BULL. AUSTRAL. MATH. SOC. 11G05, 11R58
VOL. 58 (1998) [353-357]

INTEGRAL POINTS ON ELLIPTIC CURVES OVER FUNCTION FIELDS OF POSITIVE CHARACTERISTIC

AMÍLCAR PACHECO

Let K be a one variable function field of genus g defined over an algebraically closed field k of characteristic $p > 0$. Let E/K be a non-constant elliptic curve. Denote by M_K the set of places of K and let $S \subset M_K$ be a non-empty finite subset .

Mason in his paper "Diophantine equations over function fields" Chapter VI, Theorem 14 and Voloch in "Explicit p-descent for elliptic curves in characteristic p" Theorem 5.3 proved that the number of S-integral points of a Weiertrass equation of E/K defined over R_S is finite. However, no explicit upper bound for this number was given. In this note, under the extra hypotheses that E/K is semi-stable and $p > 3$, we obtain an explicit upper bound for this number for a certain class of Weierstrass equations called S-minimal.

1. INTRODUCTION

The paper is organised as follows. In Section 2 we introduce some preliminaries on the canonical height and torsion points of E. In Section 3 we show our main result on S-integral points.

2. PRELIMINARIES

Let $\widehat{h} : E(\overline{K}) \to \mathbb{R}$ be the canonical height of E. Given a place $\mathfrak{p}$ of K, let $v_{\mathfrak{p}}$ be the normalised valuation of K corresponding to $\mathfrak{p}$, $K_{\mathfrak{p}}$ the completion of K with respect to $v_{\mathfrak{p}}$ and $\lambda_{\mathfrak{p}} : E(K_{\mathfrak{p}}) \to \mathbb{R}$ the Néron function associated to $\mathfrak{p}$ (see [8, Chapter VI]).

Suppose that E/K is semi-stable. Let X be a smooth irreducible projective curve defined over k with function field K. Denote by $\varphi_{\mathcal{E}} : \mathcal{E} \to X$ the semi-stable minimal model of E/K. Let $j_{\mathcal{E}} : X \to \mathbb{P}^1_k$ be the j-map induced by $\varphi_{\mathcal{E}}$ and p^e its inseparable degree. In the sequel we regard $j_{\mathcal{E}}$ as an element of K.

Goldfeld and Szpiro in [2, Proposition 11] gave an explicit version of a Theorem of Manin in which $\widehat{h}$ is computed in terms of an intersection number in $\mathcal{E}$. This allows the

Received 27th January, 1998
This work was partially supported by CNPq research grant number 300896/91-3 and Pronex, Brazil.

decomposition $\widehat{h}(P) = \sum\limits_{\mathfrak{p}\in M_K} \lambda_{\mathfrak{p}}(P)$ and reduces the problem of finding a lower bound for the canonical height of points P of infinite order of E to bounding Néron's functions at P. The main ingredient to obtain a global result is the following lemma due to Hindry and Silverman.

Lemma 1. [4, Proposition 1.2] *Let $\mathfrak{p} \in M_K$ be such that $v_{\mathfrak{p}}(j_{\mathcal{E}}) < 0$. For any distinct points $P_0, \cdots, P_N \in E(K_{\mathfrak{p}})$ we have* $\sum\limits_{i\neq l} \lambda_{\mathfrak{p}}(P_i - P_l) \geqslant \Big((N+1)^2/12 v_{\mathfrak{p}}(j_{\mathcal{E}}^{-1})\Big) - \Big((N+1)v_{\mathfrak{p}}(j_{\mathcal{E}}^{-1})/12\Big)$.

Definition 2: Let $\mathfrak{D}_{E/K}$ be the minimal discrimimant of E/K and $\mathfrak{F}_{E/K}$ its conductor. Denote $d_{E/K} = \deg(\mathfrak{D}_{E/K})$ and $f_{E/K} = \deg(\mathfrak{F}_{E/K})$. Let $\sigma_{E/K} = d_{E/K}/f_{E/K}$ be the Szpiro's ratio of E/K. Since E/K is semi-stable, $d_{E/K} = \deg(j_{\mathcal{E}}) = \Big[K : k(j_{\mathcal{E}})\Big]$.

