Pacific Journal of Mathematics

INTEGER POINTS ON ELLIPTIC CURVES

WEN-CHEN CHI, KING FAI LAI AND KI-SENG TAN

Volume 222 No. 2 December 2005

PACIFIC JOURNAL OF MATHEMATICS
Vol. 222, No. 2, 2005

INTEGER POINTS ON ELLIPTIC CURVES

WEN-CHEN CHI, KING FAI LAI AND KI-SENG TAN

We study Lang's conjecture on the number of S-integer points on an elliptic curve over a number field. We improve the exponent of the bound of Gross and Silverman from quadratic to linear by using the S-unit equation method of Evertse and a formula on 2-division points.

1. Introduction

Let E be an elliptic curve defined over an algebraic number field k of degree d. For a finite set S of places of k containing all the archimedean ones, we denote the ring of S-integers of k by $\mathbb{O}_S$. Serge Lang conjectured that if the Weierstrass equation of E is quasiminimal, then the cardinality of the set $E(\mathbb{O}_S)$ of $\mathbb{O}_S$-integer points of E should be bounded in terms of the field k, the cardinality of S and the rank of the group $E(k)$ of k-rational points of E [Lang 1978, p. 140]. Silverman [1987] proved Lang's conjecture when E has integral j-invariant. In general, if $j(E)$ is nonintegral for at most δ places of k, then a bound was also given with δ involved. However he did not compute the constants involved. Gross and Silverman [1995] used Roth's theorem to obtain an explicit bound. To state their theorem, let us write the Weierstrass equation of the elliptic curve E as

$$Y^2 = X^3 + \mathscr{A}X + \mathscr{B}, \tag{1–1}$$

where $\mathscr{A}, \mathscr{B} \in \mathbb{O}_S$. Put $\Delta = 4\mathscr{A}^3 + 27\mathscr{B}^2$. Write $j(E)$ for the j-invariant of E. Let D_k and R_k be the discriminant and the regulator of k. Let M_k be the set of all places of k. For a place $v \in M_k$, let k_v be the completion of k at v and let $|\ |_v$ be such that, for $z \in \mathbb{Q}$,

$$|z|_v = |z|_p^{[k_v:\mathbb{Q}_p]/[k:\mathbb{Q}]},$$

MSC2000: primary 11D45; secondary 11G05, 14K12.

Keywords: elliptic curves, S-integers, integer points, S-unit equations, 2-division points, Lang's conjecture.

Chi and Tan were supported in part by the National Science Council of Taiwan, grants NSC91-2115-M-003-006 and NSC89-2115-M-002-003 respectively.

where p is the place of $\mathbb{Q}$ lying under v and $|\ |_p$ is the usual absolute value. We use h_k to denote the multiplicative height. Namely, for $x \in k$

$$h_k(x) = \prod_{v \in M_k} \max(|x|_v, 1).$$

We shall write s for the cardinality of the set S.

Theorem 1.1 [1995]. *Suppose that (1–1) is quasiminimal and that*

$$6d(60d^2 \log 6d)^d \left(\frac{2}{\sqrt{3}}\right)^{d(d-1)/2} \cdot \max(R_k, \log|D_k|, 1).$$

is at most

$$\max\left\{\log h_k(j(E)), \log|\mathrm{Norm}_{k/\mathbb{Q}}(\Delta)|\right\}.$$

Then

$$\#E(\mathbb{O}_S) \leq 2 \cdot 10^{11} \cdot d \cdot \delta^{3d} \cdot (32 \cdot 10^9)^{r\delta+s}.$$

In this paper, we take a completely different approach. By using a formula on 2-division points from [2002], we associate to an S-integer point an unit equation over an extension of k. Then we use the machinery developed by J.-H. Evertse [1984] to obtain a quantitative bound for the number of S-integer points. Let $\mathcal{D}_{E/k}$ be the ideal of the minimal discriminant of E/k. Then we have

$$(\Delta) = \mathcal{D}_{E/k} \cdot \prod_v P_v^{12\chi_v}, \tag{1–2}$$

where P_v is the prime ideal corresponding to the place v and $\chi_v \in \mathbb{Z}$. For $v \in S$, $\chi_v \geq 0$. We factor the cubic over the algebraic closure $\bar{k}$ of k as

$$X^3 + \mathcal{A}X + \mathcal{B} = (X-\alpha)(X-\beta)(X-\gamma).$$

Let $k_1 = k(\alpha, \beta, \gamma)$ and $m = [k_1 : k]$. Further, let $M_{k,0}$ be the set of all nonarchimedean places in k.

Definition 1.2. Let w be a nonarchimedean place over a field extension K/k_1. If the valuations $w(\alpha-\beta)$, $w(\beta-\gamma)$, $w(\gamma-\alpha)$ are all equal, we say that E has *G-type reduction* at w; otherwise, we say that E has *M-type reduction* at w.

In fact, if w' is another place of K such that both w and w' are sitting over a place $v \in M_{k,0}$, then the reductions of E at w and w' are of the same type. Therefore, we will say that at v, the reduction of E is also of that type. Furthermore, in the case where $v(2) = 0$, E has G-type reduction if and only if it has good or potential good reduction (see Lemma 3.1).

Define

$$\begin{aligned} S_0 &= \{v \in M_{k,0} \setminus S \mid v(2)=0,\ \chi_v = 0,\ v(\Delta) > 0,\ v(j(E)) \geq 0\}, \\ S_1 &= \{v \in M_{k,0} \mid \chi_v > 0,\ v(j(E)) \geq 0\}, \\ S_m &= \{v \in M_{k,0} \mid E \text{ has M-type reduction at } v\}, \\ S' &= S \setminus (S_0 \cup S_1 \cup S_m). \end{aligned}$$

Let s_1, s_m, s' be the cardinality of S_1, S_m, S'. Then s_m is at most $\delta + d$.

With the notations above, we can now state our main result.

