ROOT NUMBERS AND RANKS IN POSITIVE CHARACTERISTIC

B. CONRAD, K. CONRAD, AND H. HELFGOTT

Abstract. For a global field K and an elliptic curve $\mathscr{E}_\eta$ over $K(T)$, Silverman's specialization theorem implies $\mathrm{rank}(\mathscr{E}_\eta(K(T))) \le \mathrm{rank}(\mathscr{E}_t(K))$ for all but finitely many $t \in \mathbf{P}^1(K)$. If this inequality is strict for all but finitely many t, the elliptic curve $\mathscr{E}_\eta$ is said to have *elevated rank*. All known examples of elevated rank for $K = \mathbf{Q}$ rest on the parity conjecture for elliptic curves over $\mathbf{Q}$, and the examples are all isotrivial.

Some additional standard conjectures over $\mathbf{Q}$ imply that there does not exist a non-isotrivial elliptic curve over $\mathbf{Q}(T)$ with elevated rank. In positive characteristic, an analogue of one of these additional conjectures is false. Inspired by this, for the rational function field $K = \kappa(u)$ over any finite field κ with characteristic $\neq 2$, we construct an explicit 2-parameter family $E_{c,d}$ of non-isotrivial elliptic curves over $K(T)$ (depending on arbitrary $c, d \in \kappa^\times$) such that, under the parity conjecture, each $E_{c,d}$ has elevated rank.

To Mike Artin on his 70th birthday

1. Introduction

Let K be a global field and let $\mathscr{E}_\eta$ be an elliptic curve over $K(T)$. This curve uniquely extends to a minimal regular proper elliptic fibration $\mathscr{E} \to \mathbf{P}^1_K$. The group $\mathscr{E}_\eta(K(T))$ is finitely generated, by the Lang–Néron theorem [17, Thm. 1]. (See [5, §6] for a proof of the Lang–Néron theorem using the language of schemes.) For all but finitely many $t \in \mathbf{P}^1(K)$, the specialization $\mathscr{E}_t$ of $\mathscr{E}$ at $T = t$ is an elliptic curve over K. This paper is concerned with a comparison between the ranks of $\mathscr{E}_\eta(K(T))$ and $\mathscr{E}_t(K)$ as t varies.

By Silverman's specialization theorem [30, Thm. C], the specialization map

$$\mathscr{E}_\eta(K(T)) = \mathscr{E}(\mathbf{P}^1_K) \to \mathscr{E}_t(K)$$

at $T = t$ is injective for all but finitely many $t \in \mathbf{P}^1(K)$. (To be precise, Silverman's theorem only applies to non-constant $\mathscr{E}_\eta$. Injectivity of the specialization map for constant $\mathscr{E}_\eta$ is elementary.) Thus, the *generic rank* $r(\mathscr{E}_\eta) := \mathrm{rank}(\mathscr{E}_\eta(K(T)))$ satisfies

$$r(\mathscr{E}_\eta) \le \mathrm{rank}(\mathscr{E}_t(K)) \tag{1.1}$$

for all but finitely many t. The elliptic curve $\mathscr{E}_\eta$ (or the fibration $\mathscr{E} \to \mathbf{P}^1_K$, or the family $\{\mathscr{E}_t\}_{t\in\mathbf{P}^1(K)}$) is said to have *elevated rank* if (1.1) is a strict inequality for all but finitely many $t \in \mathbf{P}^1(K)$.

How are examples of elevated rank constructed? The only known technique depends on the *parity conjecture*: for every elliptic curve E over the global field K,

$$(-1)^{\mathrm{rank}(E(K))} \stackrel{?}{=} W(E),$$

2000 *Mathematics Subject Classification.* 11G05,11G40.

Key words and phrases. elliptic curve, root number, function fields.

We thank N. Boston, I. Dolgachev, A.J. de Jong, B. Mazur, D. Pollack, B. Poonen, K. Rubin, E. Spiegel, R. Vakil, and A. Venkatesh for helpful conversations. B.C. thanks the NSF (DMS-0093542) and the Sloan Foundation for support, and H.H. thanks the CRM (Montreal) for support.

where $W(E)$ is the global root number of E. The spirit of the parity conjecture is that $W(E)$ is supposed to be the sign in the functional equation of the L-function of E, but such a functional equation is not yet known to exist in general. Therefore, we adopt the convention that the global root number is defined to be the product of local root numbers. The local root numbers are defined in all cases via representation theory [6] and are equal to 1 at non-archimedean places of good reduction. Some convenient formulas for local root numbers at non-archimedean places will be recalled in Theorem 3.1. The analytic and representation-theoretic descriptions of $W(E)$ are known to agree when K is $\mathbf{Q}$ or a global function field, by work of Deligne, Drinfeld, Wiles, and others. In particular, since our focus in this paper will be the cases when $K = \mathbf{Q}$ or when K is a rational function field over a finite field, the reader can think about $W(E)$ in either way.

To find elliptic curves with elevated rank, one tries to construct $\mathscr{E} \to \mathbf{P}^1_K$ such that $W(\mathscr{E}_t)$ has opposite sign to $(-1)^{r(\mathscr{E}_\eta)}$ with at most finitely many exceptions. That is, we want

$$W(\mathscr{E}_t) = -(-1)^{r(\mathscr{E}_\eta)} \tag{1.2}$$

for all but finitely many $t \in \mathbf{P}^1(K)$. Assuming the parity conjecture for elliptic curves over K, (1.1) and (1.2) imply that (1.1) is a strict inequality for all but finitely many t, so the $\mathscr{E}_t$'s have elevated rank.

Because of the role of the parity conjecture in this strategy, all known examples of elevated rank are, strictly speaking, conditional. Moreover, so far this idea has only been carried out when $K = \mathbf{Q}$. The first (conditional) examples of elevated rank were found by Cassels and Schinzel [1]. These are quadratic twists over $\mathbf{Q}(T)$ of the elliptic curve $y^2 = x^3 - x$:

$$\mathscr{E}_{n,\eta} : n(1 + T^4)y^2 = x^3 - x, \tag{1.3}$$

where n is a (squarefree) positive integer satisfying $n \equiv 7 \bmod 8$. Each $\mathscr{E}_{n,\eta}$ should have elevated rank, because the group $\mathscr{E}_{n,\eta}(\mathbf{Q}(T))$ has rank 0 and $W(\mathscr{E}_{n,t}) = -1$ for every $t \in \mathbf{Q}$. We exclude $t = \infty$ because $\mathscr{E}_{n,\infty}$ is not smooth. (Although $\mathscr{E}_{n,t}(\mathbf{Q})$ should have a point of infinite order for each $t \in \mathbf{Q}$, there cannot be an algebraic formula for a point of infinite order on $\mathscr{E}_{n,t}(\mathbf{Q})$ as t varies through an infinite subset of $\mathbf{Q}$, since such a formula would give an element of infinite order in the group $\mathscr{E}_{n,\eta}(\mathbf{Q}(T))$.) More generally, for any elliptic curve $E_{/\mathbf{Q}}$, Rohrlich [26, Prop. 9] proved that there is a quadratic twist $\mathscr{E}_\eta$ of $E_{/\mathbf{Q}(T)}$ by a quartic irreducible in $\mathbf{Q}[T]$ such that $\mathscr{E}_\eta(\mathbf{Q}(T))$ has rank 0 and $W(\mathscr{E}_t) = -1$ for every $t \in \mathbf{Q}$.

Nekovář has proved the parity conjecture for any elliptic curve over $\mathbf{Q}$ with finite Tate–Shafarevich group [21], [29, p. 463], but this does not make any examples of elevated rank over $\mathbf{Q}$ unconditional, since there are no non-constant families $\mathscr{E} \to \mathbf{P}^1_{\mathbf{Q}}$ such that $\mathscr{E}_t$ is known to have a finite Tate–Shafarevich group for all but finitely many $t \in \mathbf{P}^1(\mathbf{Q})$. Similarly, the recent work of Kato and Trihan [15] (as well as earlier work of Artin–Tate, Milne, Schneider, and others) on the Birch and Swinnerton-Dyer conjecture in characteristic p does not have any impact on the conditional nature of the parity conjecture in characteristic p as it is applied to the examples considered in this paper.

The examples of Cassels–Schinzel and Rohrlich over $\mathbf{Q}(T)$ are quadratic twists. The appeal of quadratic twists is that there are simple formulas that describe the variation of root numbers under quadratic twists over $\mathbf{Q}$ [28, Cor. to Prop. 10], [29, Thm. 7.2]. However, a family of quadratic twists exhibits no "geometric" variation: it is isotrivial (that is, $j(\mathscr{E}_\eta) \in K$, with no T-dependence), and conversely any isotrivial family is either a family of quadratic twists or is a family of quartic (resp. cubic or sextic) twists with $j(\mathscr{E}_\eta) = 1728$ (resp. $j(\mathscr{E}_\eta) = 0$).

The main question we address in this paper is the following: for a global field K, does there exist a *non-isotrivial* elliptic curve over $K(T)$ with elevated rank? In Appendix A, we explain why some standard conjectures over $\mathbf{Q}$ imply that the answer to this question for $K = \mathbf{Q}$ is *no*. There are natural analogues of these standard conjectures over a rational function field $\kappa(u)$ over a finite field κ, but (as we explain in Appendix B) one of these conjectures is false over $\kappa(u)$. This suggests that our question might have an affirmative answer in the function field case.

Here is our example. Let κ be a finite field with characteristic $p \neq 2$, and choose any $c, d \in \kappa^\times$. Let $F = \kappa(u)$ and consider the elliptic curve

$$\mathscr{E}_\eta : y^2 = x^3 + (c(T^2+u)^{2p} + du)x^2 - (c(T^2+u)^{2p} + du)^3 x \tag{1.4}$$

over $F(T)$. The Weierstrass model (1.4) over $F(T)$ has the form $y^2 = x^3 + Ax^2 - A^3x$. The j-invariant $j(\mathscr{E}_\eta) \in F(T)$ is not in F, so $\mathscr{E}_{\eta/F(T)}$ is non-isotrivial. An inspection of the poles of $j(\mathscr{E}_\eta)$ on $\mathbf{P}^1_F$ shows that changing (c, d) changes $j(\mathscr{E}_\eta)$.

Let $\mathscr{E} \to \mathbf{P}^1_F$ be the minimal regular proper elliptic fibration with generic fiber (1.4). For all $t \in \mathbf{P}^1(F)$, the specialization $\mathscr{E}_t$ of $\mathscr{E}$ at $T = t$ is an elliptic curve.

Theorem 1.1. *Let $F = \kappa(u)$, where $\mathrm{char}(\kappa) \neq 2$, and fix a choice of $c, d \in \kappa^\times$. Let $\mathscr{E}_{\eta/F(T)}$ be as in (1.4), depending on the choice of c and d. For every $t \in \mathbf{P}^1(F)$, we have $W(\mathscr{E}_t) = 1$. If $t \neq \infty$, then $\mathscr{E}_t(F)$ has positive rank. Moreover, $\mathrm{rank}(\mathscr{E}_\eta(F(T))) = 1$ and*

$$W(\mathscr{E}_t) = -(-1)^{\mathrm{rank}(\mathscr{E}_\eta(F(T)))}$$

for all $t \in \mathbf{P}^1(F)$.

Thus, if the parity conjecture is true for elliptic curves over F, the $\mathscr{E}_t$'s are a non-isotrivial family with elevated rank.

Remark 1.2. When $t = \infty$, the fiber $\mathscr{E}_t$ in Theorem 1.1 is the constant elliptic curve $y^2 = x^3 - c^3x$ over F. The elliptic curve $\mathscr{E}_\infty$ therefore has global root number 1, and it must have rank 0 (since F is a function field of genus 0 over the finite field κ).

We expect that $\mathscr{E}_t(F)$ has rank 2 except for a set of $t \in \mathbf{P}^1(F)$ with density 0 (as measured by height), but we have no idea how to prove this expectation.

Remark 1.3. We did not search for non-isotrivial examples of elevated rank with generic rank 0 or in characteristic 2, but we expect that such examples exist. (The curve defined by (1.4) in characteristic 2 is not smooth.) Our example has non-empty locus of nodal fibers in $\mathbf{P}^1_F$ that is nowhere F-étale. We expect any example of elevated rank to have this property.

Remark 1.4. For fixed $p \neq 2$, consider the algebraic family $\mathscr{E}_t$ where κ and (c, d) vary (in characteristic p) but the logarithmic height of $t \in \kappa(u)^\times$ (*i.e.*, the maximum of the degrees of its numerator and denominator) is bounded by some integer $B > 0$. This is a family parameterized by the κ-points (c, d, t) of a smooth $\mathbf{F}_p$-scheme that is determined by B.

For fixed $c, d \in \kappa^\times$, the assertions in Theorem 1.1 concerning the fibral root numbers and the generic rank for the associated elliptic curve in (1.4) are unaffected by replacing κ with a finite extension. (This is also crucial in the proof of Theorem 1.1; see (4.6) and the surrounding text.) Thus, granting the parity conjecture, Theorem 1.1 implies that there is a systematic "rank gap" ≥ 1 between generic and special Mordell–Weil ranks over the connected components of the family of planar Weierstrass models $\mathscr{E}_t$ as (c, d, t) and κ vary with $\mathrm{height}(t) \leq B$. This is a contrast with a theorem in [14, §9] asserting that there is an average "rank gap" $\leq 1/2$ (or exactly $1/2$ under conjectures of Tate) between generic and special Mordell–Weil ranks of Jacobians of certain *universal* families of pencils of smooth plane curves in characteristic p. (The pencils considered in [14, §9] are induced by smooth surfaces in $\mathbf{P}^1 \times \mathbf{P}^2$, but the closure of (1.4) in $\mathbf{P}^1_F \times_F \mathbf{P}^2_F$ is not F-smooth.)

Here is an overview of how we prove Theorem 1.1. To compute the rank of a Mordell–Weil group, we wish to use a 2-descent, and this is simplest when there is a rational point of order 2 and we are not in characteristic 2. Weierstrass models for such elliptic curves can always be brought to the form $y^2 = x^3 + Ax^2 + Bx$ with the 2-torsion point equal to $(0,0)$.

Step 1: For an odd prime p, consider the non-isotrivial elliptic curve over $\mathbf{F}_p(T)$ given by the Weierstrass model with $A = T$, $B = -T^3$:

$$E_T : y^2 = x^3 + Tx^2 - T^3x.$$

For every $t \in \kappa(u)$ with $t \neq 0, -1/4$, the specialization E_t may be considered as an elliptic curve over $\kappa(u)$. We will compute the reduction type of E_t at every place of $\kappa(u)$. When $\mathrm{char}(\kappa) = 3$, the 2-torsion point (0,0) will prevent the intervention of wild ramification.

Step 2: We show that $Q_T = (-T, T^2) \in E_T(\mathbf{F}_p(T))$ has infinite order, so Q_t has infinite order in $E_t(\kappa(u))$ for every $t \in \kappa(u)$ such that $t \notin \kappa$. This uses an extension to characteristic p of the classical Nagell–Lutz criterion in characteristic 0.

Step 3: Letting $h(T) = cT^{2p} + du$, where $c, d \in \kappa^\times$, we use algebraic properties of the defining Weierstrass model for E_T to find a simple formula (3.16) for $W(E_{h(t)})$ for *every* $t \in \kappa(u)$. (Note $h(t) \notin \kappa$ for each t.) The formula (3.16) for $W(E_{h(t)})$ implies that $W(E_{h(t^2+u)}) = 1$ for all $t \in \kappa(u)$; the elliptic curve $E_{h(T^2+u)}$ is (1.4). Our specific choice of $h(T)$ is partly motivated by the study of the characteristic-p Möbius function in [4].

Step 4: As just noted, $\mathscr{E}_\eta$ in (1.4) is $E_{h(T^2+u)}$. The point $Q_{h(T^2+u)}$ on this curve has infinite order, and we use this point to show that $\mathscr{E}_t(F)$ has positive rank for all $t \in \mathbf{P}^1(F) - \{\infty\}$. A mixture of geometric, arithmetic, and cohomological arguments is used to prove that the rank of $\mathscr{E}_\eta(F(T))$ is ≤ 1 (so the rank is exactly 1). The essential inputs are the Lang–Néron theorem over an algebraic closure $\overline{\kappa}$, the geometry of the locus of bad reduction for $\mathscr{E}_\eta$ over $\mathbf{P}^1 \times \mathbf{P}^1$, and some arithmetic considerations with the Chebotarev density theorem. Standard geometric upper bounds on the $F(T)$-rank give very large bounds when applied to $\mathscr{E}_\eta$. It therefore seems hopeless to calculate the rank of $\mathscr{E}_\eta(F(T))$ via purely geometric methods, even though the generic-rank conclusion in Theorem 1.1 holds over $\overline{\kappa}$.

Steps 1 and 2 are carried out in §2, Step 3 is carried out in §3, and Step 4 is carried out in §4–§6. The bulk of the work is in Step 4, which the geometrically-inclined reader may prefer to read directly after Step 1. We note that Steps 2 and 3 are logically independent, as are Steps 3 and 4. (Clearly Step 2 is used in Step 4.)

In Appendix A, we review previous work on variation of root numbers in families over $\mathbf{Q}$. The reason to expect the possibility of different behavior in positive characteristic is explained in Appendix B. These appendices are expository, but they should help the reader to have the proper perspective on our work.

Our notation is standard, with two exceptions: F denotes the rational function field $\kappa(u)$, where κ is a finite field that is assumed to have characteristic $\neq 2$ unless otherwise stated, and in some calculations in a field we shall use the shorthand $x \sim y$ to denote the relation $x = yz^2$ for a non-zero z (see Definition 3.2).

2. Reduction type and rank for $y^2 = x^3 + Tx^2 - T^3x$

We begin with two elementary lemmas concerning reduction types for an elliptic curve over the fraction field of a discrete valuation ring. We write $\mathcal{K}$ for the fraction field and v for the normalized (*i.e.*, $\mathbf{Z}$-valued) discrete valuation on $\mathcal{K}$, with valuation ring $\mathscr{O}_{\mathcal{K}}$ and residue field k. Both lemmas are standard when $\mathrm{char}(k) \neq 2, 3$, so a key point of the proofs is to include the case $\mathrm{char}(k) = 3$. For an elliptic curve E over $\mathcal{K}$, we let Δ, c_4, and c_6 denote the usual parameters associated to a Weierstrass model for E over $\mathcal{K}$. (As is well-known, $\Delta \bmod (\mathcal{K}^\times)^{12}$, $c_4 \bmod (\mathcal{K}^\times)^4$, and $c_6 \bmod (\mathcal{K}^\times)^6$ are independent of the choice of Weierstrass model.)

Lemma 2.1. *Let E be an elliptic curve over $\mathcal{K}$ with potentially good reduction. If there is good reduction then $v(\Delta) \equiv 0 \bmod 12$. The converse holds in either of the two following situations:*

(1) $\mathrm{char}(k) \neq 2, 3$*,*
(2) $\mathrm{char}(k) \neq 2$ *and* $E(\mathcal{K})[2] \neq O$*.*

Proof. The necessity of the congruence condition for good reduction is obvious. When $\mathrm{char}(k) \neq 2, 3$, all integral Weierstrass models can be put in the form $y^2 = x^3 + \alpha x + \beta$, so the sufficiency of the congruence condition for good reduction in case (1) is proved by direct calculation using the standard formulas for j and Δ (in terms of α and β) and using the coordinate changes $(x, y) \mapsto (\gamma^2 x, \gamma^3 y)$ with $\gamma \in \mathcal{K}^\times$.

For sufficiency in case (2), we may suppose $\mathscr{O}_{\mathcal{K}}$ is strictly henselian. Thus, k is separably closed with $\mathrm{char}(k) \neq 2$, so Δ must be a square in $\mathcal{K}^\times$ since $v(\Delta)$ is even. By the 2-torsion hypothesis, for any Weierstrass $\mathcal{K}$-model $y^2 = f(x)$ for E there is at least one $\mathcal{K}$-rational root of the cubic f. The discriminant of f is a square in $\mathcal{K}^\times$, so f splits over $\mathcal{K}$ and hence $E[2]$ is $\mathcal{K}$-split.

