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 $\mathcal{O}_S$. Serge Lang conjectured that if the Weierstrass equation of $E$ is quasiminimal, then the cardinality of the set $E(\mathcal{O}_S)$ of $\mathcal{O}_S$-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 $\delta$ places of $k$, then a bound was also given with $\delta$ 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

$$(1-1) \quad Y^2 = X^3 + aX + B,$$

where $a, B \in \mathcal{O}_S$. Put $\Delta = 4a^3 + 27B^2$. 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 $| \cdot |_v$ be such that, for $z \in \mathbb{Q}$,

$$|z|_v = |z|_{p^{[k_v:Q_p]/[k:Q]}}.$$
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

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

Then

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

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 \( \mathfrak{D}_{E/k} \) be the ideal of the minimal discriminant of \( E/k \). Then we have

\[
(\Delta) = \mathfrak{D}_{E/k} \cdot \prod_v P_v^{12\chi_v},
\]

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

\[
X^3 + aX + b = (X - \alpha)(X - \beta)(X - \gamma).
\]

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

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.**

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

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

\[ \left| \text{Norm}_{k/Q} \prod_{v \in S_1} P^x_v \right| \leq |D_k|^6, \]

and hence

\[ s_1 \leq 6 \log |D_k|. \]

The exponent in the Gross–Silverman bound is *quadratic* in \( \delta \) 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. \( \geq 2006 \)].

**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
\[
(f - \alpha_i)(f^{(i)} - \alpha_j) = (\alpha_i - \alpha_j)(\alpha_i - \alpha_{j'}),
\]
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 \( \text{Gal}(K_w/k_v) \). 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
\[
\tilde{Y} = Y/\pi^{3m}, \quad \tilde{X} = (X - \alpha)/\pi^{2m},
\]
\[
\tilde{\beta} = (\beta - \alpha)/\pi^{2m}, \quad \tilde{\gamma} = (\gamma - \alpha)/\pi^{2m}.
\]
where $\pi$ 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, $\tilde{v}(j_{\tilde{E}}) = \tilde{v}(j_E) < 0$ 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 $\tilde{E}$ be the reduction of $E$ at $v$. As usual, for $P \in E(k_v)$, we denote its image under the reduction map $E(k_v) \to \tilde{E}(\mathbb{F}_v)$ by $\tilde{P}$. Put

$$E_0(k_v) = \{ P \in E(k_v) \mid \tilde{P} \in \tilde{E}_n s(\mathbb{F}_v) \},$$

where $\tilde{E}_ns$ is the set of nonsingular points of $\tilde{E}$. 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 $P_1, P_2 \in E(\mathbb{Q}_v)$, let $Q_i = (f_i, g_i) \in E(\mathbb{Q}_w)$, for $i = 1, 2$, be such that $2Q_i = P_i$. If $Q_1 - Q_2 \in E_0(k_v)$, then

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

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

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

where $\pi$ 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

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

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

$$0 \to \hat{E}_1 \to \hat{E}_0 \to \tilde{E}_ns \to 0,$$

where $\tilde{E}_ns$ 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
   \[
   R \in \hat{E}_m \setminus \hat{E}_{m+1} \iff w(\tilde{t}) = m \iff (w(\tilde{X}) = -2m \text{ and } w(\tilde{Y}) = -3m).
   \]
2. If \( m = 0 \) and \( \epsilon = 0 \), then
   \[
   R \in \hat{E}_0 \setminus \hat{E}_1 \iff w(\tilde{t}) \leq 0 \iff (w(\tilde{X}) \geq 0 \text{ and } w(\tilde{Y}) \geq 0).
   \]
3. If \( m = 0 \) and \( \epsilon = 1 \), then
   \[
   R \in \hat{E}_0 \setminus \hat{E}_1 \iff w(\tilde{t}) = 0 \iff (w(\tilde{X}) = 0 \text{ and } w(\tilde{Y}) = 0).
   \]

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 \( w(f - \alpha) \leq 0 \). Since \( \tilde{f} = (f - \alpha)/\pi^{2a} \), \( \tilde{g} = g/\pi^{3a} \), we have \( w(\tilde{f}) \leq -2a \). By Lemma 3.3, we have \( \tilde{Q} \in \hat{E}_a \subset \hat{E}_0 \). \[\square\]

