ACTA ARITHMETICA
161.4 (2013)

Elliptic curves over function fields with a large set of integral points

by

Ricardo P. Conceição (Oxford, GA)

1. Introduction. Inspired by the work of Caporaso, Harris and Mazur [4], Abramovich [1] asked if there could exist a uniform bound for the number of integral points on elliptic curves over the rationals (¹). As he pointed out, this cannot be a true statement: simply choose any elliptic curve with positive rank, and make a change of coordinates to "clean the denominators" of an arbitrary number of rational points. This kind of construction forces a change on the integral model of the elliptic curve, and it is natural to ask whether some kind of uniformity on the number of integral points holds if the integral model is restricted. Abramovich [1, Theorem 2] gives a positive answer to this question for stably minimal models of elliptic curves over $\mathbb{Q}$ under the assumption of the following conjecture.

Conjecture 1.1 (Lang–Vojta). *Let X be a variety of log-general type defined over $\mathbb{Q}$ and let $\mathcal{X}$ be any model of X over $\mathbb{Z}$. Then the set of integral points $\mathcal{X}(\mathbb{Z})$ is not Zariski dense in $\mathcal{X}$.*

Here we focus on the following simpler (but already non-trivial) uniformity result, which is also a consequence of the Lang–Vojta conjecture.

Theorem 1.2 ([1, Section 3]). *Let $y^2 = x^3 + Ax + B$ be an elliptic curve with A and B integers. Suppose the Lang–Vojta conjecture is true over $\mathbb{Q}$. Then for any square-free non-zero integer D, the number of integral points on the quadratic twist $Dy^2 = x^3 + Ax + B$ is bounded independently of D.*

Our present work follows a long tradition in arithmetic geometry of testing the plausibility of a statement over number fields by working with

2010 *Mathematics Subject Classification*: 11G05, 11G35, 14H05.
Key words and phrases: elliptic curves, integral points, Lang–Vojta conjecture, function fields.

(¹) Our discussion here holds over general number fields, but for simplicity of exposition we only give the statements over $\mathbb{Q}$.

an analogous statement over function fields in positive characteristic. Inspired by Theorem 1.2, we give a negative answer to the analogous question of whether there is a uniform bound for the number of separable integral points (²) on quadratic twists of elliptic curves over $\mathbb{F}_q(t)$.

THEOREM 1.3 (cf. Corollary 4.4). *Let n be a positive integer. Then over $\mathbb{F}_q(t)$ the following elliptic curves have a separable integral point for every odd divisor of n:*

(1) $(t^{q^n} - t)y^2 = x^3 - x$ *when* $q \equiv 3 \bmod 4$.
(2) $y^2 - y = (t^{q^n} - t)x^3$ *when* $q \equiv 2 \bmod 3$.

In particular, if we take n with a large number of odd divisors, we obtain examples of quadratic and cubic twists of elliptic curves with a large number of separable integral points.

These are not the only examples of elliptic curves for which this type of unboundedness result holds. Theorems 4.7 and 5.1 provide other examples of isotrivial and non-isotrivial elliptic curves with an arbitrarily large set of separable integral points.

In light of Theorem 1.2 and our results on the unboundedness of the number of integral points on elliptic curves over $\mathbb{F}_q(t)$, one could ask whether our construction can be used to produce counterexamples to a natural analogue of the Lang–Vojta conjecture over function fields. We show that this is possible in the isotrivial case.

THEOREM 1.4 (cf. Section 6). *Suppose $q \equiv 3 \bmod 4$. The affine variety defined over $\mathbb{F}_q(t)$ by*

$$z^2 = (x^3 - x)(y^3 - y)$$

is of log-general type and has a Zariski dense set of separable integral points.

In a different direction, we present an application of our results that stems from another conjecture of Lang [7, Conjecture 0.5]. This conjecture predicts that for a quasi-minimal model E of an elliptic curve over $\mathbb{Q}$, we have $|E(\mathbb{Z})| < c^r$, where c is an absolute constant and r is the rank of $E(\mathbb{Q})$. Consequently, one can argue that integral points on quasi-minimal model of elliptic curves over $\mathbb{Q}$ tend to be linearly independent. Here we present more evidence in support of this claim by proving that the explicit separable integral points constructed in Theorem 1.3 are linearly independent. In particular, this proves the existence of quadratic twists of supersingular elliptic curves with arbitrarily high rank over $\mathbb{F}_q(t)$. This well known result was first proved by Shafarevich and Tate [11]. One advantage of our construction over theirs is that we explicitly produce a large set of linearly independent points. This is an advantage that still holds in comparison to previous constructions

(²) See Section 2 for the definition of a separable integral point.

(see [2, 3, 5, 6, 12]). Only recently, Ulmer [14, 15] has provided examples of explicit points on non-isotrivial elliptic curves over $\mathbb{F}_q(t)$ that generate a subgroup of the Mordell–Weil group with finite index and large rank. In a future work, we will show that our construction may also be used to produce other examples of elliptic curves with this property.

We finish this introduction by saying a few words about the organization of this work. In Sections 2 and 3, we set notation and describe the construction that is used to produce elliptic curves with an explicit rational point. Sections 4 and 5 contain our examples of isotrivial and non-isotrivial elliptic curves with a large set of separable integral points. In Section 6, we give a proof of Theorem 1.4; and Section 7 deals with a proof of the unboundedness of the rank of the elliptic curves described in Theorem 1.3.

2. On the arithmetic of isotrivial elliptic curves

Terminology. Henceforth, q denotes a power of an *odd* prime p, $\mathbb{F}_q(t)$ is a rational function field and F' denotes the formal derivative of an element F of $\mathbb{F}_q(t)$ with respect to t.

Many of the classical finiteness results in arithmetic geometry over number fields do not translate literally to the function field setting. The aim of this section is to address some of the subtleties inherent to the function field setting and to establish notation.

We say that a point on an affine variety $V/\mathbb{F}_q(t)$ is an *integral point* if all of its coordinates lie in $\mathbb{F}_q[t]$. In contrast with Siegel's theorem over $\mathbb{Q}$, there are elliptic curves over $\mathbb{F}_q(t)$ with an infinite set of integral points.

Example 2.1. Let $D = D(t)$ be a square-free polynomial over $\mathbb{F}_q$ and $E_D : Dy^2 = f(x)$ be an elliptic curve with $f(x)$ a cubic polynomial over $\mathbb{F}_q$. If (x, y) is an integral point on E_D then

$$\{(x^{q^i}, D^{(q^i-1)/2}y^{q^i}) : i \in \mathbb{N}\} \tag{2.1}$$

is an infinite set of integral points on E_D.

Such a phenomenon needs to be taken into account when considering an analogue over $\mathbb{F}_q(t)$ to the uniformity result given by the conclusion of Theorem 1.2. To that end, we discuss some properties of isotrivial varieties over $\mathbb{F}_q(t)$.

Definition 2.2. A variety V defined over $\mathbb{F}_q(t)$ is said to be *isotrivial* if it is isomorphic to a constant variety after a finite base extension; that is, there exists a variety V_0 defined over $\mathbb{F}_q$ such that $V \times_{\operatorname{Spec}\mathbb{F}_q(t)} \operatorname{Spec} K \cong V_0 \times_{\operatorname{Spec}\mathbb{F}_q(t)} \operatorname{Spec} K$ for some finite extension $K/\mathbb{F}_q(t)$. In this case, we say that V is *based on* V_0. A variety that is not isotrivial is called *non-isotrivial.*

Definition 2.3. Let V be an isotrivial variety based on V_0. The *Frobenius endomorphism* of V is the map defined by

$$\phi^{-1} \circ \mathbf{F} \circ \phi : V \to V,$$

where $\phi : V \to V_0$ is an isomorphism given by the isotriviality of V, and $\mathbf{F}$ is the Frobenius endomorphism of the constant variety V_0.

The set $\mathrm{Orb}(P) := \{\mathbf{F}^i(P) : i \in \mathbb{N}\}$ is called the *Frobenius orbit* of the point $P \in V$.