Theorem 1.3.

$$\#E(\mathbb{O}_S) \leq 11 \times 7^{1.64r + 2.27(s'+s_1) + 3.7s_m + 10.3md}.$$

Note that we do not require the equation (1–1) to be quasiminimal. If we did so, then, by [Silverman 1984, p. 238], we would have

$$\left| \mathrm{Norm}_{k/\mathbb{Q}} \prod_{v \in S_1} P^{\chi_v} \right| \leq |D_k|^6,$$

and hence

$$s_1 \leq 6 \log |D_k|.$$

The exponent in the Gross–Silverman bound is *quadratic* in δ and r, while ours is *linear*, and our constants are smaller. Also, if the ABC Conjecture holds, our method can be applied to get a bound only in terms of r and k, in which the exponent is linear in s and r and differs from that obtained in [Hindry and Silverman 1988]. In fact, this has been achieved in [Chi et al. 2004] for the case where k is a function field of characteristic zero. Also, the method can be modified to bound the number of integer solutions to $Y^n = F(X)$; see [Chi et al. ≥ 2006].

2. A formula for 2-division points

The following result can be proved by straightforward calculations. For details, see [Tan 2002] or [Chi et al. 2004, Section 2.2].

Lemma 2.1. *In the notations preceding Theorem 1.3 a point $P = (a, b) \in E(k)$ determines an extension*

$$K = k_1(\sqrt{a-\alpha}, \sqrt{a-\beta}, \sqrt{a-\gamma})$$

depending only on the class $[P] \in E(k)/2E(k)$. Given a choice of signs for $\sqrt{a-\alpha}$, $\sqrt{a-\beta}$, and $\sqrt{a-\gamma}$ such that

$$b = \sqrt{a-\alpha}\,\sqrt{a-\beta}\,\sqrt{a-\gamma},$$

the point $Q := (f, g) \in E(K)$ *defined by*

$$f - \alpha = (\sqrt{a-\alpha} + \sqrt{a-\beta})(\sqrt{a-\alpha} + \sqrt{a-\gamma}),$$

and

$$g = (\sqrt{a-\alpha} + \sqrt{a-\beta})(\sqrt{a-\beta} + \sqrt{a-\gamma})(\sqrt{a-\gamma} + \sqrt{a-\alpha}),$$

satisfies

$$2Q = P.$$

Furthermore, if $\{\alpha_1, \alpha_2, \alpha_3\} = \{\alpha, \beta, \gamma\}$, $D_i = (\alpha_i, 0) \in E(k_1)$, $i = 1, 2, 3$, *and* $Q^{(i)} = (f^{(i)}, g^{(i)}) = Q + D_i$, *then*

$$(f - \alpha_i)(f^{(i)} - \alpha_i) = (\alpha_i - \alpha_j)(\alpha_i - \alpha_{j'}), \tag{2–1}$$

where $\{j, j'\} = \{1, 2, 3\} \setminus \{i\}$.

3. Local calculations

Given a point $P \in E(k)$, let K be the field determined by P as in Lemma 2.1. For $v \in M_k$, let K_w be the completion of K with respect to a place w lying over v. Then K_w/k_v is a Galois extension. Let I_w be the inertia subgroup of $\mathrm{Gal}(K_w/k_v)$. In this section, we assume that w is nonarchimedean and view it as an valuation from K_w onto $\mathbb{Z} \cup \{\infty\}$.

Lemma 3.1. *Suppose E has potential good reduction at a place v of k such that $v(2) = 0$. Then for any place w of K lying over v, we have*

$$w(\alpha - \beta) = w(\beta - \gamma) = w(\gamma - \alpha).$$

Proof. Suppose on the contrary that

$$w(\gamma - \alpha) > w(\alpha - \beta) = w(\beta - \gamma).$$

We can find a field extension $\tilde{K}$ of K such that $\tilde{v}(\alpha - \beta) = 2m$, $m \in \mathbb{Z}$, where $\tilde{v}$ is a place of $\tilde{K}$ lying over w. By our assumption, we have $\tilde{v}(\beta - \gamma) = 2m$ and $\tilde{v}(\gamma - \alpha) > 2m$. Consider the elliptic curve $\tilde{E}$ defined by

$$\tilde{E}: \ \tilde{Y}^2 = \tilde{X}(\tilde{X} - \tilde{\beta})(\tilde{X} - \tilde{\gamma}),$$

which was obtained from (1–1) by the change of variables

$$\tilde{Y} = Y/\pi^{3m}, \qquad \tilde{X} = (X - \alpha)/\pi^{2m},$$
$$\tilde{\beta} = (\beta - \alpha)/\pi^{2m}, \quad \tilde{\gamma} = (\gamma - \alpha)/\pi^{2m},$$

where π is a uniformizer of the prime ideal associated to $\tilde{v}$ in $\tilde{K}$. Then $\tilde{v}(\tilde{\beta}) = 0$ and $\tilde{v}(\tilde{\gamma}) > 0$. This implies that $\tilde{E}$ has multiplicative reduction at $\tilde{v}$. Consequently, $\tilde{v}(j_E) = \tilde{v}(j_{\tilde{E}}) < 0$ which contradicts our hypothesis. □

Now assume that the equation for E is minimal at v. Let $\mathbb{F}_v$ be the residue field of v and let $\bar{E}$ be the reduction of E at v. As usual, for $P \in E(k_v)$, we denote its image under the reduction map $E(k_v) \to \bar{E}(\mathbb{F}_v)$ by $\bar{P}$. Put

$$E_0(k_v) = \{P \in E(k_v) \mid \bar{P} \in \bar{E}_{ns}(\mathbb{F}_v)\},$$

where $\bar{E}_{ns}$ is the set of nonsingular points of $\bar{E}$. We have the following key lemma. Here we retain the notations in Lemma 2.1.