**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
\[
(3–1) \quad w(\tilde{f}_1) + w(\tilde{f}'_1) = 2\epsilon.
\]
Similarly,
\[
(3–2) \quad w(\tilde{f}_2) + w(\tilde{f}'_2) = 2\epsilon.
\]
First we consider the case where
\[
w(f_1 - \alpha) \leq 2a + \epsilon.
\]
Then \( w(\tilde{f}_1) \leq \epsilon \). 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, \( \tilde{Q}_1 \not\in \tilde{E}_0(K_w) \). By Lemma 3.4, \( \tilde{Q}_1 - \tilde{Q}_2 \in \tilde{E}_a \subset \tilde{E}_0 \), 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 \( w(\tilde{f}_1') = -2m \leq 0 \). Note that by Lemma 2.1 \( Q_i \in E(C_w), i = 1, 2 \) and we have \( w(f_i - \alpha) \geq 0 \). Hence,

\[
(3-3) \quad w(\tilde{f}_1') \geq -2a.
\]

This means that \( \tilde{Q}_1 \not\in \tilde{E}_{a+1} \) and \( \tilde{Q}_1 \in \tilde{E}_m \setminus \tilde{E}_{m+1} \). If \( a > m \), then by Lemma 3.3 and Lemma 3.4, we also have \( \tilde{Q}_2 \in \tilde{E}_m \setminus \tilde{E}_{m+1} \)
and hence \( w(\tilde{f}_2') = -2m \). If \( a = m \), then we have \( \tilde{Q}_2 \in \tilde{E}_a \) and hence \( w(\tilde{f}_2') \leq -2a \).

For the case where

\[
(\text{2–1}) \quad w(f_1 - \alpha) > 2a + \epsilon,
\]

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

\[
w(f - \alpha) \leq \min\{w(\alpha - \beta), w(\beta - \gamma), w(\gamma - \alpha)\}.
\]

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

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

(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 \( w(f^{(j)} - \alpha_i) \leq \epsilon \). \( \Box \)

**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

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

(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 \( i, j = 1, 2, 3 \),

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

**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
Applying Lemma 3.2 to $Q_{x}$, we see that

$$w(f(2) - \alpha) + w(f(1) - \alpha_2) = \epsilon_1 + \epsilon_2,$$

$$w(f(3) - \alpha_3) + w(f(1) - \alpha_3) = \epsilon_1 + \epsilon_2.$$  \hfill \Box

### 4. Unit equations

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

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

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

Let $(P_1, Q_1), \ldots, (P_r, Q_r)$ represent all the equivalence classes in $\mathcal{E}$. Then

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

Now, we fix an equivalence class represented by $(P_1, Q_1)$. If $(P, Q) \sim (P_1, Q_1)\text{ and } Q = (f, g), Q_1 = (f_1, g_1)$, then the quantities

$$(4-1) \quad x = (f - \alpha)/(f_i - \alpha), \quad y = (f - \beta)/(f_i - \beta),$$

$$\lambda = (f_i - \alpha)/(\beta - \alpha), \quad \mu = (\beta - f_i)/(\beta - \alpha)$$

satisfy

$$(4-2) \quad \lambda x + \mu y = 1.$$  

Note that $Q$ and $Q_1$ 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 $Q_1$, 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 $(P_1, Q_1)$. We will follow the setting in that paper. Fix a primitive third root $\rho$ of 1 and put $L = K(\rho)$. Given $(P, Q)$ in the equivalence class of $(P_1, Q_1)$, we define $x, y, \lambda, \mu$ by (4–1) and put

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

We denote by $\gamma^0$ 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 $\xi = \xi(x, y)$. We denote by $\gamma^1$ the subset consisting of those $\xi(x, y)$ 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 \(\zeta\). 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

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

**Definition 4.1.** For \(V \in M_L, \zeta \in L\), put

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

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

\[
\prod_{V \in T} m_V(\zeta) \leq 8Ah(\zeta)^{-3} \text{ for } \zeta \in \mathcal{V}^0.
\]