Let $\mathcal{K}_{\mathrm{sep}}/\mathcal{K}$ be a separable closure and let $\Gamma \subseteq \mathrm{GL}_2(\mathbf{Z}_2)$ be the image of the 2-adic representation

$$\rho_{E,2} : \mathrm{Gal}(\mathcal{K}_{\mathrm{sep}}/\mathcal{K}) \to \mathrm{Aut}(\varprojlim E[2^n](\mathcal{K}_{\mathrm{sep}})) \simeq \mathrm{GL}_2(\mathbf{Z}_2)$$

attached to E. Since $E[2]$ is $\mathcal{K}$-split, Γ has trivial reduction modulo 2. Thus, the Galois action must be pro-2, and hence tame. Since E has potentially good reduction and $\mathscr{O}_{\mathcal{K}}$ is strictly henselian, Γ must be a finite cyclic 2-group. Pick $\gamma \in \Gamma$, so $\gamma = 1 + 2x$ with $x \in \mathrm{M}_2(\mathbf{Z}_2)$. Since the 2-adic cyclotomic character over $\mathcal{K}$ is trivial,

$$1 = \det(\gamma) = 1 + 2\mathrm{Tr}(x) + 4\det(x) = -1 + \mathrm{Tr}(\gamma) + 4\det(x).$$

In particular, $\mathrm{Tr}(\gamma) \equiv 2 \bmod 4$. Elements in $\mathrm{GL}_2(\mathbf{Q}_2)$ with order 4 have characteristic polynomial $X^2 + 1$ and thus have trace 0. This shows that Γ cannot contain elements of order 4, so Γ is either trivial or has order 2. Hence, if $\mathcal{K}' \subseteq \mathcal{K}_{\mathrm{sep}}$ is the splitting field for $\rho_{E,2}$ then $[\mathcal{K}' : \mathcal{K}]$ divides 2.

The quadratic twist E' of E by $\mathcal{K}'/\mathcal{K}$ must have trivial 2-adic representation, and hence it has good reduction. Since $\mathscr{O}_{\mathcal{K}}$ is strictly henselian and $[\mathcal{K}' : \mathcal{K}]$ divides 2,

$$v(\Delta(E')) \equiv v(\Delta(E)) + 12/[\mathcal{K}' : \mathcal{K}] \equiv 12/[\mathcal{K}' : \mathcal{K}] \bmod 12$$

and $v(\Delta(E')) \equiv 0 \bmod 12$ (since E' has good reduction). Thus, $[\mathcal{K}' : \mathcal{K}] = 1$, so $E \simeq E'$ has good reduction. ■

Lemma 2.2. *Assume* $\mathrm{char}(k) \neq 2$ *and let E be an elliptic curve over $\mathcal{K}$ with potentially multiplicative reduction. The parameters c_4 and c_6 are non-zero, and there is multiplicative* *reduction if and only if* $v(c_4) \equiv 0 \bmod 4$. *When* $\mathscr{O}_{\mathcal{K}}$ *is complete, there is split multiplicative reduction if and only if* $-c_6$ *is a square in* $\mathcal{K}^\times$.

Proof. By hypothesis, j is non-integral. As is well-known, c_4 and c_6 are non-zero when $j \neq 0, 1728$. The formation of the Néron model commutes with base change to the completion, so we may suppose $\mathscr{O}_{\mathcal{K}}$ is complete. Since $2 \in \mathcal{K}^\times$, the quadratic extensions of $\mathcal{K}$ are classified by $\mathcal{K}^\times/(\mathcal{K}^\times)^2$, and since $2 \in \mathscr{O}_{\mathcal{K}}^\times$, the unramified quadratic extensions of $\mathcal{K}$ are classified by the unit classes (modulo unit squares). For $a \in \mathcal{K}^\times$, let $E^{(a)}$ denote the quadratic twist of E by the non-trivial character of $\mathrm{Gal}(\mathcal{K}(\sqrt{a})/\mathcal{K})$. Clearly

$$c_4(E^{(a)}) \equiv a^2 c_4(E) \bmod (\mathcal{K}^\times)^4, \ \ c_6(E^{(a)}) \equiv a^3 c_6(E) \bmod (\mathcal{K}^\times)^6.$$

By the theory of Tate models, there is a unique class $u = u(E)$ modulo $(\mathcal{K}^\times)^2$ such that $E^{(u)}$ has split multiplicative reduction. Moreover,

- E has multiplicative reduction if and only if u is a unit class in $\mathcal{K}^\times/(\mathcal{K}^\times)^2$,
- E has split multiplicative reduction if and only if u is trivial in $\mathcal{K}^\times/(\mathcal{K}^\times)^2$.

A direct calculation with Tate models shows $c_4(E^{(u)}) \in (\mathcal{K}^\times)^4$ and $-c_6(E^{(u)}) \in (\mathcal{K}^\times)^2$ (since $2 \in \mathscr{O}_{\mathcal{K}}^\times$). We conclude that

$$-c_6(E) \equiv u \bmod (\mathcal{K}^\times)^2,$$

so the reduction is split multiplicative if and only if $-c_6(E)$ is a square in $\mathcal{K}^\times$. Also, $u \in \mathcal{K}^\times/(\mathcal{K}^\times)^2$ is a unit class if and only if $v(u) \equiv 0 \bmod 2$, or equivalently $v(u^2) \equiv 0 \bmod 4$. Therefore, since

$$v(c_4(E)) \equiv v(c_4(E^{(u)})) - v(u^2) \equiv -v(u^2) \bmod 4,$$

the reduction is multiplicative if and only if $v(c_4(E)) \equiv 0 \bmod 4$. ■

Since we are interested in working with elliptic curves that are not in characteristic 2 and have a non-zero rational 2-torsion point, the shape of a Weierstrass model can be taken to be

$$E : y^2 = x^3 + Ax^2 + Bx. \tag{2.1}$$

The discriminant Δ and parameters c_4 and c_6 of such a model are given by the following formulas [31, p. 46]:

$$\Delta = 16B^2(A^2 - 4B), \quad c_4 = 16(A^2 - 3B), \quad c_6 = -32A(2A^2 - 9B). \tag{2.2}$$

For $P = (x, y) \in E - E[2]$, the point $[2]P$ has coordinates given by [31, pp. 58–59]:

$$[2]P = \left(\left(\frac{x^2 - B}{2y} \right)^2, -\frac{3x^2 + 2Ax + B}{2y} \left(\frac{x^2 - B}{2y} \right)^2 + \frac{x^3 - Bx}{2y} \right). \tag{2.3}$$

We set $A = T$ and $B = -T^3$ in (2.1), giving the elliptic curve

$$E_T : y^2 = x^3 + Tx^2 - T^3 x \tag{2.4}$$

over $\mathbf{F}_p(T)$ with $p \neq 2$. By (2.2), the discriminant and j-invariant of (2.4) are

$$\Delta = 16T^8(1 + 4T), \quad j = \frac{c_4^3}{\Delta} = \frac{256(1 + 3T)^3}{T^2(1 + 4T)}, \tag{2.5}$$

and the parameters c_4 and c_6 are

$$c_4 = 16T^2(1 + 3T), \quad c_6 = -32T^3(2 + 9T). \tag{2.6}$$

$v(t)$	Reduction Type
>0, even	multiplicative
>0, odd	(pot. mult.) additive
<0, $\equiv 0 \bmod 4$	good
<0, $\not\equiv 0 \bmod 4$	(pot. good) additive
$=0$, $v(1+4t)=0$	good
$=0$, $v(1+4t)>0$	multiplicative

TABLE 1. Reduction types for E_t, $t \in F - \kappa$

For each $t \in F = \kappa(u)$ with $t \notin \kappa$, the Weierstrass model

$$E_t : y^2 = x^3 + tx^2 - t^3x \tag{2.7}$$

defines an elliptic curve over F. (If $t \in \kappa - \{0, -1/4\}$ then E_t is also an elliptic curve over F, but assuming $t \notin \kappa$ will avoid some unnecessary complications.)

Theorem 2.3. *Fix $t \in F = \kappa(u)$ with $t \notin \kappa$. Let v be a place on F. The reduction type of E_t at v is as in Table 1.*

Proof. Specializing (2.5) and (2.6), the parameters of E_t are

$$\Delta = 16t^8(1+4t), \quad j = \frac{256(1+3t)^3}{t^2(1+4t)}, \quad c_4 = 16t^2(1+3t), \quad c_6 = -32t^3(2+9t). \tag{2.8}$$

(We write Δ instead of $\Delta|_{T=t}$, and likewise for the other parameters.) None of the parameters in (2.8) is 0, since $t \notin \kappa$.

If $v(t) > 0$ then

$$v(\Delta) = 8v(t), \quad v(c_4) = 2v(t), \quad v(j) = -2v(t) < 0,$$

so there is potentially multiplicative reduction. Using Lemma 2.2, there is multiplicative reduction when $v(t)$ is even and there is additive reduction when $v(t)$ is odd.

If $v(t) < 0$ and $\mathrm{char}(\kappa) > 3$ then

$$v(\Delta) = 9v(t), \quad v(c_4) = 3v(t), \quad v(j) = 0,$$

so there is potentially good reduction. If $v(t) < 0$ and $\mathrm{char}(\kappa) = 3$, then

$$v(\Delta) = 9v(t), \quad v(c_4) = 2v(t), \quad v(j) = -3v(t) > 0,$$

so again there is potentially good reduction. Using Lemma 2.1 in both cases, there is good reduction when $v(t) \equiv 0 \bmod 4$ and there is additive reduction otherwise.

Finally, suppose $v(t) = 0$, so

$$v(\Delta) = v(1+4t), \quad v(c_4) = v(1+3t).$$

Both $1+4t$ and $1+3t$ have non-negative valuation at v, and the valuations are not both positive. If $v(1+4t) = 0$ then $v(j) = 3v(c_4) \geq 0$, so there is good reduction (by Lemma 2.1). If $v(1+4t) > 0$ then $v(c_4) = 0$, so $v(j) = -v(\Delta) < 0$. This implies (by Lemma 2.2) that there is multiplicative reduction at v in such cases. ∎

Now we turn to the Mordell–Weil group of the generic fiber, $E_T(\mathbf{F}_p(T))$. As before, $p \neq 2$. Two obvious non-zero rational points are $(0,0)$ and $Q = (-T, T^2)$. (There is another obvious non-zero rational point, (T^2, T^3), but this is $(0,0) + Q$.) We will prove that Q has infinite order, so $\mathrm{rank}(E_T(\mathbf{F}_p(T))) \geq 1$.

For elliptic curves over $\mathbf{Q}$, explicit rational points are usually checked to be non-torsion by the Nagell–Lutz integrality criterion. This criterion is really a collection of local criteria over $\mathbf{Z}_{(p)}$ for all primes p. We need an analogue for discrete valuation rings with positive characteristic. Here is a version over arbitrary discrete valuation rings.

Theorem 2.4. *Let R be a discrete valuation ring with residue field k of characteristic $p \geq 0$, and let $\mathcal{K}$ be its fraction field. Let $E_{/\mathcal{K}}$ be an elliptic curve, and let $P \in E(\mathcal{K})$ be a non-zero torsion point.*

If there exists a Weierstrass model of E over R such that one of the affine coordinates of P does not lie in R then the scheme-theoretic closure of $\langle P \rangle \subseteq E(\mathcal{K})$ in the Néron model of E over R is a finite flat local R-group. In particular, $p > 0$ and P has p-power order. If in addition $\mathrm{char}(\mathcal{K}) = p$*, then $E_{/\mathcal{K}}$ has potentially supersingular reduction and $j(E) \in \mathcal{K}$ is a pth power.*

It follows from the Oort–Tate classification and Cartier duality that the only example of a non-trivial finite flat local group scheme over $\mathbf{Z}_{(p)}^{\mathrm{sh}}$ with p-power order and cyclic constant generic fiber is μ_2 for $p = 2$. Thus, Theorem 2.4 recovers the integrality of non-trivial torsion points on Weierstrass $\mathbf{Z}$-models of the form $y^2 = f(x)$ (for which non-zero 2-torsion points must have the form $(x_0, 0)$ with $x_0 \in \mathbf{Z}$).

Proof. Let $W \subseteq \mathbf{P}^2_R$ be the chosen Weierstrass R-model for E (so there is a chosen isomorphism $W_{\mathcal{K}} \simeq E$ as pointed curves over $\mathcal{K}$). Let $W^{\mathrm{sm}} \subseteq W$ be the open R-smooth locus of W, and let $\varepsilon \in W(R) = W(\mathcal{K}) = E(\mathcal{K})$ be the section $[0,1,0]$, so $\varepsilon \in W^{\mathrm{sm}}(R)$. Since P viewed as a point

$$\widetilde{P} \in W(\mathcal{K}) - \{[0,1,0]\} \subseteq \mathbf{A}^2(\mathcal{K}) = \mathcal{K} \times \mathcal{K}$$

is assumed to have at least one coordinate not in R, as a point of $\mathbf{P}^2(\mathcal{K}) = \mathbf{P}^2(R)$ its reduction in $\mathbf{P}^2(k)$ cannot lie in $\mathbf{A}^2_k$. Therefore, the reduction must lie on the line at infinity. However, by the theory of Weierstrass models we know that W_k has ε_k as its unique point on this line, so the reduction of $\widetilde{P}$ is ε_k. Since $\varepsilon_k \in W_k^{\mathrm{sm}}$, we conclude that $\widetilde{P} \in W^{\mathrm{sm}}(R)$.

Let $\mathscr{E}$ be the Néron model of E over R. By the Néron mapping property, there is a unique map $W^{\mathrm{sm}} \to \mathscr{E}$ over R extending the identification of $\mathcal{K}$-fibers with E. This map carries ε to the identity element in $\mathscr{E}(R)$, so the image of $\widetilde{P}$ in $\mathscr{E}(R)$ reduces to the identity in $\mathscr{E}_k$. In other words, under the equality $E(\mathcal{K}) = \mathscr{E}(R)$, the reduction of P in the closed fiber $\mathscr{E}_k$ of the Néron model must be the identity.

Let $N > 1$ be the order of P. By the Néron mapping property, P defines a map of R-groups $\mathbf{Z}/N\mathbf{Z} \to \mathscr{E}$ that is a closed immersion on the generic fiber. Since the R-group $\mathbf{Z}/N\mathbf{Z}$ is proper and the target $\mathscr{E}$ is separated over the Dedekind domain R, the scheme-theoretic image of this map is a finite flat R-subgroup $G \hookrightarrow \mathscr{E}$ with order N and constant generic fiber; this must be the closure of $\langle P \rangle$. The closed fiber of G must be infinitesimal since P has reduction equal to the identity. This forces G to be local, so the characteristic p of k must be positive and the order N of G must be a power of p.

Now assume $\mathrm{char}(\mathcal{K}) = p$. We must prove that $j(E)$ is a pth power in $\mathcal{K}$ and that E has potentially supersingular reduction. To prove that $j(E)$ is a pth power in $\mathcal{K}$ when $E(\mathcal{K})$ contains a non-trivial point with p-power order, we use the classical fact that if L is a field with characteristic $p > 0$ and E is an elliptic curve over L such that there exists an étale subgroup $\Gamma \subseteq E$ with order p^n for some $n \geq 1$ (that is, E is ordinary and the connected-étale sequence of $E[p^n]$ splits over L), then $j(E) \in L$ is a p^nth power in L. To prove this fact, let $E' = E/\Gamma$, so the isogeny $E' \to E$ that is dual to the projection $E \to E'$ has kernel that is Cartier-dual to Γ. This kernel is therefore multiplicative with p-power order, so it is infinitesimal. Since E' is a 1-dimensional abelian variety in characteristic p, it contains a unique infinitesimal subgroup of order p^n. The relative n-fold Frobenius $E' \to E'^{(p^n)}$ has this subgroup as its kernel, so the two quotients E and $E'^{(p^n)}$ of E' are L-isomorphic as quotients of E'. In particular $j(E) = j(E'^{(p^n)}) = j(E')^{p^n}$ in L.

Finally, returning to our initial situation, we must show that E has potentially supersingular reduction if $\mathcal{K}$ has characteristic $p > 0$. The assumptions on R and on the coordinates of P are unaffected by replacing $\mathcal{K}$ with a finite separable extension $\mathcal{K}'$ and replacing R with a maximal-adic localization of its integral closure in $\mathcal{K}'$, so we may assume that E has semistable reduction. It must be proved that the Néron model $\mathscr{E}$ in this case has fibral identity component $\mathscr{E}_k^0$ that is a supersingular elliptic curve. Assume to the contrary, so $\mathscr{E}_k^0$ is either a torus or an ordinary elliptic curve; we seek a contradiction. In either case, the finite local subgroups of $\mathscr{E}_k^0$ are multiplicative. Hence, if we construct G as we did above (the scheme-theoretic closure of $\langle P \rangle$ in $\mathscr{E}$) then the infinitesimal closed fiber $G_k \hookrightarrow \mathscr{E}_k$ must lie in $\mathscr{E}_k^0$, so G_k is multiplicative with p-power order. Since the generic fiber $G_{\mathcal{K}}$ is constant, we conclude that the Cartier dual $G^\vee$ has multiplicative generic fiber. However, $G^\vee$ is finite and flat over R with special fiber $G_k^\vee$ that is étale, so $G^\vee$ is R-étale. This forces $G_{\mathcal{K}}^\vee$ to be both multiplicative and étale, but a non-zero étale $\mathcal{K}$-group with p-power order cannot be multiplicative when $\mathcal{K}$ has characteristic p, so we have reached a contradiction. ■

Corollary 2.5. *With notation as in Theorem* 2.4*, if* $\mathrm{char}(\mathcal{K}) = p > 0$ *and* $j(E) \in \mathcal{K}$ *is not a pth power, then non-zero torsion points in* $E(\mathcal{K})$ *have integral coordinates with respect to any Weierstrass R-model of E.*

As an application of Corollary 2.5, we have:

Corollary 2.6. *Assume* $p \neq 2$*. The* $\mathbf{F}_p(T)$*-rational point* $Q = (-T, T^2)$ *on the elliptic curve* E_T *in* (2.4) *has infinite order.*

In particular, for any field L of characteristic p and any $t \in L$ *that is transcendental over* $\mathbf{F}_p$*, the specialization* $Q_t \in E_t(L)$ *that is obtained by sending* $\mathbf{F}_p(T)$ *into L by* $T \mapsto t$ *is a point of infinite order.*

Proof. The second claim follows from the first since the field extension $\mathbf{F}_p(T) \to L$ defined by $T \mapsto t$ induces an injection of groups $E_T(\mathbf{F}_p(T)) \to E_t(L)$.

To see that Q has infinite order in $E_T(\mathbf{F}_p(T))$, first note the j-invariant of E_T, as given in (2.5), is not a pth power in $\mathbf{F}_p(T)$. Therefore, by Corollary 2.5, an $\mathbf{F}_p(T)$-rational point on E_T has infinite order provided that, using the Weierstrass model (2.4) for E_T, some non-zero multiple of the point has an x- or y-coordinate that is non-integral at a finite place on $\mathbf{F}_p(T)$. (The Weierstrass model (2.4) is integral away from ∞.)

Since $x(Q)$ and $y(Q)$ are integral away from ∞ and $y(Q) \neq 0$, we double Q. By (2.3),

$$[2](Q) = \left(\left(\frac{T+1}{2} \right)^2, \frac{(T+1)(T^2 - 4T - 1)}{8} \right).$$

Thus, $x([2]Q)$ and $y([2]Q)$ are integral away from ∞ and $y([2]Q) \neq 0$, so we double again and find

$$x([4](Q)) = \left(\frac{(T+1)^4 + 16T^3}{4(T+1)(T^2 - 4T - 1)} \right)^2.$$

This is non-integral at the place $T + 1$, so we are done. ■

Remark 2.7. By the Lang–Néron theorem, the group $E_T(\overline{\mathbf{F}}_p(T))$ is finitely generated. This group has rank at least 1, since we have exhibited an explicit element with infinite order. Theorem 1.1 implies that $E_T(L)$ has rank 1 for certain extensions L of $\overline{\mathbf{F}}_p(T)$ with transcendence degree 2 over $\mathbf{F}_p$, so *a posteriori* we conclude that $E_T(\overline{\mathbf{F}}_p(T))$ has rank 1. Presumably the proof of Theorem 1.1 can be modified to give a direct proof that $E_T(\overline{\mathbf{F}}_p(T))$ has rank 1, without requiring the use of such auxiliary fields L.

3. Root numbers

For E_T as in (2.4), we will compute the local root numbers $W_v(E_t)$ for $t \in \kappa(u)$ with $t \notin \kappa$. Let us first collect a general list of local root number formulas. This is well-known for residue characteristic $p \neq 2, 3$, but we include some cases with $p = 3$.