Lemma 3.2. *Assume that at v, where $v(2) = 0$, the Weierstrass equation (1–1) is minimal and E has potential good reduction. For $P_1, P_2 \in E(\mathbb{O}_v)$, let $Q_i = (f_i, g_i) \in E(K_w)$, for $i = 1, 2$, be such that $2Q_i = P_i$. If $Q_1 - Q_2 \in E_0(k_v)$, then*

$$w(f_1 - \alpha) = w(f_2 - \alpha) \quad \textit{and} \quad w(f_1 - \beta) = w(f_2 - \beta).$$

Before we give the proof of Lemma 3.2, we recall some basic facts on the formal group associated to an elliptic curve.

Suppose $w(\alpha - \beta) = 2a + \epsilon$, where $a \in \mathbb{N} \cup \{0\}$ and $\epsilon = 0$ or 1. By Lemma 3.1, $w(\beta - \gamma) = w(\gamma - \alpha) = 2a + \epsilon$. Consider the change of variables

$$\tilde{Y} = Y/\pi^{3a}, \qquad \tilde{X} = (X - \alpha)/\pi^{2a},$$
$$\tilde{\beta} = (\beta - \alpha)/\pi^{2a}, \quad \tilde{\gamma} = (\gamma - \alpha)/\pi^{2a},$$

where π is a uniformizer of the prime ideal associated to w. Then

$$\tilde{E}: \ \tilde{Y}^2 = \tilde{X}(\tilde{X} - \tilde{\beta})(\tilde{X} - \tilde{\gamma}),$$

is a minimal Weierstrass equation for E over K_w. For $i = 1, 2$, let $\tilde{Q}_i = (\tilde{f}_i, \tilde{g}_i)$, be the points on $\tilde{E}$ corresponding to Q_i. Let $\hat{E}$ be the formal group associated to $\tilde{E}/K_w$. For $m \geq 0$, set

$$\hat{E}_m = \begin{cases} \tilde{E}_0(K_w) & \text{if } m = 0, \\ \hat{E}(\pi^m \mathbb{O}_{K_w}) & \text{if } m > 0. \end{cases}$$

Then we have the filtration

$$\cdots \subset \hat{E}_{m+1} \subset \hat{E}_m \subset \cdots \subset \hat{E}_1 \subset \hat{E}_0.$$

Also, recall that we have the exact sequence

$$0 \longrightarrow \hat{E}_1 \longrightarrow \hat{E}_0 \longrightarrow \bar{\tilde{E}}_{ns} \longrightarrow 0,$$

where $\bar{\tilde{E}}_{ns}$ is the nonsingular part of the reduction of $\tilde{E}$.

For a point $R=(\tilde{X},\tilde{Y})$ in $\tilde{E}(K_w)$, let $\tilde{t}=-\tilde{X}/\tilde{Y}$. The following lemma follows easily from [Silverman 1986, Chapter IV].

Lemma 3.3. *Let notations be as above.*

(1) *If* $m>0$, *then*

$$R\in\hat{E}_m\setminus\hat{E}_{m+1}\Longleftrightarrow w(\tilde{t})=m\Longleftrightarrow\big(w(\tilde{X})=-2m \textit{ and } w(\tilde{Y})=-3m\big).$$

(2) *If* $m=0$ *and* $\epsilon=0$, *then*

$$R\in\hat{E}_0\setminus\hat{E}_1\Longleftrightarrow w(\tilde{t})\le 0\Longleftrightarrow\big(w(\tilde{X})\ge 0 \textit{ and } w(\tilde{Y})\ge 0\big).$$

(3) *If* $m=0$ *and* $\epsilon=1$, *then*

$$R\in\hat{E}_0\setminus\hat{E}_1\Longleftrightarrow w(\tilde{t})=0\Longleftrightarrow\big(w(\tilde{X})=0 \textit{ and } w(\tilde{Y})=0\big).$$

Note that if $\epsilon=0$, then $\tilde{E}$ has good reduction at w. In this case, $\hat{E}_0=\tilde{E}(K_w)$.

Lemma 3.4. *Under the hypothesis of Lemma 3.2, suppose that* $w(\alpha-\beta)=2a+\epsilon$ *and* $Q=(f,g)\in E_0(k_v)$. *Then* $\tilde{Q}\in\hat{E}_a\subset\hat{E}_0$.

Proof. Recall that the reduction of E is

$$\bar{E}:\ \ \bar{Y}^2=(\bar{X}-\bar{\alpha})(\bar{X}-\bar{\beta})(\bar{X}-\bar{\gamma}).$$

The singularity of $\bar{E}$ is $(\bar{\alpha},0)$.

If $Q=(f,g)\in E_0(k_v)$, then $w(f-\alpha)\le 0$. Since $\tilde{f}=(f-\alpha)/\pi^{2a}$, $\tilde{g}=g/\pi^{3a}$, we have $w(\tilde{f})\le -2a$. By Lemma 3.3, we have $\tilde{Q}\in\hat{E}_a\subset\hat{E}_0$. □

Proof of Lemma 3.2. We apply Lemma 2.1 with $\alpha_1=\alpha$, $\alpha_2=\beta$, and $\alpha_3=\gamma$. Then $Q_1'=Q_1+(\alpha,0)$, and so on. By (2–1), we have

$$(f_1-\alpha)(f_1'-\alpha)=(\alpha-\beta)(\alpha-\gamma).$$

This and Lemma 3.1 imply

$$w(f_1-\alpha)+w(f_1'-\alpha)=2(2a+\epsilon),$$

and

$$w(\tilde{f}_1)+w(\tilde{f}_1')=2\epsilon. \tag{3–1}$$

Similarly,

$$w(\tilde{f}_2)+w(\tilde{f}_2')=2\epsilon. \tag{3–2}$$

First we consider the case where

$$w(f_1-\alpha)\le 2a+\epsilon.$$

Then $w(\tilde{f}_1) \le \epsilon$. If $w(\tilde{f}_1) > 0$, then $w(\tilde{f}_1) = \epsilon = 1$. In this situation, $\tilde{E}$ has additive reduction at w and $(0,0)$ is the singularity of the reduction. Therefore, $\tilde{Q}_1 \notin \tilde{E}_0(K_w)$. By Lemma 3.4, $\tilde{Q}_1 - \tilde{Q}_2 \in \hat{E}_a \subset \hat{E}_0$, and consequently $\tilde{Q}_2$ is not in $\tilde{E}_0(K_w)$. Hence $w(\tilde{f}_2) > 0$. By (3–1), we also have $w(\tilde{f}_1') = 1$. Repeating the above argument, we also conclude that $w(\tilde{f}_2') > 0$. Then (3–2) implies that $w(\tilde{f}_2) = w(\tilde{f}_2') = 1$.

