *Compositio Math.* **99**:1 (1995), 33–58. MR 96j:11076 Zbl 0878.14028

[Manin and Hazewinkel 1974] Y. I. Manin and M. Hazewinkel, *Cubic forms: algebra, geometry, arithmetic*, North-Holland, Amsterdam, 1974. MR 57 #343 Zbl 0582.14010

[Mazur 1992] B. Mazur, "The topology of rational points", *Experiment. Math.* **1**:1 (1992), 35–45. MR 93j:14020 Zbl 0784.14012

[Munshi 2007] R. Munshi, "Density of positive rank fibers in elliptic fibrations", *J. Number Theory* **125**:1 (2007), 254–266. MR 2008d:11051 Zbl 1126.11031

[Munshi 2010] R. Munshi, "Density of positive rank fibers in elliptic fibrations, II", *Int. J. Number Theory* **6**:1 (2010), 15–23. MR 2011m:11118 Zbl 05687122

[Nekovář 2001] J. Nekovář, "On the parity of ranks of Selmer groups, II", *C. R. Acad. Sci. Paris Sér. I Math.* **332**:2 (2001), 99–104. MR 2002e:11060 Zbl 1090.11037

[Neukirch 1999] J. Neukirch, *Algebraic number theory*, Grundlehren der Math. Wiss. **322**, Springer, Berlin, 1999. MR 2000m:11104 Zbl 0956.11021

[Persson 1990] U. Persson, "Configurations of Kodaira fibers on rational elliptic surfaces", *Math. Z.* **205**:1 (1990), 1–47. MR 91f:14035 Zbl 0722.14021

[Rizzo 2003] O. G. Rizzo, "Average root numbers for a nonconstant family of elliptic curves", *Compositio Math.* **136**:1 (2003), 1–23. MR 2005b:11074 Zbl 1021.11020

[Rohrlich 1993] D. E. Rohrlich, "Variation of the root number in families of elliptic curves", *Compositio Math.* **87**:2 (1993), 119–151. MR 94d:11045 Zbl 0791.11026

[Rohrlich 1996] D. E. Rohrlich, "Galois theory, elliptic curves, and root numbers", *Compositio Math.* **100**:3 (1996), 311–349. MR 97m:11075 Zbl 0860.11033

[Serre 2008] J.-P. Serre, *Topics in Galois theory*, 2nd ed., Research Notes in Mathematics **1**, A K Peters, Wellesley, MA, 2008. MR 2008i:12010 Zbl 1128.12001

[Shioda 1990] T. Shioda, "On the Mordell–Weil lattices", *Comment. Math. Univ. St. Paul.* **39**:2 (1990), 211–240. MR 91m:14056 Zbl 0725.14017

[Silverman 1992] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1992. MR 95m:11054 Zbl 0585.14026

[Silverman 1994] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer, New York, 1994. MR 96b:11074 Zbl 0911.14015

[Stopple 2003] J. Stopple, *A primer of analytic number theory: from Pythagoras to Riemann*, Cambridge University Press, Cambridge, 2003. MR 2004m:11143 Zbl 1029.11001

[Swinnerton-Dyer 1962] H. P. F. Swinnerton-Dyer, "Two special cubic surfaces", *Mathematika* **9** (1962), 54–56. MR 25 #3413 Zbl 0103.38302

[Tate 1979] J. Tate, "Number theoretic background", pp. 3–26 in *Automorphic forms, representations and L-functions* (Corvallis, OR., 1977), vol. 2, edited by A. Borel and W. Casselman, Proc. Sympos. Pure Math. **33**, Amer. Math. Soc., Providence, 1979. MR 80m:12009 Zbl 0422.12007

[Ulas 2007] M. Ulas, "Rational points on certain elliptic surfaces", *Acta Arith.* **129**:2 (2007), 167–185. MR 2008h:11063 Zbl 1142.11017

[Ulas 2008] M. Ulas, "Rational points on certain del Pezzo surfaces of degree one", *Glasg. Math. J.* **50**:3 (2008), 557–564. MR 2009g:11034 Zbl 1223.14041

[Várilly-Alvarado 2008] A. Várilly-Alvarado, "Weak approximation on del Pezzo surfaces of degree 1", *Adv. Math.* **219**:6 (2008), 2123–2145. MR 2009j:14045 Zbl 1156.14017

Communicated by Hendrik W. Lenstra
Received 2010-09-22 Revised 2010-09-26 Accepted 2010-10-24

varilly@rice.edu
Department of Mathematics, Rice University, MS 136,
Houston, TX 77005, United States
http://math.rice.edu/~av15/

Algebra & Number Theory

www.jant.org

See inside back cover or www.jant.org for submission instructions.

The subscription price for 2011 is US $150/year for the electronic version, and $210/year (+$35 shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA.

Algebra & Number Theory (ISSN 1937-0652) at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY
mathematical sciences publishers
http://msp.org/

A NON-PROFIT CORPORATION

Typeset in LaTeX

Algebra & Number Theory

Volume 5 No. 5 2011

Mutation classes of $\tilde{A}_n$-quivers and derived equivalence classification of cluster tilted algebras of type $\tilde{A}_n$ 567
JANINE BASTIAN

Kazhdan–Lusztig polynomials and drift configurations 595
LI LI and ALEXANDER YONG

Renormalization and quantum field theory 627
RICHARD E. BORCHERDS

Density of rational points on isotrivial rational elliptic surfaces 659
ANTHONY VÁRILLY-ALVARADO

1937-0652(2011)5:5;1-C