Theorem 3.1. *Let $\mathcal{K}$ be a local field, with finite residue field of characteristic $p \neq 2$ and normalized valuation $v : \mathcal{K}^\times \to \mathbf{Z}$. Let $\chi_{\mathcal{K}}$ be the quadratic character of the residue field of $\mathcal{K}$, and let E be an elliptic curve over $\mathcal{K}$.*

(1) *Assume E has potentially good reduction, and if $p = 3$ then assume $E(\mathcal{K})[2] \neq O$. Define $e = 12/\gcd(v(\Delta), 12)$. We have $e \in \{1, 2, 3, 4, 6\}$, with $3 \nmid e$ when $p = 3$, and the local root number $W_{\mathcal{K}}(E)$ can be computed by the following formulas:*

$$W_{\mathcal{K}}(E) = \begin{cases} 1 & \text{if } e = 1, \\ \chi_{\mathcal{K}}(-1) & \text{if } e = 2 \text{ or } 6, \\ \chi_{\mathcal{K}}(-3) & \text{if } e = 3, \\ \chi_{\mathcal{K}}(-2) & \text{if } e = 4. \end{cases}$$

(2) *Suppose E has potentially multiplicative reduction. If the reduction is additive then $W_{\mathcal{K}}(E) = \chi_{\mathcal{K}}(-1)$. If the reduction is multiplicative and $c_6 = c_6(E)$ is computed using any Weierstrass $\mathcal{K}$-model of E, then $W_{\mathcal{K}}(E) = -1$ when $-c_6$ is a square in $\mathcal{K}^\times$ and $W_{\mathcal{K}}(E) = 1$ when $-c_6$ is not a square in $\mathcal{K}^\times$.*

Proof. We first address the properties of e in the cases with potentially good reduction. By the method of proof of Lemma 2.1(2), if E has potentially good reduction then it acquires good reduction over a quadratic extension of a splitting field for $E[2]$. This splitting field is a tame Galois extension with degree dividing 6, so Lemma 2.1 implies that e must divide 12 and moreover that if $p = 3$ then $3 \nmid e$. The tameness and Lemma 2.1 ensure that e is the order of the image of inertia in the ℓ-adic representation for E (any $\ell \neq p$). The cyclicity of tame inertia therefore rules out the possibility $e = 12$, since there are infinitely many rational primes $\ell > 3$ for which the 12th cyclotomic polynomial Φ_{12} has no quadratic factors over $\mathbf{Q}_\ell$.

Before we treat the general case, let us consider the special case $\mathcal{K} = \mathbf{Q}_p$ with $p \neq 2$. In this case, the proposed formulas are proved by Rohrlich for $p > 3$ in [26, Prop. 2] when the reduction is potentially good and (using Lemma 2.2) in [26, Prop. 3] when the reduction is potentially multiplicative. (Also see [27, Prop. 3] for further discussion in the multiplicative case.) By Lemma 2.1(2) and Lemma 2.2, the proofs of [26, Prop. 2, 3] work in our cases when $p = 3$. (The additional 2-torsion hypothesis in potentially good reduction cases for $p = 3$ avoids wild ramification.)

Rohrlich's proofs in [26] and [27] are representation-theoretic and rest on papers of Deligne [6] and Tate [33] that are valid for local fields with any residual (or generic) characteristic. Thus, these proofs carry over to the general case (with residue characteristic

$v(t)$	$W_v(E_t)$
> 0, even	hard to use
> 0, odd	$\chi_v(-1)$
< 0, even	$\chi_v(-1)^{v(t)/2}$
< 0, odd	$\chi_v(-2)$
$= 0$, $v(1+4t) = 0$	1
$= 0$, $v(1+4t) > 0$	$-\chi_v(2)$

TABLE 2. Local root numbers on E_t, $t \in F - \kappa$

$\neq 2$, and with a non-trivial rational 2-torsion point in potentially good cases when $p = 3$). The "p" in most of the arguments in [26] and [27] should be replaced with the size of the residue field of $\mathcal{K}$, say q, and the Legendre symbol $(\frac{a}{p})$ should be replaced with the Kronecker symbol $(\frac{a}{q})$. (Note that when q is an odd prime prime power and $a \in \mathbf{Z}$ is prime to q, $(\frac{a}{q}) = \chi_{\mathcal{K}}(a)$.) A general discussion in the context of local and global fields of characteristic 0 may also be found in [28]. ■

Using Theorems 2.3 and 3.1, we now compute the local root numbers $W_v(E_t)$ for every $t \in F = \kappa(u)$ with $t \notin \kappa$. Let χ be the quadratic character of κ and let χ_v be the quadratic character of the residue field at v. For $a \in \kappa$, we have $\chi_v(a) = \chi(a)^{\deg v}$, where $\deg v$ is the degree of the residue field of v over κ. (Thus, $\chi_v = \chi$ when $\deg v = 1$.) Table 2 summarizes the results, and we will see why the first row is undesirable.

The second, third, fourth, and fifth rows are cases of additive or good reduction (by Table 1 in Theorem 2.3), and these are left to the reader to check via Theorem 3.1. (The third row is the union of two cases from Table 1 with $v(t) < 0$, namely $v(t) \equiv 0, 2 \bmod 4$. These two cases are checked separately.) It remains to compute $W_v(E_t)$ in two cases: (i) $v(t)$ is positive and even, and (ii) $v(1+4t) > 0$. Both are cases of multiplicative reduction, so Theorem 3.1 requires us to check if $-c_6(E_t)$ is a square in the multiplicative group $F_v^\times$ of the completion of F at v. Let us first introduce some convenient notation.

Definition 3.2. Let L be a field. For $x, y \in L$, write $x \sim y$ when $x = yz^2$ for some $z \in L^\times$.

When $v(t)$ is positive and even, in $F_v^\times$ we compute from (2.6) at $T = t$ that

$$\begin{aligned} -c_6 &= 32t^3(2+9t) \\ &\sim 2t(2+9t) \\ &\sim t \quad \text{since } v(t) > 0. \end{aligned}$$

Thus, by Theorem 3.1(2), $W_v(E_t) = -1$ if t is a square in $F_v^\times$ and $W_v(E_t) = 1$ otherwise.

The last case is $v(1+4t) > 0$. In $F_v^\times$,

$$\begin{aligned} -c_6 &= 32t^3(2+9t) \\ &\sim 2t(2+9t) \\ &\sim 2t^2 \quad \text{since } v(1+4t) > 0 \\ &\sim 2. \end{aligned}$$

Thus, by Theorem 3.1(2), the last entry in Table 2 is confirmed:

$$v(1+4t) > 0 \Longrightarrow W_v(E_t) = -\chi_v(2). \tag{3.1}$$

$v(t)$	$W_v(E_{t^2})$
> 0	-1
< 0	$\chi_v(-1)^{v(t)}$
$= 0,\ v(1+4t^2) = 0$	1
$= 0,\ v(1+4t^2) > 0$	$-\chi_v(2)$

TABLE 3. Local root numbers on E_{t^2}, $t \in F - \kappa$

The E_t's do not have easily manageable global root numbers. There are two main problems. First, the local root number in the first row of Table 2 depends on whether or not t is a square in $F_v^\times$, and that is not something we can easily control. Second, the last row in Table 2 introduces *systematic* minus signs. To appreciate the nature of these difficulties, and how we can avoid them by a change of variables that is peculiar to characteristic p, let us first try to eliminate the difficulties in the first row of Table 2 by forcing "t" to be a square: we study the elliptic curve E_{T^2}. Table 2 is easily translated into this context, and the results are collected in Table 3. The systematic minus signs in the first and last rows of Table 3 will cause serious problems.

Write $t = g_1/g_2$, where $g_1, g_2 \in \kappa[u]$ are non-zero and relatively prime. The product of the local root numbers $W_v(E_{t^2})$ over all v yields the global root number formula

$$\begin{aligned} W(E_{t^2}) &= W_\infty(E_{t^2}) \prod_{\substack{v\neq\infty \\ v(t)>0}} (-1) \cdot \prod_{\substack{v\neq\infty \\ v(t)<0}} \chi_v(-1)^{v(t)} \cdot \prod_{\substack{v\neq\infty \\ v(1+4t^2)>0}} (-\chi_v(2)) \\ &= W_\infty(E_{t^2}) \cdot (-1)^{\#\{\pi:\pi|g_1\}} \cdot \chi(-1)^{\sum_{\pi|g_2}(\deg\pi)\,\mathrm{ord}_\pi(g_2)} \cdot \prod_{\pi|(4g_1^2+g_2^2)} (-\chi(2)^{\deg\pi}) \\ &= W_\infty(E_{t^2}) \cdot (-1)^{\#\{\pi:\pi|g_1\}+\#\{\pi:\pi|(4g_1^2+g_2^2)\}} \cdot \chi(-1)^{\deg g_2} \cdot \chi(2)^{\sum_{\pi|(4g_1^2+g_2^2)}\deg\pi}, \end{aligned}$$

where π runs over monic irreducibles in $\kappa[u]$. This formula is unwieldy because we cannot control the parity of the number of irreducible factors of g_1 or $4g_1^2 + g_2^2$ as t varies. We also cannot control the parity of $\sum_{\pi|(4g_1^2+g_2^2)} \deg\pi$ because it is hard to determine when $4g_1^2 + g_2^2$ is separable, though this second problem could be eliminated if we only consider κ in which $\chi(2) = 1$. Studying E_{t^2} is not helping us to get constant global root numbers at most t (as is essentially necessary in any example of elevated rank).

Instead of merely simplifying the first row of Table 2 by replacing t with t^2 in E_t, we need to eliminate the intervention of the first row of Table 2. To accomplish this, we will introduce a change of variables in t such that the numerator is always squarefree, and thus in particular never has positive even valuation at places of F. We also need to acquire control over the product of minus signs contributed from the last row of Table 2, and this will be achieved by arguments that are peculiar to positive characteristic.

A "squarefree" change of variables is impossible in characteristic 0, but the pth power map provides a mechanism to find such a change of variables in characteristic p. The basic idea is that, for all $t \in F = \kappa(u)$, $t^p + u$ has a squarefree numerator and has a pole at ∞, and thus, for all places v of F, $v(t^p + u)$ is never both positive and even. With this noted, define

$$h(T) = cT^{2p} + du, \tag{3.2}$$

where $c, d \in \kappa^\times$. The use of the exponent $2p$ instead of p will create a counterexample to Chowla's two-variable conjecture over $\kappa[u]$ (see the appendices for a discussion of this conjecture and its relevance to the study of elevated rank); in concrete terms, this even exponent will force certain otherwise unknown non-zero quantities we meet later to be squares. The role of c and d in $h(T)$ is to provide us with the family of examples in Theorem 1.1 for each $p \neq 2$, rather than just one example for each $p \neq 2$. (The reader may take $c = d = 1$ throughout.)

For $h(T)$ as in (3.2), consider the elliptic curve $E_{h(T)}$ over $F(T)$, obtained by replacing T with $h(T)$ in (2.4). We can run through all of our previous work with $h(t)$ in place of t (rather than t^2 in place of t), and now t can be any element of F since $h(t) \notin \kappa$ for all $t \in F$. (Table 3 only lists root numbers in fibers over $t \in F - \kappa$.) We will compute $W(E_{h(t)})$ for all $t \in F$.

Write $t = g_1/g_2$, where $g_1, g_2 \in \kappa[u]$ are relatively prime with $g_2 \neq 0$, so

$$h(t) = \frac{cg_1^{2p} + dug_2^{2p}}{g_2^{2p}}. \tag{3.3}$$

Call the numerator and denominator, respectively, f_1 and f_2:

$$f_1 = cg_1^{2p} + dug_2^{2p}, \quad f_2 = g_2^{2p}. \tag{3.4}$$

Obviously $f_1, f_2 \neq 0$. Since $(g_1, g_2) = 1$, clearly $(f_1, f_2) = 1$. Moreover, since $f_1' = dg_2^{2p} = df_2$, f_1 is squarefree. Thus, for all finite places v of F, $v(h(t))$ is never both positive and even at v. Since

$$\mathrm{ord}_\infty(h(t)) = \mathrm{ord}_\infty(ct^{2p} + du) = \begin{cases} -1 & \text{if } \mathrm{ord}_\infty(t) \geq 0, \\ 2p\,\mathrm{ord}_\infty(t) & \text{if } \mathrm{ord}_\infty(t) < 0, \end{cases} \tag{3.5}$$

we see $h(t)$ has a pole at ∞ for every $t \in F$.

We begin computing local root numbers for $E_{h(t)}$ over F by starting with the place at ∞, where $\chi_\infty = \chi$. Using (3.5) and Table 2 (with $h(t)$ in place of t),

$$W_\infty(E_{h(t)}) = \begin{cases} \chi(-2), & \text{if } \mathrm{ord}_\infty(t) \geq 0, \\ \chi(-1)^{\mathrm{ord}_\infty(t)}, & \text{if } \mathrm{ord}_\infty(t) < 0. \end{cases} \tag{3.6}$$

Now let v be a finite place on F. Since $h(t)$ has a squarefree numerator, we get from Table 2 that

$$v \neq \infty,\ v(h(t)) > 0 \Longrightarrow v(h(t)) = 1 \Longrightarrow W_v(E_{h(t)}) = \chi_v(-1) = \chi(-1)^{\deg v}.$$

Since $h(t)$ has a perfect square g_2^{2p} as its denominator, Table 2 implies

$$v \neq \infty,\ v(h(t)) < 0 \Longrightarrow W_v(E_{h(t)}) = \chi_v(-1)^{v(h(t))/2} = \chi(-1)^{(\deg v)\cdot v(g_2)}.$$

If $v(h(t)) = 0$, then Table 2 (with $h(t)$ in place of t) tells us that if $v(1 + 4h(t)) = 0$ then $W_v(E_{h(t)}) = 1$, whereas

$$v(1 + 4h(t)) > 0 \Longrightarrow W_v(E_{h(t)}) = -\chi_v(2) = -\chi(2)^{\deg v}.$$

Combining all of this local information, for $t \in F$ the global root number $W(E_{h(t)})$ is

$$W_\infty(E_{h(t)}) \prod_{\substack{v\neq\infty \\ v(h(t))>0}} \chi(-1)^{\deg v} \prod_{\substack{v\neq\infty \\ v(h(t))<0}} \chi(-1)^{(\deg v)\cdot v(g_2)} \prod_{\substack{v\neq\infty \\ v(1+4h(t))>0}} (-\chi(2)^{\deg v}). \tag{3.7}$$

Referring back to Table 1 with $h(t)$ in place of t, the local root numbers for $E_{h(t)}$ at places of multiplicative reduction appear in (3.7) as the terms in the last product.

Writing (3.7) in terms of the numerator and denominator of $h(t)$,

$$\begin{aligned} W(E_{h(t)}) &= W_\infty(E_{h(t)}) \prod_{\pi|f_1} \chi(-1)^{\deg \pi} \prod_{\pi|f_2} \chi(-1)^{(\deg \pi)\operatorname{ord}_\pi(g_2)} \prod_{\pi|(4f_1+f_2)} (-\chi(2)^{\deg \pi}) \\ &= W_\infty(E_{h(t)}) \prod_{\pi|f_1} \chi(-1)^{\deg \pi} \prod_{\pi|g_2} \chi(-1)^{(\deg \pi)\operatorname{ord}_\pi(g_2)} \prod_{\pi|(4f_1+f_2)} (-\chi(2)^{\deg \pi}) \\ &= W_\infty(E_{h(t)}) \prod_{\pi|f_1} \chi(-1)^{\deg \pi} \cdot \chi(-1)^{\deg g_2} \cdot \prod_{\pi|(4f_1+f_2)} (-\chi(2)^{\deg \pi}). \end{aligned}$$

Set

$$f = 4f_1 + f_2 = 4cg_1^{2p} + (4du+1)g_2^{2p}. \tag{3.8}$$

Since $(f, f') = 1$, f is squarefree. We already saw that f_1 is squarefree as well, so our global root number formula simplifies to

$$W(E_{h(t)}) = W_\infty(E_{h(t)})\chi(-1)^{\deg f_1}\chi(-1)^{\deg g_2}\mu(f)\chi(2)^{\deg f}, \tag{3.9}$$

where μ is the Möbius function on $\kappa[u]$ (defined much like its classical counterpart over $\mathbf{Z}$).

Remark 3.3. Let us clarify how this calculation is analogous to what is seen in work over $\mathbf{Q}(T)$. Let the *Liouville function* λ on $\kappa[u]$ be the totally multiplicative function whose value on irreducible elements is -1, so if f is separable (*i.e.*, is squarefree) in $\kappa[u]$ then $\mu(f) = \lambda(f)$. In (3.9), we therefore have an appearance of $\lambda(f)$ as a contribution from local root numbers at places of multiplicative reduction. As is explained in Appendix A, the Liouville function on $\mathbf{Z}$ arises in a similar manner in the study of average root numbers for elliptic curves over $\mathbf{Q}(T)$ that have a point of multiplicative reduction on $\mathbf{P}^1_{\mathbf{Q}}$. Another similarity with the situation in characteristic 0 is that λ is being computed on an element $f \in \kappa[u]$ that is the value at (g_1, g_2) of a homogeneous 2-variable polynomial over $\kappa[u]$, where g_1 and g_2 are relatively prime. (Consider g_1 and g_2 in (3.8) as specializations of independent indeterminates over $\kappa[u]$.) Compare this with the appearance of $\lambda(f_{\mathscr{E}}(m,n))$ in the discussion at the end of Appendix A.

To simplify (3.9) further, we compute the degrees in the exponents. This depends on the relative sizes of $\deg g_1$ and $\deg g_2$. Let

$$n_1 = \deg g_1, \quad n_2 = \deg g_2,$$

with the standard convention $n_1 = -\infty$ when $g_1 = 0$, so

$$\deg f_1 = \begin{cases} 2pn_2 + 1 & \text{if } n_1 \le n_2, \\ 2pn_1 & \text{if } n_1 > n_2, \end{cases} \quad \deg f_2 = 2pn_2. \tag{3.10}$$

By inspection, $\deg f_1 > \deg f_2$, so

$$\deg f = \begin{cases} 2pn_2 + 1 & \text{if } n_1 \le n_2, \\ 2pn_1 & \text{if } n_1 > n_2. \end{cases} \tag{3.11}$$

Using (3.6), (3.9), (3.10), and (3.11),

$$W(E_{h(t)}) = \begin{cases} \chi(-2)\chi(-1)\chi(-1)^{n_2}\mu(f)\chi(2) & \text{if } n_1 \le n_2, \\ \chi(-1)^{n_2-n_1} \cdot 1 \cdot \chi(-1)^{n_2} \cdot \mu(f) \cdot 1 & \text{if } n_1 > n_2, \end{cases}$$

so

$$W(E_{h(t)}) = \begin{cases} \chi(-1)^{n_2}\mu(f) & \text{if } n_1 \le n_2, \\ \chi(-1)^{n_1}\mu(f) & \text{if } n_1 > n_2, \end{cases} \tag{3.12}$$

where $t = g_1/g_2 \in \kappa(u)$ is expressed in reduced form and f is defined in (3.8). (The two cases in (3.12) are classified by the sign of $\text{ord}_\infty(t) = n_2 - n_1$.)

To complete the calculation of $W(E_{h(t)})$ for $t \in F$, we need to compute $\mu(f)$. For this, we use a remarkable fact: the Möbius function in characteristic p is a more accessible object than its classical counterpart over $\mathbf{Z}$. Indeed, there is a formula for the Möbius function on $\kappa[u]$ *other* than its definition. In particular, the explicit calculation of

$$\mu(f) = \mu(4cg_1^{2p} + (4du + 1)g_2^{2p}), \tag{3.13}$$

where g_1 and g_2 appear through their pth powers, can be done without factoring. (Nothing of the sort can be said for classical variants such as $\mu_{\mathbf{Z}}(m^2 + 5n^2)$.)

The alternative Möbius formula (in Lemma 3.4 below) uses discriminants, so to avoid any possible confusion on signs and scalar factors, let us briefly recall how to define the discriminant of a polynomial. For any field K and any non-zero polynomial $P = P(u)$ in $K[u]$ with degree n, the *discriminant* of P is

$$\text{disc}_K\, P := (-1)^{n(n-1)/2} \cdot (\text{lead}\, P)^{n-2} \cdot \prod_{i=1}^{n} P'(\gamma_i) \in K, \tag{3.14}$$

where $\gamma_1, \ldots, \gamma_n$ are the roots of P (repeated with multiplicity) in a splitting field and $\text{lead}\, P \in K^\times$ is the leading coefficient of P. Obviously $\text{disc}_K(cP) = c^{2n-2} \cdot \text{disc}_K(P)$ for $c \in K^\times$. (In [4], which motivated the work in this section, a different definition of the discriminant is used that is invariant under $K^\times$-scaling of P. That definition differs from (3.14) by an even power of $\text{lead}\, P$. Discriminants will only matter up to a non-zero square scaling factor for our purposes, because of the quadratic character in (3.15) below, so the different discriminants used in [4] and here are not incompatible for the intended applications.)

Lemma 3.4. *Let κ be a finite field with odd characteristic, and let χ be the quadratic character on κ, with $\chi(0) = 0$. For any non-zero polynomial $P \in \kappa[u]$,*

$$\mu(P) = (-1)^{\deg P}\chi(\text{disc}_\kappa\, P), \tag{3.15}$$

where $\text{disc}_\kappa\, P$ is the discriminant of the polynomial P.