Now, assume that $w(\tilde{f}_1) = -2m \le 0$. Note that by Lemma 2.1 $Q_i \in E(\mathbb{O}_w)$, $i = 1, 2$ and we have $w(f_i - \alpha) \ge 0$. Hence,

$$w(\tilde{f}_i) \ge -2a. \tag{3–3}$$

This means that $\tilde{Q}_1 \notin \hat{E}_{a+1}$ and $\tilde{Q}_1 \in \hat{E}_m \setminus \hat{E}_{m+1}$. If $a > m$, then by Lemma 3.3 and Lemma 3.4, we also have

$$\tilde{Q}_2 \in \hat{E}_m \setminus \hat{E}_{m+1}$$

and hence $w(\tilde{f}_2) = -2m$. If $a = m$, then we have $\tilde{Q}_2 \in \hat{E}_a$ and hence $w(\tilde{f}_2) \le -2a$. By (3–3), we have $w(\tilde{f}_2) = -2m$, too.

For the case where

$$w(f_1 - \alpha) > 2a + \epsilon,$$

we consider f_1', which, according to (2–1), satisfies

$$w(f_1' - \alpha) < 2a + \epsilon.$$

Then the argument above can be applied to verify that

$$w(f_2' - \alpha) = w(f_1' - \alpha).$$

We complete the proof by applying (2–1). □

Let K be as given in Lemma 2.1 and let w be a nonarchimedean place of K. A point $Q = (f, g) \in E(K_w)$ is called *special* if

$$w(f - \alpha) < \min\{w(\alpha - \beta), w(\beta - \gamma), w(\gamma - \alpha)\}.$$

If Q is special, then

$$w(f - \alpha) = w(f - \beta) = w(f - \gamma).$$

Put $\{\alpha_1, \alpha_2, \alpha_3\} = \{\alpha, \beta, \gamma\}$, and let $Q^{(i)}$ be as in Lemma 2.1.

Lemma 3.5. *Suppose that $Q^{(0)} = Q \in E(K_w)$ and E has G-type reduction at w with*

$$w(\alpha_1 - \alpha_2) = w(\alpha_2 - \alpha_3) = w(\alpha_3 - \alpha_1) = \epsilon.$$

(1) *If Q is special and $w(f-\alpha_1)=\epsilon-e<\epsilon$, then for $j=1,2,3$, $Q^{(j)}$ is not special and*

$$w(f^{(j)}-\alpha_i)=\begin{cases}\epsilon+e & \textit{if } i=j,\\ \epsilon & \textit{if } i\neq j.\end{cases}$$

(2) *If every $Q^{(j)}$ is not special for $j=0,1,2,3$, then, for every i and j,*

$$w(f^{(j)}-\alpha_i)=\epsilon.$$

Proof. Suppose that Q is special. By (2–1),

$$w(f^{(j)}-\alpha_j)=2w(\alpha-\beta)-w(f-\alpha)=\epsilon+e.$$

If $i\neq j$, then

$$w(f^{(j)}-\alpha_i)=w(f^{(j)}-\alpha_j+\alpha_j-\alpha_i)=\min(\epsilon+e,\epsilon)=\epsilon.$$

If every $Q^{(j)}$, $j=0,1,2,3$, is not special, then for every i, $w(f^{(j)}-\alpha_i)\geq\epsilon$. By (2–1) again, we must have $w(f^{(j)}-\alpha_i)\leq\epsilon$. □

Lemma 3.6. *Suppose that $Q\in E(K_w)$ and E has M-type reduction with*

$$\epsilon_1=w(\alpha_1-\alpha_2)=w(\alpha_1-\alpha_3)<w(\alpha_2-\alpha_3)=\epsilon_2.$$

(1) *If Q is special and $w(f-\alpha_1)=\epsilon_1-e<\epsilon_1$, then, for $j=1,2,3$, $Q^{(j)}$ is not special and*

$$w(f^{(j)}-\alpha_i)=\begin{cases}\epsilon_1+e & \textit{if } i=j=1,\\ \epsilon_2+e & \textit{if } i=j=2,3,\\ \epsilon_1 & \textit{if } (j=1,\ i\neq 1)\textit{or } (i=1,\ j\neq 1),\\ \epsilon_2 & \textit{if } i,j=2,3,\ j\neq i.\end{cases}$$

(2) *If every $Q^{(j)}$, $j=0,1,2,3$, is not special and $w(f-\alpha_2)=\epsilon_1+e$, then*

$$\epsilon_1=w(f-\alpha_1)\leq\epsilon+e=w(f-\alpha_3)\leq\epsilon_2.$$

Moreover, for $i,j=1,2,3$,

$$w(f^{(j)}-\alpha_i)=\begin{cases}\epsilon_1+e & \textit{if } j=1, i\neq 1\\ \epsilon_1 & \textit{if } i=1\\ \epsilon_2-e & \textit{if } i\neq 1, j\neq 1.\end{cases}$$

Proof. Most of the proof is similar to that of Lemma 3.5. Only the valuations of $f^{(1)}-\alpha_i$, $i\neq 1$, need special calculation. But, since $Q^{(1)}=Q^{(2)}+D_3$ and

