J. Aust. Math. Soc. **77** (2004), 197–208

INTEGRAL POINTS ON ELLIPTIC CURVES OVER FUNCTION FIELDS

W.-C. CHI, K. F. LAI and K.-S. TAN

(Received 8 January 2003; revised 28 May 2003)

Communicated by King Lai

Abstract

We prove a new formula for the number of integral points on an elliptic curve over a function field without assuming that the coefficient field is algebraically closed. This is an improvement on the standard results of Hindry-Silverman.

2000 *Mathematics subject classification*: primary 11G05; secondary 14H52.

1. Introduction

Serge Lang has conjectured that on a minimal Weierstrass equation of an elliptic curve over a number field, the number of integral points should be bounded solely in terms of the field and the rank of the group of rational points [4, page 140]. Hindry and Silverman [3] proved an analogue of Lang's conjecture for non-constant elliptic curves over zero-characteristic one-dimensional function fields. Influenced by the original work of Mason [5], we use a formula on 2-divison points given by Tan [7] and the method of Evertse [1, 2] to prove another analogue of Lang's conjecture for these curves.

Let K be the field of rational functions on an algebraic curve of genus g over the constant field k of characteristic 0. We do not assume that k is algebraically closed. Let M_K denote the set of all places of K. For a finite subset S of M_K, denote by $\mathcal{O}_S$ the ring of S-integers of K. Consider a non-constant elliptic curve E defined by

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathcal{O}_S. \tag{1}$$

The set of S-integral points of this curve is $E(\mathcal{O}_S) = \{P \in E(K) : x(P), y(P) \in \mathcal{O}_S\}$. Let $\Delta = -(4A^3 + 27B^2)$ be the discriminant of the equation (1) and $\mathcal{D}_{E/K}$ be the divisor of the minimal discriminant of E/K. Then we have

$$(2) \qquad (\Delta) = \mathcal{D}_{E/K} + 12 \sum_{v \in M_K} \rho_v \cdot v,$$

for some integers ρ_v, where $\rho_v \geq 0$, if $v \notin S$. Let α, β, γ be the three roots of $x^3 + Ax + B = 0$ (in some extension field) and let m be the degree $[K(\alpha, \beta, \gamma) : K]$ which is at most 6. Define

$$S_1 = \{v \in M_K : v \notin S, v(\Delta) > 0, \rho_v = 0\} \quad \text{and}$$
$$S_2 = \{v \in M_K : v \notin S, \rho_v > 0\}.$$

Denote by s, s_1, s_2 the cardinality of S, S_1 and S_2. Denote the rank of $E(K)$ by r. Let $h_K(\mathcal{D}_{E/K})$ be the height of $\mathcal{D}_{E/K}$ (see Section 2.1). Put

$$a_E = \begin{cases} 144 & \text{if } h_K(\mathcal{D}_{E/K}) \geq 24(g-1); \\ (8\pi^2(g-1))^{2/3} & \text{if } h_K(\mathcal{D}_{E/K}) < 24(g-1), \end{cases}$$

$$b_E = \begin{cases} 20 \cdot 10^{5.75} + 1 & \text{if } h_K(\mathcal{D}_{E/K}) \geq 24(g-1); \\ 20 \cdot 10^{5.5+11.5g} + 1 & \text{if } h_K(\mathcal{D}_{E/K}) < 24(g-1). \end{cases}$$

THEOREM. $|E(\mathcal{O}_S)| \leq a_E \cdot (b_E)^r + 810 \cdot 24^r \cdot 2^{24m(s+s_2)}$.

Let us compare the above theorem with the result of Hindry and Silverman ([3]). Let

$$c_E = \begin{cases} 10^{7.1} & \text{if } h_K(\mathcal{D}_{E/K}) \geq 24(g-1); \\ 10^{7+12g} & \text{if } h_K(\mathcal{D}_{E/K}) < 24(g-1). \end{cases}$$

THEOREM 1.1 ([3, Theorem 0.6]). *Let K be a one-dimensional function field of characteristic* 0 *and genus g, and let E/K be a non-constant elliptic curve given by an S-minimal equation* (1). *Then* $|E(\mathcal{O}_S)| \leq a_E(c_E\sqrt{|S|})^r$.

First, we note that in our theorem, we do not need to restrict ourselves to the cases where E is S-minimal. Also, in [3], there is no explicit formula given for the symbol $|S|$. Consider the elliptic curve E defined over $K = \mathbb{Q}(t)$ by $Y^2 = X^3 - p(t)X$, where $p(t) = t^{2l} + 2t^l + 2$, and l is a large integer. Its discriminant is $\Delta = 4p(t)^3$. Take $S = \{\infty, v_{p(t)}\}$ and $R = (x, y) = (-1, t^l - 1)$. Then R is an S-integral point of E. The Weil height of y is l, but the size of S is 2. If Proposition 8.2 in [3] is to be true, then $|S|$ should not be the cardinality of S which is 2 here. Instead $|S|$

should be $2l+1$, which is the size of the places of $\overline{\mathbb{Q}}(t)$ sitting over S. But then we see that there are countably infinitely many cases where our bound is better than Hindry-Silverman's bound.

