Bull. Aust. Math. Soc. **102** (2020), 177–185
doi:10.1017/S0004972720000155

ON INTEGRAL POINTS ON ISOTRIVIAL ELLIPTIC CURVES OVER FUNCTION FIELDS

RICARDO CONCEIÇÃO

(Received 24 June 2019; accepted 14 January 2020; first published online 27 March 2020)

Abstract

Let k be a finite field and L be the function field of a curve C/k of genus $g \geq 1$. In the first part of this note we show that the number of separable S-integral points on a constant elliptic curve E/L is bounded solely in terms of g and the size of S. In the second part we assume that L is the function field of a hyperelliptic curve $C_A : s^2 = A(t)$, where $A(t)$ is a square-free k-polynomial of odd degree. If ∞ is the place of L associated to the point at infinity of C_A, then we prove that the set of separable $\{\infty\}$-points can be bounded solely in terms of g and does not depend on the Mordell–Weil group $E(L)$. This is done by bounding the number of separable integral points over $k(t)$ on elliptic curves of the form $E_A : A(t)y^2 = f(x)$, where $f(x)$ is a polynomial over k. Additionally, we show that, under an extra condition on $A(t)$, the existence of a separable integral point of 'small' height on the elliptic curve $E_A/k(t)$ determines the isomorphism class of the elliptic curve $y^2 = f(x)$.

2010 *Mathematics subject classification*: primary 11G05; secondary 11G20.

Keywords and phrases: elliptic curves, function fields, Lang's conjecture.

1. Introduction

Let k be a finite field and L be the function field of a curve C/k. The purpose of this note is to discuss arithmetical properties satisfied by integral points on isotrivial elliptic curves over L, that is, when the j-invariant of the elliptic curve is an element of k. More specifically, we study integral points on constant elliptic curves and some of their quadratic twists.

The first property is related to a long-standing conjecture of S. Lang that roughly says that the number of integral points is bounded independently of the model, for a certain class of models. To make this statement more precise, let L be a number field, S a finite set of places of L containing the archimedean places, R_S the ring of S-integers of L and E an elliptic curve over L.

Conjecture 1.1 (Lang). The number of S-integral points on a quasi-minimal model of an elliptic curve E/L is bounded solely in terms of the field L, the set S and the rank of the Mordell–Weil group $E(L)$.

For more information on this conjecture, including the definition of the quasi-minimal model of an elliptic curve, we refer the reader to the introduction of [1].

Hindry and Silverman [1] show that Lang's conjecture is a consequence of Szpiro's celebrated conjecture. Moreover, they prove that Lang's conjecture is true unconditionally if L is the function field of a curve over a field of characteristic zero and E/L is nonconstant. In Section 2 we prove the following theorem and we explain how it can be seen as a version of Lang's conjecture for constant elliptic curves over function fields, that is, when E/L can be defined by a Weierstrass cubic over k.

THEOREM 1.2. *Let E/k be an elliptic curve, C/k a curve of genus $g \geq 1$ and $S \subset C$ a finite nonempty set of points. Then the number of nonconstant separable k-morphisms $\psi : C \longrightarrow E$ satisfying $\psi^{-1}(O) \subset S$ is bounded by*

$$(2\sqrt{|S| + 4(g-1)} + 1)^{4g}.$$

Notice that, unlike Lang's conjecture, the above bound on the number of integral points on constant elliptic curves is in terms solely of the genus of C and $|S|$ and not the rank of its Mordell–Weil group. Moreover, our bound is 'geometric' in that it does not depend on the base field k of the curve C, but only on the geometry of C. Below, for a specific choice of S, we give a bound in terms of g that is arithmetic in nature, that is, dependent on k.

We let $A(t)$ be a square-free polynomial of odd degree $d > 1$ over a finite field k of odd characteristic. We write ∞ for the point at infinity of the curve $C_A : y^2 = A(t)$. Let $f(x)$ be a cubic polynomial over k defining an elliptic curve $E : y^2 = f(x)$ with point at infinity O. We prove in Corollary 3.3 that the number of nonconstant separable k-morphisms $\psi : C_A \longrightarrow E$ satisfying $\psi^{-1}(O) \subset \{\infty\}$ is bounded above by $|k|^{2d-3}$. As before, the above bound is independent of the rank of the Mordell–Weil group.