$Q^{(1)} = Q^{(3)} + D_2$, by (2–1), we have

$$w(f^{(2)} - \alpha_2) + w(f^{(1)} - \alpha_2) = \epsilon_1 + \epsilon_2,$$
$$w(f^{(3)} - \alpha_3) + w(f^{(1)} - \alpha_3) = \epsilon_1 + \epsilon_2. \qquad \square$$

4. Unit equations

Let

$$\mathscr{C} = \{(P, Q) \mid P \in E(\mathbb{O}_S),\ 2Q = P\}.$$

For $(P_1, Q_1), (P_2, Q_2) \in \mathscr{C}$, we define an equivalence relation as follows:

$$(P_1, Q_1) \sim (P_2, Q_2) \quad \text{if and only if } Q_1 - Q_2 \in 12E(k).$$

Let $(P_1, Q_1), \ldots, (P_c, Q_c)$ represent all the equivalence classes in $\mathscr{C}$. Then

$$c \leq 4 \times E(k)/24E(k) \leq 4 \times 24^{r+2}.$$

Now, we fix an equivalence class represented by (P_l, Q_l). If $(P, Q) \sim (P_l, Q_l)$ and $Q = (f, g)$, $Q_l = (f_l, g_l)$, then the quantities

$$\begin{aligned} x &= (f - \alpha)/(f_l - \alpha), \quad & y &= (f - \beta)/(f_l - \beta), \\ \lambda &= (f_l - \alpha)/(\beta - \alpha), \quad & \mu &= (\beta - f_l)/(\beta - \alpha) \end{aligned} \tag{4–1}$$

satisfy

$$\lambda x + \mu y = 1. \tag{4–2}$$

Note that Q and Q_l determine the same field extension K/k. Let

$$\tilde{S} = \{w \mid w \in M_K \text{ and } w|v, \text{for some } v \in S' \cup S_1 \cup S_m\}.$$

Using (2–1), we see that x and y are units at every place w not sitting over $S \cup S_0 \cup S_1 \cup S_m$. For $v \in S_0$, E has additive reduction at v. Therefore,

$$12E(k_v) \subset E_0(k_v).$$

Applying Lemma 3.2 to Q and Q_l, we see that (4–2) is an $\tilde{S}$-unit equation.

Now we apply the theory of [Evertse 1984] to bound the cardinality of the equivalence class of (P_l, Q_l). We will follow the setting in that paper. Fix a primitive third root ρ of 1 and put $L = K(\rho)$. Given (P, Q) in the equivalence class of (P_l, Q_l), we define x, y, λ, μ by (4–1) and put

$$\xi = \xi(x, y) = \lambda x - \rho\mu y,\ \eta = \eta(x, y) = \lambda x - \rho^2\mu y,\ \zeta = \zeta(x, y) = \xi/\eta.$$

We denote by $\mathscr{V}^0$ the set of those $\zeta \in L$ for which an $\tilde{S}$-unit solution (x, y) of (4–2) exists with $\lambda x/\mu y$ not a root of one and such that $\zeta = \zeta(x, y)$. We denote by $\mathscr{V}^1$ the subset consisting of those $\zeta(x, y)$ such that x and y are defined by (4–1) using a point (P, Q) in the equivalence class of (P_l, Q_l). We can recover x and y from ζ. Therefore, it is enough to bound the number of elements in $\mathcal{V}^1$.

Let T be the set of places of L sitting over $\tilde{S}$ and put

$$A = \Big(\prod_{V\in T} |3|_V\Big)^{1/2} \prod_{V\in T} |\lambda\mu|_V \Big(\prod_{V\notin T} \max(|\lambda|_V \cdot |\mu|_V)\Big)^3.$$

Definition 4.1. For $V \in M_L$, $\zeta \in L$, put

$$m_V(\zeta) = \min_{i=0,1,2}(1, \max(|1-\rho^i\zeta|_V, |1-\rho^{-i}\zeta^{-1}|_V).$$

Lemma 4.2 [Evertse 1984, Lemma 3]. *We have*

$$\prod_{V\in T} m_V(\zeta) \le 8Ah(\zeta)^{-3} \quad \textit{for } \zeta \in \mathcal{V}^0.$$

The next lemma follows by direct calculation.

Lemma 4.3. *Suppose that $V \in M_L$ is nonarchimedean and $\zeta = \zeta(x, y) \in \mathcal{V}^0$.*

(1) *If $|\mu y|_V < 1$, then*

$$\begin{aligned} m_V(\zeta) &= |1-\zeta|_V = |(1-\rho)\mu y|_V \\ &< |1-\rho^i\zeta|_V, \ \textit{for } i \ne 0. \end{aligned}$$

(2) *If $|\lambda x|_V < 1$, then*

$$\begin{aligned} m_V(\zeta) &= |1-\rho\zeta|_V = |(1-\rho)\lambda x|_V \\ &< |1-\rho^i\zeta|_V, \ \textit{for } i \ne 1. \end{aligned}$$

(3) *If $|\lambda x|_V^{-1} < 1$, then*

$$\begin{aligned} m_V(\zeta) &= |1-\rho^2\zeta|_V = |(1-\rho)(\lambda x)^{-1}|_V \\ &< |1-\rho^i\zeta|_V, \textit{ for } i \ne 2. \end{aligned}$$

(4) *If $|\lambda x|_V = |\mu y|_V = 1$, then*

$$\begin{aligned} m_V(\zeta) &= |1-\zeta|_V = |1-\rho\zeta|_V \\ &= |1-\rho^2\zeta|_V = |1-\rho|_V. \end{aligned}$$

Definition 4.4. For a ζ in $\mathcal{V}^0$ and $V \in T$, we choose a $\rho_V \in \{1, \rho, \rho^2\}$ such that

$$m_V(\zeta) = \min(1, \max(|1-\rho_V\zeta|_V, |1-\rho_V^{-1}\zeta^{-1}|_V)).$$

If V is nonarchimedean and we are in case (4) of the preceding lemma, we choose $\rho_V = 1$.