Convention. Given a finite set T we denote by $|T|$ its cardinal.

Proposition 3. *The set $\mathcal{S}_\sigma = \Big\{P \in E(K) ; \widehat{h}(P) \leqslant d_{E/K}\sigma_{E/K}^{-2}/96\Big\}$ has at most $2\sigma_{E/K}^2$ elements.*

Proof: Suppose that $|\mathcal{S}_\sigma| > 2\sigma_{E/K}^2$. Let $N \geqslant 1$ be any integer such that $2\sigma_{E/K}^2 < N+1 \leqslant |\mathcal{S}_\sigma|$. Let $\mathfrak{p} \in M_K$ be such that $v_{\mathfrak{p}}(j_{\mathcal{E}}) \geqslant 0$. It follows from [5, Chapter XI, Theorem 5.1] that for any $P \in E(K)$, $\lambda_{\mathfrak{p}}(P) \geqslant 0$. Given $P_0, \cdots, P_N \in E(\overline{K})$, let $H = \max\limits_{0\leqslant i\leqslant N} \widehat{h}(P_i)$. It follows from the triangle inequality that $H \geqslant \Big(1/(4N(N+1))\Big) \sum\limits_{i\neq l} \widehat{h}(P_i - P_l)$. Hence, Proposition 1 implies $H \geqslant \Big(1/(48N)\Big) \sum\limits_{\mathfrak{p}}{}' \Big(((N+1)/v_{\mathfrak{p}}(j_{\mathcal{E}}^{-1})) - v_{\mathfrak{p}}(j_{\mathcal{E}}^{-1})\Big)$, where where $\sum\limits_{\mathfrak{p}}{}'$ denotes the sum over $\mathfrak{p} \in M_K$ such that $v_{\mathfrak{p}}(j_{\mathcal{E}}) < 0$. Since $\sum\limits_{\mathfrak{p}}{}' v_{\mathfrak{p}}(j_{\mathcal{E}}^{-1}) = d_{E/K}$ and $\Big|\Big\{\mathfrak{p} \in M_K ; v_{\mathfrak{p}}(j_{\mathcal{E}}) < 0\Big\}\Big| = f_{E/K}$, $H \geqslant \Big(1/(48N)\Big)\Big((N+1)d_{E/K}\sigma_{E/K}^{-2} - d_{E/K}\Big)$. By hypothesis $N+1 > 2\sigma_{E/K}^2$, therefore $H > d_{E/K}\sigma_{E/K}^{-2}/96$. ∎

Corollary 4. *For every $P \in E(K)$ of infinite order we have $\widehat{h}(P) \geqslant (d_{E/K}\,\sigma_{E/K}^{-6})/1536$.*

Proof: Suppose that $\widehat{h}(P) < d_{E/K}\sigma_{E/K}^{-6}/1536$. For any integer n such that $1 \leqslant n \leqslant 4\sigma_{E/K}^2$, $\widehat{h}(nP) = n^2\widehat{h}(P) = d_{E/K}\sigma_{E/K}^{-2}/96$. But this shows that $|\mathcal{S}_\sigma| \geqslant 4\sigma_{E/K}^2$, which contradicts Proposition 3. ∎

Corollary 4 implies the following version of a conjecture of Lang (see [3, Theorem 0.2]).

Theorem 5. *For every $P \in E(K)$ of infinite order there exists a constant $c_2(j_{\mathcal{E}}, g)$ depending on g and on the inseparable degree p^e of $j_{\mathcal{E}} : X \to \mathbb{P}_k^1$ such that $\widehat{h}(P) \geqslant c_2(j_{\mathcal{E}}, g)d_{E/K}$, where $c_2(j_{\mathcal{E}}, g)$ is equal to $\Big((2.18)10^{-10}\Big)p^{-6e}$, if $d_{E/K} \geqslant 24p^e(g-1)$ and to $\Big((3.4)10^{-12}\Big)p^{-6e}g^{-6}$, if $d_{E/K} < 24p^e(g-1)$.*