In Section 3, to prove that the bound in Corollary 3.3 holds, we consider integral points over $k(t)$ on elliptic curves of the form $E_A : A(t)y^2 = f(x)$. Using elementary methods, we prove that if $P = (F, G)$ is a separable integral point on E_A then

$$\deg F < \deg A - 1.$$

Additionally, in Section 3 we show that E_A can have a separable integral point of much lower degree only for certain curves E. Indeed, Theorem 3.4 shows that if $\deg A'(t) = 0$ and $P = (F, G)$ is a separable integral point on E_A satisfying

$$\deg F \leq \frac{\deg A - 1}{2},$$

then $j(E) = 1728$.

2. Lang's conjecture for constant elliptic curves

We start this section by explaining why Theorem 1.2 is a version of Lang's conjecture for constant elliptic curves over finite fields. At the end of the section we provide a proof of this theorem.

https://doi.org/10.1017/S0004972720000155 Published online by Cambridge University Press

Let E be an elliptic curve defined over a finite field k, let $L = k(C)$ be the function field of a curve C of genus $g \geq 1$ and let $S \subset C$ be a finite nonempty set of points. Recall that our aim is to bound the number of S-integral points of E in terms solely of L, S and rank $E(L)$.

The set $\mathrm{Mor}_k(C, E)$ of k-morphisms from C to E is an abelian group canonically isomorphic to the Mordell–Weil group $E_0(L)$, where $E_0 = E \times_k L$ (see [3, Proposition 6.1]). Under this isomorphism, if $O \in E(k)$ is the point at infinity then the k-morphisms $\psi : C \longrightarrow E$ satisfying $\psi^{-1}(O) \subset S$ correspond to S-integral points on E_0/L. A k-morphism satisfying this condition is called *S-integral*.

In this setting, the set of S-integral morphisms is not finite. Indeed, observe that if $\phi : E \longrightarrow E$ is the Frobenius endomorphism on E and ψ is an S-integral morphism, then for every integer $n \geq 0$, the k-morphism $g_n = \phi^n \circ \psi$ is S-integral. To avoid such pathological examples, when discussing S-integral morphisms we disregard those that are inseparable.

Also, we assume that all of our S-integral morphisms are nonconstant for the following reason. Notice that with the exception of the constant morphism with value ∞, all constant morphisms in $\mathrm{Mor}_k(C, E)$ are S-integral. Moreover, under the isomorphism $E_0(L) \cong \mathrm{Mor}_k(C, E)$, the set of constant morphisms $\mathrm{Mor}_k^0(C, E)$ satisfies $E_0(k) \cong \mathrm{Mor}_k^0(C, E)$. Therefore, by the Hasse–Weil theorem the number of S-integral morphisms that are constant is bounded by the size of k. Thus to prove Lang's conjecture for constant elliptic curves, we only need to bound the number of nonconstant separable S-integral morphisms in terms of L, S and $\mathrm{rank}\,\mathrm{Mor}_k(C, E)$.

Recall that the degree map, $\deg : \mathrm{Mor}_k(C, E) \longrightarrow \mathbb{Z}$, defines a nondegenerate quadratic form on $\mathrm{Mor}_k(C, E)/\mathrm{Mor}_k^0(C, E)$ that can be extended to a positive definite quadratic form on the real vector space $\mathrm{Mor}_k(C, E) \otimes \mathbb{R}$. As a consequence, $\mathrm{Mor}_k(C, E)/\mathrm{Mor}_k^0(C, E)$ is a lattice in $\mathrm{Mor}_k(C, E) \otimes \mathbb{R}$. This fact and the next result are the last ingredients needed in our proof of Theorem 1.2.

LEMMA 2.1. *Let V be an $\mathbb{R}$-vector space of dimension r, $\Lambda \subset V$ be a lattice and $q : V \longrightarrow \mathbb{R}$ be a positive definite quadratic form on V. If T is a positive real number then*

$$|\{x \in \Lambda : q(x) \leq T\}| \leq \left(2\sqrt{\frac{T}{\lambda}} + 1\right)^r$$

for $\lambda = \min\{q(x) : x \in \Lambda, x \neq 0\}$.