Remark 2.4. (1) Notice that the Frobenius endomorphism need not be defined over $\mathbb{F}_q(t)$ and is well defined up to conjugation by elements of $\mathrm{Aut}(V)$.

(2) In Example 2.1, we see that the set defined by (2.1) is the Frobenius orbit of the point (x, y) on E_D.

(3) We note that if P is an integral point on an isotrivial elliptic curve E, then $\mathbf{F}(P)$ need not be an integral point. In fact, let $D = D(t)$ be a polynomial over $\mathbb{F}_q$ and let $E/\mathbb{F}_q(t)$ be the elliptic curve defined by $y^2 = x^3 + D$. Then E is an isotrivial elliptic curve based on the elliptic curve defined over $\mathbb{F}_q$ by $y^2 = x^3 + 1$. It is not hard to see that the Frobenius endomorphism of E is given by $\mathbf{F}(x, y) = (x^q D^{(-q+1)/3}, y^q D^{(-q+1)/2})$.

The Frobenius orbit of an integral point may or may not contain an infinite number of integral points. In any case, a finiteness result analogous to Siegel's theorem exists over $\mathbb{F}_q(t)$ if, instead of counting integral points, we count the number of *separable integral points.*

Definition 2.5. A point P on a variety $V/\mathbb{F}_q(t)$ is said to be *separable* if it is not contained in the Frobenius orbit of any other point of V.

Remark 2.6. Notice that if V is non-isotrivial then every point is a separable point.

Example 2.7. Assume the hypotheses of Example 2.1. Suppose $P = (x, y)$ is a point on the quadratic twist $Dy^2 = f(x)$. Then P is separable if, and only if, $x' \neq 0$.

Next we provide a simple proof of the finiteness of the number of separable integral points on quadratic twists of constant elliptic curves. This result shows that it is appropriate to ask whether the number of separable integral points on a family of isotrivial quadratic twists can be uniformly bounded.

Theorem 2.8. *Let $D = D(t)$ and $f = f(x)$ be square-free polynomials defined over $\mathbb{F}_q$. Suppose* $\deg f = 3$ *and (F, G) is a separable integral point on $Dy^2 = f(x)$ over $\mathbb{F}_q(t)$. Then G divides F' and* $\deg D/3 \leq \deg F < \deg D - 1$.

In particular, the set of separable integral points on $Dy^2 = f(x)$ is finite.

Proof. Since $(F,G) = (F(t),G(t))$ is a separable point, Example 2.7 shows that $F' \neq 0$. This integral point induces an identity on $\mathbb{F}_q[t]$:

$$D(t)G(t)^2 = f(F(t)). \tag{2.2}$$

By equating degrees in this identity we obtain the lower bound $\deg D \leq 3\deg F$. By differentiating equation (2.2) we are led to

$$D'(t)G(t)^2 + 2D(t)G(t)G'(t) = F'(t)f'(F(t)). \tag{2.3}$$

Let β be a root of $G(t)$ of multiplicity r. By (2.2), we see that $(t-\beta)^r$ divides $f(F(t))$, and by (2.3), we conclude that $(t-\beta)^r$ divides $F'(t)f'(F(t))$. Notice that $(t-\beta, f'(F(t))) = 1$, since $f(x)$ has no repeated roots. Hence $(t-\beta)^r$ divides $F'(t)$ and, as a consequence, $G(t)$ divides $F'(t)$. Therefore $\deg G \leq \deg F - 1$. After equating degrees in (2.2) and using the previous inequality, we obtain the desired upper bound on $\deg F$. ∎

3. Obtaining multisections on certain elliptic surfaces. Our main objective is to construct elliptic curves containing an arbitrary number of separable integral points. We show in this section that an adaptation of a procedure due to T. Shioda can be used as a first step towards this purpose.

Let k be any field. In [9, Section 2], Shioda considers surfaces in $\mathbb{P}^3_k$ that are defined by four monomials

$$\mathcal{X}_A = \mathcal{X}_A(c_0,c_1,c_2,c_3) : \sum_{i=0}^{3} c_i X_0^{a_{i0}} X_1^{a_{i1}} X_2^{a_{i2}} X_3^{a_{i3}} = 0, \tag{3.1}$$

where $A = (a_{ij})_{0\leq i,j\leq 3}$ is a 4×4 matrix with non-negative integral coefficients. Shioda calls $\mathcal{X}_A$ a *Delsarte surface* with matrix A when it satisfies

- $\det A \neq 0$ in k;
- $\sum_{j=0}^{3} a_{ij}$ is independent of $i = 0,1,2,3$;
- for any j, some a_{ij} is 0.

Notice that the surface defined by

$$c_0X_0^d + c_1X_1^d + c_2X_2^d + c_3X_3^d = 0$$

is a Delsarte surface with matrix dI_4, where I_4 is the identity matrix of dimension 4. In this case we will denote $\mathcal{X}_{dI_4}$ simply by $\mathcal{F}_d$ and we will refer to it as a *Fermat surface of degree d*.

For any Delsarte surface $\mathcal{X}_A = \mathcal{X}_A(c_0,c_1,c_2,c_3)$, A^{-1} is a 4×4 matrix with rational entries. If $\mathcal{X}_C = \mathcal{X}_C(c_0,c_1,c_2,c_3)$ is another Delsarte surface then there exists an integer d such that $B = dA^{-1}C = (b_{ij})_{0\leq i,j\leq 3}$ has integer entries. This easily implies the existence of a dominant rational map

$\mathcal{X}_{dC} \dashrightarrow \mathcal{X}_A$ defined by

$$(X_0, X_1, X_2, X_3) \mapsto \Big(\prod_{j=0}^{3} X_j^{b_{0j}}, \prod_{j=0}^{3} X_j^{b_{1j}}, \prod_{j=0}^{3} X_j^{b_{2j}}, \prod_{j=0}^{3} X_j^{b_{3j}} \Big).$$

In particular, for any Delsarte surface $\mathcal{X}_A$ there exists an integer d and a dominant rational map $\mathcal{F}_d \dashrightarrow \mathcal{X}_A$ from a Fermat surface of degree d.

In what follows we deal with surfaces which are not necessarily Delsarte surfaces. Nonetheless, we can associate to them a matrix of exponents and use the above procedure to construct explicit dominant rational maps among them. Ultimately we use these rational maps to construct non-constant sections on certain elliptic surfaces with a fibration over $\mathbb{P}^1_k$. But before we present these examples, we recall briefly some facts about elliptic surfaces that will be used in our discussion.

Let $K = k(t)$ be a rational function field and E/K be an elliptic curve. Associated to E is a fibered elliptic surface $\pi : \mathcal{E} \to \mathbb{P}^1_k$, as described in [13, Lecture 3]. A *section* of $\mathcal{E}$ is a k-rational morphism $P : \mathbb{P}^1_k \to \mathcal{E}$ such that $\pi \circ P : \mathbb{P}^1_k \to \mathbb{P}^1_k$ is the identity map. The set of sections of $\mathcal{E}$ is in bijection with the set of $k(t)$-rational points on E.

A *multisection* M of an elliptic fibration $\pi : \mathcal{E} \to \mathbb{P}^1_k$ is an irreducible subvariety $M \subset \mathcal{E}$ of dimension one such that the projection map $\pi : M \to \mathbb{P}^1_k$ has non-zero degree. After a suitable finite base extension $C \to \mathbb{P}^1_k$, the fiber product $M_C := M \times_{\mathbb{P}^1_k} C$ is a section of $\mathcal{E} \times_{\mathbb{P}^1_k} C \to C$. Notice that M_C corresponds to a rational point on the base extension $E \times_{\mathrm{Spec}(K)} \mathrm{Spec}(k(C))$.