Proof. This formula is trivial when P has a multiple factor: both sides are 0. When P is separable (that is, squarefree) and has r prime factors, (3.15) is the same as: $\chi(\text{disc}_\kappa\, P) = (-1)^{\deg P - r}$. Written this way, (3.15) appears in [32, Cor. 1]. The properties of finite fields that are most essential in the proof of [32, Cor. 1] are perfectness and pro-cyclicity of their Galois theory. (The only reason to assume $\text{char}(\kappa) \neq 2$ is that the Möbius formula can then be given in terms of the quadratic character; a formula when $\text{char}(\kappa) = 2$ can be found in [4] and [32], but it uses a lift to characteristic 0. We omit this formula since we do not need it.) ■

Direct computation of polynomial discriminants can often be unwieldy, so applications of Lemma 3.4 usually rest on the connection between discriminants and resultants (see [4] and [32]); such work with resultants requires special care in positive characteristic. In our specific situation we will be able to extract the required information directly from the definition of the discriminant, so we will not need to use resultants.

In (3.12) we have to compute $\mu(f)$ for $f = 4cg_1^{2p} + (4du+1)g_2^{2p}$ such that $g_2 \neq 0$ and $(g_1, g_2) = 1$. The peculiar coefficient of g_2^{2p} is an artifact of our elliptic curve $E_{h(T)}$. We shall carry out the Möbius calculation for a cleaner expression and then return to $\mu(f)$.

Lemma 3.5. *Let κ be a finite field with characteristic $p \neq 2$. Using the convention $\deg(0) = -\infty$, for $a, b \in \kappa^\times$ and relatively prime $g_1, g_2 \in \kappa[u]$ we have*

$$\mu(ag_1^{2p} + bug_2^{2p}) = \begin{cases} -\chi(-1)^{\deg g_2} & \text{if } \deg g_1 \leq \deg g_2, \\ \chi(-1)^{\deg g_1} & \text{if } \deg g_1 > \deg g_2. \end{cases}$$

Proof. The cases when $g_1 = 0$ or $g_2 = 0$ are trivial, so we now suppose both are non-zero. Set $g = ag_1^{2p} + bug_2^{2p}$, $n_1 = \deg g_1$, $n_2 = \deg g_2$. Since $g' = bg_2^{2p}$ and $(g_1, g_2) = 1$, g is squarefree. We have (with notation as in Definition 3.2)

$$\deg g = \begin{cases} 2pn_2 + 1 & \text{if } n_1 \leq n_2, \\ 2pn_1 & \text{if } n_1 > n_2, \end{cases} \quad \text{lead}\, g \sim \begin{cases} b & \text{if } n_1 \leq n_2, \\ a & \text{if } n_1 > n_2. \end{cases}$$

Let $n = \deg g$, so in a splitting field the set of distinct roots of g may be labelled as $\{\gamma_1, \ldots, \gamma_n\}$. Since $g' = bg_2^{2p}$, it follows that $\prod_i g'(\gamma_i)$ is in $\kappa^\times$ and may be computed modulo squares:

$$\prod_i g'(\gamma_i) = b^{\deg g} \cdot \prod_i g_2(\gamma_i)^{2p} \sim b^{\deg g}$$

because $\prod_i g_2(\gamma_i) \in \kappa^\times$. Hence,

$$\mathrm{disc}_\kappa(g) = (-1)^{n(n-1)/2} (\text{lead}\, g)^{n-2} \cdot \prod_{i=1}^n g'(\gamma_i) \sim (-1)^{n(n-1)/2} (b \cdot \text{lead}\, g)^n.$$

Since $b \cdot \text{lead}\, g \sim b^2$ when n is odd (that is, when $n_1 \leq n_2$), we conclude

$$\mathrm{disc}_\kappa(g) \sim (-1)^{n(n-1)/2} \sim (-1)^{\max(n_1, n_2)}$$

by the formula for n. By (3.15), $\mu(g) = (-1)^n \chi(\mathrm{disc}_\kappa(g)) = (-1)^n \chi(-1)^{\max(n_1, n_2)}$. ■

It is now a simple matter to finish the computation of the global root number:

Theorem 3.6. *Let $h(T) = cT^{2p} + du$, where $c, d \in \kappa^\times$. Let E_T be defined as in (2.4). For any $t \in F = \kappa(u)$, the elliptic curve $E_{h(t)}$ over F satisfies*

$$W(E_{h(t)}) = \begin{cases} -1 & \text{if } \mathrm{ord}_\infty(t) \geq 0, \\ 1 & \text{if } \mathrm{ord}_\infty(t) < 0. \end{cases} \tag{3.16}$$

Proof. Write $t = g_1/g_2$ where $g_2 \neq 0$ and $(g_1, g_2) = 1$. We may apply Lemma 3.5 to the polynomial $f = 4cg_1^{2p} + (4du+1)g_2^{2p}$ by making the linear change of variables $u \mapsto u - 1/4d$ that preserves degrees. This yields

$$\mu(f) = \begin{cases} -\chi(-1)^{n_2}, & \text{if } n_1 \leq n_2, \\ \chi(-1)^{n_1}, & \text{if } n_1 > n_2, \end{cases} \tag{3.17}$$

where $n_1 = \deg g_1$ and $n_2 = \deg g_2$ (and $n_1 = -\infty$ if $g_1 = 0$). Combining (3.17) with the global root number formula (3.12) yields (3.16). ■

To force the global root number to be 1, we want only the second case of (3.16) to occur. This can be achieved by a simple trick (related to (3.2), but initially inspired by [16, p. 57]): replace t with $t^2 + u$, which has a pole at ∞ for every t in $F = \kappa(u)$. Thus,

$$W(E_{h(t^2+u)}) = 1 \tag{3.18}$$

for *every* $t \in F = \mathbf{P}^1_F(F) - \{\infty\}$. Since (1.4) is the Weierstrass model in the definition of $E_{h(T^2+u)}$, we see that (1.4) is not as arbitrary as it may have initially appeared to be. Combining (3.18) with Remark 1.2 settles the root number aspect of Theorem 1.1.

4. Generic rank bound I. Specialization at points of height 0

Write (1.4) in the form

$$\mathscr{E}_\eta : y^2 = x^3 + h(T^2+u)x^2 - (h(T^2+u))^3 x, \tag{4.1}$$

where $h(T) = cT^{2p} + du$ and $c, d \in \kappa^\times$. We have shown in §3 that for each $t \in \mathbf{P}^1(F)$, $\mathscr{E}_t$ is an elliptic curve over F with global root number 1. The elliptic curve $\mathscr{E}_\eta$ over $F(T) = \kappa(u,T)$ is obtained from $E_{T/\mathbf{F}_p(T)}$ in (2.4) by replacing T with the element $h(T^2+u) \in F(T) = \kappa(u,T)$ that is not in κ, so the point $(-T, T^2) \in E_T(\mathbf{F}_p(T))$ goes over to the point

$$Q = (-h(T^2+u), (h(T^2+u))^2) \in \mathscr{E}_\eta(F(T)) \tag{4.2}$$

that has infinite order (Corollary 2.6). For every $t \in F$ the specialization $h(t^2+u) \in \kappa(u)$ is not in κ, so the specialization of Q in $\mathscr{E}_t(F)$ must likewise have infinite order for all $t \in F$. Thus, all specializations $\mathscr{E}_t(F)$ at $t \in \mathbf{P}^1(F) - \{\infty\}$ have positive rank. This settles the rank aspect of Theorem 1.1 for the F-rational fibers. (We already noted in Remark 1.2 that $\mathscr{E}_\infty(F)$ has rank 0.)

The remainder of this paper is devoted to proving that the generic Mordell–Weil group $\mathscr{E}_\eta(F(T))$, which we know has rank at least 1, has rank exactly 1. This will complete the proof of Theorem 1.1.

Since the cubic polynomial in x given by the Weierstrass model (4.1) defining $\mathscr{E}_\eta$ is the product of x and an irreducible quadratic polynomial in $F(T)[x]$, the only nontrivial rational 2-torsion is the point $(0,0)$. Therefore

$$\dim_{\mathbf{F}_2} \mathscr{E}_\eta(F(T))/2 \cdot \mathscr{E}_\eta(F(T)) = 1 + \mathrm{rank}(\mathscr{E}_\eta(F(T))). \tag{4.3}$$

A point of infinite order in $\mathscr{E}_\eta(F(T))$ is given in (4.2), so the generic rank is 1 if and only if the dimension in (4.3) is at most 2.

Viewing $F(T) = \kappa(u,T)$ as the function field of $\mathbf{P}^1 \times \mathbf{P}^1$, we shall now consider specialization along the u-line. We will specialize at generic points of $\{u_0\} \times \mathbf{P}^1_\kappa$ for closed points $u_0 \in \mathbf{P}^1_\kappa$; these generic points are identified with the closed points of height 0 on the u-line $\mathbf{P}^1_{\kappa(T)}$ over $\kappa(T)$. For such u_0, let its residue field be written as $\kappa_0 = \kappa(u_0)$; this is a finite field and the notation κ_0 will be used constantly in what follows. If $u_0 \neq \infty$ then we also write u_0 to denote the image of the indeterminate u under the quotient map $\kappa[u] \twoheadrightarrow \kappa_0$.

Using (2.5) and (2.6), the parameters Δ and c_4 for (4.1) are given by

$$\Delta = 16(h(T^2+u))^8(1+4h(T^2+u)), \quad c_4 = 16(h(T^2+u))^2(1+3h(T^2+u)). \tag{4.4}$$

From the formula for Δ, we see that for all closed points $u_0 \in \mathbf{A}^1_\kappa$, the u_0-specialization of (4.1) is an elliptic curve over $\kappa_0(T)$. The elliptic curves $\mathscr{E}_t$ for $t \in \mathbf{P}^1(F)$ all live over the fixed global field $F = \kappa(u)$, but the u_0-specializations $\mathscr{E}_{u_0}$ of $\mathscr{E}_\eta$ live over the global fields $\kappa_0(T) = \kappa(u_0)(T)$ that vary. The notation $\mathscr{E}_{u_0}$ presents no risk of confusion with the notation $\mathscr{E}_t$ for specialization at $t \in \mathbf{P}^1(F)$ because we will never again use such T-specializations.

Let us briefly describe a natural but ultimately unsuccessful strategy for using the $\mathscr{E}_{u_0}$'s to show that the dimension in (4.3) is at most 2. We can prove a "height 0" version of Silverman's specialization theorem for abelian varieties, and from this it follows that for all but finitely many height-0 points $u_0 \in \mathbf{P}^1_{\kappa(T)}$, the specialization map

$$\mathscr{E}_\eta(F(T)) \to \mathscr{E}_{u_0}(\kappa_0(T)) \tag{4.5}$$

at u_0 is injective. Thus, it would suffice to prove $\mathrm{rank}(\mathscr{E}_{u_0}(\kappa_0(T))) \leq 1$ for infinitely many u_0. For an infinite set of points u_0 (specifically, the ones arising from Theorem 5.1 below), we can prove $\mathrm{rank}(\mathscr{E}_{u_0}(\kappa_0(T))) \leq 3$. (Switching root number calculations to the u_0-side, we also can show $W(\mathscr{E}_{u_0}) = -1$. This suggests, but does not prove, that $\mathscr{E}_{u_0}(\kappa_0(T))$ has rank 1 or 3.) For such u_0, the subspace V_{u_0} of everywhere-unramified classes in the 2-Selmer group $S^{[2]}(\mathscr{E}_{u_0/\kappa_0(T)})$ is 2-dimensional, and we can show that $\mathrm{rank}(\mathscr{E}_{u_0}(\kappa_0(T))) = 1$ (resp. < 3) if and only if the natural map $V_{u_0} \to Ш(\mathscr{E}_{u_0})[2]$ is injective (resp. non-zero). The Cassels–Tate pairing of the image of a basis of V_{u_0} in $Ш(\mathscr{E}_{u_0})[2]$ can be calculated by using a method of Cassels [2], but unfortunately it always turns out to be trivial! Thus, we do not know how to prove that V_{u_0} has non-zero image in $Ш(\mathscr{E}_{u_0})[2]$ for infinitely many of the points u_0 as in Theorem 5.1, and hence we do not know if $\mathrm{rank}(\mathscr{E}_{u_0}(\kappa_0(T))) < 3$ (let alone if $\mathscr{E}_{u_0}(\kappa_0(T))$ has rank 1) for infinitely many u_0.

Here is the successful strategy for using arithmetic information from the $\mathscr{E}_{u_0}$'s to bound the dimension in (4.3). We are aiming to prove that $\mathscr{E}_\eta(\kappa(u,T))$ has rank 1, and in (4.2) we have already found a point of infinite order, so it suffices to bound the rank from above by 1 after replacing κ with a finite extension κ' that may depend on the parameters $c, d \in \kappa^\times$ that were used in the definition of $\mathscr{E}_\eta$. Since $\mathscr{E}_\eta(\overline{\kappa}(u,T))$ is *finitely generated* (Lang–Néron), we may replace κ with a suitable finite extension (depending on c and d) to reduce to the case when $\mathscr{E}_\eta(\overline{\kappa}(u,T)) = \mathscr{E}_\eta(\kappa(u,T))$. Now consider the commutative diagram of natural maps

$$\begin{array}{ccc} \mathscr{E}_\eta(\kappa(u,T))/2\cdot\mathscr{E}_\eta(\kappa(u,T)) & \longrightarrow & \mathscr{E}_\eta(\overline{\kappa}(u,T))/2\cdot\mathscr{E}_\eta(\overline{\kappa}(u,T)) \\ \downarrow & & \downarrow \\ \mathscr{E}_{u_0}(\kappa_0(T))/2\cdot\mathscr{E}_{u_0}(\kappa_0(T)) & \longrightarrow & \mathscr{E}_{\overline{u}_0}(\overline{\kappa}(T))/2\cdot\mathscr{E}_{\overline{u}_0}(\overline{\kappa}(T)) \end{array} \tag{4.6}$$

in which $\overline{u}_0 \in \mathbf{A}^1_\kappa(\overline{\kappa})$ is a choice of geometric point over a closed point $u_0 \in \mathbf{A}^1_\kappa$, and both vertical maps are defined by the valuative criterion for properness. Since we adjusted κ so that $\mathscr{E}_\eta(\overline{\kappa}(u,T)) = \mathscr{E}_\eta(\kappa(u,T))$, the top side of (4.6) is an *isomorphism*. Therefore (4.3) is at most 2 if

- the right side of (4.6) is injective for *all but finitely many* $\overline{\kappa}$-points $\overline{u}_0 \in \mathbf{A}^1_\kappa(\overline{\kappa})$,
- the image of the map along the bottom side of (4.6) is at most 2-dimensional for *infinitely many* closed points $u_0 \in \mathbf{A}^1_\kappa$ (equipped with one of the finitely many choices of $\overline{\kappa}$-point $\overline{u}_0$ over u_0).

We consider these two respective assertions as "geometric" and "arithmetic" in nature.

Remark 4.1. We do not know *a priori* that the left side of (4.6) is injective for all but finitely many (or even infinitely many) u_0, though this injectivity does follow *a posteriori* from our proof that $\mathscr{E}_\eta(F(T))$ has rank 1; the *a priori* difficulty is due to the fact that κ is not separably closed (see Theorem 4.4). However, even if we did know such injectivity, it would be useless because our rank bounds for $\mathscr{E}_{u_0}(\kappa_0(T))$ are not good enough. The purpose of considering (4.6) is precisely to circumvent our lack of information concerning the groups $\mathscr{E}_{u_0}(\kappa_0(T))$.

We shall now undertake the geometric part of the argument (injectivity of the right side of (4.6) for all but finitely many $\overline{u}_0$). This will be deduced from a more general specialization result for abelian varieties. Let us isolate the essential geometric properties of $\mathscr{E}_\eta$ before we pass to an axiomatized setup with an abelian variety. Consider the surface $S = \mathbf{P}^1_\kappa \times \mathbf{P}^1_\kappa$ with factors having respective coordinates u and T. By general "smearing out" principles, $\mathscr{E}_\eta$ extends to an elliptic curve $\mathscr{E}_V$ over a dense open $V \subseteq S$. (In fact, there is a unique maximal such open V, containing all others, and the elliptic curve $\mathscr{E}_V$ extending $\mathscr{E}_\eta$ over this V is unique. This follows from a general lemma of Faltings [7, §2, Lemma 1], but we do not need it.) Pick some choice of V and $\mathscr{E}_V$. There are finitely many (if any) codimension-1 points in S not in V, and if $\mathscr{E}_\eta$ has good reduction at such a point s then we can "smear out" the proper Néron model over $\mathscr{O}_{S,s}$ and glue it to $\mathscr{E}_V$ so as to increase V to contain s. Doing this finitely many times, we may assume V contains all codimension-1 points of S where $\mathscr{E}_\eta$ has good reduction.

The complement $S - V$ consists of finitely many curves and isolated closed points. Since $\mathscr{E}_{u_0}$ is smooth for all closed points $u_0 \in \mathbf{A}^1_\kappa$, the curves in the complementary locus

$$S - V \subseteq \mathbf{P}^1_\kappa \times \mathbf{P}^1_\kappa$$

are "non-vertical" except for possibly $\{\infty\} \times \mathbf{P}^1_\kappa$. Put in geometric terms, when the bad locus for $\mathscr{E}_\eta$ over S is fibered over the T-line it "moves" in the fibers $S_t = \mathbf{P}^1$ except for possibly at the point ∞ in these fibers. We need to analyze the situation along the vertical line $u = \infty$.

Lemma 4.2. *The elliptic curve $\mathscr{E}_\eta$ in* (4.1) *has bad reduction at the codimension-*1 *generic point η_∞ of the line $u = \infty$ in S, with reduction type that is potentially good. The ramification of $\mathscr{E}_\eta[2]$ at η_∞ is tame.*

Proof. Since $\deg_u(h(T^2+u)) = 2p$, we see from (4.4) that $\deg_u(\Delta) = 18p$ is not divisible by 12. Therefore, there is bad reduction at η_∞. The j-invariant $j(\mathscr{E}_\eta)$ is a unit at η_∞ because j in (2.5) is a unit at ∞, so the reduction at η_∞ is potentially good. Since $\mathscr{E}_\eta[2](\eta_\infty) \neq O$ and the residue characteristic at η_∞ is not 2, the 2-torsion $\mathscr{E}_\eta[2]$ is tamely ramified at η_∞. ∎

Now we pass to a general situation that uses the properties proved in Lemma 4.2. Let k be a separably closed field and let S be a connected geometrically-normal k-scheme of finite type, equipped with a surjective k-morphism $S \to \mathbf{P}^1_k$ whose fibers are geometrically reduced and whose generic fiber is geometrically irreducible. By [10, IV_3, 9.7.7] there is a dense open in $\mathbf{P}^1_k$ over which S has geometrically integral fibers. In the above discussion, $k = \overline{\kappa}$ and S is the product of the projective u-line and projective T-line over k with projection $S \to \mathbf{P}^1_k$ onto the u-line.

Let A be an abelian variety of dimension $g \geq 1$ over the function field $k(S)$. For all but finitely many closed points $u \in \mathbf{P}^1_k$, A has good reduction A_{η_u} at the codimension-1 generic point η_u of the geometrically integral fiber S_u in the normal S; we write $k(S_u)$ to denote the function field of this fiber. By the valuative criterion for properness we have a specialization mapping

$$\rho_u : A(k(S)) \to A_{\eta_u}(k(S_u))$$

for such u. (Since we are not assuming that the Chow $k(S)/k$-trace of A vanishes, $A(k(S))$ might not be finitely generated. Hence, ρ_u cannot be defined by elementary denominator-chasing with a finite set of elements and their relations in $A(k(S))$, so we really do need the valuative criterion for properness in order to define ρ_u; more specifically we cannot expect $A(k(S))$ to "smear out" beyond the codimension-1 local ring on S at the generic point η_u of S_u.) Motivated by the goal of proving that the right side of (4.6) is injective with only finitely many exceptions, we want to analyze the kernel of the reduced map

$$\rho_u \bmod n : \; A(k(S))/n \cdot A(k(S)) \to A_{\eta_u}(k(S_u))/n \cdot A_{\eta_u}(k(S_u))$$

for suitable integers n and for u avoiding a finite set of closed points on $\mathbf{P}^1_k$. To this end, we first prove a general finiteness lemma.