PROOF. Let $\Lambda(T) = \{x \in \Lambda : q(x) \leq T\}$, for a fixed real number $T > 0$. Suppose that a and b are distinct elements of $\Lambda(T)$ such that $\overline{a} = \overline{b}$ in $\Lambda/n\Lambda$, for some positive integer n. Therefore there exists a nonzero $u \in \Lambda$ such that $a - b = nu$. As a consequence, if $\lambda = \min\{q(x) : x \in \Lambda, x \neq 0\}$ then

$$n^2\lambda \leq n^2 q(u) = q(nu) = q(a - b) \leq 2q(a) + 2q(b) \leq 4T,$$

and

$$n \leq \sqrt{\frac{4T}{\lambda}}.$$

https://doi.org/10.1017/S0004972720000155 Published online by Cambridge University Press

Hence, if we choose n such that $\sqrt{4T/\lambda}+1 \geq n > \sqrt{4T/\lambda}$, then the set $\Lambda(T)$ will inject into $\Lambda/n\Lambda$. This implies

$$|\{x \in \Lambda : q(x) \leq T\}| \leq |\Lambda/n\Lambda| \leq n^r \leq \left(\sqrt{\frac{4T}{\lambda}}+1\right)^r. \qquad \square$$

Proof of Theorem 1.2. Let $\psi : C \longrightarrow E$ be a nonconstant separable map satisfying $\psi^{-1}(O) \subset S$. Let $e_\psi(P)$ denote the ramification index of ψ at a point $P \in C$ and denote by R_ψ the support of the ramification divisor of ψ. The Riemann–Hurwitz formula shows that

$$2g-2 \geq \sum_{P \in R_\psi} (e_\psi(P)-1) = \sum_{P \in R_\psi} e_\psi(P) - |R_\psi| \geq 2|R_\psi| - |R_\psi| = |R_\psi|$$

and

$$\sum_{P \in R_\psi} e_\psi(P) \leq 2g-2+|R_\psi| \leq 4(g-1).$$

Thus

$$\begin{aligned}\deg \psi &= \sum_{P \in \psi^{-1}(O)} e_\psi(P) = \sum_{P \in \psi^{-1}(O) \cap R_\psi^c} 1 + \sum_{P \in \psi^{-1}(O) \cap R_\psi} e_\psi(P) \\ &\leq |S| + \sum_{P \in R_\psi} e_\psi(P) \leq |S| + 4(g-1).\end{aligned}$$

This shows that a nonconstant separable morphism $\psi : C \longrightarrow E$ satisfying $\psi^{-1}(O) \subset S$ is contained in the set

$$\{\psi \in \mathrm{Mor}_k(C,E)/\mathrm{Mor}_k^0(C,E) : \deg \psi \leq |S| + 4(g-1)\}.$$

If we let $V = \mathrm{Mor}_k(C,E) \otimes \mathbb{R}$, $\Lambda = \mathrm{Mor}_k(C,E)/\mathrm{Mor}_k^0(C,E)$ and $q = \deg$ then Lemma 2.1 shows that the number of nonconstant separable S-integral morphisms is bounded by

$$\left(2\sqrt{\frac{|S|+4(g-1)}{\lambda}}+1\right)^r$$

where $\lambda = \min\{\deg \psi : \psi \in \mathrm{Mor}_k(C,E) \setminus \mathrm{Mor}_k^0(C,E)\}$. The result follows by noticing that $\lambda \geq 1$ and that, for constant elliptic curves, $r \leq 4g$ (see [2, 10.1]). $\square$

One can improve the upper bound given in Theorem 1.2 by decreasing the upper bound on the degree of nonconstant separable S-integral morphisms or finding a nontrivial lower bound for $\min\{\deg \psi : \psi \in \mathrm{Mor}_k(C,E) \setminus \mathrm{Mor}_k^0(C,E)\}$.

3. Integral points on quadratic twists

Let k be a finite field of odd characteristic. Let $A(t)$ be a square-free polynomial defined over k of odd degree $d > 1$ and let C_A denote the curve defined by $s^2 = A(t)$. We let E/k be an elliptic curve defined by $y^2 = f(x)$, for some cubic polynomial $f(x)$. Let O and ∞ be the points at infinity of E and C_A, respectively.

https://doi.org/10.1017/S0004972720000155 Published online by Cambridge University Press

3.1. Bounding separable integral points on constant elliptic curves over function fields of hyperelliptic curves. As discussed in Section 2, the set of nonconstant separable k-morphisms $\psi : C_A \longrightarrow E$ satisfying $\psi^{-1}(O) \subset \{\infty\}$ can be thought of as 'integral points' on the elliptic curve E over L, the function field of C_A. Theorem 1.2 shows that the number of such morphisms can be bounded in terms of $g = (d-1)/2$. In this section, we give an upper bound (see Corollary 3.3) that depends only on d and the size of k.