Next we apply the above discussion to several examples. For all of these examples we assume that:

- all varieties are defined over a field k with $\mathrm{char}(k) \neq 2, 3$;
- x, y and z are coordinates of $\mathbb{P}^2_k$ and t is the coordinate of $\mathbb{A}^1_k$;
- d, r and s are integers satisfying $d, s > 1$ and $r = d/s$;
- $\mathcal{F}_d$ is the Fermat surface in $\mathbb{P}^3_k$ defined by $X_0^d - X_1^d = X_2^d - X_3^d$; and
- for $1 \leq i, j \leq 4$, ℓ_{ij} is the line on $\mathcal{F}_d$ of the form $\ell_{12} = (t, t, 1, 1)$, where the indices indicate the position of t in the 4-tuple.

Example 3.1. Let U_1 be the closed subset of $\mathbb{P}^2 \times \mathbb{A}^1$ defined by the equation $(t^d - t)y^2z = x^3 - xz^2$. We associate to U_1 a matrix of exponents

$$\begin{pmatrix} 0 & 2 & 1 & d \\ 0 & 2 & 1 & 1 \\ 3 & 0 & 0 & 0 \\ 1 & 0 & 2 & 0 \end{pmatrix}.$$

Let $e = d - 1$. By following Shioda's procedure we obtain a rational map

$\pi : \mathcal{F}_{2(d-1)} \dashrightarrow U_1$ given by

$$[X_0 : X_1 : X_2 : X_3] \mapsto ([X_0 X_2^e X_3^{e/2} : X_1^d X_2^{e/2} : X_0 X_3^{3e/2}], X_0^2/X_1^2).$$

Let $\mathcal{E}_1$ be the elliptic surface associated to (the generic fiber of) U_1. The image $\pi(\ell_{13})$ is the curve $([t^{d-1} : t^{(d-3)/2} : 1], t^2)$ on U_1. Its closure on $\mathcal{E}_1$ is a multisection of the fibration $\mathcal{E}_1 \to \mathbb{P}^1_k$.

Suppose $d \equiv 3 \bmod 4$ and let C_1 be the projective curve given by $u = t^2$. Thus the multisection above gives rise to a section on $\mathcal{E}_1 \times_{\mathbb{P}^1_k} C_1$: namely, the closure on $\mathcal{E}_1 \times_{\mathbb{P}^1_k} C_1$ of the curve $([u^{(d-1)/2} : u^{(d-3)/4} : 1], u)$. Notice that this section corresponds to the integral point $(u^{(d-1)/2}, u^{(d-3)/4})$ on the curve $(u^d - u)y^2 = x^3 - x$ defined over $k(u)$.

EXAMPLE 3.2. Let $U_2 \subset \mathbb{P}^2 \times \mathbb{A}^1$ be the closed set defined by the equation $y^2 z - yz^2 = (t^d - t)x^3$. Let $e = d - 1$. In this case, we obtain a rational map $\mathcal{F}_{2e} \dashrightarrow U_2$ given by

$$[X_0 : X_1 : X_2 : X_3] \mapsto ([X_0^e X_1^e X_3^d : X_0^{3e} X_2 : X_1^{3e} X_2], X_2^3/X_3^3).$$

Let $\mathcal{E}_2$ be the elliptic surface associated to U_2. Under the above rational map, the images of the lines ℓ_{12} and ℓ_{34} do not yield any non-constant curve on U_2. On the other hand, the lines ℓ_{13} and ℓ_{24} yield the same multisection of $\mathcal{E}_2$: the closure on $\mathcal{E}_2$ of the curve $([t^{d-2} : t^{3(d-1)} : 1], t^3)$.

Let C_2 be the projective curve given by $u = t^3$. If $d \equiv 2 \bmod 3$, the closure on $\mathcal{E}_2 \times_{\mathbb{P}^1_k} C_2$ of the curve $([u^{(d-2)/3} : u^{d-1} : 1], u)$ is a section.

EXAMPLE 3.3. Consider the hypersurface $\mathcal{X}_D : X_0^s + X_1^s - X_2^d - X_3^d = 0$ in the weighted projective space $\mathbb{P}(r, r, 1, 1)$. Let $U_3 \subset \mathbb{P}^2 \times \mathbb{A}^1$ be the closed set defined by $y^2 z = x^3 + (t^d + 1)z^3$ and let B be the matrix

$$\begin{pmatrix} 0 & 2 & 1 & 0 \\ 3 & 0 & 0 & 0 \\ 0 & 0 & 3 & d \\ 0 & 0 & 3 & 0 \end{pmatrix}^{-1} \begin{pmatrix} s & 0 & 0 & 0 \\ 0 & s & 0 & 0 \\ 0 & 0 & d & 0 \\ 0 & 0 & 0 & d \end{pmatrix}.$$

If $6 \mid s$ and (consequently) $6 \mid d$ then associated to B is the rational map $\mathcal{X}_D \dashrightarrow U_3$ given by

$$[X_0 : X_1 : X_2 : X_3] \mapsto ([-X_1^{s/3} X_3^{d/6} : X_0^{s/2} : X_3^{d/2}], X_2/X_3). \tag{3.2}$$

The image of the curve $(u^r, 1, u, 1) \subset \mathcal{X}_D$ under this rational map is the curve $([-1 : u^{d/2} : 1], u)$ on U_3.

Another rational curve on $\mathcal{X}_D$ is $(1, u^r, u, 1)$. Associated to it is the curve $([-u^{d/3} : 1 : 1], u)$ on U_3. The other two trivial curves on $\mathcal{X}_D$, $(u^r, 1, 1, u)$ and $(1, u^r, u, 1)$, do not yield curves on U_3 different from the ones above.

Example 3.4. Let D and $\mathcal{X}_D$ be as in the previous example. Let $U_4 \subset \mathbb{P}^2 \times \mathbb{A}^1$ be the closed set defined by $y^2z = x^3 - (t^d+1)xz^2$. If we assume that $4 \mid s$, then the map

$$[X_0 : X_1 : X_2 : X_3] \mapsto ([-X_1^{s/2}X_3^{d/4} : X_0^{s/2}X_1^{s/4} : X_3^{3d/4}], X_2/X_3) \tag{3.3}$$

is a rational map $\mathcal{X}_D \dashrightarrow U_4$.

Following the method applied in the previous examples, we obtain the curves $([-1 : u^{d/2} : 1], u)$ and $([-u^{d/2} : u^{d/4} : 1], u)$ on U_4.

Our construction can also be used to explain the explicit points on non-isotrivial elliptic curves recently found by Ulmer [14, 15].

Example 3.5. For an integer $f \geq 0$, one can easily verify (see [14, Section 3]) that the Legendre elliptic curve $y^2 = x(x+1)(x+t^{p^f+1})$ over $\mathbb{F}_q(t)$ contains the integral point $P = (t, t(t+1)^{(p^f+1)/2})$.

To show how our procedure can be used to construct this point, first consider the closed subset U_5 of $\mathbb{P}^2 \times \mathbb{A}^2$ defined by

$$zy^2 = x^3 + zv^dx^2 + zx^2 + u^dxz^2.$$

Notice that by setting $v = u$ in the defining equation of U_5, we recover the surface $E : zy^2 = x(x+z)(x+zu^d)$ in $\mathbb{P}^2 \times \mathbb{A}^1$ associated to the Legendre elliptic curve.