Here is the sketch of the proof. We first divide the set of S-integer points into two subsets, the first contains points with heights bounded above by a constant which depends on E, the second contains the remaining points. We bound the cardinality of the first set by using the counting method from [3] which applies the result of Mason [5]. For the second set, we associate to an S-integer point some unit equations over certain field extension and use the machinery developed by Evertse [1, 2].

2. Heights and 2-division points

2.1. Heights Let us fix our convention on the heights on fields. We can consider K as a finite extension of a rational function field $k(t)$.

Let I be a maximal set of pairwise non-associate irreducible polynomials in $k[t]$. For $\xi(t) \in k(t)^*$, write $\xi(t) = C\prod_{\eta\in I}\eta^{n_\eta(\xi)}$, where $C \in k^*$ and only finitely many of the integers $n_\eta(\xi)$ are non-zero. Put $v_\eta(\xi) = \deg(\eta)n_\eta(\xi)$. Define $\deg(v_\eta) = \deg(\eta)$.

If $\xi = \xi_1/\xi_2$, with $\xi_1, \xi_2 \in k[t]$, put $v_\infty(\xi) = \deg(\xi_2) - \deg(\xi_1)$. Also, define $\deg(v_\infty) = 1$. Then we have the product formula

$$\sum_{v\in M_{k(t)}} v(\xi) = 0,$$

where $M_{k(t)} = \{v_\infty\} \cup \{v_\eta : \eta \in I\}$ is the set of valuations on $k(t)$.

Following Evertse [2, Section 1.3], we have on K a set M_K of valuations which are normalized with respect to $M_{k(t)}$ and the product formula $\sum_{v\in M_K} v(\xi)$, for every $\xi \in K^*$ also holds. Thus each valuation $v \in M_K$ is obtained from a rational irreducible divisor, denoted as $[v]$.

For any $v \in M_K$, there is an associated $v_0 \in M_{k(t)}$ and a positive integer e_v such that $v(\xi) = e_v v_0(\xi)$, for every $\xi \in k(t)^*$. Let K_v, $k(t)_{v_0}$ be respectively the completions of K and $k(t)$. Then the degree of v is defined as follows

$$\deg(v) = [K_v : k(t)_{v_0}]\deg(v_0).$$

The height h_K on K is defined by $h_K(\xi) = \sum_{v\in M_K} \max\{0, -v(\xi)\}$, if $\xi \in K^*$ and $h_K(0) = 0$.

For a divisor $\mathscr{C} = \sum_{v\in M_K} m_v[v]$, put $h_K(\mathscr{C}) = \sum_{v\in M_K} \max\{0, m_v\}\deg(v)$.

2.2. 2-division points In this section, we quote some results from [7]. All the statements can be easily checked.

Let $P = (\xi, \eta) \in E(\mathscr{O}_s)$, $K_1 = K(\alpha, \beta, \gamma)$ and $L = K_1(\sqrt{\xi - \alpha}, \sqrt{\xi - \beta}, \sqrt{\xi - \gamma})$. Fix a choice of square roots, and let

$$\zeta - \alpha = \left(\sqrt{\xi - \alpha} + \sqrt{\xi - \beta}\right)\left(\sqrt{\xi - \alpha} + \sqrt{\xi - \gamma}\right).$$

Then there exists $\tau \in L$ such that the point $Q = (\zeta, \tau)$ in $E(L)$ satisfies $2Q = P$. Moreover, if $D_0 = (\alpha, 0) \in E[2]$ and $Q' = (\zeta', \tau') = Q + D_0$ in $E(L)$, then

(3) $$(\zeta' - \alpha)(\zeta - \alpha) = (\alpha - \beta)(\alpha - \gamma).$$

From this, we see that if T, T_1, T_2 are respectively valuations in M_L sitting over respectively those in S, S_1, S_2, and $T_3 = T \cup T_1 \cup T_2$, then $\zeta - \alpha, \zeta - \beta, \zeta - \gamma$ are all T_3-units.

Note that if P' is another point in $E(K)$ such that $P - P' \in 2E(K)$, then from the Kummer sequence, both P and P' determine the same class in $H^1(K, E[2])$ and, in particular, they determine the same extension L/K. Therefore, the extension L/K only depends on the image of P in $E(K)/2E(K)$.

3. The units equation

3.1. The units equation For $P = (\xi, \eta)$, there are four choices of $Q = (\zeta, \tau) \in E(L)$ such that $2Q = P$. For each such Q, let

$$M = \max\left\{h_L\left(\frac{\zeta - \alpha}{\alpha - \beta}\right), h_L\left(\frac{\zeta - \beta}{\beta - \gamma}\right), h_L\left(\frac{\zeta - \gamma}{\gamma - \alpha}\right)\right\}.$$

An element σ in $\{(\zeta - \alpha)/(\alpha - \beta), (\zeta - \beta)/(\beta - \gamma), (\zeta - \gamma)/(\alpha - \gamma)\}$ is called maximal if $h_L(\sigma) = M$.