PROOF: Szpiro's theorem on the minimal discriminant of elliptic curves over function fields states that $d_{E/K} \leqslant 6p^e(2g-2+f_{E/K})$ (see [**9**, Théorème 1]). Hence, $\sigma_{E/K}^{-1} \geqslant (6p^e)^{-1} - (2g-2)d_{E/K}^{-1}$. In the case where $d_{E/K} \geqslant 24p^e(g-1)$, we obtain $\sigma_{E/K} \leqslant 12p^e$. Otherwise, $\sigma_{E/K} \leqslant d_{E/K} < 24p^e(g-1)$. These two inequalities and Corollary 4 prove the theorem. ∎

REMARK 6. Theorem 5 slightly improves [**3**, Theorem 0.2] in the sense that the lower bound for the canonical height of points of infinite order depends polynomially on $\sigma_{E/K}$, instead of exponentially. This had already been remarked and proved for elliptic curves over number fields by David (see [**1**, Corollaire 1.5]) using transcendence methods, which in contrast with Hindry-Silverman's method is global rather than local.

As a consequence of Proposition 3 we obtain an upper bound for the torsion subgroup $E(K)_{\text{tor}}$ of $E(K)$.

THEOREM 7. $\left|E(K)_{\text{tor}}\right| \leqslant 2\sigma_{E/K}^2$.

REMARK 8. In [**2**, Theorem 13] Goldfeld and Szpiro proved that $\left|E(K)_{\text{tor}}\right| \leqslant \left(6p^e((2g-2)f_{E/K}^{-1}+1)\right)^2$. It follows from Szpiro's discriminant theorem that the bound of Theorem 7 is twice the bound of [**2**, Theorem 13]; however the method is different.

3. INTEGRAL POINTS

DEFINITION 9: Let $R_S \subset K$ be the ring of S-integers and $R_S^* \subset R_S$ the group of S-units. Let L be a finite extension of K and $\alpha \in L$. Define $h_L(\alpha) = \left[L : k(\alpha)\right]$, if $\alpha \notin k$, otherwise $h_L(\alpha) = 0$. Denote by S_L the set of places of L lying over S. Let g_L be the genus of L, $R_{S_L} \subset L$ the ring of S_L-integers and $R_{S_L}^* \subset R_{S_L}$ the subgroup of S_L-units.

DEFINITION 10: Let $y^2 = f(x)$ be a Weierstrass equation for E/K. Suppose that $f(X) \in R_S[X]$ and denote by Δ its discriminant. This equation is called S-minimal if $h_K(\Delta)$ is minimal subject to $f(X) \in R_S[X]$.

DEFINITION 11: Let $f(X) = (X-\varepsilon_1)(X-\varepsilon_2)(X-\varepsilon_3)$ be the factorisation of $f(X)$ in $\overline{K}[X]$. Given $P = (x_P, y_P) \in E(R_S)$ and $i \in \{1,2,3\}$, let $\xi_i^2 = x_P - \varepsilon_i$ and $L = K(\varepsilon_1, \varepsilon_2, \varepsilon_3, \xi_1, \xi_2, \xi_3)$. For any permutation $\{i, l, m\}$ of the elements of $\{1,2,3\}$, let $\Xi = \left\{(\xi_i - \xi_l)/(\xi_i - \xi_m), (\xi_i - \xi_l)/(\xi_i + \xi_m), (\xi_i + \xi_l)/(\xi_i - \xi_m), (\xi_i + \xi_l)/(\xi_i + \xi_m)\right\}$.

The main result needed to obtain an explicit bound for the number of S-integral points of an S-minimal Weierstrass equation for E is an upper bound for the height of the y-coordinates of integral points (see [**3**, Proposition 8.2]). Before doing this it is necessary to obtain an upper bound for the height of S-units.