The set U_5 determines a matrix of exponents

$$\begin{pmatrix} 0 & 2 & 1 & 0 & 0 \\ 3 & 0 & 0 & 0 & 0 \\ 2 & 0 & 1 & d & 0 \\ 2 & 0 & 1 & 0 & 0 \\ 1 & 0 & 2 & 0 & d \end{pmatrix},$$

which, following Shioda, can be used to obtain a dominant rational map from the Fermat hypersurface $X_0^d - X_1^d - X_2^d - X_3^d - X_4^d = 0$ to U_5. This map is given by

$$[X_0 : X_1 : X_2 : X_3 : X_4] \mapsto \left([X_1^dX_3^{d/2} : X_0^{d/2}X_1^d : X_3^{3d/2}], \left(\frac{X_2}{X_3}, \frac{X_1X_4}{X_3^2}\right)\right).$$

If we set $u = X_2/X_3 = (X_1X_4)/X_3^2 = v$, we conclude that

$$[X_0 : X_1 : X_2 : X_3 : X_4] \mapsto ([X_1^dX_3^{d/2} : X_0^{d/2}X_1^d : X_3^{3d/2}], X_2/X_3)$$

defines a dominant rational map $\phi : \mathcal{S}_2 \dashrightarrow E$, where $\mathcal{S}_2$ is the surface in $\mathbb{P}^4$ defined by

$$\begin{cases} X_0^d - X_1^d - X_2^d - X_3^d - X_4^d = 0, \\ X_1X_4 = X_2X_3. \end{cases}$$

When $d = p^f + 1$, the surface $\mathcal{S}_2$ contains the curve $\ell : (u^d+1, u, u^d, 1, u^{p^f})$. The image $\phi(\ell)$ is the curve $([u^d, u^d(u^d+1)^{d/2}, 1], u^d)$ on U_5. If $\mathcal{E}_5 \to \mathbb{P}^1$ is the elliptic surface associated to $E/\mathbb{F}_q(t)$, then $\phi(\ell)$ corresponds to a section of $\mathcal{E}_5 \times_{\mathbb{P}^1} C$, where C is the projective curve defined by $t = u^d$. Finally, this section yields the rational point P given above.

Remark 3.6. Let M be a multisection of an elliptic surface $\mathcal{E} \to C$, and let $C_0 \to C$ be a Galois base extension such that $M_0 := M \times_C C_0$ is a section of $\mathcal{E} \times_C C_0$. We obtain a section of $\mathcal{E} \to C$ by considering the trace $\sum_\sigma (M_0)^\sigma$, where the summation is over all elements of $\mathrm{Gal}(k(C_0)/k(C))$. In all of the previous examples, the trace of the multisections does not yield any new information: a multisection will either be traced down to the zero section or to an integer multiple of the original section.

4. Isotrivial elliptic curves with a large set of integral points. In this section and the next, we consider the generic fiber of the elliptic surfaces studied in Examples 3.1 through 3.5 and show that over $\mathbb{F}_q(t)$ these elliptic curves may have an arbitrarily large set of separable integral points. In the isotrivial case we achieve this result in two distinct ways, which we now proceed to explain.

4.1. A construction related to additive polynomials. Example 3.1 shows that over $k(t)$ the elliptic curve defined by $(t^d - t)y^2 = x^3 - x$ contains the integral point

$$(t^{(d-1)/2}, t^{(d-3)/4}) \quad \text{when } d \equiv 3 \bmod 4, \tag{4.1}$$

and Example 3.2 proves that $y^2 - y = (t^d - t)x^3$ contains the point

$$(t^{(d-2)/3}, t^{d-1}) \quad \text{when } d \equiv 2 \bmod 3. \tag{4.2}$$

The existence of both of these points can be interpreted in the following way. Consider the elliptic curve E defined over the function field $k(u)$ by $uy^2 = x^3 - x$. When $d \equiv 3 \bmod 4$, the point defined by (4.1) can be seen as a point on the base extension $E \times_{\mathrm{Spec}(k(u))} \mathrm{Spec}(k(t))$, where $k(t)/k(u)$ is the field extension defined by $u = t^d - t$. By assuming this point of view, we will be able to construct extra integral points on the elliptic curves $(t^{q^n} - t)y^2 = x^3 - x$ and $y^2 - y = (t^{q^n} - t)x^3$ defined over $\mathbb{F}_q(t)$. The points we construct are defined over certain extensions $\mathbb{F}_q(t)/\mathbb{F}_q(u)$ where u is transcendental over $\mathbb{F}_q$ and t satisfies $u = B(t)$, with $B(t)$ an $\mathbb{F}_q$-additive polynomial. For this reason we present some facts about additive polynomials that will be needed shortly. We start with their definition.

Definition 4.1. An $\mathbb{F}_q$-*additive polynomial* $A(t)$ is a polynomial in $\mathbb{F}_q[t]$ of the form

$$A(t)=\sum_{i=0}^{n} a_i t^{q^i}.$$

We will denote the set of all $\mathbb{F}_q$-additive polynomials by $\mathbb{F}_q[\mathbf{F}]$.

An additive polynomial can be seen as an $\mathbb{F}_q$-polynomial in the indeterminate $\mathbf{F}$, the q-Frobenius map $t \mapsto t^q$. Indeed, start by defining $\mathbf{F}^0(t) := t$. Then the ith self-composition of $\mathbf{F}$ is the polynomial $\mathbf{F}^i(t) = t^{q^i}$, and so an additive polynomial $A(t)$ is the same as an $\mathbb{F}_q$-linear combination of powers of Frobenius, $A_0(\mathbf{F}) = \sum_{i=0}^{n} a_i \mathbf{F}^i$. It turns out that the set $\mathbb{F}_q[\mathbf{F}]$ has the structure of a ring isomorphic to $\mathbb{F}_q[X]$.

Lemma 4.2. *Let $A(t), B(t) \in \mathbb{F}_q[\mathbf{F}]$ and $\alpha \in \mathbb{F}_q$. Then:*

(1) *$A(t) + B(t) \in \mathbb{F}_q[\mathbf{F}]$;*
(2) *$\alpha A(t) \in \mathbb{F}_q[\mathbf{F}]$;*
(3) *$A(B(t)) \in \mathbb{F}_q[\mathbf{F}]$.*

Furthermore, $\mathbb{F}_q[\mathbf{F}]$ can be endowed with a ring structure with multiplication defined by $A(t) \circ B(t) := A(B(t))$, and the map

$$P(X)=\sum_{i=0}^{n} a_i X^i \mapsto P(\mathbf{F}) := \sum_{i=0}^{n} a_i \mathbf{F}^i$$

is a ring isomorphism between $\mathbb{F}_q[X]$ and $\mathbb{F}_q[\mathbf{F}]$.

Proof. (1) and (2) are trivial. To prove (3), write

$$A(t)=\sum_{i=0}^{n} a_i \mathbf{F}^i = A_0(\mathbf{F}) \quad \text{and} \quad B(t)=\sum_{j=0}^{m} b_j \mathbf{F}^j = B_0(\mathbf{F}).$$

From the identity

$$(x+y)^p = x^p + y^p, \tag{4.3}$$

true in any commutative ring of characteristic p, it follows that

$$\begin{aligned} A(B(t)) &= \sum_{i=0}^{n} a_i \mathbf{F}^i\Big(\sum_{j=0}^{m} b_j \mathbf{F}^j\Big) = \sum_{i=0}^{n} a_i \Big(\sum_{j=0}^{m} \mathbf{F}^i(b_j \mathbf{F}^j)\Big) \\ &= \sum_{i=0}^{n} a_i \Big(\sum_{j=0}^{m} b_j \mathbf{F}^{i+j}\Big) = \sum_{i=0}^{n}\sum_{j=0}^{m} a_i b_j \mathbf{F}^{i+j} \in \mathbb{F}_q[\mathbf{F}]. \end{aligned}$$

Thus (3) is proved. Associativity is inherited from $\mathbb{F}_q[t]$ and the distribution law follows from (4.3). So $\mathbb{F}_q[\mathbf{F}]$ is a ring. Notice that the latter equation also proves that $A_0(\mathbf{F}) \circ B_0(\mathbf{F}) = (A_0 B_0)(\mathbf{F})$, and so the map $P(X) \mapsto P(\mathbf{F})$ is multiplicative. Hence it is a ring isomorphism, since it is clearly an additive bijective map. ∎

We are now ready to prove one of our main results which is a generalization of Theorem 1.3:

THEOREM 4.3. *Let $m_1, \ldots, m_l$ be distinct odd positive integers. Suppose $A(t) = A_0(\mathbf{F})$ is an $\mathbb{F}_q$-additive square-free polynomial such that $X^{m_i} - 1$ divides $A_0(X)$ for all $1 \le i \le l$. Then the following elliptic curves contain at least l separable integral points over $\mathbb{F}_q(t)$:*

(1) $A(t)y^2 = x^3 - x$ *when* $q \equiv 3 \bmod 4$.
(2) $y^2 - y = A(t)x^3$ *when* $q \equiv 2 \bmod 3$.