For a nonarchimedean place $v \in S' \cup S_1 \cup S_m$, let

$$T_v = \{V \in T \mid V|v\}.$$

Recall that if $\zeta \in \mathcal{V}^1$, there is an associated $(P, Q) \in \mathcal{C}$.

From now on, we fix the indices so that $\alpha_1 = \alpha$, $\alpha_2 = \beta$, $\alpha_3 = \gamma$, $D_i = (\alpha_i, 0)$, and as before, we put $Q^{(i)} = Q + D_i$.

Definition 4.5. Let ζ be in $\mathcal{V}^1$ and let V be a nonarchimedean place. We say that ζ is *of type* i, where $i = 0, 1, 2, 3$, if $Q^{(i)}$ is special at V. If none of the $Q^{(i)}$ is special, we say that ζ is *of type* 4.

Consider the set of numbers

$$\left|(f^{(j)} - \alpha_{j_1})/(\alpha_{j_1} - \alpha_{j_2})\right|_V$$

and their inverses, where we take $j = 0, 1, 2, 3,\ \ j_1, j_2 = 1, 2, 3,$ and $j_1 \neq j_2$. By the *conductor* of ζ at V we mean the set $C_V(\zeta)$ consisting of all those numbers in this set which are at most one. We list the elements of $C_V(\zeta)$ as $c_{V,i}$ with $i = 0, 1, 2, \dots$ and $c_{V,0} = 1$. If E has G-type reduction at V, then Lemma 3.5 implies that

$$C_V = \begin{cases} \{1, c_{V,1}\} & \text{if } \zeta \text{ is of type } 0, 1, 2, 3; \\ \{1\} & \text{if } \zeta \text{ is of type } 4. \end{cases}$$

Also, if E has M-type reduction at V, then Lemma 3.6 implies that

$$C_V = \begin{cases} \{1, c_{V,1},\ c_{V,2}\} & \text{if } \zeta \text{ is of type } 0, 1, 2, 3; \\ \{1, c_V\} \text{ or } \{1, c_{V,1},\ c_{V,2}\} & \text{if } \zeta \text{ is of type } 4. \end{cases}$$

Set $\mathcal{G} = \mathrm{Gal}(L/k)$. Then $\mathcal{G}$ acts transitively on T_v and for $z \in L$, $\sigma \in \mathcal{G}$, we have

$$|z|_{\sigma(V)} = |\sigma^{-1}(z)|_V. \tag{4–3}$$

For $z = (f - \alpha)/(\alpha - \beta)$, or $z = (f - \beta)/(\alpha - \beta)$, we have

$$\sigma^{-1}(z) \in \{(f^{(j)} - \alpha_i)/(\alpha_i - \alpha_{i'}) \mid j = 0, 1, 2, 3,\ i, i' = 1, 2, 3\}.$$

From these facts and Lemma 4.3, we can deduce the next result:

Lemma 4.6. *Let $v \in S' \cup S_1 \cup S_m$ be a nonarchimedean place and let V_0 be a place in T_v. Then, for a given $\zeta \in \mathcal{V}^1$, the map $T_v \to \{1, \rho, \rho^2\}$, $V \mapsto \rho_V$, depends only on the type of ζ at V_0. Moreover, if E has G-type reduction at v and $C_{V_0} = \{1\}$ or $\{1, c_{V_0,1}\}$, there is a decomposition*

$$T_v = T_v^0 \cup T_v^1,$$

which depends only on the type of ζ such that

$$m_V = \begin{cases} 1 & \text{if } V \in T_v^0 \\ c_{V_0,1} & \text{if } V \in T_v^1. \end{cases}$$

Also, if E has M-type reduction at v, there is a decomposition

$$T_v = T_v^0 \cup T_v^1 \cup T_v^2,$$

which depends only on the type of ζ such that

$$m_V = \begin{cases} 1 & \text{if } V \in T_v^0, \\ c_{V_0,1} & \text{if } V \in T_v^1, \\ c_{V_0,2} & \text{if } V \in T_v^2. \end{cases}$$

Let $v \in S' \cup S_1 \cup S_m$ be a nonarchimedean place. We fix a place V_0 in T_v, and put $t_v^i = \# T_v^i$. If E has G-type reduction at v, define

$$m_v = c_{V_0,1}^{t_v^1}.$$

If E has M-type reduction at v, define

$$m_{v,1} = c_{V_0,1}^{t_v^1} \quad \text{and} \quad m_{v,2} = c_{V_0,2}^{t_v^2}.$$

Here we use the convention that if T_v^i is empty, the associated m_v or $m_{v,i}$ is 1.

The following lemma is similar to [Evertse 1984, Lemma 5]. Let S_∞ and T_∞ be respectively the set of all infinite places in k and L, also, let $s_\infty = \# S_\infty$ and $t_\infty = \# T_\infty$. Note that every place in T_∞ is complex, and hence

$$t_\infty = [L:\mathbb{Q}]/2 \le 4md.$$

For a real number B with $0 < B < 1$, put

$$R(B) = (1-B)^{-1} B^{B/(B-1)}.$$

Lemma 4.7. *Let B be a real number with $1/2 \le B < 1$. There exists a set $\mathcal{W}_1$ of cardinality at most*

$$5^{s'+s_1+s_m-s_\infty} \times 3^{t_\infty} \times R(B)^{s'+s_1+2s_m-s_\infty+t_\infty-1},$$

consisting of tuples $((\rho_V)_{V\in T}, (\Gamma_V)_{V\in T})$ with $\rho_V^3 = 1$ and $\Gamma_V \ge 0$ for $V \in T$ and $\sum_{V\in T} \Gamma_V = B$ with the following property: for every $\zeta \in \mathcal{V}^1$ there is a tuple $((\rho_V)_{V\in T}, (\Gamma_V)_{V\in T}) \in \mathcal{W}_1$ such that ζ satisfies

$$\min(1, |1-\rho_V\zeta|_V) \le (8Ah(\zeta)^{-3})^{\Gamma_V}, \ \text{for } V \in T. \tag{4–4}$$