Let us write any one of the following equations

(α) $$\left(\frac{\zeta - \alpha}{\alpha - \beta}\right) - \left(\frac{\zeta - \beta}{\alpha - \beta}\right) + 1 = 0,$$

(β) $$\left(\frac{\zeta - \beta}{\beta - \gamma}\right) - \left(\frac{\zeta - \gamma}{\beta - \gamma}\right) + 1 = 0,$$

(γ) $$\left(\frac{\zeta - \gamma}{\gamma - \alpha}\right) - \left(\frac{\zeta - \alpha}{\gamma - \alpha}\right) + 1 = 0$$

as

(δ) $$x_0 + x_1 + x_2 = 0,$$

where $\delta \in \{\alpha, \beta, \gamma\}$. Put $\underline{x} = (x_0, x_1, x_2)$ and say that $(Q, \underline{x})$ is *associated with* P (through (δ)). We call $\underline{x}$ maximal, if x_0 is maximal. We define

$$h_L(\underline{x}) = \sum_{w \in M_L} \max\{-w(x_0), -w(x_1), -w(x_2)\}.$$

Then we have $h_L(\underline{x}) = h_L(x_0)$.

Let C be a constant whose value will be determined latter. Let I be the set consisting of those $(P, Q, \underline{x})$ such that $P \in E(\mathscr{O}_S)$, $(Q, \underline{x})$ is associated with P, $\underline{x}$ is maximal, and $h_L(\underline{x}) \leq Ch_L(\mathscr{D}_{E/K})$.

For $\delta \in \{\alpha, \beta, \gamma\}$, let II_δ be the set consisting of those $(P, Q, \underline{x})$ such that $P \in E(\mathscr{O}_S)$, $(Q, \underline{x})$ is associated with P through (δ), $\underline{x}$ is maximal, and $h_L(\underline{x}) > Ch_L(\mathscr{D}_{E/K})$.

Let $\tilde{I}$, $\tilde{II}_\delta$ be the image of I, II_δ under the projections $I \longrightarrow E(\mathscr{O})$, $II_\delta \to E(\mathscr{O})$, by $(P, Q, \underline{x}) \mapsto P$.

3.2. Case I Suppose that $(P, Q, \underline{x}) \in I$ and $Q = (\zeta, \tau)$. Then

$$(4) \quad h_L\left(\frac{\tau^4}{\Delta}\right) \leq 2\left(h_L\left(\frac{\zeta-\alpha}{\alpha-\beta}\right) + h_L\left(\frac{\zeta-\beta}{\beta-\gamma}\right) + h_L\left(\frac{\zeta-\gamma}{\gamma-\alpha}\right)\right) \leq 6h_L(\underline{x}).$$

Let $\hat{h}_K$ (respectively, $\hat{h}_L$) denote the canonical height of E over K (respectively, over L).

LEMMA 3.1. *If $P \in \tilde{I}$, then $\hat{h}_K(P) \leq (1/3)(1+6C)h_K(\mathscr{D}_{E/K})$.*

PROOF. Let $(Q, \underline{x})$ be associated with P. We have

$$\hat{h}_K(P) = (1/[L:K])\hat{h}_L(P), \quad h_K(\mathscr{D}_{E/K}) = (1/[L:K])h_L(\mathscr{D}_{E/K})$$

It suffices to show $\hat{h}_L(P) \leq (4/12)(1+6C)h_L(\mathscr{D}_{E/K})$. This will follow from $h_L(\mathscr{D}_{E/L}) \leq h_L(\mathscr{D}_{E/K})$, $\hat{h}_L(P) = 4\hat{h}_L(Q)$, (4) and [3, Proposition 8.3] which says that $\hat{h}_L(Q) \leq (1/12)h_L(\tau^4/\Delta) + 1/12h_L(\mathscr{D}_{E/L})$. □

LEMMA 3.2. *Let $\tilde{I}'$ be the set of $P \in E(K)$ such that*

$$\hat{h}_K(P) \leq (1/3)(1+6C)h_K(\mathscr{D}_{E/K}).$$

Then $\tilde{I} \subset \tilde{I}'$ and $E(K)_{\mathrm{tor}} \subset I'$. Moreover,

(1) $|\tilde{I}'| \leq 144(4(10^{11.5}(1+6C))^{1/2}+1)^r$, *if* $h_K(\mathscr{D}_{E/K}) \geq 24(g-1)$;

(2) $|\tilde{I}'| \leq (8\pi^2(g-1))^{2/3}(4(10^{11+23g}(1+6C))^{1/2}+1)^r$, *if* $h_K(\mathscr{D}_{E/K}) < 24(g-1)$.

PROOF. We follow the method used in the proof of [3, Theorem 8.1], where a counting lemma from [6] is used. Thus we have

$$|\tilde{I}'| \leq |E(K)_{\mathrm{tor}}| \left(2\sqrt{4(1+6C)h_K(E)/\mu}+1\right)^r,$$

where $h_K(E) = (1/12)h_K(\mathscr{D}_{E/K})$, and

$$\mu = \begin{cases} 10^{-11.5}h_K(E) & \text{if } h_K(E) \geq 2(g-1), \\ 10^{-11-23g}h_K(E) & \text{if } h_K(E) < 2(g-1). \end{cases}$$

Also,

$$|E(K)_{\mathrm{tor}}| \leq \begin{cases} 144 & \text{if } h_K(E) \geq 2(g-1), \\ (8\pi^2(g-1))^{2/3} & \text{if } h_K(E) < 2(g-1). \end{cases}$$ □