Proof. To prove part (1), notice that under the hypothesis of the theorem we have $q^{m_i} \equiv 3 \bmod 4$. Therefore, if in (4.1) we take $d = q^{m_i}$ and $k = \mathbb{F}_q$, we obtain the point

$$P_i(u) = (u^{(q^{m_i}-1)/2}, u^{(q^{m_i}-3)/4})$$

on the twist $(u^{q^{m_i}} - u)y^2 = x^3 - x$ defined over $\mathbb{F}_q(u)$.

By assumption, for each $1 \le i \le l$ there exists a polynomial $B_i(X) \in \mathbb{F}_q[X]$ such that $A_0(X) = (X^{m_i} - 1)B_i(X)$. Under the isomorphism defined in Lemma 4.2, this equation gives us an identity:

$$A(t) = B_i(\mathbf{F})^{q^{m_i}} - B_i(\mathbf{F}). \tag{4.4}$$

Let $K = \mathbb{F}_q(t)$ be the extension of $\mathbb{F}_q(u)$ defined by $u = B_i(\mathbf{F})$. The lift of the point P_i to K,

$$Q_i = P_i(B_i(\mathbf{F})) = (B_i(\mathbf{F})^{(q^{m_i}-1)/2}, B_i(\mathbf{F})^{(q^{m_i}-3)/4}), \tag{4.5}$$

is a point on the twist $A(t)y^2 = x^3 - x$.

If we let $\deg A(t) = q^a$, then the degree of the first coordinate of Q_i is $(q^a - q^{a-m_i})/2$. So Q_i and Q_j are distinct points for $i \neq j$. Since $A(t)$ is square-free, we have $(B_i(\mathbf{F})^{(q^{m_i}-1)/2})' \neq 0$. Thus it follows from Example 2.7 that Q_i is a separable integral point for all $1 \le i \le l$.

The second part is proved in a similar way. The hypothesis of the theorem and (4.2) give us the polynomial point $(u^{(q^{m_i}-2)/3}, u^{q^{m_i}-1})$ on the elliptic curve $y^2 - y = (u^{q^{m_i}} - u)x^3$. The identity (4.4) implies that the integral point $S_i = (B_i(\mathbf{F})^{(q^{m_i}-2)/3}, B_i(\mathbf{F})^{q^{m_i}-1})$ is on the curve $y^2 - y = A(t)x^3$ defined over K. Observe that the degree of the second coordinate of S_i is $q^a - q^{a-m_i}$, which shows that the S_i's are all distinct.

The Frobenius orbit of a rational point (x, y) on $y^2 - y = A(t)x^3$ is $\{(A(t)^{(q^i-1)/3}x^{q^i}, y^{q^i}) : i \in \mathbb{N}\}$. Thus a point (x_0, y_0) on $y^2 - y = A(t)x^3$ is a separable point if $y_0' \neq 0$. Since $(B_i(\mathbf{F})^{q^{m_i}-1})' \neq 0$, we conclude that S_i is a separable integral point for all i. ∎

Our main example of elliptic curves with an unbounded number of separable integral points is now an easy consequence of this result.

Corollary 4.4. *Let n be a positive integer. Then over $\mathbb{F}_q(t)$ the following elliptic curves have a separable integral point for every odd divisor of n:*

(1) $(t^{q^n} - t)y^2 = x^3 - x$ *when* $q \equiv 3 \bmod 4$.
(2) $y^2 - y = (t^{q^n} - t)x^3$ *when* $q \equiv 2 \bmod 3$.

Proof. Under the isomorphism defined in Lemma 4.2, the $\mathbb{F}_q$-additive polynomial $A(t) = t^{q^n} - t$ corresponds to the polynomial $A_0(X) = X^n - 1$. It is well known that $X^m - 1$ divides $A_0(X)$ if and only if m divides n. Therefore, in the above theorem, we can take m_i to be the odd divisors of n. ∎

4.2. A construction related to a surface containing many rational curves. We now provide a different construction of twists of elliptic curves with a large set of separable integral points. These elliptic curves are given by the generic fiber of the elliptic surfaces discussed in Examples 3.3 and 3.4. Recall that in these examples, for integers $d, s > 1$ and r satisfying $r = d/s$, we defined the surface

$$\mathcal{S} : X_0^s + X_1^s = X_2^d + X_3^d, \tag{4.6}$$

in the weighted projective space $\mathbb{P}_k(r, r, 1, 1)$. This surface contains the curves $(t^r, 1, t, 1)$ and $(1, t^r, t, 1)$ which, following the procedure described in Section 3, yield integral points on the curves $y^2 = x^3 + t^d + 1$ and $y^2 = x^3 - (t^d + 1)x$ when $6 \mid s$ and $4 \mid s$ respectively. The following sequence of results is used to prove that $\mathcal{S}$ will contain many other rational curves when we specialize to the case where $s = q^m + 1$, $d = q^n + 1$ and $r = d/s$ are integers, and $k = \mathbb{F}_q$. This is a consequence of the fact that the *orthogonal group* $O_2(\mathbb{F}_q)$ acts on the surface $\mathcal{S}$.

Lemma 4.5. *Suppose $A = (a_{ij}) \in O_2(\mathbb{F}_q)$. Then for any non-negative integer m, the identity*

$$(a_{11}X + a_{12}Y)^{q^m+1} + (a_{21}X + a_{22}Y)^{q^m+1} = X^{q^m+1} + Y^{q^m+1}$$

holds over $\mathbb{F}_q[X, Y]$.

Proof. This is proved by rewriting the binomial $X^{q^m+1} + Y^{q^m+1}$ as a product of matrices.

$$\begin{aligned}
X^{q^m+1} + Y^{q^m+1} &= (X^{q^m} \quad Y^{q^m})\begin{pmatrix} X \\ Y \end{pmatrix} = (X^{q^m} \quad Y^{q^m})A^t A\begin{pmatrix} X \\ Y \end{pmatrix} \\
&= \left[A\begin{pmatrix} X^{q^m} \\ Y^{q^m} \end{pmatrix}\right]^t \left[A\begin{pmatrix} X \\ Y \end{pmatrix}\right] \\
&= \begin{pmatrix} (a_{11}X + a_{12}Y)^{q^m} \\ (a_{21}X + a_{22}Y)^{q^m} \end{pmatrix}^t \begin{pmatrix} a_{11}X + a_{12}Y \\ a_{21}X + a_{22}Y \end{pmatrix} \\
&= (a_{11}X + a_{12}Y)^{q^m+1} + (a_{21}X + a_{22}Y)^{q^m+1}. \ \blacksquare
\end{aligned}$$

COROLLARY 4.6. *Let n and m be positive integers. Let $d = q^n + 1$ and $s = q^m + 1$, and suppose that $r = d/s$ is an integer. Let $\mathcal{S}/\mathbb{F}_q$ be the surface defined by (4.6). Then for any two matrices $A = (a_{ij})$ and $B = (b_{ij})$ in $O_2(\mathbb{F}_q)$, the rational curve $(a_{11}u^r + a_{12}, a_{21}u^r + a_{22}, b_{11}u + b_{12}, b_{21}u + b_{22})$ is contained in $\mathcal{S}$.*

Proof. In the previous lemma take $X = u^r$ and $Y = 1$ to obtain

$$(a_{11}u^r + a_{12})^{q^m+1} + (a_{21}u^r + a_{22})^{q^m+1} = (u^r)^{q^m+1} + 1 = u^{q^n+1} + 1.$$

Another application of the previous lemma, with $X = u$, $Y = 1$ and $m = n$, implies

$$(b_{11}u + b_{12})^{q^n+1} + (b_{21}u + b_{22})^{q^n+1} = u^{q^n+1} + 1.$$

So

$$(a_{11}u^r + a_{12})^{q^m+1} + (a_{21}u^r + a_{22})^{q^m+1} = (b_{11}u + b_{12})^{q^n+1} + (b_{21}u + b_{22})^{q^n+1},$$

as claimed. ∎

We are ready to prove the main result of this section.