To obtain this new bound, we relate the set of ∞-integral k-morphisms to integral points on a quadratic twist of E. We let E_A be the elliptic curve defined over $k(t)$ by $A(t)y^2 = f(x)$. An *integral point* (F, G) on E_A is a point such that $F, G \in k[t]$.

LEMMA 3.1. *The set of nonconstant integral points on E_A is in bijection with the set of nonconstant k-morphisms $\psi : C_A \longrightarrow E$ satisfying $\psi^{-1}(O) \subset \{\infty\}$. Moreover, integral points (F, G) with $F' \neq 0$ correspond to nonconstant separable k-morphisms, and vice versa.*

PROOF. Clearly, the map

$$(F(t), G(t)) \longmapsto \psi(s, t) = (F(t), sG(t))$$

defines a bijection between the set of integral points on E_A and the set of k-morphisms $\psi : C_A \longrightarrow E$ of the form

$$\psi(s, t) = (F(t), sG(t)), \tag{3.1}$$

for some polynomials $F(t)$ and $G(t)$. A morphism of this form satisfies $\psi^{-1}(O) \subset \{\infty\}$. Thus, we are left to show that any k-morphism $\psi : C_A \longrightarrow E$ satisfying $\psi^{-1}(O) \subset \{\infty\}$ is given by (3.1).

Let $\sigma(t, s) = (t, -s)$ be the hyperelliptic involution of C_A. Using the group law on E, we define the morphism $\psi \circ \sigma + \psi : C_A \longrightarrow E$ which is invariant under the action of the group generated by σ. Hence $\psi \circ \sigma + \psi$ factors through $\mathbb{P}^1$, the quotient of C_A by the group generated by σ. Since a nonconstant map from $\mathbb{P}^1$ to E does not exist, $\psi^{-1}(O) \subset \{\infty\}$ implies that $\psi \circ \sigma + \psi = O$, that is, $\psi \circ \sigma = -\psi$.

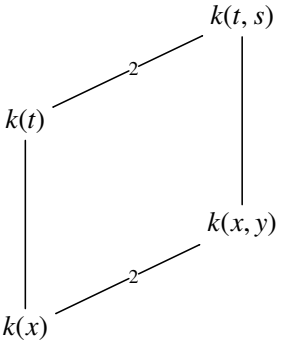
Let us write $\psi(t, s) = (F_0(t, s), G_0(t, s))$, for some rational functions F_0 and G_0 of $k(C_A)$. The equation

$$(F_0(t, -s), G_0(t, -s)) = \psi(t, -s) = \psi \circ \sigma = -\psi = (F_0(t, s), -G_0(t, s))$$

implies that $F_0(t, s) = F(t)$ is a rational function on t and that $G_0(t, s) = sG(t)$, where $G(t)$ is a rational function on t. Since $\psi^{-1}(O) \subset \{\infty\}$, we see that both $F(t)$ and $G(t)$ are polynomials and ψ has the desired form.

https://doi.org/10.1017/S0004972720000155 Published online by Cambridge University Press

To prove the 'moreover' part of the theorem, we look at the diagram of the function field extensions determined by (3.1):



Both degree-two extensions are separable. Hence $k(t,s)/k(x,y)$ is separable if and only if $k(t)/k(x)$ is separable. The polynomial $F(T)-x \in k(x)[T]$ is irreducible, so the extension $k(t)/k(x)$ is separable if and only if $(F(T)-x)' = F'(T) \neq 0$. □

In light of the previous result, we say that (F,G) on E_A is a *separable integral point* if $F, G \in k[t]$ and $F' \neq 0$. In the next result we bound the 'height' of such points.

Lemma 3.2. *Let (F,G) be a separable integral point on E_A. Then G divides F' and $d/3 \leq \deg F < d-1$.*

Proof. An integral point $(F,G) = (F(t), G(t))$ on E_A satisfies the identity

$$A(t)G(t)^2 = f(F(t)). \tag{3.2}$$

By equating degrees, we arrive at $d \leq 3 \deg F$.