3.3. Local calculations Let $v \in S_1$ and K_v be the completion of K at v. Then (1) is a local minimal Weierstrass equation of E/K_v. Let L_w be the completion of L at w sitting over v. For $P = (\xi, \eta) \in E(K_v)$, $Q = (\zeta, \tau) \in E(L_w)$ such that $2Q = P$, let

$$\begin{aligned} x_{0,\alpha} &= (\zeta-\alpha)/(\alpha-\beta), & x_{1,\alpha} &= -(\zeta-\beta)/(\alpha-\beta), & x_{2,\alpha} &= 1, \\ x_{0,\beta} &= (\zeta-\alpha)/(\beta-\gamma), & x_{1,\beta} &= -(\zeta-\gamma)/(\beta-\gamma), & x_{2,\beta} &= 1, \\ x_{0,\gamma} &= (\zeta-\gamma)/(\gamma-\alpha), & x_{1,\gamma} &= -(\zeta-\alpha)/(\gamma-\alpha), & x_{2,\gamma} &= 1. \end{aligned} \tag{5}$$

Suppose that E/K_v has multiplicative reduction at v. Then exactly one element among the set $\{\alpha-\beta, \beta-\gamma, \gamma-\alpha\}$ has positive valuation and the others are local units. We assume that $v(\beta-\gamma) > 0$ and $v(\alpha-\beta) = v(\gamma-\alpha) = 0$. Let $Q' = (\zeta', \tau') = Q + (\alpha, 0)$. Then (3) implies that $w(\zeta-\alpha) = w(\zeta'-\alpha) = 0$.

Similarly, if $Q'' = (\zeta'', \tau'') = Q + (\beta, 0)$, then from $(\zeta-\beta)(\zeta''-\beta) = (\beta-\alpha)(\beta-\gamma)$, we get $w(\zeta-\beta) \leq w(\beta-\gamma)$. We also have $w(\zeta-\gamma) \leq w(\beta-\gamma)$. Therefore,

$$\begin{aligned} w(x_{1,\alpha}) &= \max\{w(x_{0,\alpha}), w(x_{1,\alpha}), w(x_{2,\alpha})\}, \\ w(x_{2,\beta}) &= \max\{w(x_{0,\beta}), w(x_{1,\beta}), w(x_{2,\beta})\}, \\ w(x_{0,\gamma}) &= \max\{w(x_{0,\gamma}), w(x_{1,\gamma}), w(x_{2,\gamma})\}. \end{aligned}$$

We have proved the following lemma.

LEMMA 3.3. *Suppose that $v \in S_1$ and w is a place of L above v. If E/K_v has multiplicative reduction, then there exist $i_\alpha, i_\beta, i_\gamma \in \{0, 1, 2\}$, which depend on E/K_v only such that for every $P \in E(K_v)$, we have*

$$\begin{aligned} w(x_{i_\alpha,\alpha}) &= \max\{w(x_{0,\alpha}), w(x_{1,\alpha}), w(x_{2,\alpha})\}, \\ w(x_{i_\beta,\beta}) &= \max\{w(x_{0,\beta}), w(x_{1,\beta}), w(x_{2,\beta})\}, \\ w(x_{i_\gamma,\gamma}) &= \max\{w(x_{0,\gamma}), w(x_{1,\gamma}), w(x_{2,\gamma})\}. \end{aligned}$$

For $\hat{P} = (\hat{\xi}, \hat{\eta}) \in E(K_v)$, $\hat{Q} = (\hat{\zeta}, \hat{\tau}) \in E(L_w)$ such that $2\hat{Q} = \hat{P}$, define $\hat{x}_{j,\alpha}, \hat{x}_{j,\beta}, \hat{x}_{j,\gamma}$, $j = 0, 1, 2$, as in (5). We denote by $E_0(K_v)$ (respectively, $E_1(K_v)$) the set of elements in $E(K_v)$ whose reduction at v are smooth (respectively, the identity).

LEMMA 3.4. *Suppose $v \in S_1$, E/K_v has additive reduction at v and w is a place of L sitting over v. For $P \in E(K_v)$, $Q \in E(L_w)$ such that $2Q = P$, there exist $i_\alpha, i_\beta, i_\gamma \in \{0, 1, 2\}$, which depends on E/K_v and Q and such that if $\hat{P} \in E(K_v)$, $\hat{Q} \in E(L_w)$ with $2\hat{Q} = \hat{P}$ and $\hat{Q} - Q \in E_0(K_v)$, then*

$$w(\hat{x}_{i_{\alpha,\alpha}}) = \max\{w(\hat{x}_{0,\alpha}), w(\hat{x}_{1,\alpha}), w(\hat{x}_{2,\alpha})\},$$
$$w(\hat{x}_{i_{\beta,\beta}}) = \max\{w(\hat{x}_{0,\beta}), w(\hat{x}_{1,\beta}), w(\hat{x}_{2,\beta})\},$$
$$w(\hat{x}_{i_{\gamma,\gamma}}) = \max\{w(\hat{x}_{0,\gamma}), w(\hat{x}_{1,\gamma}), w(\hat{x}_{2,\gamma})\}.$$