THEOREM 4.7. *Let n be an odd positive integer. Then over $\mathbb{F}_{q^2}(t)$, the following elliptic curves have a separable integral point for each positive divisor of n:*

(1) $y^2 = x^3 - (t^{q^n+1} + 1)x$ *when* $q \equiv 3 \bmod 4$.
(2) $y^2 = x^3 + t^{q^n+1} + 1$ *when* $q \equiv 2 \bmod 3$.

Proof. Let m be a divisor of n and let $d = q^n + 1$ and $s = q^m + 1$. Then the fact that n is odd implies that $r = d/s$ is an integer.

To prove part (1), we first notice that the assumption $q \equiv 3 \bmod 4$ implies that $4 \mid s$. Consequently, (3.3) defines a rational map from the surface $\mathcal{S}/\mathbb{F}_{q^2}$, defined by (4.6), to the surface in $\mathbb{P}^2 \times \mathbb{A}^1$ defined by $y^2z = x^3 + (t^{q^n+1} + 1)xz^2$.

Let B be the 2×2 identity matrix and let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in O_2(\mathbb{F}_{q^2})$ be such that $cd \neq 0$. Notice that such a matrix exists over $\mathbb{F}_{q^2}$. From Corollary 4.6 we obtain the rational curve $(au^r + b, cu^r + d, u, 1) \subset \mathcal{S}$. Its image under the rational map (3.3) is the curve

$$\left(\left[-(cu^r + d)^{(q^m+1)/2} : (au^r + b)^{(q^m+1)/2}(cu^r + d)^{(q^m+1)/4} : 1\right], u\right)$$

on the surface $y^2z = x^3 + (t^{q^n+1} + 1)xz^2$. Consequently, we obtain the point

$$R_m = \left(-(ct^r + d)^{(q^m+1)/2}, (at^r + b)^{(q^m+1)/2}(ct^r + d)^{(q^m+1)/4}\right)$$

on the elliptic curve E defined over $\mathbb{F}_{q^2}(t)$ by $y^2 = x^3 - (t^{q^n+1} + 1)x$. The binomial expansion of the first coordinate of R_m contains the non-zero monomial $-cd^{(q^m-1)/2}t^r/2$, thus for each divisor m of n we obtain a distinct integral point on E.

Let $D = t^d + 1$. The Frobenius orbit of a point (x_0, y_0) on E is given by

$$\{(x_0^{q^i}/D^{(q^i-1)/2}, y_0^{q^i}/D^{3(q^i-1)/4}) : i \in \mathbb{N}\}.$$

Therefore R_m is a separable integral point, since for any $i \in \mathbb{N}$, the polynomial $D^{(q^i-1)/2}(ct^r + d)^{(q^m+1)/2}$ is not a qth power.

The second part is proved in a similar way. Under the assumption $q \equiv 2 \bmod 3$, all the hypotheses of Corollary 4.6 and Example 3.3 are satisfied. The image of the curve $(au^r + b, cu^r + d, u, 1) \subset \mathcal{S}$ under the rational map (3.2) yields the integral point

$$S_m = \big(-(ct^r + d)^{(q^m+1)/3}, (at^r + b)^{(q^m+1)/2}\big)$$

on the curve $E_0 : y^2 = x^3 + t^{q^n+1} + 1$ over $\mathbb{F}_{q^2}(t)$. The binomial expansion of $-(ct^r + d)^{(q^m+1)/3}$ shows that the S_m are distinct points on E_0 for distinct divisors m of n. It is easy to check, using part (3) of Remark 2.4, that S_m is a separable integral point for all m. ∎

5. Non-isotrivial elliptic curves with a large set of integral points. The following theorem provides examples of non-isotrivial elliptic curves with an arbitrarily large set of integral points.

Theorem 5.1. *Let n be a positive odd integer and $a, b, c \in \mathbb{F}_q$ with $ac \neq 0$. Then for $d = q^n + 1$ the elliptic curves defined over $\mathbb{F}_q(t)$ by*

$$y^2 = x(x + 1)(x + t^d)$$

and

$$y^2 = (ax^2 + bx + c)(cx^2 + bt^d x + at^{2d})$$

each contain an integral point for every divisor of n.

Proof. Let m be a divisor of n; then $r = (q^n + 1)/(q^m + 1)$ is an integer.

The first elliptic curve is the Legendre curve discussed in Example 3.5. In this example we showed that over the rational function field $\mathbb{F}_q(u)$, the curve $E_1 : y^2 = x(x + 1)(x + u^{q^m+1})$ contains the point $P = (u, u(u + 1)^{(p^m+1)/2})$. If we let $K = \mathbb{F}_q(t)$ be the extension of $\mathbb{F}_q(u)$ defined by $u = t^r$, then E_1/K is defined by the equation $y^2 = x(x + 1)(x + t^d)$ and contains the point $(t^r, t^r(t^r + 1)^{(p^m+1)/2})$.

For the second elliptic curve, we let $f(x) = ax^2 + bx + c$. Then for every divisor m of n it is easily verified that

$$(t^r, t^r f(t^r)^{(p^m+1)/2})$$

is an integral point on $y^2 = (ax^2 + bx + c)(cx^2 + bt^d x + at^{2d})$. ∎

Remark 5.2. Abramovich showed in [1, Corollary 1] that the existence of a uniform bound on the number of integral points on semistable elliptic curves over $\mathbb{Q}$ is a consequence of the Lang–Vojta conjecture. Our previous result shows that over function fields no such uniform bound exists. Indeed, for an odd n with a large number of divisors, the curve $y^2 = x(x+1)(x+t^{q^n+1})$ contains a large set of integral points and is a semistable elliptic curve (see [14, Section 7]).

6. An isotrivial counter-example to an analogue of the Lang–Vojta conjecture over $\mathbb{F}_q(t)$. Recall the statement of Theorem 1.4: the isotrivial affine variety defined over $\mathbb{F}_q(t)$ by

$$\mathcal{K} : z^2 = (x^3 - x)(y^3 - y) \tag{6.1}$$

is of log-general type and has a Zariski dense set of separable integral points when $q \equiv 3 \bmod 4$. In this section we prove this statement.

REMARK 6.1. The arguments in this section can be adapted to prove that the variety defined over $\mathbb{F}_q(t)$ by $u^3 = (x^2 - x)(y^2 - y)(z^2 - z)$ is of log-general type and, when $q \equiv 2 \bmod 3$, has a Zariski dense set of separable integral points. We leave the details to the reader.

We start from the definition of a log-general type variety.

DEFINITION 6.2. Let V be a variety defined over a field k.

- Let $\bar{V}$ be a non-singular complete variety and D be a divisor on $\bar{V}$ with simple normal crossings. We say that $\bar{V}$ is a *smooth completion* of V with *smooth boundary* D if $V = \bar{V}\backslash D$.
- Let V be a variety with a smooth completion $\bar{V}$ and smooth boundary D. If for every natural number m we have $l_{\bar{V}}(m(K_{\bar{V}} + D)) = 0$, define $\bar{\kappa}(V) = -\infty$. Otherwise, let
$$\bar{\kappa}(V) = \max_{m\in\mathbb{N}}\{\dim \phi_m(\bar{V})\},$$
where ϕ_m is the rational map associated to the divisor $m(K_{\bar{V}} + D)$. The number $\bar{\kappa}(V)$ is called the *logarithmic Kodaira dimension* of V.
- V is said to be of *log-general type* if $\bar{\kappa}(V) = \dim(V)$.