Lemma 4.3. *Let V be a geometrically integral variety over a field k and let B be an abelian variety over $K = k(V)$. For all non-zero integers m with $\mathrm{char}(k) \nmid m$, the group $B(K)/m \cdot B(K)$ is finite if k is separably closed. The same holds for arbitrary non-zero integers m if k is algebraically closed.*

Proof. We shall use Chow's theory of the K/k-trace [18, Ch. VIII]. Here are the key points of this theory (for our purposes). In the category of pairs (B_0, f_0) consisting of an abelian variety B_0 over k and a map $f_0 : (B_0)_K \to B$ of abelian varieties over K, there is a final object $(\mathrm{Tr}_{K/k}(B), \tau)$ and the canonical map $\tau : (\mathrm{Tr}_{K/k}(B))_K \to B$ has infinitesimal kernel. This object is the *K/k-trace* of B. Obviously the map

$$\mathrm{Tr}_{K/k}(B)(k) \hookrightarrow \mathrm{Tr}_{K/k}(B)(K) \xrightarrow{\tau} B(K)$$

is injective. The Lang–Néron theorem [17, Thm. 1] says that the quotient group

$$B(K)/\mathrm{Tr}_{K/k}(B)(k) \tag{4.7}$$

is finitely generated. (To the best of our knowledge, all published references on these topics are written in pre-Grothendieck terminology; the reader is referred to [5] for a discussion of the Chow trace and Lang–Néron theorem using scheme-theoretic methods.)

Now assume that k is separably closed. Since $\mathrm{Tr}_{K/k}(B)(k)$ is the group of rational points of an abelian variety over a separably closed field, it is m-divisible (and the restriction $\mathrm{char}(k) \nmid m$ can be removed if k is algebraically closed). Thus,

$$\mathrm{Tr}_{K/k}(B)(k) \subseteq m \cdot B(K),$$

so

$$B(K)/m \cdot B(K) \simeq (B(K)/\mathrm{Tr}_{K/k}(B)(k))/m \cdot (B(K)/\mathrm{Tr}_{K/k}(B)(k)).$$

This yields the desired finiteness because (4.7) is finitely generated. ■

We return to the abelian variety $A_{/k(S)}$ described before Lemma 4.3.

Theorem 4.4. *Assume that k is separably closed and that for all closed points $u \in \mathbf{P}^1_k$ distinct from ∞, A has good reduction at some generic point of the (possibly reducible) geometrically-reduced fiber S_u. Assume moreover that at some generic point η_∞ of the fiber S_∞ there is potentially good reduction.*

Fix $n \in \mathbf{Z}$ with $|n| > 1$ such that $\mathrm{char}(k) \nmid n$, and assume that the Galois splitting field of the finite étale $k(S)$-group $A[n]$ is tamely ramified at the codimension-1 point $\eta_\infty \in S$.

The mod-n reduction

$$\rho_u \bmod n : \; A(k(S))/n \cdot A(k(S)) \to A_{\eta_u}(k(S_u))/n \cdot A_{\eta_u}(k(S_u))$$

of the specialization map along S_u *is injective for all but finitely many closed points* $u \in \mathbf{P}^1_k$.

The tameness assumption is equivalent to the condition that A acquires good reduction over a finite separable extension of $k(S)$ that is tame at a place over η_∞ (this is explained in the proof), and so this hypothesis is automatically satisfied when every positive prime $\ell \leq 2g+1$ is a unit in k (that is, $\mathrm{char}(k) = 0$ or $\mathrm{char}(k) > 2g+1$). Thus, by setting $g = 1$ and $n = 2$ in Theorem 4.4, we may conclude via Lemma 4.2 (which also gives the desired tameness in characteristic 3) that the right side of (4.6) is injective for all but finitely many $\overline{u}_0 \in \mathbf{A}^1_\kappa(\overline{\kappa})$.

Proof. The hypotheses on S and A are preserved under extension of the base field. Moreover, if $\overline{k}$ is an algebraic closure of k then we claim that the natural map

$$A(k(S))/n \cdot A(k(S)) \to A(\overline{k}(S))/n \cdot A(\overline{k}(S))$$

is injective, so we may reduce to the case when k is algebraically closed. The case of characteristic 0 is trivial, so we can assume $\mathrm{char}(k) = p > 0$. It suffices to check more generally that if K is a field with characteristic $p > 0$ and G is a commutative K-group of finite type then the map $G(K)/n \cdot G(K) \to G(K')/n \cdot G(K')$ is injective for any purely inseparable algebraic extension K'/K and any integer n not divisible by p. We may assume $K' = K^{1/p}$, so we get an identification $G(K') \simeq G^{(p)}(K)$ that identifies the inclusion $G(K) \to G(K')$ with the map on K-points induced by the relative Frobenius morphism $F_G : G \to G^{(p)}$. Since $[p] : G \to G$ factors through F_G [11, $\mathrm{VII_A}$, §4.3], it suffices to prove that the p-torsion in $G(K)/n \cdot G(K)$ vanishes, and this is clear since $p \nmid n$.

Let $W \subseteq S$ be a dense open such that A extends to an abelian scheme A_W over W. The complement $S - W$ contains at most finitely many codimension-1 points of S, and if A has good reduction at any such point s then we may glue A_W with a smearing-out of the proper Néron model of A over $\mathscr{O}_{S,s}$ to increase W to contain a neighborhood of s. Thus, by the hypothesis on reduction for A, we may suppose that no fiber S_u over a closed any point $u \in \mathbf{P}^1_k$ is disjoint from W except for possibly S_∞. This property of W is unaffected by shrinking W in codimension ≥ 2. Let η be the generic point of S.

By Lemma 4.3 with $V = S$, $A(k(S))/n \cdot A(k(S))$ is finite. We conclude from the pigeonhole principle that if ρ_u mod n has nontrivial kernel for infinitely many u (ignoring the finitely many for which S_u is reducible, in which case ρ_u is not defined), then some non-zero

$$\overline{R} \in A(k(S))/n \cdot A(k(S))$$

is killed by ρ_u mod n for infinitely many u. Thus, it suffices to prove that if $R_\eta \in A(k(S))$ has the property that $\rho_u(R_\eta)$ lies in $n \cdot A_{\eta_u}(k(S_u))$ for infinitely many u (ignoring the finitely many u for which ρ_u is not defined) then $R_\eta \in n \cdot A(k(S))$.

Choose $R_\eta \in A(k(S))$ such that $\rho_u(R_\eta)$ lies in $n \cdot A_{\eta_u}(k(S_u))$ for infinitely many u. By denominator-chasing, R_η extends (uniquely) to $R_U \in A_W(U)$ for some dense open $U \subseteq W$. The valuative criterion for properness extends R_U over each of the finitely many codimension-1 points of W not contained in U. Thus, by shrinking W in codimension ≥ 2 if necessary, we may assume that R_η extends to a section $R \in A_W(W)$ of the abelian scheme $A_W \to W$.

The pullback of $[n] : A_W \to A_W$ along $R \in A_W(W)$ is a finite étale cover

$$[n]^{-1}(R) \to W. \tag{4.8}$$

Our goal is to prove that (4.8) has a section over the generic point $\eta = \operatorname{Spec} k(S)$ of W. Let L be a residue field on $[n]^{-1}(R)_\eta = [n]^{-1}(R_\eta)$, so L is a finite separable extension of $k(S)$, say with degree d_L. We want $d_L = 1$ for some such L.

Lemma 4.5. *For each L, the subfield $k(\mathbf{P}^1)$ is algebraically closed in L.*

Proof. Let $K/k(\mathbf{P}^1)$ be the algebraic closure of $k(\mathbf{P}^1)$ in L, so $K/k(\mathbf{P}^1)$ is a finite separable extension because $L/k(\mathbf{P}^1)$ is a finitely generated separable extension (as $k(S)$ is separable over $k(\mathbf{P}^1)$, since the generic fiber of $S \to \mathbf{P}^1$ is geometrically integral). The intermediate fields K and $k(S)$ in the separable extension $L/k(\mathbf{P}^1)$ are linearly disjoint over $k(\mathbf{P}^1)$ because $K/k(\mathbf{P}^1)$ is algebraic and $k(\mathbf{P}^1)$ is algebraically closed in $k(S)$. Thus, if $\theta \in \mathbf{P}^1$ is the generic point then the function field

$$K(S_\theta) := K \otimes_{k(\mathbf{P}^1)} k(S) \tag{4.9}$$

of the geometrically integral generic fiber $S_{\theta/K}$ is identified with the intermediate composite field $K \cdot k(S)$ in $L/k(S)$. The hypothesis on the good reduction of A implies that for every closed point $u \in \mathbf{P}^1 - \{\infty\}$, some generic point η_u of the reduced fiber S_u lies in W. Hence, since $[n]^{-1}(R) \to W$ is a finite étale cover, the residue field L on $[n]^{-1}(R_\eta)$ is unramified over the discrete valuation on $k(S)$ arising from some such η_u for every closed point $u \in \mathbf{P}^1 - \{\infty\}$. It follows that for every such u, the intermediate finite separable extension $K(S_\theta)/k(S)$ is also unramified at some generic point η_u of S_u.

We also need to understand the ramification behavior of $L/k(S)$ at the discrete valuation on $k(S)$ arising from a generic point η_∞ on the reduced fiber S_∞ such that A has potentially good reduction over a tame extension at η_∞; the existence of such an η_∞ was one of our initial assumptions on A. We claim that $L/k(S)$ is tamely ramified at *all* places of L over η_∞. Some care will be required because $L/k(S)$ may be non-Galois.

The first step is to check that L admits at least one place that is tame over η_∞, and to do this it suffices to choose a separable closure of the residue field at η_∞ and to show that $[n]^{-1}(R_\eta)$ splits over a tame extension of the fraction field of the associated strict henselization $\mathscr{O}^{\mathrm{sh}}_{S,\eta_\infty}$. Since $A[n]$ is assumed to be tamely ramified at η_∞, there exists a finite tame extension F' over the fraction field of $\mathscr{O}^{\mathrm{sh}}_{S,\eta_\infty}$ such that $A[n]_{F'}$ is a constant group. We can assume $|n| > 1$, so there exists a prime $\ell | n$ and $\ell \neq \mathrm{char}(k)$. Since $A[n]_{F'}$ is constant, the Galois-action on the ℓ-adic Tate module of $A_{/F'}$ has pro-ℓ image that is finite (since A has potentially good reduction at η_∞), so after replacing F' with a suitable ℓ-power (hence *tame*) extension we can assume that $A_{/F'}$ has good reduction. Let $\mathscr{A}$ denote the proper Néron model of $A_{/F'}$ over the integral closure $\mathscr{O}_{F'}$ of $\mathscr{O}^{\mathrm{sh}}_{S,\eta_\infty}$ in F'. The group $A(F') = \mathscr{A}(\mathscr{O}_{F'})$ is n-divisible because $\mathscr{O}_{F'}$ is strictly henselian and n is not divisible by the residue characteristic of $\mathscr{O}_{F'}$, so $[n]^{-1}(R_\eta)(F') \neq \emptyset$. Since $A[n]_{F'}$ is split, it follows that the étale $A[n]$-torsor $[n]^{-1}(R_\eta)$ must therefore be split over F'. Hence, L admits a $k(S)$-embedding into F', so $L/k(S)$ is tamely ramified at some place w_L over the discrete valuation on $k(S)$ arising from η_∞.

By definition, L is a residue field on an étale $A[n]$-torsor $[n]^{-1}(R_\eta)$ over $k(S)$, and (by hypothesis) the $k(S)$-group $A[n]$ splits over a finite Galois extension $M/k(S)$ that is tamely ramified over η_∞. Thus, the factor fields of the finite étale M-algebra $L \otimes_{k(S)} M$ are residue fields on the torsor $[n]^{-1}(R_\eta)_M$ for a finite constant group over M (namely, the constant group $A[n]_M$). Hence, the factor fields L_i of $L \otimes_{k(S)} M$ are Galois over M and the L_i's are pairwise M-isomorphic. Pick a place w_M on M lifting the place η_∞ on $k(S)$. Since w_M and w_L lift the same place on $k(S)$, we can find a factor field L_{i_w} of $L \otimes_{k(S)} M$ and a place

v_{i_w} on L_{i_w} that lifts the places w_L and w_M. The place v_{i_w} on L_{i_w} must be tame over the place w_M because w_L is tame over η_∞ on $k(S)$. The extension L_{i_w}/M is Galois, so L_{i_w}/M is tame at *all* places over w_M. Since the L_i's are pairwise M-isomorphic and w_M is an arbitrary place on M over η_∞, every L_i is tame over every place on M lifting η_∞. Since *all* places of M over η_∞ are tame over η_∞, we conclude that all places lying over η_∞ on each L_i are tame over η_∞. Upon choosing some L_{i_0}, the extension $L/k(S)$ is a subextension of $L_{i_0}/k(S)$ and hence $L/k(S)$ is tamely ramified at *all* places over η_∞. The same therefore holds for the intermediate extension $K(S_\theta)/k(S)$ in (4.9).

Summarizing our conclusions, the finite separable extension $K(S_\theta) = K \otimes_{k(\mathbf{P}^1)} k(S)$ over $k(S)$ is unramified at some generic point of the reduced fiber S_u for each $u \neq \infty$ and is tamely ramified over some generic point of the reduced fiber S_∞. The reducedness of the fibers implies that a uniformizer at a closed point $u \in \mathbf{P}^1$ pulls back to be a uniformizer in the local ring at the codimension-1 point η_u on the normal variety S. Hence, the discrete valuation on $k(\mathbf{P}^1)$ associated to u has ramification index 1 under the discrete valuation on $k(S)$ associated to η_u, and the corresponding residue field extension is separable (because the residue field at u is the field k that is algebraically closed). It follows by classical valuation theory and (4.9) that if η_u is unramified (resp. tamely ramified) in $K(S_\theta)$ then u must be unramified (resp. tamely ramified) in K. Hence, the finite separable (possibly non-Galois) extension $K/k(\mathbf{P}^1)$ is unramified away from ∞ and is tamely ramified at *all* places over ∞. Since k is separably closed, we conclude that $K = k(\mathbf{P}^1)$. ■

We return to the proof of Theorem 4.4. Let $\mathscr{C}_L$ be the connected component of $[n]^{-1}(R)$ with function field L. Since $L/k(\mathbf{P}^1)$ is a finitely generated separable extension, it follows from Lemma 4.5 that the fiber of $\mathscr{C}_L$ over the generic point of $\mathbf{P}^1_k$ must be geometrically integral over $k(\mathbf{P}^1)$. By [10, IV_3, 9.7.7], there is a Zariski-dense open $U_L \subseteq \mathbf{A}^1_k$ such that the fiber $(\mathscr{C}_L)_u$ is geometrically integral over $k(u)$ for all $u \in U_L$. By removing finitely many closed points from U_L, we may (and do) also assume that S_u is geometrically integral over $k(u)$ for all $u \in U_L$. Since $[n]^{-1}(R)$ is finite étale over W and the open subset $W_u \subseteq S_u$ is non-empty for all $u \in \mathbf{A}^1_k$, the finite étale map $(\mathscr{C}_L)_u \to W_u$ has degree

$$[k(\mathscr{C}_L) : k(W)] = [L : k(S)] = d_L$$

for all points $u \in U_L$.

Choose $u \in \cap_L U_L$, where L runs over all the residue fields on $[n]^{-1}(R_\eta)$. We have just proved that the fiber $(\mathscr{C}_L)_u$ is connected (even geometrically integral over $k(u)$) for all L. It follows that $\{(\mathscr{C}_L)_u\}_L$ is the set of connected components of the finite étale W_u-scheme $[n]^{-1}(R)_u = [n]^{-1}(R_u)$ and the map

$$(\mathscr{C}_L)_u \to W_u \subseteq S_u$$

is étale with generic degree d_L for all L. Membership in $\cap_L U_L$ omits only finitely many closed points u, so by the hypothesis $\rho_u(R_\eta) \in n \cdot A_{\eta_u}(k(S_u))$ for infinitely many u (with $\rho_u(R_\eta)$ the generic point of the section R_u of A_W over W_u) we conclude that there exists a closed point $u' \in \cap_L U_L$ such that

$$\rho_{u'}(R_\eta) \in n \cdot A_{\eta_{u'}}(k(S_{u'})).$$

In particular, the $W_{u'}$-étale scheme $[n]^{-1}(R_{u'})$ has a $k(S_{u'})$-rational point. This rational point lies in some fibral connected component $(\mathscr{C}_{L_0})_{u'}$, so the generic degree d_{L_0} of this component over $S_{u'}$ must equal 1. ■

5. Generic rank bound II. Arithmetic arguments

Our remaining task is to prove that the bottom side of (4.6) is injective for infinitely many closed points $u_0 \in \mathbf{A}^1_\kappa$. In Theorem 5.1 we will find infinitely many points u_0 such that the elliptic curve $\mathscr{E}_{u_0/\kappa_0(T)}$ over the global field $\kappa_0(T)$ has exactly two places of bad reduction, and in §6 we will prove injectivity along the bottom of (4.6) for such u_0.

As preparation for the study of the image along the bottom side of (4.6) for well-chosen closed points $u_0 \in \mathbf{A}^1_\kappa$, we fix an arbitrary u_0 and find the reduction type of $\mathscr{E}_{u_0}$ at each place of $\kappa_0(T)$. After we find these reduction types, the points u_0 that will become our focus of interest will be those such that $\mathscr{E}_{u_0}$ has the smallest possible number of physical points of bad reduction on the T-line $\mathbf{P}^1_{\kappa_0}$.

Recall that (4.1) defines $\mathscr{E}_\eta$ in terms of $h(T^2+u)$, where $h(T) = cT^{2p} + du$. From (4.4), the discriminant of (4.1) involves $h(T^2+u)$ and $1+4h(T^2+u)$. Under a u_0-specialization, $h(T^2+u)$ becomes a pth power in $\kappa_0[T]$:

$$h(T^2+u)|_{u=u_0} = (c^{1/p}(T^2+u_0)^2 + d^{1/p}u_0^{1/p})^p.$$

Likewise, $1+4h(T^2+u)$ specializes to a pth power in $\kappa_0[T]$:

$$(1+4h(T^2+u))|_{u=u_0} = (1+4(c^{1/p}(T^2+u_0)^2 + d^{1/p}u_0^{1/p}))^p.$$

For all but finitely many closed points $u_0 \in \mathbf{A}^1_\kappa$, the pth-root polynomials

$$\pi_1 := c^{1/p}(T^2+u_0)^2 + d^{1/p}u_0^{1/p}, \quad \pi_2 := 1+4\pi_1 \tag{5.1}$$

are separable in $\kappa_0[T]$. (These quartics over the finite field κ_0 may be reducible for many points u_0, and so even in characteristic $p > 3$ these quartics may be fail to be separable for some non-empty finite set of points u_0. In Theorem 5.1 below, we will show that for infinitely many u_0 we can do much better than mere separability.) We now restrict attention to those u_0 such that the two polynomials in (5.1) are both separable. (Our notation π_1 and π_2 does not indicate the dependence on u_0; it would be more accurate to write π_{1,u_0} and π_{2,u_0}, but we simply ask the reader to remember the dependence on u_0.)

Specializing (4.4) at u_0, the Weierstrass model that defines $\mathscr{E}_{u_0/\kappa_0(T)}$ has parameters

$$\Delta|_{u=u_0} = 16\pi_1^{8p}\pi_2^p, \quad c_4|_{u=u_0} = 16\pi_1^{2p}(1+3\pi_1^p) = 16\pi_1^{2p}(\pi_2-\pi_1)^p, \tag{5.2}$$

and this Weierstrass model is integral away from $T=\infty$. Thus, the only possible bad reduction for $\mathscr{E}_{u_0}$ over the T-line $\mathbf{P}^1_{\kappa_0}$ is at ∞ and at the zeros of π_1 and π_2.

What is the behavior of $\mathscr{E}_{u_0}$ at the point $\infty \in \mathbf{P}^1_{\kappa_0}$? We return to Lemmas 2.1 and 2.2. Both π_1 and π_2 have degree 4 in $\kappa_0[T]$, so by (5.2) we have

$$\mathrm{ord}_\infty(\Delta|_{u=u_0}) = -36p.$$

When $\mathrm{char}(\kappa) > 3$,

$$\mathrm{ord}_\infty(c_4|_{u=u_0}) = -12p, \quad \mathrm{ord}_\infty(j|_{u=u_0}) = 0.$$

When $\mathrm{char}(\kappa) = 3$,

$$\mathrm{ord}_\infty(c_4|_{u=u_0}) = -8p, \quad \mathrm{ord}_\infty(j|_{u=u_0}) = 12p.$$

Thus, there is potentially good reduction at $T=\infty$ in all cases, and Lemma 2.1 ensures that this reduction is good.