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
   \[
   m_V(\zeta) = |1 - \zeta|_V = (1 - \rho)\mu y|_V < |1 - \rho^i \zeta|_V, \text{ for } i \neq 0.
   \]

2. If \(|\lambda x|_V < 1\), then
   \[
   m_V(\zeta) = |1 - \rho \zeta|_V = (1 - \rho)\lambda x|_V < |1 - \rho^i \zeta|_V, \text{ for } i \neq 1.
   \]

3. If \(|\lambda x V^{-1}| < 1\), then
   \[
   m_V(\zeta) = |1 - \rho^2 \zeta|_V = (1 - \rho)(\lambda x)^{-1}|_V < |1 - \rho^i \zeta|_V, \text{ for } i \neq 2.
   \]

4. If \(|\lambda x|_V = |\mu y|_V = 1\), then
   \[
   m_V(\zeta) = |1 - \zeta|_V = |1 - \rho \zeta|_V = |1 - \rho^2 \zeta|_V = |1 - \rho|_V.
   \]

**Definition 4.4.** For a \(\zeta\) 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 \( \zeta \in \mathbb{V}^1 \), there is an associated \( (P, Q) \in \mathcal{E} \).

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 \( \zeta \) be in \( \mathbb{V}^1 \) and let \( V \) be a nonarchimedean place. We say that \( \zeta \) 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 \( \zeta \) is of type 4.

Consider the set of numbers
\[
\left| \left( f^{(j)} - \alpha_{j_i} \right)/(\alpha_{j_1} - \alpha_{j_2}) \right|_V
\]
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 \( \zeta \) 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 \( i = 0, 1, 2, \ldots \) 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 \( \mathcal{G} = \text{Gal}(L/k) \). Then \( \mathcal{G} \) acts transitively on \( T_v \) and for \( z \in L, \sigma \in \mathcal{G} \), we have
\[
(4–3) \quad |z|_{\sigma(v)} = |\sigma^{-1}(z)|_V.
\]

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 \( \zeta \in \mathbb{V}^1 \), the map \( T_v \to \{1, \rho, \rho^2\} \), \( V \mapsto \rho_V \), depends only on the type of \( \zeta \) 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 $\xi$ 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 $\xi$ 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

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

If $E$ has M-type reduction at $v$, define

$$m_v,1 = c_{V_0,1}^t \quad \text{and} \quad m_v,2 = c_{V_0,2}^t.$$

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 $S_\infty$ and $T_\infty$ 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 $T_\infty$ is complex, and hence

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

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 $1/2 \leq B < 1$. There exists a set $\mathcal{W}_1$ of cardinality at most

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

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

$$\min(1, |1 - \rho_V \xi|_V) \leq (8Ah(\xi)^{-3})^{\Gamma_V}, \quad \text{for } V \in T.$$  

(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 \( \#I \leq q := s' + s_1 + 2s_m - s_\infty + t_\infty. \) For \( \xi \in \mathcal{V}^1 \) 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

\[
\prod_{(w, j) \in I} m_{w, j} \leq 8Ah(\xi)^{-3}, \quad \text{for } \xi \in \mathcal{V}^1.
\]

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

\[
m_{w, j} \leq (8Ah(\xi)^{-3})^{\Phi_{w, j}}.
\]

Here the tuples can be chosen such that if \( m_{w, j} = 1 \), then \( \Phi_{w, j} = 0 \). In particular, if \( T_v \) 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 \( \rho_v \)'s.

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

\[
5^{s' + s_1 + s_m - s_\infty} \times 3^{t_\infty} \times R(B)^{s' + s_1 + 2s_m - s_\infty + t_\infty - 1} \leq 5^{s' + s_1 + s_m - s_\infty} \times 3^{t_\infty} \times (49/3)^{s' + s_1 + 2s_m - s_\infty + t_\infty - 1} \leq 2/25 \times (3/49) \times (245/3)^{s' + s_1} \times (12005/9)^{s_m} \times (3/245)^{s_\infty} \times (7)^{2t_\infty}.
\]

We note that \( t_\infty \) is at most \( 4md \). A simple calculation shows that

\[
\#\mathcal{W}^1 \leq 2/25 \times (3/49) \times 7^{2.27(s' + s_1) + 3.7s_m + 8md} \times (3/245)^{s_\infty}.
\]
By [Evertse 1984, (36)], we have \( h(\lambda x/\mu y) \leq 2h(\zeta(x, y)) \). All of this yields the following lemma.