REMARK 6.3. The logarithmic Kodaira dimension has the following properties:

(1) $\bar{\kappa}(V \times W) = \bar{\kappa}(V) + \bar{\kappa}(W)$ [8, Theorem 11.3];
(2) If C is a curve and $D \subset C$ is finite set of points with $|D| \geq 3$ then $\bar{\kappa}(C\backslash D) = 1$ [8, §11.2(d)];
(3) If $f : V \to W$ is an étale covering between non-singular varieties then $\bar{\kappa}(V) = \bar{\kappa}(W)$ [8, Theorem 11.10].

The above properties will be useful in the proof of the first part of Theorem 1.4.

LEMMA 6.4. *$\mathcal{K}$, defined as in* (6.1), *is a variety of log-general type.*

Proof. To prove that $\mathcal{K}$ is a log-general type variety, denote by $\bar{\mathcal{K}}$ the projective completion of $\mathcal{K} \subset \mathbb{P}^3$. The projection on the x, y coordinates defines a rational map $\pi : \bar{\mathcal{K}} \dashrightarrow \mathbb{P}^1 \times \mathbb{P}^1$ such that the singular locus S of $\bar{\mathcal{K}}$ is contained in the fibers over $0, 1$ and ∞. Therefore $\bar{\mathcal{K}}$ is non-singular above $W := (\mathbb{P}^1 \backslash \{0, 1, \infty\}) \times (\mathbb{P}^1 \backslash \{0, 1, \infty\})$.

Let $\beta : \bar{V} \to \bar{\mathcal{K}}$ be the blow-up of $\bar{\mathcal{K}}$ along S and let $V := \beta^{-1}(\bar{\mathcal{K}} \backslash S)$. We can always assume that $\bar{V}$ is a smooth completion of V [8, Theorem 7.21]. By definition, $\mathcal{K}$ will be of log-general type if V is. Since $\dim V = \dim \mathcal{K} = 2$, we only need to show that $\bar{\kappa}(V) = 2$.

The restriction of π to $\pi^{-1}(W)$ is an étale covering of W, therefore $\pi \circ \beta : V \to W$ is an étale covering. To finish the proof, we use properties (1)–(3) in Remark 6.3 to show that

$$\bar{\kappa}(V) = \bar{\kappa}(W) = \bar{\kappa}(\mathbb{P}^1 \backslash \{0, 1, \infty\}) + \bar{\kappa}(\mathbb{P}^1 \backslash \{0, 1, \infty\}) = 2. \blacksquare$$

We now give a proof of Theorem 1.2 that works for isotrivial elliptic curves.

THEOREM 6.5. *Let $y^2 = f(x)$ be an elliptic curve defined over $\mathbb{F}_q$. If the set of separable integral points on the affine variety defined over $\mathbb{F}_q(t)$ by $z^2 = f(x_1)f(x_2)$ is not Zariski dense, then for any non-zero square-free polynomial $D \in \mathbb{F}_q[t]$ the number of separable integral points on the quadratic twists $Dy^2 = f(x)$ is bounded independently of D.*

Proof. Let $E_1 : y^2 = f(x)$ and $\mathcal{K} : z^2 = f(x_1)f(x_2)$.

Assume that the set of separable integral points on $\mathcal{K}$ is not Zariski dense. Thus there exists a polynomial $g(x_1, x_2, z)$ with integral coefficients and prime to $z^2 - f(x_1)f(x_2)$ such that all separable integral points in $\mathcal{K}$ are contained in

$$\begin{cases} z^2 = f(x_1)f(x_2), \\ g(x_1, x_2, z) = 0. \end{cases}$$

In the system above we use the first equation to eliminate from $g(x_1, x_2, z)$ powers of z of order ≥ 2. That way we find polynomials $g_0 = g_0(x_1, x_2)$ and $g_1 = g_1(x_1, x_2)$ such that the separable integral points on $\mathcal{K}$ satisfy the equation

$$g_0(x_1, x_2) + g_1(x_1, x_2)z = 0. \tag{6.2}$$

Notice that g_0 and g_1 are not both identically zero, otherwise g would be divisible by $z^2 - f(x_1)f(x_2)$. Also, we have $\deg g_0, \deg g_1 \leq \deg g$.

Let E_D be the twist $Dy^2 = f(x)$ of E_1 and $\phi : E_D \times E_D \to \mathcal{K}$ be the morphism defined by

$$((x_1, y_1), (x_2, y_2)) \mapsto (x_1, x_2, Dy_1y_2). \tag{6.3}$$

The q-Frobenius action on $\mathcal{K}$ is given by $(x_1, x_2, z) \mapsto (x_1^q, x_2^q, z^q)$. Therefore, from Example 2.7 it follows that if P is a separable integral point on

$E_D \times E_D$ then the image $\phi(P)$ is a separable integral point on $\mathcal{K}$. In particular, by (6.2) the separable integral points $((x_1, y_1), (x_2, y_2))$ on $E_D \times E_D$ satisfy the equation

$$g_0(x_1, x_2) + D g_1(x_1, x_2) y_1 y_2 = 0. \tag{6.4}$$

Fix $D \neq 0$. If for every separable integral point $(x_0, y_0) \in E_D$ we know that $\overline{g}_0(X) := g_0(x_0, X)$ and $\overline{g}_1(X) := g_1(x_0, X)$ are both identically zero as polynomials in X, then x_0 is a root of a polynomial of degree $\leq \deg g$. Indeed, in that case x_0 is a root of the coefficients of $\overline{g}_0(X)$ and $\overline{g}_1(X)$. As a consequence, the number of separable integral points on E_D is bounded by $2 \deg g$, independently of D.

Therefore we may assume that there exists a separable integral point $(x_0, y_0) \in E_D$ such that $\overline{g}_0(X)$ and $\overline{g}_1(X)$ are not both identically zero polynomials. Assume further that $y_0 \neq 0$. Thus, from (6.4) we find that any other separable integral point $(x, y) \in E_D$ satisfies the polynomial equation

$$h_0(x) + h_1(x) y = 0 \tag{6.5}$$

with $h_0(X) = \overline{g}_0(X)$ and $h_1(X) = D\overline{g}_1(X) y_0$. Note that $\deg h_0, \deg h_1 \leq \deg g$.

The number of separable integral points $(x, y) \in E_D$ that satisfy $h_1(x) = 0$ is bounded above by $2 \deg h_1 \leq 2 \deg g$, and this bound does not depend on D. On the other hand, if $(x, y) \in E_D$ is such that $h_1(x) \neq 0$ then by (6.5) we have $y = -h_0(x)/h_1(x)$. From the equation defining E_D, it follows that x satisfies the polynomial equation

$$f(x) h_1(x)^2 - D h_0(x)^2 = 0$$

of degree at most $2 \deg g + 3$. This means that the number of separable integral points $(x, y) \in E_D$ with $h_1(x) \neq 0$ is bounded above by $4 \deg g + 6$. Once more we obtain an upper bound that does not depend on D, and the result follows. ∎

Below we provide the last ingredient in the proof of Theorem 1.4.

Corollary 6.6. *Let $\mathcal{K}$ be defined as in* (6.1). *If $q \equiv 3 \bmod 4$ then $\mathcal{K}$ has a Zariski dense set of separable integral points.*

Proof. Suppose that the set of separable integral points on $\mathcal{K}$ is not Zariski dense. Theorem 6.5 implies that the number of separable integral points on the family of quadratic twists $Dy^2 = x^3 - x$ remains bounded as D runs through square-free polynomials over $\mathbb{F}_q$. But when $q \equiv 3 \bmod 4$, this contradicts Theorem 1.3 and completes the proof. ∎

7. Elliptic curves with an explicit large set of linearly independent points. In this section we prove that the points found in Theorem 4.3 are linearly independent.