Now we analyze the reduction types at points x_j in the zero-scheme of π_j on $\mathbf{P}^1_{\kappa_0}$. Since π_1 is separable in $\kappa_0[T]$ (by our choice of u_0), we see from (5.2) that for any x_1,

$$\mathrm{ord}_{x_1}(\Delta|_{u=u_0}) = 8p, \quad \mathrm{ord}_{x_1}(c_4|_{u=u_0}) = 2p \equiv 2 \bmod 4.$$

Therefore $\mathrm{ord}_{x_1}(j(\mathscr{E}_{u_0})) = 6p - 8p = -2p < 0$. By Lemma 2.2, there must be (potentially multiplicative) additive reduction at x_1. Similarly, we compute

$$\mathrm{ord}_{x_2}(\Delta|_{u=u_0}) = p, \quad \mathrm{ord}_{x_2}(c_4|_{u=u_0}) = 0,$$

so $\mathrm{ord}_{x_2}(j(\mathscr{E}_{u_0})) = -p < 0$. By Lemma 2.2, there is multiplicative reduction at x_2.

We have shown that the Néron model $N(\mathscr{E}_{u_0}) \to \mathbf{P}^1_{\kappa_0}$ enjoys the following reduction properties:

(a) good reduction at all closed points of $\mathbf{P}^1_{\kappa_0}$ away from zeros of π_1 and π_2,
(b) multiplicative reduction at zeros x_2 of π_2, with $\mathrm{ord}_{x_2}(j_{u_0}) = -p$.
(c) additive reduction at zeros x_1 of π_1, with $\mathrm{ord}_{x_1}(j_{u_0}) = -2p < 0$.

Properties (b) and (c) will be used in our work with Néron models and Selmer groups in §6, but now we focus on (a). The most favorable u_0's for our purposes will be those such that $\mathscr{E}_{u_0}$ has the least possible number of physical points of bad reduction, so we want to find many u_0 such that π_1 and π_2 are both irreducible in $\kappa_0[T]$. For such u_0, $\mathscr{E}_{u_0}$ has exactly two physical points of bad reduction on $\mathbf{P}^1_{\kappa_0}$.

Theorem 5.1. *There exist infinitely many closed points $u_0 \in \mathbf{A}^1_\kappa$ such that $\pi_1, \pi_2 \in \kappa_0[T]$ are irreducible.*

To find the infinitely many u_0 as in the theorem will require some effort, so let us first sketch the basic idea. In (5.1) we see that $u_0 \in \kappa_0$ intervenes in π_1 and π_2 through the value $u_0^{1/p} \in \kappa_0$, so to put ourselves in the position of specializing polynomials in u we apply arithmetic Frobenius of κ_0 to the coefficients of π_1 and π_2. This leads us to consider the polynomials

$$\Pi_1(u,T) := c(T^2 + u^p)^2 + du, \;\; \Pi_2(u,T) := 1 + 4\Pi_1(u,T) \in \kappa[u][T]. \tag{5.3}$$

For any closed point $u_0 \in \mathbf{A}^1_\kappa$, the specialization $\Pi_j(u_0,T) \in \kappa_0[T]$ is the image of $\pi_j \in \kappa_0[T]$ under the arithmetic Frobenius automorphism of κ_0. Thus, Theorem 5.1 is equivalent to the existence of infinitely many $u_0 \in \mathbf{A}^1_\kappa$ such that both $\Pi_1(u_0,T)$ and $\Pi_2(u_0,T)$ are irreducible in $\kappa_0[T]$, where $\kappa_0 = \kappa(u_0)$ is varying with u_0. It is this equivalent statement that we will actually prove (Theorem 5.8 below).

Expanding Π_1 and Π_2 as polynomials in $\kappa(u)[T]$, we have

$$\Pi_1 = c\left(T^4 + 2u^pT^2 + u^{2p} + \frac{du}{c}\right), \;\; \Pi_2 = 4c\left(T^4 + 2u^pT^2 + u^{2p} + \frac{du}{c} + \frac{1}{4c}\right). \tag{5.4}$$

It is left to the reader to check that Π_1 and Π_2 are separable and irreducible over $\kappa(u)$, via the following elementary criterion concerning polynomials of the form $X^4 + aX^2 + b$.

Lemma 5.2. *Let K be a field with* $\mathrm{char}(K) \neq 2$. *A polynomial $f = X^4 + aX^2 + b \in K[X]$ is separable if and only if b and $a^2 - 4b$ are non-zero. It is irreducible if b and $a^2 - 4b$ are non-squares in $K^\times$.*

Proof. The condition for separability is obvious. We now assume that b and $a^2 - 4b$ are non-squares in $K^\times$. Since $a^2 - 4b$ is not a square, f has no roots in K and has no factors of the form $X^2 - c$ in $K[X]$. Thus, if we write the four roots of f in a splitting field as $\pm r_1$ and $\pm r_2$, a non-trivial monic factor of f in $K[X]$ must have the form $(X \pm r_1)(X \pm r_2)$. If such a factor exists then $r_1 r_2 \in K$ and $b = (r_1 r_2)^2$, contradicting the assumption that b is a non-square in K. ■

In view of the irreducibility of each Π_j in $\kappa(u)[T]$ and our desire to prove

$$\Pi_1(u_0, T),\ \Pi_2(u_0, T) \in \kappa_0[T]$$

are irreducible for infinitely many closed points $u_0 \in \mathbf{A}^1_\kappa$, our problem resembles Hilbert irreducibility. However, finite fields are not Hilbertian and anyway we are not generally specializing u at elements of κ (since $[\kappa_0 : \kappa] > 1$ with only finitely many exceptions).

The main idea that will produce the desired u_0's is the following theorem. It gives a group-theoretic criterion for a polynomial over a global field to specialize to an irreducible polynomial over the residue field at infinitely many places (see Remark 5.4).

Theorem 5.3. *Let K be a global field and let $f \in K[T]$ be a monic separable irreducible polynomial of degree n. Let K'/K be a splitting field for f and let $G = \mathrm{Gal}(K'/K)$. For any non-archimedean place v of K at which f has integral coefficients, $f \bmod v$ is irreducible over the residue field $\mathbf{F}_v$ at v if and only if v is unramified in K' and the Frobenius elements over v in G act as n-cycles on the set of roots of f in K'.*

Proof. Let r be a root of f in K'. If f is v-integral and $f \bmod v$ is separable, then the discriminant of f is a v-adic unit, so v is unramified in $K(r)$. Since K' is a composite of such extensions of K, in such cases v must be unramified in K'. Let v' be a place of K' over a place v in K that is unramified in K'. The action of $\mathrm{Frob}(v'|v)$ on the n roots of f in K' is identified with the action of the finite-field Frobenius $x \mapsto x^{\#\mathbf{F}_v}$ on the full set of n roots of $f \bmod v$ (in $\mathbf{F}_{v'}$). In particular, $f \bmod v$ is irreducible over $\mathbf{F}_v$ if and only if v is unramified in K' and $\mathrm{Frob}(v'|v)$ acts as an n-cycle on the roots of f. ∎

Remark 5.4. In the setting of Theorem 5.3, if $r \in K'$ is a root of f and $H \subseteq G$ is the subgroup associated to the intermediate field $K(r) \subseteq K'$, then an element $\gamma \in G$ acts as an n-cycle on the set of roots of f in K' if and only if the cyclic subgroup $\langle \gamma \rangle$ is a set of representatives for the coset space G/H of order n. We conclude by Chebotarev's density theorem that $f \bmod v$ is irreducible for infinitely many places v of K if and only if G/H admits a set of representatives that is a cyclic subgroup of G.

Corollary 5.5. *Let K be a global field and let $f \in K[T]$ be a monic separable irreducible polynomial of degree n. The following are equivalent (restricting attention to non-archimedean places at which the coefficients of f are integral):*

1. *There is some place v such that $f \bmod v$ is irreducible.*
2. *There is a positive proportion of places v such that $f \bmod v$ is irreducible.*

Proof. The implication (2) $\Rightarrow$ (1) is trivial, and the converse follows from Theorem 5.3 and Chebotarev's density theorem. ∎

Example 5.6. Let f satisfy the hypotheses in Theorem 5.3, and let $\{r_1, \ldots, r_n\}$ be an ordering of the set of roots of f in K'. Identify $G = \mathrm{Gal}(K'/K)$ with a subgroup $\overline{G} \subseteq S_n$ via the G-action on the r_j's. By Theorem 5.3, $f \bmod v$ is irreducible for infinitely many v if and only if $\overline{G}$ contains an n-cycle.

1. If G is isomorphic to S_n as abstract groups (where $n = \deg f$), then $\overline{G} = S_n$. Since $\overline{G}$ contains an n-cycle, $f \bmod v$ is irreducible for infinitely many v.
2. What if G is isomorphic to A_n (as abstract groups)? Since A_n embeds into S_n with only one possible image, and A_n contains an n-cycle if and only if n is odd, we see that $f \bmod v$ is irreducible infinitely often if and only if n is odd.

(3) What if G (and thus $\overline{G}$) is isomorphic to D_n (as abstract groups) with $n > 2$? Then $\overline{G}$ is isomorphic to D_n as a permutation group, so $f \bmod v$ is irreducible infinitely often.

The identification of $\overline{G}$ with D_n as a permutation group was explained to us by D. Pollack. Write $\overline{G} = \langle \sigma, \tau \rangle$, where $\sigma^n = 1$, $\tau^2 = 1$ and $\tau\sigma\tau^{-1} = \sigma^{-1}$. Since $\langle \sigma \rangle$ is normal in $\overline{G}$ and $\overline{G}$ is a transitive subgroup of S_n, all $\langle \sigma \rangle$-orbits have the same length. Therefore, since σ has order n it must be an n-cycle. Writing $\sigma = (1, 2, \ldots, n)$, $\tau\sigma\tau^{-1} = \sigma^{-1}$ says $(\tau(1), \tau(2), \ldots, \tau(n)) = (n, n-1, \ldots, 1)$ as n-cycles. We can replace τ in the presentation of $\overline{G}$ with $\tau\sigma^k$ for any k, so we may assume $\tau(1) = 1$. Identifying j with $e^{2\pi i(j-1)/n}$, σ and τ are now the standard generators for D_n in its natural action on an n-gon.

(4) What if f is a normal polynomial; *i.e.*, G has order n? A transitive subgroup of order n in S_n contains an n-cycle if and only if it is cyclic, so the reduction of f at infinitely many places is irreducible if G is cyclic but not otherwise.

(5) In the preceding four examples, the structure of the Galois group G as an abstract group was sufficient to determine if the permutation group $\overline{G}$ contains an n-cycle. However, this is not generally the case. For example, there is a group of size $2592 = 2^5 \cdot 3^4$ admitting two transitive actions of degree 12 such that one action contains 12-cycles and the other does not. The actions were found for us by N. Boston using MAGMA; they are the 245th and 246th transitive groups of degree 12 in MAGMA's enumeration. MAGMA also realizes both of these transitive groups as Galois groups over $\mathbf{Q}$.

We now apply these ideas to the polynomials $\Pi_1(u, T)$ and $\Pi_2(u, T)$ from (5.4). To determine their Galois groups over $\kappa(u)$, we use the following classical lemma.

Lemma 5.7. *Let K be a field with $\mathrm{char}(K) \neq 2$, and let $f = X^4 + aX^2 + b \in K[X]$ be separable and irreducible. Let K'/K be a splitting field and $G = \mathrm{Gal}(K'/K)$. We have the following possibilities for G as an abstract group:*

- *$G \simeq \mathbf{Z}/4\mathbf{Z}$ if and only if $b(a^2 - 4b) \in K^\times$ is a square, in which case the quadratic subfield is $K(\sqrt{b}) = K(\sqrt{a^2 - 4b})$,*
- *$G \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ if and only if $b \in K^\times$ is a square, in which case the quadratic subfields are $K(\sqrt{a^2 - 4b})$, $K(\sqrt{-a + 2\sqrt{b}})$, and $K(\sqrt{-a - 2\sqrt{b}})$ for a fixed choice of $\sqrt{b} \in K^\times$,*
- *$G \simeq D_4$ if and only if b and $b(a^2 - 4b)$ are not squares in $K^\times$, in which case the quadratic subfields are $K(\sqrt{a^2 - 4b})$, $K(\sqrt{b})$, and $K(\sqrt{b(a^2 - 4b)})$. The unique quadratic subfield over which K' is a cyclic extension is $K(\sqrt{b(a^2 - 4b)})$.*

Proof. This classification of Galois groups according to properties of the coefficients can be found as an exercise in many basic algebra books, although usually it is stated only over $\mathbf{Q}$. In that spirit, the other assertions are left as an exercise for the reader. ■

To apply Lemma 5.7 to Π_1 and Π_2, we look at (5.4) and label the coefficients inside the parentheses as

$$A_1 = 2u^p, \;\; B_1 = u^{2p} + \frac{du}{c}, \;\; A_2 = 2u^p, \;\; B_2 = u^{2p} + \frac{du}{c} + \frac{1}{4c},$$

so $\Pi_j = T^4 + A_jT^2 + B_j$ modulo $\kappa^\times$-scaling. Since we used Lemma 5.2 to prove that each Π_j is separable and irreducible, we already know that B_j and $A_j^2 - 4B_j$ are non-squares in $\kappa(u)^\times$. A direct calculation also shows that $B_j(A_j^2 - 4B_j)$ is a non-square in $\kappa(u)^\times$. Therefore, by Lemma 5.7, each of Π_1 and Π_2 has Galois group over $\kappa(u)$ that is isomorphic to D_4. Example 5.6(3) now tells us that Π_1 and Π_2 each have infinitely many irreducible u_0-specializations. What about simultaneous irreducible specializations? This is what we need to resolve in order to complete the proof of Theorem 5.1.

Theorem 5.8. *There exist infinitely many u_0 such that $\Pi_1(u_0, T)$ and $\Pi_2(u_0, T)$ are both irreducible in $\kappa_0[T]$.*

Proof. Let $L_j/\kappa(u)$ be a splitting field of Π_j, so $\mathrm{Gal}(L_j/\kappa(u))$ is isomorphic to D_4. We will show L_1 and L_2 are linearly disjoint over $\kappa(u)$. It will then follow, by the Chebotarev density theorem, that any pair of Frobenius elements in $\mathrm{Gal}(L_1/\kappa(u)) \times \mathrm{Gal}(L_2/\kappa(u))$ are both attached to infinitely many common places on $\kappa(u)$. Theorem 5.3 and Example 5.6(3) then imply there are infinitely many u_0 such that $\Pi_1(u_0, T)$ and $\Pi_2(u_0, T)$ are both irreducible in $\kappa_0[T]$.

Any intermediate extension in $L_j/\kappa(u)$, other than $\kappa(u)$, contains a quadratic extension of $\kappa(u)$ since every proper subgroup of a 2-group is contained in a subgroup of index 2. We will show that L_1 and L_2 do not contain quadratic subfields (over $\kappa(u)$) that are $\kappa(u)$-isomorphic, so they must be linearly disjoint over $\kappa(u)$.

Inspection shows the only occurrences of non-trivial common factors among

$$B_1, \;\; A_1^2 - 4B_1, \;\; B_2, \;\; A_2^2 - 4B_2 \tag{5.5}$$

are: the linear polynomial $A_1^2 - 4B_1$ divides B_1 and (when $c = 4d^{2p}$) the linear polynomial $A_2^2 - 4B_2$ divides B_1. Since B_1 is separable with $\deg B_1 > 2$, we conclude that the four elements in (5.5) are multiplicatively independent modulo squares in $\kappa(u)^\times$. This independence modulo squares, coupled with the list of quadratic subfields in the D_4-case of Lemma 5.7, shows L_1 and L_2 do not share a common quadratic extension of $\kappa(u)$. Thus, they are linearly disjoint over $\kappa(u)$. ■

6. Generic rank bound III. Cohomological arguments

By Theorem 5.1, there are infinitely many closed points $u_0 \in \mathbf{A}^1_\kappa$ such that the "specialized" polynomials

$$\pi_1 = c^{1/p}(T^2 - u_0)^2 + d^{1/p}u_0^{1/p}, \;\; \pi_2 = 1 + 4\pi_1 \tag{6.1}$$

in $\kappa_0[T]$ are both irreducible. *These are the only u_0 that we shall henceforth consider.*

We view π_1 and π_2 as closed points on $\mathbf{A}^1_{\kappa_0} \subseteq \mathbf{P}^1_{\kappa_0}$. The arithmetic of

$$\mathscr{E}_{u_0} : y^2 = x^3 + \pi_1^p x^2 - \pi_1^{3p} x \tag{6.2}$$

for such u_0 is our focus of interest, as this will provide the information that we need to prove that the image of the bottom map in (4.6) has dimension ≤ 2 for these points u_0. This will complete the proof that $\mathscr{E}_\eta(F(T))$ has rank 1, thereby concluding the proof of Theorem 1.1.

Rather than work with $\mathscr{E}_{u_0}$, it will simplify matters to work with the elliptic curve

$$\mathscr{E}'_{u_0} : y^2 = x^3 + \pi_1 x^2 - \pi_1^3 x; \tag{6.3}$$

this elliptic curve is p-isogenous to $\mathscr{E}_{u_0} = (\mathscr{E}'_{u_0})^{(p)}$, so by oddness of p it follows that the map along the bottom of (4.6) is canonically identified with the map

$$\mathscr{E}'_{u_0}(\kappa_0(T))/2 \cdot \mathscr{E}'_{u_0}(\kappa_0(T)) \to \mathscr{E}'_{u_0}(\overline{\kappa}_0(T))/2 \cdot \mathscr{E}'_{u_0}(\overline{\kappa}_0(T)), \tag{6.4}$$

where $\overline{\kappa}_0$ is an algebraic closure of κ_0. We shall prove that (6.4) is injective for the points u_0 presently under consideration.

The reduction properties of the Néron model $N(\mathscr{E}_{u_0}) \to \mathbf{P}^1_{\kappa_0}$ were worked out in §5 (see above Theorem 5.1), and the additive and multiplicative properties are the same for the Néron model of the isogenous elliptic curve $\mathscr{E}'_{u_0}$. Thus, letting $j'_{u_0} = j(\mathscr{E}'_{u_0})$, for points u_0 such that π_1 and π_2 are irreducible in $\kappa_0[T]$ we obtain the following properties for $N(\mathscr{E}'_{u_0})$:

- good reduction at all closed points of $\mathbf{P}^1_{\kappa_0}$ away from π_1 and π_2,
- multiplicative reduction at π_2, with $\mathrm{ord}_{\pi_2}(j'_{u_0}) = -1$,
- additive reduction at π_1 that is potentially multiplicative, with $\mathrm{ord}_{\pi_1}(j'_{u_0}) = -2$.

By the theory of Tate models for multiplicative reduction, the component group for the Néron model at π_2 is trivial, so the π_2-fiber $N(\mathscr{E}'_{u_0})_{\pi_2}$ is a torus.

Fix a geometric point $\overline{\pi}_1$ over the point $\{\pi_1\} \in \mathbf{P}^1_{\kappa_0}$. The reduction at π_1 is (additive and) potentially multiplicative, and $\mathrm{ord}_{\pi_1}(j'_{u_0}) = -2$ is negative and even. We need to know the structure of the component group of the additive geometric fiber of the Néron model at $\overline{\pi}_1$. This can be deduced from Tate's algorithm, but we give here a direct proof via general principles.

Lemma 6.1. *Let R be a discrete valuation ring with residue field k and fraction field K, and let E be an elliptic curve over K with Néron model $N(E)$ over R. Assume that* $\mathrm{ord}_R(j(E))$ *is negative and even, that E has additive reduction over R, and that* $\mathrm{char}(k) \neq 2$.

If k is perfect and $\overline{k}/k$ is an algebraic closure, then the geometric component group $N(E)_{\overline{k}}/N(E)^0_{\overline{k}}$ is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

Proof. The formation of the Néron model over a discrete valuation ring commutes with base change to a strict henselization and to a completion, so we may assume that k is separably closed and that R is complete. Since $\mathrm{ord}_R(j(E)) < 0$, it follows from Tate's theory that E is a quadratic twist of the Tate curve E_0 over K with j-invariant $j(E)$. Since $\mathrm{char}(k) \neq 2$ and R is strictly henselian, the Tate parameter q_{E_0} must be a square in $K^\times$ because $\mathrm{ord}_R(q_{E_0}) = -\mathrm{ord}_R(j(E_0)) = -\mathrm{ord}_R(j(E))$ is even. Thus, the 2-torsion on the Tate curve E_0 is a constant group over K. This property of the 2-torsion is unaffected by quadratic twisting, so $E[2]$ is a constant group over K.