To show that G divides F', let β be a root of $G(t)$ of multiplicity r. By (3.2), $(t-\beta)^r$ divides $f(F(t))$ and, consequently, $F(\beta)$ is a root of $f(x)$. By differentiating (3.2), we arrive at

$$A'(t)G(t)^2 + 2A(t)G(t)G'(t) = F'(t)f'(F(t)) \tag{3.3}$$

and we conclude that $(t-\beta)^r$ divides $F'(t)f'(F(t))$. If $\gcd(t-\beta, f'(F(t))) \neq 1$ then $F(\beta)$ is a root of $f'(x)$, contradicting the fact that $f(x)$ has no repeated roots. Hence $(t-\beta)^r$ divides $F'(t)$, which shows that G divides F'.

The desired upper bound for $\deg F$ follows from the fact that $G(t)$ divides $F'(t)$. Indeed, this statement implies $\deg G \leq \deg F - 1$ and, after comparing degrees in (3.2), we arrive at $\deg F < d-1$. □

Corollary 3.3. *The number of nonconstant separable k-morphisms $\psi : C_A \longrightarrow E$ satisfying $\psi^{-1}(O) \subset \{\infty\}$ is bounded by $|k|^{2d-3}$.*

Proof. By Lemma 3.1, it is enough to count the number of integral points (F,G) on E_A with $F' \neq 0$. From Lemma 3.2, $\deg G \leq \deg F - 1$ and $\deg F < d-1$. Therefore, $\deg G < d-2$ and the number of integral points (F,G) on E_A with $F' \neq 0$ is at most

$$|\{(F,G) : F, G \in k[t], \deg F < d-1, \deg G < d-2\}| = |k|^{d-1} \cdot |k|^{d-2},$$

as desired. □

https://doi.org/10.1017/S0004972720000155 Published online by Cambridge University Press

3.2. Integral points on quadratic twists and isomorphism classes. In Lemma 3.2 we proved that if (F, G) is a separable integral point on $E_A : A(t)y^2 = f(x)$, then $d/3 \le \deg F < d - 1$. In this section we prove that if we assume the existence of a separable integral point (F, G) with $d/3 \le \deg F \le (d-1)/2$ then $j(E) = 1728$, where E is the elliptic curve defined by $y^2 = f(x)$.

THEOREM 3.4. *Suppose $A'(t) \equiv \gamma \in \mathbb{F}_q^*$. Let $E : y^2 = f(x)$ be an elliptic curve defined over k. Suppose (F, G) is an integral point of $E_A/k(t)$ satisfying $F' \neq 0$. Then the following three conditions are equivalent:*

(A) $2 \deg F \le d - 1$;
(B) $2 \deg G \le \deg F - 1$;
(C) $G^2 = \beta F'$, *for some* $\beta \in k^*$.

Furthermore, if any one of the above conditions is true then $j(E) = 1728$.

PROOF. From (3.2), $d + 2 \deg G = 3 \deg F$, and from this it easily follows that (A) is equivalent to (B). It is also clear that (C) implies (B), so all we need to show is that (B) implies (C).

Since both F and G are defined over k, a constant β satisfying (C) is an element of k. Therefore, to prove that (B) implies (C) we may work over an extension of k where $f(x)$ factors.

Let $f(x) = (x - \alpha_0)(x - \alpha_1)(x - \alpha_2)$ and denote $F - \alpha_i$ by F_i, for $i \in \{0, 1, 2\}$. Then

$$f(F) = F_0 F_1 F_2,$$

the F_i are pairwise coprime and

$$F_i F_j \equiv (\alpha_l - \alpha_i)(\alpha_l - \alpha_j)) \pmod{F}_l, \tag{3.4}$$

for $\{i, j, l\} = \{0, 1, 2\}$.

By equating degrees in (3.2), we obtain $\deg F_i \equiv d \equiv 1 \pmod 2$. Consequently, by unique factorisation and (3.2), we can find a nonconstant polynomial N_i satisfying

$$\gcd(A, F_i) = N_i.$$

Since the F_i are pairwise coprime, we can find a polynomial S_i such that

$$F_i = N_i S_i^2. \tag{3.5}$$

We write $s_i = \deg S_i$ and assume, without loss of generality, that

$$s_0 \ge s_1 \ge s_2 \ge 0. \tag{3.6}$$

Also, observe that

$$G = S_0 S_1 S_2 \tag{3.7}$$

and

$$A = N_0 N_1 N_2. \tag{3.8}$$

https://doi.org/10.1017/S0004972720000155 Published online by Cambridge University Press