PROOF. Put $R = \hat{Q} - Q = (\zeta_0, \tau_0)$. Let a be $\min\{w(\alpha - \beta), w(\beta - \gamma), w(\gamma - \alpha)\}$. Then $a > 0$. Let $L'_{w'}$ be an extension of L_w such that

$$\min\{w'(\alpha - \beta), w'(\beta - \gamma), w'(\gamma - \alpha)\} = 2m$$

for some positive integer m. Then $E/L'_{w'}$ has semi-stable reduction at w'. In fact, if $\pi_{w'}$ is a prime element of $L'_{w'}$, then the substitution

$$\begin{cases} \tilde{x} = \pi_{w'}^{-2m}(x - \alpha), \\ \tilde{y} = \pi_{w'}^{-3m} y, \end{cases} \tag{6}$$

transforms (1) into

$$\tilde{E} : \tilde{y}^2 = (\tilde{x} - \tilde{\alpha})(\tilde{x} - \tilde{\beta})(\tilde{x} - \tilde{\gamma}), \tag{7}$$

where $\tilde{\alpha} = 0$, $\tilde{\beta} = \pi_{w'}^{-2m}(\beta - \alpha)$, $\tilde{\gamma} = \pi_{w'}^{-2m}(\gamma - \alpha)$ are all local integers and at least two elements in the set $\{\tilde{\alpha} - \tilde{\beta}, \tilde{\beta} - \tilde{\gamma}, \tilde{\gamma} - \tilde{\alpha}\}$ are local units. We assume that

$$w'(\tilde{\alpha} - \tilde{\beta}) = 0 = w'(\tilde{\alpha} - \tilde{\gamma}). \tag{8}$$

Denote the transformation of R (respectively, Q, $D_0 := (\alpha, 0)$, $D_1 := (\beta, 0)$, $D_2 := (\gamma, 0)$, $Q' := Q + D_0$, $Q'' := Q + D_1$, $Q''' := Q + D_2$) under (6) by $\tilde{R} = (\tilde{\zeta}_0, \tilde{\tau}_0)$ (respectively, $\tilde{Q} = (\tilde{\zeta}, \tilde{\tau})$, $\tilde{D}_0 = (\tilde{\alpha}, 0)$, $\tilde{D}_1 = (\tilde{\beta}, 0)$, $\tilde{D}_2 = (\tilde{\gamma}, 0)$, $\tilde{Q}' = (\tilde{\zeta'}, \tilde{\tau'}) = \tilde{Q} + \tilde{D}_0$, $\tilde{Q}'' = (\tilde{\zeta''}, \tilde{\tau''}) = \tilde{Q} + \tilde{D}_1$, $\tilde{Q}''' = (\tilde{\zeta'''}, \tilde{\tau'''}) = \tilde{Q} + \tilde{D}_2$). We introduce similar notations for $\hat{Q}$. Because $R \in E_0(K_v)$, we have $\tilde{R} \in \tilde{E}_1(L'_w)$. Since $\tilde{\hat{Q}}' = \tilde{Q} + \tilde{D}_0 + \tilde{R} = \tilde{Q}' + \tilde{R}$, the reductions at w' of $\tilde{\hat{Q}}'$ and $\tilde{Q}'$ are the same. In particular, the reduction of $\tilde{\hat{Q}}'$ is the identity if and only if that of $\tilde{Q}'$ is identity. Consequently, we have that $w'(\tilde{\hat{x}}'_{0,\alpha}) < 0$ if and only if $w'(\tilde{x}'_{0,\alpha}) < 0$. From (3) and (8), we have that $w'(\tilde{\hat{x}}_{0,\alpha}) > 0$ if and only if $w'(\tilde{x}_{0,\alpha}) > 0$.

Note that for $j = 0, 1, 2$, and $\delta = \alpha, \beta, \gamma$, we have $\tilde{x}_{j,\delta} = x_{j,\delta}$, and $\tilde{\hat{x}}_{j,\delta} = \hat{x}_{j,\delta}$.

If $\tilde{E}/L'_{w'}$ has good reduction at w', then $w'(\beta - \gamma) = 0$ and so as before we see that $w'(x_{j,\delta}) > 0$ is equivalent to $w'(\hat{x}_{j,\delta}) > 0$, for $j = 0, 1, 2$ and $\delta = \alpha, \beta, \gamma$. We then choose $i_\alpha, i_\beta, i_\gamma$ in the following way. If for a $\delta \in \{\alpha, \beta, \gamma\}$, we have $w(x_{j,\delta}) > 0$ for some j, then we choose $i_\delta = j$. Otherwise, we choose $i_\delta = 2$. This proves the lemma for the potentially good reduction case.

It remains to prove the case where $\tilde{E}/L'_{w'}$ has multiplicative reduction. By (8), we must have $w'(\tilde{\beta} - \tilde{\gamma}) > 0$. From $\tilde{\tilde{Q}} = \tilde{Q} + \tilde{R}$ we have $\tilde{\tilde{Q}} \notin \tilde{E}_0(L'_{w'})$ if and only if $\tilde{Q} \notin \tilde{E}_0(L'_{w'})$. Consequently, we have $w'(\tilde{\tilde{\xi}} - \tilde{\beta}) > 0$ if and only if $w'(\tilde{\xi} - \tilde{\beta}) > 0$. From (8), we see that $w'(\tilde{\tilde{x}}_{1,\alpha}) > 0$ if and only if $w'(\tilde{x}_{1,\alpha}) > 0$.