PROPOSITION 12. *Let $y^2 = f(x)$ be a Weierstrass equation for E/K. Suppose that $f(X) \in R_S[X]$, $\Delta \in R_S^*$ and $p > 2$. For any $\eta \in \Xi$ we have $h_L(\eta) \leqslant 2p^e\left(2g_L - 2 + |S_L|\right)$.*

https://doi.org/10.1017/S0004972700032329 Published online by Cambridge University Press

PROOF: Let $t = (\varepsilon_3 - \varepsilon_1)/(\varepsilon_2 - \varepsilon_1)$ and denote by $y^2 = x(x-1)(x-t)$ a Legendre form of E/K. Note that since the inseparable degree of $j_{\mathcal{E}}$ is p^e, $j_{\mathcal{E}} \in K^{p^e} - K^{p^{e+1}}$. But $j_{\mathcal{E}} = 2^8(t^2-t+1)^3/(t^2(t-1)^2)$, thus $t \notin L^{p^{e+1}}$. Furthermore, any permutation of 1, 2 and 3 replaces t by an element of $\Big\{t, 1-t, 1/t, 1/(t-1), t/(t-1), (t-1)/t\Big\}$. Therefore, for any distinct $i, l, m \in \{1,2,3\}$, $\kappa = (\varepsilon_l - \varepsilon_i)/(\varepsilon_m - \varepsilon_i) = \Big((\xi_i - \xi_l)/(\xi_i - \xi_m)\Big)\Big((\xi_i + \xi_l)/(\xi_i + \xi_m)\Big) \notin L^{p^{e+1}}$. Suppose that for any $\eta \in \Xi$ we have $\eta \notin L^{p^{e+1}}$. Let $0 \leqslant r, s \leqslant e$ be the smallest integers such that $\kappa \in L^{p^r} - L^{p^{r+1}}$ and $\eta \in L^{p^s} - L^{p^{s+1}}$, respectively. Denote $\kappa_r = \kappa^{p^r}$ and $\eta_s = \eta^{p^s}$. Observe that $\kappa_r, 1-\kappa_r, \eta_s, 1-\eta_s \in R^*_{S_L} \cap (L - L^p)$. It follows from [**6**, Chapter VI, Lemma 10] that $h_L(\kappa_r), h_L(\eta_s) \leqslant 2g_L - 2 + |S_L|$. Hence, $h_L(\kappa), h_L(\eta) \leqslant p^e\Big(2g_L - 2 + |S_L|\Big)$. If some $\eta \in \Xi$ lies in $L^{p^{e+1}}$, then $\tau = \kappa\eta^{-1} \notin L^{p^{e+1}}$. By using the same argument as above we conclude that $h_L(\tau) \leqslant p^e\Big(2g_L - 2 + |S_L|\Big)$. Therefore, $h_L(\eta) = h_L(\kappa) + h_L(\tau) \leqslant 2p^e\Big(2g_L - 2 + |S_L|\Big)$, which proves the proposition. ∎

PROPOSITION 13. *With the same hypothesis and notation of Proposition 12, suppose furthermore that $p > 3$. For any $P = (x_P, y_P) \in E(R_S)$ we have $h_K(y_P^4/\Delta) \leqslant 48p^e\Big(2g - 2 + |S|\Big)$.*

PROOF: The proof follows the same lines as [**3**, Proposition 8.2] replacing [**3**, (42)] by the inequality of Proposition 12. However, we need to remark that the Riemann-Hurwitz formula can be applied for L/K, because $p > 3$ implies that L/K is separable and has no wild ramification. ∎

In order to obtain an explicit upper bound for $|E(R_S)|$, recall from [**7**, Lemma 1.2 (a)] that $\Big|E(R_S)\Big| \leqslant \Big|E(K)_{\text{tor}}\Big|(1 + 2\sqrt{\beta/\alpha})^{r_E}$, where $\alpha = \min\Big\{\widehat{h}(P)\,;\, P \in (E(K) - E(K)_{\text{tor}}) \cap E(R_S)\Big\}$, $\beta = \max\Big\{\widehat{h}(P)\,;\, P \in E(R_S)\Big\}$ and $r_E = \operatorname{rank}\Big(E(K)\Big)$. The lower bound α is obtained from Theorem 5.