Given (3.7) and (3.8), it follows from (3.3) that

$$\gamma G^2 + 2N_0N_1N_2S_0S_1S_2(S_0'S_1S_2 + S_0S_1'S_2 + S_0S_1S_2') = F'(F_0F_1 + F_0F_2 + F_1F_2).$$

Thus, from (3.5),

$$\gamma G^2 + 2N_0S_0S_0'F_1F_2 + 2N_1S_1S_1'F_0F_2 + 2N_2S_2S_2'F_0F_1 = F'(F_0F_1 + F_0F_2 + F_1F_2).$$

For $l \in \{0, 1, 2\}$, this equality and (3.4) imply

$$G^2 + 2\beta_l N_l S_l S_l' \equiv \beta_l F_l' \pmod{F}_l, \tag{3.9}$$

where

$$\beta_l = (\alpha_l - \alpha_i)(\alpha_l - \alpha_j)/\gamma. \tag{3.10}$$

Since

$$F' = F_i' = N_i' S_i^2 + 2N_i S_i S_i', \tag{3.11}$$

(3.9) yields

$$G^2 \equiv \beta_l N_l' S_l^2 \pmod{F}_l.$$

Clearly, $\deg(N_l' S_l^2) < \deg F_l = \deg F$. Therefore if (B) is true, we get $\deg G^2 < \deg F$; and ultimately,

$$G^2 = \beta_l N_l' S_l^2 \tag{3.12}$$

for $l \in \{0, 1, 2\}$.

Now consider $\{i, l\} = \{1, 2\}$. Multiplying (3.11) by β_i and using (3.12),

$$\beta_i F' = G^2 + 2\beta_i N_i S_i S_i'.$$

Lemma 3.2 implies that G divides $2\beta_i N_i S_i S_i'$. Thus, from (3.7),

$$S_0 S_l \mid 2\beta_i N_i S_i',$$

since $(S_0 S_l, N_i) = 1$. This in turn implies

$$S_0 S_l \mid 2\beta_i S_i'.$$

Notice that $S_i' = 0$, for $i = 1, 2$, since otherwise (3.6) would imply

$$s_i \le s_0 + s_l \le s_i - 1.$$

Thus, (3.11) becomes

$$F_i' = N_i' S_i^2,$$

and (3.12) gives

$$G^2 = \beta_i N_i' S_i^2 = \beta_i F_i' = \beta_i F'.$$

This finishes the proof that (A), (B) and (C) are equivalent.

To show the second part, assume that one of the equivalent statements (A), (B) or (C) is true. Then the last equality shows that necessarily $\beta = \beta_1 = \beta_2$, since $F' \neq 0$.

https://doi.org/10.1017/S0004972720000155 Published online by Cambridge University Press

By performing a change of variable $x \longmapsto x + \alpha_0$, we obtain an elliptic curve isomorphic to E, and we may assume that $\alpha_0 = 0$. Therefore, from (3.10) we arrive at

$$\frac{\alpha_1(\alpha_1 - \alpha_2)}{\gamma} = \beta_1 = \beta_2 = \frac{\alpha_2(\alpha_2 - \alpha_1)}{\gamma}.$$

Thus, $\alpha_1^2 = \alpha_2^2$. Since the α_i are all distinct, we have $\alpha_1 = -\alpha_2 \neq 0$. This shows that E is isomorphic over k (or an extension of k) to $y^2 = x^3 - a^2x$, for $a = \alpha_2$. Since this last elliptic curve has j-invariant 1728, the result follows. □

We give an example to show that the hypotheses in Theorem 3.4 do not give vacuous conditions.

Example 3.5. Let k be a finite field of size $q \equiv 3 \pmod 4$. Then

$$(t^{(q-1)/2}, t^{(q-3)/4})$$

is a separable integral point on $(t^q - t)y^2 = x^3 - x$.

References

[1] M. Hindry and J. H. Silverman, 'The canonical height and integral points on elliptic curves', *Invent. Math.* **93**(2) (1988), 419–450.

[2] D. Ulmer, 'Elliptic curves with large rank over function fields', *Ann. of Math. (2)* **155**(1) (2002), 295–315.

[3] D. Ulmer, 'Elliptic curves over function fields', in: *Arithmetic of L-functions*, IAS/Park City Mathematics Series, 18 (American Mathematical Society, Providence, RI, 2011), 211–280.

RICARDO CONCEIÇÃO, Gettysburg College,
300 N Washington St., Gettysburg, PA 17325, USA
e-mail: rconceic@gettysburg.edu

https://doi.org/10.1017/S0004972720000155 Published online by Cambridge University Press