**Lemma 4.8.** The total number of \((P, Q) \sim (P_1, Q_1)\) with \(Q = (f, g)\) such that \(h((f - \alpha)/(f - \beta)) \geq e^8\) is at most

\[
6/49 \times 7^{2.27(s' + s_1)} + 7.2m + 8md \times (3/245)^{t_\infty}.
\]

**Proof of Theorem 1.3.** We first fix the equivalence class of \((P_1, Q_1)\). We follow the argument in [Evertse 1984, p. 583]. Let \(\tilde{s} = \#S\). The group of \(\tilde{S}\)-units is the direct product of \(s\) 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

\[
\mathcal{V}^1 \rightarrow \prod_{V \in \tilde{S} \setminus \tilde{S}_{\infty}} K^*_V,
\]

\[
\zeta \rightarrow ((f - \alpha)/(f - \beta)|_V),
\]

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 \(\phi\), 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 \(s_3 := t_{\infty} + s'_1 + s_1 + s_m - s_{\infty}\) 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 \(\omega\) be a fixed element of this set and let \(\theta\) be a fixed \(n\)th root of \(\omega\). By [Evertse 1984, Lemma 1], the number of nonzero \(z\) in \(K\) with \(h(\theta z) < e^{8/n}\) is at most \(5(2e^{24/n})^{[K:Q]}\). Also, the fraction \((f - \alpha)/(f - \beta)\) determines \(\zeta\). Using these and taking \(n = 49/3\), we see that the cardinality of the subset of \(\mathcal{V}^1\) consisting of those \(\zeta\) with \(h((f - \alpha)/(f - \beta)) < e^8\) is at most

\[
5^{s'/s_1 + s_m - s_{\infty}} \times 5 n^{s_3} (2e^{24/n})^{[K:Q]} \leq (245/3)^{s'/s_1 + s_m - s_{\infty}} \times 5 \times (49/3)^{t_{\infty}} \times 8.79^{4md}
\]

\[
\leq 5 \times 7^{2.27(s'/s_1 + s_m) + 10.3md} \times (3/245)^{t_{\infty}}.
\]
Therefore,
\[
\# \mathcal{E} \leq 4 \times |E(k)/24E(k)| \times (3/245)^{s_\infty} \times (6/49 \times 7^{2.27(s' + s_1) + 3.7s_n + 8md} \\
+ 3/49 \times 7^{2.27(s' + s_1 + s_n) + 10.3md}) \\
\leq 4 \times |E(k)_{tor}/24E(k)_{tor}| \times (3/245)^{s_\infty} \times 24^r \times 6 \times 7^{2.27(s' + s_1) + 3.7s_n + 10.3md} \\
\leq 4 \times 6 \times |E(k)_{tor}/24E(k)_{tor}| \times (3/245)^{s_\infty} \times 7^{1.64r + 2.27(s' + s_1) + 3.7s_n + 10.3md}.
\]

The map \( e \mapsto E(C_S) \) given by \((P, Q) \mapsto P\) is 4 to 1. If \( s_\infty \geq 2 \), then
\[
6 \times |E(k)_{tor}/24E(k)_{tor}| \times (3/245)^{s_\infty} \leq 6 \times 24^2 \times (3/245)^2 < 1,
\]
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 \( E(k)_{tor} \) contains a subgroup of the form \( \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \), then \( N \leq 6 \). Consequently, we have \( |E(k)_{tor}/24E(k)_{tor}| \leq 24 \times 6 \) and hence
\[
6 \times |E(k)_{tor}/24E(k)_{tor}| \times (3/245)^{s_\infty} \leq 36 \times 24 \times (3/245) < 11,
\]
as we wished to show. \( \square \)

References


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