Also, the reductions at w' of $\tilde{\tilde{Q}}''$ and $\tilde{Q}''$ are the same, and this leads to the equivalence between $w'(\tilde{\tilde{\xi}}'' - \tilde{\beta}) < 0$ and $w'(\tilde{\xi}'' - \tilde{\beta}) < 0$. From $(\tilde{\xi} - \tilde{\beta})(\tilde{\xi}'' - \tilde{\beta}) = (\tilde{\beta} - \tilde{\alpha})(\tilde{\beta} - \tilde{\gamma})$ it follows that $w'(\tilde{x}_{0,\beta}) > 0$ if and only if $w'(\tilde{\tilde{x}}_{0,\beta}) > 0$.

We can use methods similar to the above to show that $w'(\hat{x}_{j,\delta}) > 0$ if and only if $w'(x_{j,\delta}) > 0$ for $\delta \in \{\alpha, \beta, \gamma\}$, $j \in \{0, 1, 2\}$. We then let

$$i_\delta = \begin{cases} j & \text{if } \ w'(x_{j,\delta}) > 0; \\ 2 & \text{if } \ w'(x_{0,\delta}) = w'(x_{1,\delta}) \le 0. \end{cases}$$ □

3.4. Case II For $\underline{x} = (x_0, x_1, x_2) \in P^2(L)$, $w \in M_L$, put

$$m_w(\underline{x}) = \min\{w(x_0), w(x_1), w(x_2)\} - \max\{w(x_0), w(x_1), w(x_2)\}.$$

LEMMA 3.5. *If $\delta \in \{\alpha, \beta, \gamma\}$, $P \in \tilde{II}_\delta$, and $(Q, \underline{x})$ is associated to P, then*

$$\sum_{w \in T_1} m_w(\underline{x}) \ge -(1/2) h_L(\mathscr{D}_{E/K}).$$

PROOF. Without loss of generality, we may assume that

$$\delta = \alpha, \quad \underline{x} = \left(\frac{\zeta - \alpha}{\alpha - \beta}, -\frac{\zeta - \beta}{\alpha - \beta}, 1 \right).$$

Let $Q' = (\zeta', \tau') = Q + D_0$ as before. Then (3) implies that

$$-w(\alpha - \beta) \le w((\zeta - \alpha)/(\alpha - \beta)) \le w(\alpha - \gamma).$$

Similarly, we have

$$-w(\alpha - \beta) \le w((\zeta - \beta)/(\alpha - \beta)) \le w(\beta - \gamma).$$

If $\max\{w((\zeta - \alpha)/(\alpha - \beta)), w((\zeta - \beta)/(\alpha - \beta)), 0\} > 0$, then

$$\min\{w((\zeta - \alpha)/(\alpha - \beta)), w((\zeta - \beta)/(\alpha - \beta)), 0\} = 0$$

and $m_w(\underline{x}) \ge -(1/2) w(\Delta_{E/K})$.

If $\max\{w((\zeta-\alpha)/(\alpha-\beta)), w((\zeta-\beta)/(\alpha-\beta)), 0\} = 0$, then

$$\min\{w(\zeta-\beta/\alpha-\beta), w(\zeta-\beta/\alpha-\beta), 0\} \leq 0$$

and $m_w(\underline{x}) \geq -(1/2)w(\Delta_{E/K})$. Therefore,

$$\sum_{w\in T_1} m_w(\underline{x}) \geq \sum_{w\in T_1} -(1/2)w(\Delta_{E/K}) \geq -(1/2)h_L(\mathscr{D}_{E/K}). \qquad \square$$

LEMMA 3.6. *If* $\delta \in \{\alpha, \beta, \gamma\}$, $(P, Q, \underline{x}) \in II_\delta$, *then*

$$\sum_{w\in T\cup T_2} m_w(x) < -3(1-(1/6C))h_L(\underline{x}). \tag{9}$$

PROOF. Recall that $T_3 = T \cup T_1 \cup T_2$. Following the proof of [2, Lemma 2] and using the product formula we have

$$\begin{aligned}
&\sum_{w\in T_3} m_w(\underline{x})\\
&\quad= \sum_{w\in T_3}((w(x_0)+w(x_1)+w(x_2)) - 3\max\{-w(x_0), -w(x_1), -w(x_2)\})\\
&\quad= \sum_{w\in M_L}((w(x_0)+w(x_1)+w(x_2)) - 3\max\{-w(x_0), -w(x_1), -w(x_2)\})\\
&\quad= -3h_L(\underline{x}).
\end{aligned}$$

By Lemma 3.5, we have

$$\sum_{w\in T\cup T_2} m_w(\underline{x}) - (1/2)h_L(\mathscr{D}_{E/K}) \leq \sum_{w\in T\cup T_2} m_w(\underline{x}) + \sum_{w\in T_1} m_w(\underline{x}) = -3h_L(\underline{x}),$$

and therefore,

$$\sum_{w\in T\cup T_2} m_w(\underline{x}) < -(3h_L(\underline{x}) - (1/2C)h_L(\underline{x})) = -3(1-(1/6C))h_L(\underline{x}). \qquad \square$$

The extension L/K depends only on the class of P in $E(K)/2E(K)$. For each class $\overline{P}_0$ in $E(K)/2E(K)$ and for $\delta \in \{\alpha, \beta, \gamma\}$, denote by $II_{\delta,\overline{P}_0}$ the set of $(P, Q, \underline{x})$ in II_δ such that $\overline{P} = \overline{P}_0$; and by $\tilde{II}_{\delta,\overline{P}_0}$ its image in $E(\mathscr{O}_s)$. Every P in $\tilde{II}_{\delta,\overline{P}_0}$ determines the same field extension L/K.