Proof. Consider the index set

$$I = \{(w, j) \mid (j = 1,\ w \in (S' \cup S_1 \cup T_\infty) \setminus (S_m \cup S_\infty)) \text{ or } (j = 1, 2,\ w \in S_m)\}.$$

Then $\#I \le q := s' + s_1 + 2s_m - s_\infty + t_\infty$. For $\zeta \in \mathcal{V}^1$ and $(w, j) \in I$, let

$$m_{w,j} = \begin{cases} m_v & \text{if } w = v \in (S' \cup S_1) \setminus (S_m \cup S_\infty), \\ m_V & \text{if } w = V \in T_\infty, \\ m_{v,1} & \text{if } w = v \in S_m \text{ and } j = 1, \\ m_{v,2} & \text{if } w = v \in S_m \text{ and } j = 2. \end{cases}$$

By Lemma 4.2, we have

$$\prod_{(w,j)\in I} m_{w,j} \le 8Ah(\zeta)^{-3}, \quad \text{for } \zeta \in \mathcal{V}^1. \tag{4–5}$$

We know form [Evertse 1984, Lemma 4] that there exists a set $\mathcal{W}$ of cardinality at most $R(B)^{q-1}$ consisting of tuples $(\Phi_{w,j})_{(w,j)\in I}$ such that for every $\zeta \in \mathcal{V}^1$ there is a tuple $(\Phi_{w,j})_{(w,j)\in I}$ such that

$$m_{w,j} \le (8Ah(\zeta)^{-3})^{\Phi_{w,j}}.$$

Here the tuples can be chosen such that if $m_{w,j} = 1$, then $\Phi_{w,j} = 0$. In particular, if T_v^j is empty, we put $\Phi_{w,j}/t_v^j = 0$. We define

$$\Gamma_V = \begin{cases} 0 & \text{if } V \in T_v^0 \text{ for some } v \in S' \cup S_1 \cup S_m \setminus S_\infty, \\ \Phi_{w,1}/t_v^1 & \text{if } V \in T_v^1 \text{ for some } v \in (S' \cup S_1 \cup S_m) \setminus S_\infty, \\ \Phi_{w,2}/t_v^2 & \text{if } V \in T_v^2 \text{ for some } v \in S_m, \\ \Phi_{w,j} & \text{if } V \in T_\infty. \end{cases}$$

Then inequality (4–4) holds. By Lemma 4.6, there are at most $5^{s'+s_1+s_m-s_\infty} \times 3^{t_\infty}$ choices of ρ_V's. □

Now take $B = 0.846$. The total number of $\zeta \in \mathcal{W}^1$ that satisfy a fixed system (4–4) and for which we have $h(\zeta) \ge e^8/2$ is at most 25 (see [Evertse 1984, p. 583]). The cardinality of $\mathcal{W}^1$ is at most

$$\begin{aligned} &5^{s'+s_1+s_m-s_\infty} \times 3^{t_\infty} \times R(B)^{s'+s_1+2s_m-s_\infty+t_\infty-1} \\ &\qquad \le 5^{s'+s_1+s_m-s_\infty} \times 3^{t_\infty} \times (49/3)^{s'+s_1+2s_m-s_\infty+t_\infty-1} \\ &\qquad \le 2/25 \times (3/49) \times (245/3)^{s'+s_1} \times (12005/9)^{s_m} \times (3/245)^{s_\infty} \times (7)^{2t_\infty}. \end{aligned}$$

We note that t_∞ is at most $4md$. A simple calculation shows that

$$\#\mathcal{W}^1 \le 2/25 \times (3/49) \times 7^{2.27(s'+s_1)+3.7s_m+8md} \times (3/245)^{s_\infty}$$

By [Evertse 1984, (36)], we have $h(\lambda x/\mu y) \le 2h(\zeta(x, y))$. All of this yields the following lemma.

Lemma 4.8. *The total number of* $(P, Q) \sim (P_l, Q_l)$ *with* $Q = (f, g)$ *such that* $h((f-\alpha)/(f-\beta)) \ge e^8$ *is at most*

$$6/49 \times 7^{2.27(s'+s_1)+7.2s_m+8md} \times (3/245)^{s_\infty}.$$

Proof of Theorem 1.3. We first fix the equivalence class of (P_l, Q_l). We follow the argument in [Evertse 1984, p. 583]. Let $\tilde{s} = \#\tilde{S}$. The group of $\tilde{S}$-units is the direct product of $\tilde{s}$ multiplicative cyclic groups, one of which is finite. The fraction $(f-\alpha)/(f-\beta)$ is a $\tilde{S}$-unit. We assume that for each $v \in S' \cup S_1 \cup S_m \setminus S_\infty$, a place $V_v \in T_v$ is chosen. Consider the index set

$$\Phi := \{(i_v)_v \mid i_v = 1, 2, 3, 4, 5,\ v \in S' \cup S_1 \cup S_m \setminus S_\infty\}.$$

For each $\phi = (i_v)_v \in \Phi$, let

$$\mathcal{V}^1_\phi = \{\zeta \in \mathcal{V}^1 \mid \zeta \text{ is of type } i_v \text{ at every } v \in S' \cup S_1 \cup S_m \setminus S_\infty\}.$$