THEOREM 7.1. *Let $m_1, \dots, m_l$ be distinct odd positive integers. Suppose $A(t) = A_0(\mathbf{F})$ is an $\mathbb{F}_q$-additive square-free polynomial such that $X^{m_i} - 1$ divides $A_0(X)$ for all $1 \le i \le l$. Let E_A be the elliptic curve defined by $A(t)y^2 = x^3 - x$. Suppose $q \equiv 3 \bmod 4$. Then the points $\{Q_1, \dots, Q_l\} \subset E_A(\mathbb{F}_q(t))$ defined by (4.5) are $\mathbb{Z}$-linearly independent.*

Proof. Let $C/\mathbb{F}_q$ be the smooth projective curve defined by $s^2 = A(t)$, and let $L = \mathbb{F}_q(C)$ be its function field. Let $E/\mathbb{F}_q$ be the elliptic curve defined by $y^2 = x^3 - x$ and $E_A/\mathbb{F}_q(t)$ be the elliptic curve defined by $A(t)y^2 = x^3 - x$. Notice that E_A and E are isomorphic over L via the isomorphism

$$(x, y) \mapsto (x, sy).$$

The set $\mathrm{Mor}_{\mathbb{F}_q}(C, E)$ of $\mathbb{F}_q$-morphisms from C to E is an abelian group canonically isomorphic to the Mordell–Weil group $E(L)$ (see [13, Proposition 6.1]).

For $P = (F, G) \in E_A(\mathbb{F}_q(t))$, we let $\phi_P : C \to E$ be the $\mathbb{F}_q$-morphism $\phi_P(t, s) = (F(t), sG(t))$. As a consequence of the above discussion, the map

$$\Gamma : E_A(\mathbb{F}_q(t)) \to \mathrm{Mor}_{\mathbb{F}_q}(C, E), \quad P \mapsto \phi_P, \tag{7.1}$$

is an injective group homomorphism.

Let $Q_i = (F_i, G_i)$ be given as in (4.5) and let $\phi_i = \Gamma(Q_i)$. It remains to prove that the set $\{\phi_i\} \subset \mathrm{Mor}_{\mathbb{F}_q}(C, E)$ is $\mathbb{Z}$-linearly independent. First notice that $B_i(\mathbf{F})$, given as in (4.4), is a square-free $\mathbb{F}_q$-additive polynomial. Consequently, there exists $\beta_i \in \mathbb{F}_q^*$ such that $F_i' = \beta_i G_i^2$. Let $\omega_E = dx/y$ be the invariant differential on E and let ω_C be the non-zero differential dt/s on C. Thus

$$\phi_i^*(\omega_E) = \frac{d\phi_i^*(x)}{\phi_i^*(y)} = \frac{F_i' dt}{sG_i} = \beta_i G_i \omega_C.$$

Since the G_i's have distinct degrees, $\{\phi_i^*(\omega_E)/\omega_C\} \subset L$ is an $\mathbb{F}_q$-linearly independent set. The fact that E is supersingular [10, Example 4.5] allows us to use the lemma below to finish the proof of our result. ∎

LEMMA 7.2. *Let C be a smooth projective curve and E be a supersingular elliptic curve, both defined over $\mathbb{F}_q$. Let ω_E and ω_C be non-zero differentials on E and C, respectively. Let $\{\phi_i\}_{i=1}^n$ be a subset of $\mathrm{Mor}_{\mathbb{F}_q}(C, E)$, the set of $\mathbb{F}_q$-morphisms from C to E. If $\{\phi_i^*(\omega_E)/\omega_C\}_{i=1}^n$ is an $\mathbb{F}_q$-linearly independent set in $\mathbb{F}_q(C)$ then $\{\phi_i\}_{i=1}^n$ is a set of $\mathbb{Z}$-linearly independent morphisms in $\mathrm{Mor}_{\mathbb{F}_q}(C, E)$.*

Proof. For an integer m, let $[m]$ denote the multiplication-by-m map on E. Suppose, by contradiction, that there exists a non-trivial $\mathbb{Z}$-linear combination $\sum_{i=1}^n [a_i]\phi_i = O$. Let p^j be the largest power of p that divides a_i, for $1 \le i \le n$. Then

$$[p^j]\Big(\sum_{i=1}^{n}[b_i]\phi_i\Big) = O,$$

where $b_i = a_i/p^j$. The p-torsion group of a supersingular elliptic curve is trivial [10, Theorem 3.1], therefore $\sum_{i=1}^{n}[b_i]\phi_i = O$ is a $\mathbb{Z}$-linear combination of the ϕ_i's with at least one of its coefficients prime to p, say b_0. The linearity of the pullback of differentials (see [10, Theorem 5.2] for a proof of this fact when C is an elliptic curve) implies that

$$0 = \Big(\sum_{i=1}^{n}[b_i]\phi_i\Big)^*(\omega_E) = \sum_{i=1}^{n}(\phi_i^* b_i^*)(\omega_E) = \sum_{i=1}^{n} b_i\phi_i^*(\omega_E).$$

Hence

$$\sum_{i=1}^{n} b_i \frac{\phi_i^*(\omega_E)}{\omega_C} = 0.$$

By assumption $\{\phi_i^*(\omega_E)/\omega_C\}_{i=1}^{n}$ is an $\mathbb{F}_q$-linearly independent set. Therefore $p \mid b_i$ for all i. But this contradicts the fact that p is prime to b_0, and the result follows. ∎

REMARK 7.3. Notice that a similar argument can be used to prove the linear independence of the explicit points on the cubic twists $A(t)x^3 = y^2 - y$ found in Theorem 4.3.

Acknowledgments. I would like to thank José Felipe Voloch for his invaluable support and guidance during the completion of this work. I am also grateful to Douglas Ulmer for several discussions about the topics in this article and, in particular, for introducing me to the elliptic curves appearing in Theorem 5.1. Finally, I would like to thank the anonymous referee for a careful reading of the manuscript.

References

[1] D. Abramovich, *Uniformity of stably integral points on elliptic curves*, Invent. Math. 127 (1997), 307–317.

[2] L. Berger, *Towers of surfaces dominated by products of curves and elliptic curves of large rank over function fields*, J. Number Theory 128 (2008), 3013–3030.

[3] I. I. Bouw, C. Diem, and J. Scholten, *Ordinary elliptic curves of high rank over $\overline{\mathbb{F}}_p(x)$ with constant j-invariant*, Manuscripta Math. 114 (2004), 487–501.

[4] L. Caporaso, J. Harris, and B. Mazur, *Uniformity of rational points*, J. Amer. Math. Soc. 10 (1997), 1–35.

[5] C. Diem and J. Scholten, *Ordinary elliptic curves of high rank over $\overline{\mathbb{F}}_p(x)$ with constant j-invariant. II*, J. Number Theory 124 (2007), 31–41.

[6] N. D. Elkies, *Mordell–Weil lattices in characteristic 2. I. Construction and first properties*, Int. Math. Res. Notices 1994, no. 8, 343 ff., approx. 18 pp.

[7] M. Hindry and J. H. Silverman, *The canonical height and integral points on elliptic curves*, Invent. Math. 93 (1988), 419–450.
[8] S. Iitaka, *An Introduction to Birational Geometry of Algebraic Varieties*, Grad. Texts in Math. 76, Springer, 1982.
[9] T. Shioda, *An explicit algorithm for computing the Picard number of certain algebraic surfaces*, Amer. J. Math. 108 (1986), 415–432.
[10] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, New York, 1992.
[11] J. Tate and I. R. Šafarevič, *The rank of elliptic curves*, Dokl. Akad. Nauk SSSR 175 (1967), 770–773.
[12] D. Ulmer, *Elliptic curves with large rank over function fields*, Ann. of Math. (2) 155 (2002), 295–315.
[13] D. Ulmer, *Elliptic curves over function fields*, in: Arithmetic of L-functions, IAS/Park City Math. Ser. 18, Amer. Math. Soc., Providence, RI, 2011, 211–280.
[14] D. Ulmer, *Explicit points on the Legendre curve*, arXiv:1002.3313v2 (2012).
[15] D. Ulmer, *On Mordell–Weil groups of Jacobians over function fields*, J. Inst. Math. Jussieu 12 (2013), 1–29.

Ricardo P. Conceição
Oxford College of Emory University
100 Hamill Street
Oxford, GA 30054, U.S.A.
E-mail: rconcei@emory.edu

Received on 4.11.2012
and in revised form on 13.6.2013 (7251)