The following lemma is the additive form of [2, Lemma 1].

LEMMA 3.7. *Let B be a real number with* $0 < B < 1$, *let Y be an index set of cardinality* $q \geq 1$ *and put* $R(B) = (1-B)^{-1}B^{B/(B-1)}$. *Then there exists a set W of cardinality at most* $\max(1, (2B)^{-1})R(B)^{q-1}$, *consisting of tuples* $(\Gamma_j^0)_{j\in Y}$ *with* $\Gamma_j^0 \geq 0$,

$j \in Y$ and $\sum_{j\in Y} \Gamma_j^0 = B$ with the following property: for every set of real F_j, $j \in Y$, and real Λ with $F_j \le 0, \forall j \in Y$ and $\sum_{j\in Y} F_j \le \Lambda$ there exists a tuple $(\Gamma_j)_{j\in Y} \in W$ such that $F_j \le \Gamma_j^0 \Lambda$, for all $j \in Y$.

For a real number $0 < B < 1$, write $B_1 = B(1-(1/6C))$.

LEMMA 3.8. *Let B be a real number satisfying $1/2 \le B < 1$. For each $\overline{P}_0 \in E(K)/2E(K)$, there exists a set $W_{\overline{P}_0}$ of cardinality at most $3^{t+t_2} R(B)^{t+t_{2-1}}$, consisting of tuples $(i(w)_{w\in T\cup T_2}, (\Gamma_w)_{w\in T\cup T_2})$ with $i(w) \in \{0,1,2\}$, $\Gamma_w \ge 0$ for all $w \in T \cup T_2$ and $\sum_{w\in T\cup T_2} \Gamma_w = B_1$ such that : for every $\delta \in \{\alpha,\beta,\gamma\}$, $(P, Q, \underline{x}) \in II_{\delta,\overline{P}_0}$, there is a tuple $(i(w)_{w\in T\cup T_2}, (\Gamma_w)_{w\in T\cup T_2})$ in $W_{\overline{P}_0}$ such that*

$$(10)\quad -w(x_{i(w)}) - \max\{-w(x_0), -w(x_1), -w(x_2)\} \le 3\Gamma_w h_L(\underline{x}) \quad \text{for } w \in T \cup T_2.$$

PROOF. We apply Lemma 3.7. Take $\Lambda = -3(1-(1/6C))h_L(\underline{x})$. Let $T \cup T_2$ be the index set, set $q = |T \cup T_2|$. For each $w \in T \cup T_2$, take $F_w = m_w(\underline{x})$ and denote $\Gamma_w = \Gamma_w^0(1-(1/6C))$. Then apply the inequality (9). For each $(\underline{x})$, choose $i(w)$ such that $-w(x_{i(w)}) = \min\{-w(x_0), -w(x_1), -w(x_2)\}$. In general, for each $w \in T \cup T_2$, there are three choices for $i(w)$. □

In Lemma 3.8, for a $(P, Q, \underline{x}) \in II_{\delta,\overline{P}_0}$, we can actually extend the tuple $(i(w)_{w\in T\cup T_2}, (\Gamma_w)_{w\in T\cup T_2})$ to a tuple $(i(w)_{w\in T_3}, (\Gamma_w)_{w\in T_3})$ by taking, for $w \in T_1$, $\Gamma_w = 0$ and $i(w)$ to be the i_δ described in Lemma 3.3 and Lemma 3.4. Then we have

$$(11)\qquad -w(x_{i(w)}) - \max\{-w(x_0), -w(x_1), -w(x_2)\} \le -3\Gamma_w h_L(\underline{x}),\ w \in T_3.$$

Note that for $w \in T_1$, the choice of i_w may depend on $(P, Q, \underline{x})$.

DEFINITION 3.1. For fixed $\delta \in \{\alpha,\beta,\gamma\}$, $P_0 \in E(K)$, two triples $(P, Q, \underline{x})$, $(P', Q', \underline{x}')$ in $II_{\delta,\overline{P}_0}$ are equivalent if there is an $R \in 12E(K)$ such that $Q' = Q + R$. They are strictly equivalent if they are equivalent and there is a tuple $(i(w)_{w\in T\cup T_2}, (\Gamma_w)_{w\in T\cup T_2})$ in $W_{\overline{P}_0}$ such that both $\underline{x}$ and $\underline{x}'$ satisfy (10).

If $w \in T_1$, $w|v$ and E/K_v is of additive reduction, then $12E(K) \subset E_0(K_v)$. Therefore, by Lemma 3.3 and Lemma 3.4, if $(P, Q, \underline{x})$ and $(P', Q', \underline{x}')$ are strictly equivalent they both satisfy (11), for the same extended tuple $(i(w)_{w\in T_3}, (\Gamma_w)_{w\in T_3})$.

This proves the following lemma.