Then by (2–1) and (4–3), under the map

$$\begin{aligned} \mathcal{V}^1 &\to \textstyle\prod_{V \in \tilde{S}\setminus\tilde{S}_\infty} K_V^* \\ \zeta &\mapsto (|(f-\alpha)/(f-\beta)|_V)_V, \end{aligned}$$

the image of each $\mathcal{V}^1_\phi$ is in a coset of a subgroup which is a direct product of less than $s'+s_1+s_m-s_\infty$ multiplicative cyclic groups. This shows that, for a fixed ϕ, the set of all $(f-\alpha)/(f-\beta)$ for which $\zeta \in \mathcal{V}^1_\phi$ is in a coset of a subgroup which is a direct product of less than $s_3 := t_\infty + s' + s_1 + s_m - s_\infty$ multiplicative cyclic groups. Let n be a positive integer. Then there is an $\tilde{S}$-unit z and an element $\omega \in K$ belonging to a fixed set of cardinality at most n^{s_3} which does not depend on f such that $(f-\alpha)/(f-\beta) = \omega z^n$. Let ω be a fixed element of this set and let θ be a fixed n'th root of ω. By [Evertse 1984, Lemma 1], the number of nonzero z in K with $h(\theta z) < e^{8/n}$ is at most $5(2e^{24/n})^{[K:\mathbb{Q}]}$. Also, the fraction $(f-\alpha)/(f-\beta)$ determines ζ. Using these and taking $n = 49/3$, we see that the cardinality of the subset of $\mathcal{V}^1$ consisting of those ζ with $h((f-\alpha)/(f-\beta)) < e^8$ is at most

$$\begin{aligned} 5^{s'+s_1+s_m-s_\infty} \times 5n^{s_3}(2e^{24/n})^{[K:\mathbb{Q}]} &\le (245/3)^{s'+s_1+s_m-s_\infty} \times 5 \times (49/3)^{t_\infty} \times 8.78^{4md} \\ &\le 5 \times 7^{2.27(s'+s_1+s_m)+10.3md} \times (3/245)^{s_\infty}. \end{aligned}$$

Therefore,

$$\begin{aligned}\#\mathscr{C} &\le 4\times|E(k)/24E(k)|\times(3/245)^{s_\infty}\times(6/49\times 7^{2.27(s'+s_1)+3.7s_m+8md}\\ &\qquad\qquad\qquad\qquad\qquad\qquad + 3/49\times 7^{2.27(s'+s_1+s_m)+10.3md})\\ &\le 4\times|E(k)_{\mathrm{tor}}/24E(k)_{\mathrm{tor}}|\times(3/245)^{s_\infty}\times 24^r\times 6\times 7^{2.27(s'+s_1)+3.7s_m+10.3md}\\ &\le 4\times 6\times|E(k)_{\mathrm{tor}}/24E(k)_{\mathrm{tor}}|\times(3/245)^{s_\infty}\times 7^{1.64r+2.27(s'+s_1)+3.7s_m+10.3md}.\end{aligned}$$

The map $\mathscr{C}\to E(\mathbb{O}_S)$ given by $(P,Q)\mapsto P$ is 4 to 1. If $s_\infty\ge 2$, then

$$6\times|E(k)_{\mathrm{tor}}/24E(k)_{\mathrm{tor}}|\times(3/245)^{s_\infty}\le 6\times 24^2\times(3/245)^2<1,$$

and the theorem is proved. Otherwise, the number field k has degree at most 2, and the order of the torsion part of the multiplicative group k^* is at most 6. In this case, via Weil pairing, we see that if $E(k)_{\mathrm{tor}}$ contains a subgroup of the form $\mathbb{Z}/N\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z}$ then $N\le 6$. Consequently, we have $|E(k)_{\mathrm{tor}}/24E(k)_{\mathrm{tor}}|\le 24\times 6$ and hence

$$6\times|E(k)_{\mathrm{tor}}/24E(k)_{\mathrm{tor}}|\times(3/245)^{s_\infty}\le 36\times 24\times(3/245)<11,$$

as we wished to show. □

References

[Chi et al. 2004] W.-C. Chi, K. F. Lai, and K.-S. Tan, "Integral points on elliptic curves over function fields", *J. Aust. Math. Soc.* **77**:2 (2004), 197–208. MR 2005g:11093 Zbl 02158910

[Chi et al. $\ge$ 2006] W.-C. Chi, P.-Y. Huang, and K.-S. Tan, "Uniform bounds for the number of integer solutions to $Y^n = f(X)$". In preparation.

[Evertse 1984] J.-H. Evertse, "On equations in S-units and the Thue–Mahler equation", *Invent. Math.* **75**:3 (1984), 561–584. MR 85f:11048 Zbl 0521.10015

[Gross and Silverman 1995] R. Gross and J. Silverman, "S-integer points on elliptic curves", *Pacific J. Math.* **167**:2 (1995), 263–288. MR 96c:11057 Zbl 0824.11038

[Hindry and Silverman 1988] M. Hindry and J. H. Silverman, "The canonical height and integral points on elliptic curves", *Invent. Math.* **93**:2 (1988), 419–450. MR 89k:11044 Zbl 0657.14018

[Lang 1978] S. Lang, *Elliptic curves: Diophantine analysis*, Grundlehren der Mathematischen Wissenschaften **231**, Springer, Berlin, 1978. MR 81b:10009 Zbl 0388.10001

[Silverman 1984] J. H. Silverman, "The S-unit equation over function fields", *Math. Proc. Cambridge Philos. Soc.* **95**:1 (1984), 3–4. MR 85e:11018 Zbl 0533.10013

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1986. MR 87g:11070 Zbl 0585.14026

[Silverman 1987] J. H. Silverman, "A quantitative version of Siegel's theorem: integral points on elliptic curves and Catalan curves", *J. Reine Angew. Math.* **378** (1987), 60–100. MR 89g:11047 Zbl 0608.14021

[Tan 2002] K.-S. Tan, "A 2-division formula for elliptic curves", National Taiwan University, January 2002.

Received April 19, 2004.

WEN-CHEN CHI
DEPARTMENT OF MATHEMATICS
NATIONAL TAIWAN NORMAL UNIVERSITY
TAIPEI
TAIWAN

wchi@math.ntnu.edu.tw

KING FAI LAI
SCHOOL OF MATHEMATICS AND STATISTICS
UNIVERSITY OF SYDNEY
SYDNEY, NSW 2006
AUSTRALIA

kflai@maths.usyd.edu.au

KI-SENG TAN
DEPARTMENT OF MATHEMATICS
NATIONAL TAIWAN UNIVERSITY
TAIPEI
TAIWAN

tan@math.ntu.edu.tw