Using the Néron mapping property, we obtain a map of R-groups

$$\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \to N(E),$$

and by passing to k-fibers we arrive at a map of finite étale groups

$$\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \to N(E)_k/N(E)^0_k.$$

This map is injective by the hypothesis that the reduction is additive and $\mathrm{char}(k) \neq 2$. It is a general fact that for any discrete valuation ring R and any elliptic curve E over the fraction field of R, the component group of the closed fiber of the Néron model $N(E)$ has order at most 4 when E has additive reduction and the residue field k is perfect. This follows from the relationship between $N(E)$ and the minimal regular proper model E^{reg} over R, together with the combinatorial classification of the extended Dynkin diagrams that describe the special fiber E^{reg}_k (equipped with its intersection form) when k is *algebraically closed*; see [19, 10.2]. ■

Theorem 6.2. *The 2-torsion subgroup $N(\mathscr{E}'_{u_0})[2]$ is quasi-finite, étale, and separated over $\mathbf{P}^1_{\kappa_0}$. It is finite étale of order 4 over $\mathbf{P}^1_{\kappa_0} - \{\pi_2\}$ and has fiber of order 2 over $\{\pi_2\}$.*

Proof. Since all points on $\mathbf{P}^1_{\kappa_0}$ have residue characteristic not equal to 2, doubling on $N(\mathscr{E}'_{u_0})$ is an étale map that has fiberwise-finite kernel. Hence, $N(\mathscr{E}'_{u_0})[2]$ is a quasi-finite, étale, and separated $\mathbf{P}^1_{\kappa_0}$-group, so it is finite over an open $U \subseteq \mathbf{P}^1_{\kappa_0}$ if and only if its fiber rank is constant on U. Since $N(\mathscr{E}'_{u_0})_{\pi_2}$ is a torus, $N(\mathscr{E}'_{u_0})[2]_{\pi_2} = N(\mathscr{E}'_{u_0})_{\pi_2}[2]$ has order 2. For $x \in \mathbf{P}^1_{\kappa_0} - \{\pi_1, \pi_2\}$ the fiber $N(\mathscr{E}'_{u_0})_x$ is an elliptic curve, so its 2-torsion subgroup has order 4. It remains to check that $N(\mathscr{E}'_{u_0})[2]_{\overline{\pi}_1}$ has order 4. Consider the exact sequence of smooth groups

$$0 \to N(\mathscr{E}'_{u_0})^0_{\overline{\pi}_1} \to N(\mathscr{E}'_{u_0})_{\overline{\pi}_1} \to N(\mathscr{E}'_{u_0})_{\overline{\pi}_1}/N(\mathscr{E}'_{u_0})^0_{\overline{\pi}_1} \to 0. \tag{6.5}$$

By Lemma 6.1, the final term has order 4 and is killed by 2. Since we are not in characteristic 2, doubling is an automorphism of the additive group $N(\mathscr{E}'_{u_0})^0_{\overline{\pi}_1}$, so (6.5) splits. This gives the result. ■

Consider the two points $P'_0 = (0,0)$ and $Q'_0 = (-\pi_1, \pi_1^2)$ in $\mathscr{E}'_{u_0}(\kappa_0(T))$, where P'_0 is a rational point of order 2 and $(Q'_0)^{(p)} \in (\mathscr{E}'_{u_0})^{(p)}(\kappa_0(T)) = \mathscr{E}_{u_0}(\kappa_0(T))$ is the u_0-specialization of (4.2).

Theorem 6.3. *The natural map*

$$\mathscr{E}'_{u_0}(\kappa_0(T)) = N(\mathscr{E}'_{u_0})(\mathbf{P}^1_{\kappa_0}) \to N(\mathscr{E}'_{u_0})_{\overline{\pi}_1}/N(\mathscr{E}'_{u_0})^0_{\overline{\pi}_1} \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, \tag{6.6}$$

carries P'_0 and Q'_0 to linearly independent elements. In particular, the component group at π_1 is a constant group generated by the classes of P'_0 and Q'_0.

Proof. The meaning of the theorem is that P'_0 and Q'_0 reduce into distinct non-identity components of $N(\mathscr{E}'_{u_0})_{\overline{\pi}_1}$. By [19, 9.4/35,37] and [19, 10.2/14], the smooth locus in a minimal Weierstrass model is the relative identity component of the Néron model over any discrete valuation ring. The Weierstrass model (6.3) is minimal at π_1. Since P'_0 and Q'_0 reduce to the unique non-smooth point $(0,0)$ on the closed fiber of this model, we conclude that the reductions of P'_0 and Q'_0 in the Néron model at $\overline{\pi}_1$ do not lie in the identity component.

To see that the reductions of P'_0 and Q'_0 in the Néron model at $\overline{\pi}_1$ lie in distinct components, we just have to check that the difference $P'_0 - Q'_0 = -(P'_0 + Q'_0)$ also has reduction not in the identity component on the $\overline{\pi}_1$-fiber of the Néron model; that is, the point $P'_0 + Q'_0$ should have reduction $(0,0)$ with respect to the minimal Weierstrass model (6.3) at π_1. It is trivial to compute $P'_0 + Q'_0 = (\pi_1^2, \pi_1^3)$, and this has reduction $(0,0)$. ■

Theorem 6.4. *Let $\overline{\kappa}_0$ be an algebraic closure of $\kappa_0 = \kappa(u_0)$, with $u_0 \in \mathbf{A}^1_\kappa$ a closed point such that π_1 and π_2 as in (6.1) are irreducible in $\kappa_0[T]$. The image of the canonical map*

$$c : \mathscr{E}'_{u_0}(\kappa_0(T))/2 \cdot \mathscr{E}'_{u_0}(\kappa_0(T)) \to \mathscr{E}'_{u_0}(\overline{\kappa}_0(T))/2 \cdot \mathscr{E}'_{u_0}(\overline{\kappa}_0(T))$$

in (6.4) is spanned by $c(P'_0)$ and $c(Q'_0)$, so $\dim_{\mathbf{F}_2} \mathrm{image}(c) \leq 2$.

Proof. Let $\delta : \mathscr{E}'_{u_0}(\kappa_0(T))/2\mathscr{E}'_{u_0}(\kappa_0(T)) \to S^{[2]}(\mathscr{E}'_{u_0/\kappa_0(T)})$ be the injective Kummer map to the 2-torsion Selmer group. Let K^{h}_x denote the fraction field of the henselization $\mathscr{O}^{\mathrm{h}}_{\mathbf{P}^1_{\kappa_0},x}$ of the local ring at a closed point $x \in \mathbf{P}^1_{\kappa_0}$. For any element $\sigma \in S^{[2]}(\mathscr{E}'_{u_0/\kappa_0(T)})$, the local restriction

$$\sigma_x \in \mathrm{H}^1(K^{\mathrm{h}}_x, \mathscr{E}'_{u_0}[2])$$

is in the image of the local Kummer map δ_x at x. Write $\sigma_x = \delta_x(\xi_x)$ for a point

$$\xi_x \in \mathscr{E}'_{u_0}(K^{\mathrm{h}}_x) = N(\mathscr{E}'_{u_0})(\mathscr{O}^{\mathrm{h}}_{\mathbf{P}^1_{\kappa_0},x}).$$

By Theorem 6.3, subtracting a suitable $\mathbf{Z}$-linear combination of $\delta(P_0')$ and $\delta(Q_0')$ from σ gives a Selmer class σ' such that $\sigma'_{\pi_1} = \delta_{\pi_1}(\xi'_{\pi_1})$, where ξ'_{π_1} reduces into the identity component at π_1. Thus, $S^{[2]}(\mathscr{E}'_{u_0/\kappa_0(T)})$ is generated by $\delta(P_0')$, $\delta(Q_0')$, and classes σ' such that $\sigma'_{\pi_1} = \delta_{\pi_1}(\xi')$ for some local point ξ' in $\mathscr{E}'_{u_0}(K^{\mathrm{h}}_{\pi_1})$ that reduces into the identity component at π_1; note that this local property of σ' at π_1 is independent of the non-canonical choice of ξ' since any two choices differ by an element in $[2](\mathscr{E}'_{u_0}(K^{\mathrm{h}}_{\pi_1}))$ and doubling on $N(\mathscr{E}'_{u_0})_{\pi_1}$ kills the component group (by Lemma 6.1).

The doubling map on $N(\mathscr{E}'_{u_0})$ is fiberwise surjective over $\mathbf{P}^1_{\kappa_0}$ away from $\{\pi_1\}$ and doubling is surjective on the additive identity component at π_1 (since $p \neq 2$). Thus, for Selmer classes σ' as above with local restriction $\sigma'_x = \delta_x(\xi'_x)$, the image of ξ'_x in $\mathscr{E}'_{u_0}(K^{\mathrm{sh}}_x)$ lies in $[2]\mathscr{E}'_{u_0}(K^{\mathrm{sh}}_x)$ for every closed point $x \in \mathbf{P}^1_{\kappa_0}$ and every choice of ξ'_x (with K^{sh}_x denoting a maximal unramified extension of K^{h}_x). In other words, the inertial restriction $\sigma'_x|_{K^{\mathrm{sh}}_x}$ is a trivial cohomology class for all x. Hence, $S^{[2]}(\mathscr{E}'_{u_0/\kappa_0(T)})$ is spanned by the images of P_0' and Q_0' and the intersection of this Selmer group with the subgroup of everywhere unramified classes in $\mathrm{H}^1(\kappa_0(T), \mathscr{E}'_{u_0}[2])$.

Let us now recall how to describe the group of everywhere unramified classes in terms of étale cohomology. Let $G = N(\mathscr{E}'_{u_0})[2]$ and $\mathbf{P} = \mathbf{P}^1_{\kappa_0}$, so G is a quasi-finite separated étale commutative $\mathbf{P}$-group. If we let $i_\eta : \eta \to \mathbf{P}$ be the canonical map from the generic point η of $\mathbf{P}$, then the identity $N(\mathscr{E}'_{u_0}) = i_{\eta*}(\mathscr{E}'_{u_0})$ on the smooth site over $\mathbf{P}$ implies $G = i_{\eta*}(G_\eta)$ as étale sheaves (by passing to 2-torsion subsheaves). Thus, using the étale topology, the Leray spectral sequence $\mathrm{E}_2^{r,s} = \mathrm{H}^r(\mathbf{P}, \mathrm{R}^s i_{\eta*}(G_\eta)) \Rightarrow \mathrm{H}^{r+s}(\eta, G_\eta)$ has $\mathrm{E}_2^{r,0} = \mathrm{H}^r(\mathbf{P}, G)$, so we get an exact sequence of low-degree terms

$$0 \to \mathrm{H}^1(\mathbf{P}, G) \stackrel{\alpha}{\to} \mathrm{H}^1(\eta, G_\eta) \stackrel{\oplus\beta_x}{\to} \bigoplus_x \mathrm{H}^0(\kappa_0(x), \mathrm{H}^1(K^{\mathrm{sh}}_x, G)). \tag{6.7}$$

Here α is the canonical restriction map to the generic point and β_x is the canonical local restriction map at the non-generic point x of $\mathbf{P}$. Hence, $\mathrm{H}^1(\mathbf{P}, G) \subseteq \mathrm{H}^1(\eta, G_\eta)$ is the group of everywhere unramified classes.

In view of the preceding considerations, to prove Theorem 6.4 it suffices to prove that the restriction map

$$\mathrm{H}^1(\kappa_0(T), \mathscr{E}'_{u_0}[2]) \to \mathrm{H}^1(\overline{\kappa}_0(T), \mathscr{E}'_{u_0}[2])$$

kills the subgroup $\mathrm{H}^1(\mathbf{P}, G)$ of everywhere unramified classes, where $G = N(\mathscr{E}'_{u_0})[2]$. We will prove the stronger assertion that the map $\mathrm{H}^1(\mathbf{P}, G) \to \mathrm{H}^1(\mathbf{P}_{\overline{\kappa}_0}, G)$ vanishes.

Let $U' = \mathbf{P} - \{\pi_2\}$ and let $j' : U' \hookrightarrow \mathbf{P}$ be the canonical open immersion. By Theorem 6.2, $G|_{U'}$ is finite étale over U' and G_{π_2} has order 2 over $\kappa(\pi_2)$. Thus, the nontrivial 2-torsion point $(0,0)$ defines a short exact sequence of étale sheaves

$$0 \to \mathbf{Z}/2\mathbf{Z} \to G \to j'_!(\mathbf{Z}/2\mathbf{Z}) \to 0 \tag{6.8}$$

over $\mathbf{P}$. By considering the exact sequence of pullback sheaves on $\mathbf{P}_{\overline{\kappa}_0} = \mathbf{P}^1_{\overline{\kappa}_0}$ and using the vanishing of $\mathrm{H}^1(\mathbf{P}^1_{\overline{\kappa}_0}, \mathbf{Z}/2\mathbf{Z})$, we arrive at a commutative square

$$\begin{array}{ccc} \mathrm{H}^1(\mathbf{P}_{\overline{\kappa}_0}, G) & \longrightarrow & \mathrm{H}^1(\mathbf{P}_{\overline{\kappa}_0}, j'_!(\mathbf{Z}/2\mathbf{Z})) \\ \uparrow & & \uparrow \\ \mathrm{H}^1(\mathbf{P}, G) & \longrightarrow & \mathrm{H}^1(\mathbf{P}, j'_!(\mathbf{Z}/2\mathbf{Z})) \end{array} \tag{6.9}$$

whose top side is injective and whose vertical maps are the natural pullback maps. It therefore suffices to prove that the pullback map on the right side vanishes, and this is a property that does not involve G.

Since $j'_!(\mathbf{Z}/2\mathbf{Z})$ is represented by an étale $\mathbf{P}$-group that is quasi-affine over $\mathbf{P}$ (it is the complement in $(\mathbf{Z}/2\mathbf{Z})_{\mathbf{P}}$ of the non-identity point over $\{\pi_2\} \in \mathbf{P}$), the elements of $\mathrm{H}^1(\mathbf{P}, j'_!(\mathbf{Z}/2\mathbf{Z}))$ are in bijection with isomorphism classes of (representable) étale $j'_!(\mathbf{Z}/2\mathbf{Z})$-torsors on $\mathbf{P}$; the same holds over $\mathbf{P}_{\overline{\kappa}_0}$, and the right side of (6.9) is thereby identified with base-change on torsors. Thus, we just need to prove that every étale $j'_!(\mathbf{Z}/2\mathbf{Z})$-torsor on $\mathbf{P}$ has a $\mathbf{P}_{\overline{\kappa}_0}$-point.

Let $i : \operatorname{Spec} \kappa_0(\pi_2) \hookrightarrow \mathbf{P}$ be the closed complement to U', so we have a short exact sequence

$$0 \to j'_!(\mathbf{Z}/2\mathbf{Z}) \to \mathbf{Z}/2\mathbf{Z} \to i_*(\mathbf{Z}/2\mathbf{Z}) \to 0 \tag{6.10}$$

of étale sheaves on $\mathbf{P}$, with $i_*(\mathbf{Z}/2\mathbf{Z})$ supported at *one* physical point on $\mathbf{P}$. Thus, the natural map

$$\mathrm{H}^1(\mathbf{P}, j'_!(\mathbf{Z}/2\mathbf{Z})) \to \mathrm{H}^1(\mathbf{P}, \mathbf{Z}/2\mathbf{Z})$$

is injective. Since $\mathrm{H}^1(\mathbf{P}, \mathbf{Z}/2\mathbf{Z}) = \mathrm{H}^1(\mathbf{P}^1_{\kappa_0}, \mathbf{Z}/2\mathbf{Z}) = \mathrm{H}^1(\kappa_0, \mathbf{Z}/2\mathbf{Z})$, clearly $\mathrm{H}^1(\mathbf{P}, \mathbf{Z}/2\mathbf{Z})$ has order 2 with its nontrivial element represented by the nontrivial $\mathbf{Z}/2\mathbf{Z}$-torsor $\mathbf{P}_{\kappa'_0} \to \mathbf{P}$ for a quadratic extension κ'_0/κ_0, and the subgroup $\mathrm{H}^1(\mathbf{P}, j'_!(\mathbf{Z}/2\mathbf{Z}))$ has order 1 or 2.

The fiber of the $\mathbf{Z}/2\mathbf{Z}$-torsor $\mathbf{P}_{\kappa'_0}$ over the point $\pi_2 \in \mathbf{P}$ is a *split* double cover of $\operatorname{Spec} \kappa_0(\pi_2)$ since $\deg_{\kappa_0} \pi_2 = 4$ and $[\kappa'_0 : \kappa_0] = 2$. Removing one of the two points over $\{\pi_2\}$ in $\mathbf{P}_{\kappa'_0}$ gives an open $\mathscr{T} \subseteq \mathbf{P}_{\kappa'_0}$ that is a nontrivial $j'_!(\mathbf{Z}/2\mathbf{Z})$-torsor over $\mathbf{P}$. Hence, $\mathrm{H}^1(\mathbf{P}, j'_!(\mathbf{Z}/2\mathbf{Z}))$ has order 2 and contains $\mathscr{T}$ as its unique nontrivial element. Since $\mathscr{T}$ obviously acquires a section upon extending the ground field κ_0 to κ'_0, we conclude that $\mathscr{T}(\mathbf{P}_{\overline{\kappa}_0})$ is nonempty. ■

Appendix A. Known results over Q

In the Introduction, we saw how to search for (conditional) examples of elevated rank over $\mathbf{Q}(T)$: assume the parity conjecture over $\mathbf{Q}$ and try to construct an elliptic curve over $\mathbf{Q}(T)$ that satisfies (1.2) for all but finitely many $t \in \mathbf{P}^1(\mathbf{Q})$. We wish to explain why this sufficient strategy is essentially necessary if we also assume three additional standard conjectures over $\mathbf{Q}$. Moreover, we will see that if all of these conjectures are true then there do not exist non-isotrivial examples of elevated rank over $\mathbf{Q}(T)$. The three additional conjectures we bring in are: the density conjecture, the squarefree-value conjecture, and Chowla's conjectures.

The *density conjecture* says that for any elliptic curve $\mathscr{E}_\eta$ over $\mathbf{Q}(T)$, the rank of $\mathscr{E}_t(\mathbf{Q})$ equals $\operatorname{rank}(\mathscr{E}_\eta(\mathbf{Q}(T)))$ or $\operatorname{rank}(\mathscr{E}_\eta(\mathbf{Q}(T)))+1$ except for a set of $t \in \mathbf{P}^1(\mathbf{Q})$ with density 0, as measured by height. Granting this and the parity conjecture, any example of elevated rank over $\mathbf{Q}(T)$ will satisfy (1.2) for all t outside of a set of density 0. Therefore, if $\mathscr{E}_\eta$ has elevated rank then the average value of $W(\mathscr{E}_t)$, in the sense of the following definition, is either 1 or -1.

Definition A.1. For any elliptic curve $\mathscr{E}_\eta$ over $\mathbf{Q}(T)$, its *average root number* is

$$\operatorname{Avg}_{\mathbf{Q}} W(\mathscr{E}_t) := \lim_{N\to\infty} \frac{\sum_{t\in\mathbf{P}^1(\mathbf{Q}), h_{\mathbf{Q}}(t)<N} W(\mathscr{E}_t)}{\#\{t \in \mathbf{P}^1(\mathbf{Q}), h_{\mathbf{Q}}(t) < N\}} \tag{A.1}$$

if this limit exists, where $h_{\mathbf{Q}}$ is the standard logarithmic height function on $\mathbf{P}^1(\mathbf{Q})$ (defined by the standard normalized collection of absolute values on $\mathbf{Q}$). In the summation, the finitely many t at which $\mathscr{E}_t$ is non-smooth are dropped out.

The existence of the average root number is not evident *a priori*, and its value might depend on the choice of coordinate on $\mathbf{P}^1$. (The height $h_{\mathbf{Q}}$ depends on the coordinate.) If the average exists, then clearly $-1 \leq \mathrm{Avg}_{\mathbf{Q}} W(\mathscr{E}_t) \leq 1$. If we assume the parity and density conjectures then any example of elevated rank over $\mathbf{Q}(T)$ must have average root number 1 or -1.

Remark A.2. For any elliptic curve E_0 over $\mathbf{Q}$, Rizzo [24] proved that the set of average root numbers that unconditionally exist for quadratic twists of E_0 over $\mathbf{Q}(T)$ is dense in the interval $[-1, 1]$.

We now introduce the squarefree-value conjecture and Chowla's conjectures; these lead to a formula for $\mathrm{Avg}_{\mathbf{Q}} W(\mathscr{E}_t)$ for any elliptic curve $\mathscr{E}_\eta$ over $\mathbf{Q}(T)$. This formula turns out never to equal 1 or -1 for non-isotrivial elliptic curves over $\mathbf{Q}(T)$, thereby (conditionally) ruling out the possibility of elevated rank for such elliptic curves.