LEMMA 3.9. *Let B be a real number satisfying $1/2 \le B < 1$. For each $\delta \in \{\alpha,\beta,\gamma\}$, $\overline{P}_0 \in E(K)/2E(K)$, and each equivalent class Θ in $II_{\delta,\overline{P}_0}$, there exists a set W_Θ of cardinality at most $3^{t+t_2} R(B)^{t+t_{2-1}}$, consisting of tuples $(i(w)_{w\in T_3}, (\Gamma_w)_{w\in T_3})$*

with $i(w) \in \{0,1,2\}$, $\Gamma_w \geq 0$ *for all* $w \in T_3$ *and* $\sum_{w\in T_3} \Gamma_w = B_1$ *such that for every* $(P, Q, \underline{x}) \in \Theta$, *there exists a tuple* $(i(w)_{w\in T_3}, (\Gamma_w)_{w\in T_3})$ *in* W_Θ *such that*

$$(12) \qquad -w(x_{i(w)}) - \max\{-w(x_0), -w(x_1), -w(x_2)\} \leq 3\Gamma_w h_L(\underline{x}) \quad \textit{for} \ \ w \in T_3.$$

LEMMA 3.10. *For* $\delta \in \{\alpha, \beta, \gamma\}$, *we have* $|II_\delta| \leq 1080\,(24)^r\, 8^{2t}\, 8^{2t_2}$.

PROOF. According to [2, Theorem 2′], if $B_1 = 0.846$ then associated to a tuple in W_Θ, (11) has at most 10 solutions. We take $C = 4$. Then $B = 0.846 \cdot 24/23 \leq 0.883$. and $R(B) \leq 64/3$.

Therefore, each strictly equivalent class in $II_{\delta,\overline{P_0}}$ contains at most 10 elements. By Lemma 3.8, there are at most $(12)^{r+2}\, 3^{t+t_2} R(B)^{t+t_2-1}$ strictly equivalent classes in $II_{\delta,\overline{P_0}}$. We have $3^{t+t_2}(64/3)^{t+t_2-1} = (3/64)\, 8^{2t+2t_2}$. Since II_δ is decomposed into a disjoint union of at most 2^{r+2} subsets of the form $II_{\delta,\overline{P_0}}$, there are at most $10 \times 4 \times 24^r \times 24^2 \times 3/64 \times 8^{2t+2t_2}$ elements in II_δ. □

Let $m = |K(\alpha, \beta, \gamma) : k|$. Then $t \leq 4ms$ and $t_2 \leq 4ms_2$.

LEMMA 3.11. $|E(\mathscr{O}_s) \setminus \tilde{I}| \leq 810 \cdot 24^r \cdot 2^{24m(s+s_2)}$.

PROOF. If $P \in E(\mathscr{O}_s) \setminus I$, then four choices of signs give at least four elements in $II_\alpha \cup II_\beta \cup II_\gamma$. Therefore, $E(\mathscr{O}_s) \setminus \tilde{I}$ has cardinality not greater than $(|II_\alpha| + |II_\beta| + |II_\gamma|)/4$. □

Using the above and Lemma 3.2, we prove the following:

THEOREM 3.12. *We have*

(1) $|E(\mathscr{O}_s)| \leq 144(20 \cdot 10^{5.75} + 1)^r + 810 \cdot 24^r \cdot 2^{24m(s+s_2)}$ *if* $h_K(\mathscr{D}_{E/K}) \leq 24(g-1)$;
(2) $|E(\mathscr{O}_s)| \leq (8\pi^2(g-1))^{2/3}(20 \cdot 10^{5.5+11.5g} + 1)^r + 810 \cdot 24^r \cdot 2^{24m(s+s_2)}$, *if* $h_K(\mathscr{D}_{E/K} < 24(g-1)$.

Acknowledgement

W.-C. Chi was supported in part by the National Science Council of Taiwan, NSC91-2115-M-003-006. K.-S. Tan was supported in part by the National Science Council of Taiwan, NSC90-2115-M-002-014.

References

[1] J.-H. Evertse, 'On equations in S-units and the Thue-Mahler equation', *Invent. Math.* **75** (1984), 561–584.

[2] ———, 'On equations in two S-units over function fields of characteristic 0', *Acta Arith.* **47** (1986), 233–253.
[3] M. Hindry and J. H. Silverman, 'The canonical height and integral points on elliptic curves', *Invent. Math.* **93** (1988), 419–450.
[4] S. Lang, *Elliptic curves: Diophantine analysis* (Springer, Berlin, 1978).
[5] R. C. Mason, *Diophantine equations over function fields*, London Math. Soc. Lecture Note Ser. 96 (Cambridge University Press, Cambridge, 1984).
[6] J. H. Silverman, 'A quantitative version of Siegel's theorem', *J. Reine Angew. Math.* **378** (1987), 60–100.
[7] K.-S. Tan, 'A 2-division formula for elliptic curves', preprint, (National Taiwan University, Taipei, 2002).

Department of Mathematics
National Taiwan Normal University
Taipei
Taiwan
e-mail: wchi@math.ntnu.edu.tw

School of Mathematics and Statistics
University of Sydney
NSW 2006
Australia
e-mail: kflai@math.usyd.edu.au

Department of Mathematics
National Taiwan University
Taipei
Taiwan
e-mail: tan@math.ntu.edu.tw