REMARK 14. Since $p > 3$, we write the Weierstrass equation of E/K as $y^2 = x^3 + Ax + B$. Suppose it is S-minimal. In this case, $\beta \leqslant p^e(12g + 4|S| + 5d_{E/K})$. The proof of this inequality is the same as in [**3**, Corollary 8.5] replacing [**3**, Proposition 8.2] by Proposition 13.

THEOREM 15. *Suppose that $p > 3$ and $y^2 = x^3 + Ax + B$ is an S-minimal equation for E/K. If $d_{E/K} \geqslant 24p^e(g-1)$, then $\Big|E(R_S)\Big| \leqslant 288p^{2e}\Big(((8.57)10^5)p^{4e}\sqrt{|S|}\Big)^{r_E}$; otherwise $\Big|E(R_S)\Big| \leqslant (1152)p^{2e}g^2\Big(((2.51)10^7)p^{4e}g^4\sqrt{|S|}\Big)^{r_E}$.*

PROOF: Suppose that $d_{E/K} \geqslant 24p^e(g-1)$. Thus $g \leqslant d_{E/K}p^{-e}/24 + 1$ and $\sigma_{E/K} \leqslant 12p^e$. Since $|S| \geqslant 1$, $\beta/\alpha \leqslant \Big((4.59)10^9\Big)p^{7e}\Big(5 + (12g + 4|S|)d_{E/K}^{-1}\Big) \leqslant \Big((4.59)10^{11}\Big)p^{7e}|S|$. Theorem 7 implies $\Big|E(K)_{\text{tor}}\Big| \leqslant 2\sigma_{E/K}^2 \leqslant 288p^{2e}$. This proves the first part of the theorem. Suppose now that $d_{E/K} < 24p^e(g-1)$. In this case, since $|S| \geqslant 1$ and $g \geqslant 2$, $\beta/\alpha \leqslant \Big((2.94)10^{11}\Big)p^{7e}g^6\Big(5 + (12g + 4|S|)d_{E/K}^{-1}\Big) \leqslant \Big((3.94)10^{13}\Big)p^{7e}g^7|S|$. It follows from

https://doi.org/10.1017/S0004972700032329 Published online by Cambridge University Press

Theorem 7 that $\left|E(K)_{\mathrm{tor}}\right| \leqslant 2\sigma_{E/K}^2 < 2\Big(24p^e(g-1)\Big)^2$. Hence, the second part of the theorem is proved. $\square$

REMARK 16. Theorem 15 is an analogue for $\mathrm{char}(k) = p > 3$ of [**3**, Theorem 8.1].

REFERENCES

[1] S. David, 'Points de petite hauteur sur les courbes elliptiques', *J. Number Theory* **64** (1995), 104–129.

[2] D. Goldfeld and L. Szpiro, 'Bounds for the Tate-Shafarevich group', *Compositio Math.* **86** (1995), 71–87.

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

[4] M. Hindry and J. Silverman, 'On Lehmer's conjecture for elliptic curves', in *Séminaire de Théorie des Nombres Paris 1988-89 (1989)*, Progr. Math. **91** (Birkhaüser, Boston, MA, 1990), **pp.** 103–116.

[5] S. Lang, *Fundamentals of diophantine geometry* (Springer-Verlag, Berlin, Heidelberg, New York, 1983).

[6] R.C. Mason, *Diophantine equations over function fields*, Lecture Notes of the London Math. Soc. **96** (Cambridge University Press, Cambridge, London, 1984).

[7] J. Silverman, 'A quantitative version of Siegel's theorem: integral points on elliptic curves and Catalan curves', *J. Reine Angew. Math.* **378** (1987), 60–100.

[8] J. Silverman, *Advanced topics in the arithmetic of elliptic curves* (Springer-Verlag, Berlin, Heidelberg, New York, 1994).

[9] L. Szpiro, 'Discriminant et conducteur d'une courbe elliptique', *Astérisque* **86** (1990), 7–18.

[10] J.F. Voloch, 'Explicit p-descent for elliptic curves in characteristic p', *Compositio Math.* **74** (1990), 247–258.

Rua Guaiaquil 83
Cachambi
20785-050 Rio de Janeiro, RJ
Brasil
e-mail: amilcar@impa.br