The *squarefree-value conjecture* says that a polynomial over $\mathbf{Z}$ takes squarefree values as often as is suggested by naive probabilistic heuristics. For example, if $f(T) \in \mathbf{Z}[T]$ is squarefree, then the prediction is

$$\#\{1 \leq n \leq x : f(n) \text{ is squarefree}\} \sim Cx$$

as $x \to \infty$, where $C = \prod_p \left(1 - c_p/p^2\right)$ with c_p denoting the number of solutions to $f(T) = 0$ in $\mathbf{Z}/(p^2)$. (If $1 - c_p/p^2 = 0$ for some p, then $C = 0$ and obviously $f(n)$ is never squarefree. Otherwise C is an absolutely convergent (positive) product.) We refer the reader to work of Granville [9] for a more complete statement of this conjecture, including the variant for homogeneous polynomials in two variables over $\mathbf{Z}$. The squarefree-value conjecture is known unconditionally for polynomials in $\mathbf{Z}[T]$ with small degree, and Granville [9] deduced the general case (all degrees) from the *abc*-conjecture. (Poonen [22] extended these results to polynomials in any number of variables over $\mathbf{Z}$, but only the cases treated by Granville in one and two variables are related to the variation of root numbers in pencils of elliptic curves over $\mathbf{Q}$.)

Remark A.3. Low-degree proved instances of the squarefree-value conjecture were used in the study of ranks of elliptic curves over $\mathbf{Q}$ in [8], where families of quadratic twists were considered.

The final conjecture we need over $\mathbf{Q}$, due to Chowla [3, p. 96] in the one-variable case, concerns the average behavior of the Liouville function on values of a polynomial. Recall that Liouville's function λ is the totally multiplicative function on $\mathbf{Z}$ defined by $\lambda(\pm p) = -1$ when p is prime, $\lambda(\pm 1) = 1$, and $\lambda(0) = 0$.

The *one-variable Chowla conjecture* says that for any non-constant $f(T)$ in $\mathbf{Z}[T]$ which is not a perfect square up to sign, the sequence $\lambda(f(n))$ has average value 0 as n runs over any arithmetic progression. That is, for any arithmetic progression $a + b\mathbf{Z}$ (with $a \in \mathbf{Z}$ and $b \in \mathbf{Z}$, $b \neq 0$), as $N \to \infty$ we have

$$\frac{\sum_{n \in (a+b\mathbf{Z}) \cap [0,N]} \lambda(f(n))}{\#((a + b\mathbf{Z}) \cap [0, N])} \to 0.$$

(Clearly, with a linear change of variables, we can state this as a conjecture over all f using only $a = 0$ and $b = 1$. We prefer the above superficially more general form because it matches the two-variable conjecture more closely.)

The *two-variable Chowla conjecture* says that for any non-constant homogeneous f in $\mathbf{Z}[U, V]$ which is not a perfect square up to sign, the sequence $\lambda(f(m, n))$ has average value 0 as (m, n) runs over lattice points in any sector of the plane with vertex at the origin. More precisely, for any coset $L \subseteq \mathbf{Z}^2$ of an arbitrary sublattice of $\mathbf{Z}^2$, and any open sector $S \subseteq \mathbf{R}^2$ with positive angular measure and vertex at the origin,

$$\frac{\sum_{(m,n)\in S\cap L\cap[-N,N]^2} \lambda(f(m,n))}{\#(S \cap L \cap [-N, N]^2)} \to 0 \tag{A.2}$$

as $N \to \infty$. If the condition $(m, n) = 1$ is imposed on the terms in the sum in (A.2), then the resulting general conjecture is logically equivalent to the general conjecture (A.2).

In [12] and [13], the squarefree-value conjecture and the two-variable Chowla conjecture are used to derive (conditional) formulas for $\mathrm{Avg}_{\mathbf{Q}} W(\mathscr{E}_t)$ for any $\mathscr{E}_{\eta/\mathbf{Q}(T)}$. The analysis falls into two cases:

Case 1: The minimal regular proper model $\mathscr{E} \to \mathbf{P}^1_{\mathbf{Q}}$ has no nodal geometric fiber. (That is, $\mathscr{E}_\eta$ has no point of multiplicative reduction on $\mathbf{P}^1_{\mathbf{Q}}$.)

Case 2: The fibration $\mathscr{E} \to \mathbf{P}^1_{\mathbf{Q}}$ has a nodal geometric fiber.

Consider a non-isotrivial $\mathscr{E}_{\eta/\mathbf{Q}(T)}$ in Case 1. Let M_t denote the finite set of primes $p \in \mathbf{Z}$ such that $\mathscr{E}_t$ has multiplicative reduction at p. The collection $\{M_t\}_{t\in\mathbf{P}^1(\mathbf{Q})}$ is restricted as t varies, in the following sense. Assuming the square-free value conjecture, we have that, for any small $\varepsilon > 0$, there is a finite set of prime numbers $\mathcal{S}_\varepsilon$ such that the set of $t \in \mathbf{P}^1(\mathbf{Q})$ with $M_t \subseteq \mathcal{S}_\varepsilon$ has height density $\geq 1 - \varepsilon$. That is, roughly speaking, "most" fibers have their primes of multiplicative reduction lying in a common finite set. (This remark is implicit in [20, Lemma 2.1].) Moreover, for such t the bad primes for $\mathscr{E}_{t/\mathbf{Q}}$ outside of $\mathcal{S}_\varepsilon$ are the prime factors of values of certain irreducible primitive polynomials over $\mathbf{Z}$ that correspond to the points of additive reduction for $\mathscr{E}_\eta$ on $\mathbf{P}^1_{\mathbf{Q}}$. (In particular, these primitive polynomials are independent of t and ε.) For the study of average root numbers of elliptic curves over $\mathbf{Q}$, the essential difference between additive and multiplicative reduction is the simpler statistical variation for local root numbers in the additive case. (See the formulas in Theorem 3.1.) Assuming the squarefree-value conjecture, for "most" t the set of bad primes for $\mathscr{E}_t$ outside of $\mathcal{S}_\varepsilon$ can be controlled, and a formula

$$\mathrm{Avg}_{\mathbf{Q}} W(\mathscr{E}_t) = C_\infty \prod_p C_p \tag{A.3}$$

is thereby obtained, where C_∞ is an algebraic number in $\mathbf{R}$, each C_p is a non-zero rational number, and $\prod_p C_p$ is an absolutely convergent (non-zero) product.

Here are two examples that illustrate (A.3) (not elevated rank) for non-isotrivial elliptic curves in Case 1.

Example A.4. An example of Washington [34, §3] over $\mathbf{Q}(T)$ is

$$\mathscr{E}_\eta : y^2 = x^3 + Tx^2 - (T + 3)x + 1. \tag{A.4}$$

The point $(0, 1)$ on this curve has infinite order (use Theorem 2.4, as in the proof of Corollary 2.6). Since $\mathscr{E}$ is a rational surface, it is not difficult to prove (using either analytic methods of Rosen–Silverman or a reduction to positive characteristic and algebraic methods of Artin–Tate) that $\mathscr{E}_\eta(K(T))$ has rank 1 for every number field K.

In [25], Rizzo shows $W(\mathscr{E}_t) = -1$ for every $t \in \mathbf{Z}$. However, $W(\mathscr{E}_t) = 1$ for many non-integral $t \in \mathbf{Q}$, such as (using PARI) $t = -1/2, 1/3$, and $3/2$. An application of one of the proved instances of the squarefree-value conjecture in low degree shows that (A.3) is unconditionally true for $\mathscr{E}_\eta$ in (A.4), and a computation yields $C_\infty = 0$. Therefore, in this example, $\mathrm{Avg}_{\mathbf{Q}} W(\mathscr{E}_t) = 0$ unconditionally.

Example A.5. Let $f(T) = -5 - 2T^2$ and $g(T) = 2 + 5T^2$. Consider

$$\mathscr{E}_\eta : y^2 = x^3 + a(T)x + b(T)$$

over $\mathbf{Q}(T)$, where

$$a(T) = -27fg(f^3 - g^3)^2, \;\; b(T) = -\frac{54(f^3 + g^3)(f^3 - g^3)^3}{2}.$$

Low-degree proved instances of the squarefree-value conjecture imply that the conditional formula (A.3) is true for this $\mathscr{E}_\eta$. This leads to the explicit formula

$$\mathrm{Avg}_{\mathbf{Q}} W(\mathscr{E}_t) = \frac{1}{6} \cdot \prod_{p \neq 2,3,7,19} \left(1 - \frac{a_p}{(p+1)^2}\right) = 0.1527\ldots,$$

where $a_p = 1 + \chi_p(-1) + (1 + \chi_3(p))(1 + \chi_{19}(p))$ and χ_ℓ is the mod ℓ Legendre symbol.

A closer analysis of the work that leads to (A.3) in Case 1 shows that if the squarefree-value conjecture is assumed then $\mathrm{Avg}_{\mathbf{Q}} W(\mathscr{E}_t)$ *cannot* equal 1 or -1 in Case 1 when $\mathscr{E}_\eta$ is non-isotrivial. Therefore, if the density conjecture, parity conjecture, and squarefree-value conjecture are true, then in Case 1 there does not exist a non-isotrivial elliptic curve over $\mathbf{Q}(T)$ with elevated rank.

We turn now to Case 2, so $\mathscr{E} \to \mathbf{P}^1_{\mathbf{Q}}$ has a nodal geometric fiber. Such $\mathscr{E}$ must be non-isotrivial. The reasoning in Case 1 breaks down, since there do not exist sets of t with height density arbitrarily close to 1 such that the $\mathscr{E}_{t/\mathbf{Q}}$'s have multiplicative reduction in a common finite set of primes. Now there is a non-constant homogeneous two-variable polynomial $f_{\mathscr{E}} \in \mathbf{Z}[U, V]$, which is not a square up to sign, such that as $t \in \mathbf{P}^1(\mathbf{Q})$ varies with $\mathscr{E}_{t/\mathbf{Q}}$ smooth, the variation of the product of the local root numbers of $\mathscr{E}_{t/\mathbf{Q}}$ at the places of multiplicative reduction is governed by the variation of $\lambda(f_{\mathscr{E}}(m, n))$ where m/n is the reduced form of t. In our function field examples we have a similar conclusion, with the Liouville function on $\kappa[u]$ that assigns value -1 to irreducibles and extends to all of $\kappa[u]$ by total multiplicativity; see Remark 3.3. If we assume Chowla's two-variable conjecture for $f_{\mathscr{E}}$, then the variation of $\lambda(f_{\mathscr{E}}(m, n))$ as $t = m/n$ varies can be controlled. Using this, in [12, §1.7] it is shown that if the squarefree-value conjecture is also assumed, then $\mathrm{Avg}_{\mathbf{Q}} W(\mathscr{E}_t)$ exists and equals 0; in particular, this average does not equal 1 or -1. Thus, the parity, density, squarefree-value, and Chowla conjectures predict that no elliptic curve in Case 2 has elevated rank.

Our discussion of $\mathrm{Avg}_{\mathbf{Q}} W(\mathscr{E}_t)$ has shown that if we assume the squarefree-value conjecture and Chowla's two-variable conjecture then this average cannot equal 1 or -1 if $\mathscr{E}_\eta$ is non-isotrivial. If we accept the parity conjecture and the density conjecture, then any example of elevated rank over $\mathbf{Q}(T)$ has $\mathrm{Avg}_{\mathbf{Q}} W(\mathscr{E}_t) = 1$ or -1. Therefore, if all four conjectures are true then all examples of elevated rank over $\mathbf{Q}(T)$ must be isotrivial.

Appendix B. The surprise in characteristic p

We now replace $\mathbf{Q}$ with $F = \kappa(u)$ and replace $\mathbf{Z}$ with $\kappa[u]$, where κ is any finite field. For the moment, κ may have characteristic 2. Granting the parity conjecture over F, no new ideas should be required to construct isotrivial examples of elevated rank over $F(T)$ analogous to the examples of Cassels–Schinzel and Rohrlich. (The case of characteristic 2 is presumably more delicate.) We want to explain why it is reasonable to expect *a priori* that non-isotrivial examples of elevated rank might exist over $F(T)$, despite the conclusions over $\mathbf{Q}(T)$ in Appendix A.

The squarefree-value conjecture for multivariable polynomials over $\kappa[u]$, for κ with any characteristic, was proved by Ramsay [23] in the separable case for one variable, and was proved by Poonen [22] in general. Thus, provided that $\mathrm{char}(F) \neq 2, 3$ (to avoid problems with wild ramification at arbitrarily many places), the methods used over $\mathbf{Q}(T)$ can be adapted to prove an *unconditional* formula akin to (A.3) in the analogue of Case 1 in Appendix A. (This is the case of elliptic curves $\mathscr{E}_{\eta/F(T)}$ such that $\mathscr{E} \to \mathbf{P}^1_F$ does not have any nodal geometric fibers.) However, to adapt the $\mathbf{Q}(T)$-methods to prove that $\mathrm{Avg}_F W(\mathscr{E}_t)$ is strictly between 1 and -1 for a non-isotrivial $\mathscr{E} \to \mathbf{P}^1_F$ without nodal fibers, we need to impose a restriction that is always satisfied in characteristic 0: the points in the (non-empty) support of the conductor of $\mathscr{E}_\eta$ on $\mathbf{P}^1_F$ are étale over F. We expect that if this étale restriction on the support of the conductor is dropped, then there should be non-isotrivial examples without nodal geometric fibers such that the average root number is 1 or -1. Moreover, in all positive characteristics there should exist such examples that also have elevated rank (granting the parity conjecture).

Let us now turn to the analogue of Case 2 from Appendix A, so $\mathscr{E} \to \mathbf{P}^1_F$ has some nodal geometric fibers. The study of such elliptic fibrations in characteristic 0 uses Chowla's conjectures over $\mathbf{Z}$, as we saw in Appendix A. However, there are counterexamples to the $\kappa[u]$-analogues of Chowla's conjectures. In [4], it is shown that counterexamples to Chowla's one-variable conjecture are a common phenomenon. For example, elementary (but non-obvious) methods show that for any finite field κ with arbitrary characteristic p, $f(T) = T^{4p} + u \in \kappa[u][T]$ violates the one-variable Chowla conjecture: $\lambda(f(g)) = 1$ for every $g \in \kappa[u]$ with $g \notin \kappa$. Similarly, in the sense of Chowla's two-variable conjecture, the homogeneous polynomial

$$aX^{4p} + buY^{4p} \in \kappa[u][X, Y]$$

with $a, b \in \kappa^\times$ has rather non-random λ-values:

$$\lambda(ag_1^{4p} + bug_2^{4p}) = \begin{cases} -1 & \text{if } \deg g_1 \leq \deg g_2, \\ 1 & \text{if } \deg g_1 > \deg g_2, \end{cases} \tag{B.1}$$

for any $g_1, g_2 \in \kappa[u]$ not both zero, using the convention $\deg 0 = -\infty$. (If $p \neq 2$ then (B.1) is a special case of Lemma 3.5, replacing g_1 and g_2 in that lemma with their squares. We omit the additional considerations that are required to verify (B.1) when $p = 2$.) In particular, $\lambda(ag_1^{4p} + bug_2^{4p})$ only depends on the sign of $\mathrm{ord}_\infty(g_1/g_2) = \deg g_2 - \deg g_1$. The proof of Theorem 1.1 rests on a similar counterexample to Chowla's two-variable conjecture, with exponent $2p$ rather than $4p$. (See (3.17).) The failure of Chowla's conjecture in positive characteristic was our initial clue to the possibility that elevated rank may occur in non-isotrivial families in the function field case.

References

[1] J. W. S. Cassels, A. Schinzel, "Selmer's conjecture and families of elliptic curves," *Bull. London Math. Soc.* **14** (1982), 345–348.

[2] J. W. S. Cassels, "Second descents for elliptic curves," *J. Reine Angew. Math.* **494** (1998), 101–127.

[3] S. Chowla, *The Riemann hypothesis and Hilbert's tenth problem*, Gordon and Breach, New York, 1965.

[4] B. Conrad, K. Conrad, R. Gross, "Prime Specialization in Genus 0," submitted.
[5] B. Conrad, "Chow's K/k-image and K/k-trace, and the Lang–Néron theorem," submitted.
[6] P. Deligne, "Les constantes des équations fonctionelles des fonctions L," pp. 501–595 in *Modular Functions of One Variable*, II, Lecture Notes in Mathematics 349, Springer–Verlag, New York, 1973.
[7] G. Faltings, "Finiteness theorems for abelian varieties over number fields," Ch. II in *Arithmetic geometry* (Cornell/Silverman, ed.), Springer-Verlag, 1986.
[8] F. Gouvea, B. Mazur, "The square-free sieve and the rank of elliptic curves," *J. Amer. Math. Soc.* **4** (1991), 1–23.
[9] A. Granville, "*ABC* allows us to count squarefrees," *Internat. Math. Res. Notices* no. 19 (1998), 991–1009.
[10] A. Grothendieck, "Eléments de géométrie algébrique," *Publ. Math. IHES*, **4, 8, 11, 17, 20, 24, 28, 32** (1961-7).
[11] A. Grothendieck, "Séminaire de géométrie algébrique 3", Springer Lecture Notes **151**, Springer-Verlag, New York, 1963.
[12] H. A. Helfgott, "Root numbers and the parity problem," Ph.D. thesis, Princeton University, `http://www.arxiv.org/abs/math.NT/0305435`.
[13] H. A. Helfgott, "On the behaviour of root numbers in families of elliptic curves," submitted.
[14] A. J. de Jong, N. M. Katz, "Monodromy and the Tate conjecture: Picard numbers and Mordell–Weil ranks in families," *Israel J. Math.* **120** (2000), 47–79.
[15] K. Kato, F. Trihan, "On the conjectures of Birch and Swinnerton-Dyer in characteristic $p > 0$," *Invent. Math.* **153** (2003), 537–592.
[16] S. Kochen, "Integer-valued rational functions over the p-adic numbers: A p-adic analogue of the theory of real fields," in 1969 Number Theory (Proc. Sympos. Pure Math., Vol. XII) 57–73, Amer. Math. Soc. Providence, RI, 1969.
[17] S. Lang, A. Néron, "Rational points on abelian varieties over function fields," *American J. Math.* **81** (1959), 95–118.
[18] S. Lang, *Abelian varieties*, Interscience, New York, 1959.
[19] Q. Liu, *Algebraic geometry and arithmetic curves*, Oxford University Graduate Texts in Mathematics **6**, Oxford University Press, Oxford, 2002.
[20] E. Manduchi, "Root numbers of fibers of elliptic surfaces", *Compositio Math.* **99** (1995) no. 1, 33–58.
[21] J. Nekovář, "On the parity of ranks of Selmer groups. II," *C. R. Acad. Sci. Paris Sér. I Math.* **332** (2001), no. 2, 99–104.
[22] B. Poonen, "Squarefree values of multivariable polynomials," *Duke Math. J.* **118** (2003), 353–373.
[23] K. Ramsay, "Squarefree values of polynomials in one variable over function fields," *International Math. Res. Notices* no. 4 (1992), 97–102.
[24] O. Rizzo, "Average root numbers in families of elliptic curves," *Proc. Amer. Math. Soc.* **127** (1999), 1597–1603.
[25] O. Rizzo, "Average root numbers for a non-constant family of elliptic curves," *Compositio Math.* **136** (2003), 1–23.
[26] D. E. Rohrlich, "Variation of the root number in families of elliptic curves," *Compositio Math.* **87** (1993), 119–151.
[27] D. E. Rohrlich, "Elliptic curves and the Weil-Deligne group," in *Elliptic curves and related topics*, 125–157, CRM Proc. Lecture Notes **4** Amer. Math Soc., Providence, RI, 1994.
[28] D.E. Rohrlich, "Galois theory, elliptic curves, and root numbers," *Compositio Math.* **100** (1996), 311–349.
[29] K. Rubin, A. Silverberg, "Ranks of elliptic curves," *Bull. Amer. Math. Sci.* **39** (2002), 455–474.
[30] J. Silverman, "Heights and the specialization map for families of abelian varieties," *J. Reine Angew. Math.* **342** (1983), 197–211.
[31] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.
[32] R. G. Swan, "Factorization of polynomials over finite fields," *Pacific J. Math.* **12** (1962), 1099–1106.
[33] J. Tate, "Number theoretic background," pp. 3–26 in: *Automorphic Forms, Representations, and L-functions*, Proc. Symp. Pure Math. **33** Part 2, Amer. Math. Soc., Providence, 1979.
[34] L. Washington, "Class numbers of the simplest cubic fields," *Math. Comp.* **48** (1987), pp. 371–384.

Department of Mathematics, Univ. of Michigan, Ann Arbor, MI 48109-1109, USA
E-mail address: bdconrad@umich.edu

Department of Mathematics, Univ. of Connecticut, Storrs, CT 06269-3009, USA
E-mail address: kconrad@math.uconn.edu

Département de Mathématiques et Statistique, Université de Montréal, Montréal, QC H3C 3J7, Canada
E-mail address: helfgott@dms.umontreal.ca