# SIEGEL'S THEOREM OVER $\mathbb{Q}$

PETER S. PARK

## 1. Introduction

An *elliptic curve over* $\mathbb{Q}$ is a nonsingular projective curve defined over $\mathbb{Q}$ that has genus 1 and a specified rational point $\mathcal{O}$, which is denoted as the *point at infinity*. By a linear change of variables, any such curve can be written as a nonsingular plane cubic $C$ in short Weierstrass form, i.e., with affine part $C' : y^2 = x^3 + Ax + B$ for some $A, B \in \mathbb{Z}$ such that the discriminant $-16(4A^3 + 27B^2)$ is nonzero, where [0, 1, 0] is the point at infinity. The set of rational points $C(\mathbb{Q})$ of this elliptic curve $C$ has historically been a very interesting object of study, one important reason for which is the fact that there is a natural group structure on $C(\mathbb{Q})$ with identity element $\mathcal{O}$. Some of today's most important open problems in number theory have to do with the group properties of $C(\mathbb{Q})$, particularly its rank (by the celebrated Mordell-Weil theorem, $C(\mathbb{Q})$ is a finitely generated abelian group).

A natural diophantine question connected to the above line of inquiry is the following: what can one say about the set of *integral* points of the affine part $C'$? There are a number of reasons why answering this question is important in the study of elliptic curves; for instance, the Nagell-Lutz theorem states that a necessary condition for a rational point in $C'$ to be torsion is that it's integral. To answer a key part of this question, we will prove the following 1929 result of Carl Ludwig Siegel:

**Theorem 1.1.** *Let $C$ be a nonsingular curve over $\mathbb{Q}$ with affine part $C' : y^2 = x^3 + Ax + B$ such that $A, B \in \mathbb{Z}$. Then, $C'$ has only finitely many integral points.*

To accomplish this, we will require two main ingredients. The first is the Thue-Siegel-Roth theorem of diophantine approximation, which we have studied in our seminar.

**Theorem 1.2** (Thue-Siegel-Roth)**.** *Let $\alpha$ be an algebraic number. For any $\varepsilon > 0$, there exist only finitely many $x \in \mathbb{Q}$ such that*

$$|x - \alpha| < \frac{1}{H(x)^{2+\varepsilon}}.$$

The second is the so-called weak Mordell-Weil theorem, named this way because it is a key stepping stone to proving the aforementioned Mordell-Weil theorem.

**Theorem 1.3** (Weak Mordell-Weil)**.** *Retain the setting of Theorem 1.1. For any positive integer $m$, the quotient group $C(\mathbb{Q})/mC(\mathbb{Q})$ is finite.*

By combining these two results, we will be able to prove Theorem 1.1. In fact, we can do much better, by proving the following stronger result:

*Date*: July 21, 2016.

**Theorem 1.4.** *Retain the setting of Theorem 1.1, and suppose $C$ has infinitely many rational points. Label the rational points in $C'$ as $\{P_i\}_{i\in\mathbb{N}}$ in order of nondecreasing height of the $x$-coordinate. If we write each $x$-coordinate as a fraction in lowest terms*

$$x(P_i) = \frac{a_i}{b_i},$$

*then we have that*

$$\lim_{i\to\infty} \frac{\log|a_i|}{\log|b_i|} = 1.$$

Informally, the above result states that when looking at the $x$-coordinates of rational points (of sufficiently large height) on an elliptic curve, the numerators and denominators have about the same number of digits. It is immediate to see that this result implies Theorem 1.1, since if we suppose for the sake of a contradiction that there did exist infinitely many integral points in $C'$, then there would be an infinite subsequence $\{j_k\}_{k\in\mathbb{N}} \subset \mathbb{N}$ such that $|a_{j_k}| \to \infty$ while $|b_{j_k}| = 1$, which would contradict the statement of Theorem 1.4.

We prove Theorem 1.4 by first proving a version of Roth's Theorem for $C(\overline{\mathbb{Q}})$. Note that Roth's Theorem relates the Euclidean distance, which measures the *topological* size, and the height function, which measures the *arithmetic* size. To obtain an analogous relation for points on $C$, we will first define and prove several properties of a distance function (in the topology defined by the valuation $\infty$) and a height function on $C$. We do this in Sections 2 and 3, respectively. Then, in Section 4, we combine the results of the previous sections to prove our main theorem.

## 2. The Distance Function

We wish to define the notion of a distance function between two points $P, Q \in C(\mathbb{R})$. To this end, we define the following distance function for $t_Q \in \mathbb{R}(C)$ that has a zero at $Q$ of order $e \geq 1$:

$$d(P, t_Q) := \min\{|t_Q(P)|^{1/e}, 1\}.$$

This definition qualitatively makes sense as a function analogous to the Euclidean distance, since it is easy to see that $d(P, t_Q)$ is small precisely if $P$ is close to $Q$ in Euclidean distance. We will first show that in the limit as $P \to Q$ (i.e., limiting through any sequence of points $P \in C(\mathbb{R})$ such that $d(P, t_Q) \to 0$ for some choice of $t_Q$, and therefore for all choices), the quantity $\log d(P, t_Q)$ does not depend on the choice of $t_Q$, asymptotically speaking.

**Lemma 2.1.** *Let $t_Q, t'_Q \in \mathbb{R}(C)$ vanish at $Q \in C(\mathbb{R})$ to orders $e$ and $e'$, respectively. Then,*

$$\lim_{\substack{P\in C(\mathbb{R})\\ P\to Q}} \frac{\log d(P, t'_Q)}{\log d(P, t_Q)} = 1$$

*Proof.* Consider $\phi \in \mathbb{R}(C)$ defined as

$$\phi(P) = \frac{t'_Q(P)^e}{t_Q(P)^{e'}}, \tag{2.1}$$

Taking logarithms of the absolute values, we get

$$\log|\phi(P)| = e \log\left|t'_Q(P)\right| - e' \log|t_Q(P)|,$$

from which we have

$$\log\left|t'_Q(P)\right| = \frac{1}{e}\log|\phi(P)| + \frac{e'}{e}\log|t_Q(P)|\,. \tag{2.2}$$

For $P$ sufficiently close to $Q$, we have

$$\begin{aligned}\log d(P,t'_Q) = \log\left|t'_Q(P)\right|^{1/e'} &= \frac{1}{ee'}\log|\phi(P)| + \frac{1}{e}\log|t_Q(P)| \\ &= \frac{1}{ee'}\log|\phi(P)| + \log d(P,t_Q),\end{aligned}$$

from which one sees that

$$\lim_{\substack{P\in C(\mathbb{R})\\ P\to Q}} \frac{\log d(P,t'_Q)}{\log d(P,t_Q)} = 1 + \frac{1}{ee'}\cdot \lim_{\substack{P\in C(\mathbb{R})\\ P\to Q}} \frac{\log|\phi(P)|}{\log d(P,t_Q)}. \tag{2.3}$$

Since $\phi$ has neither a zero nor a pole at $Q$, it follows that $|\phi(P)|$ is bounded away from 0 and $\infty$ for $P$ close to $Q$. Meanwhile, as $P \to Q$, we have that $d(P,t_Q) \to 0$, and so $\log d(P,t_Q) \to -\infty$. Thus,

$$\lim_{\substack{P\in C(\mathbb{R})\\ P\to Q}} \frac{\log|\phi(P)|}{\log d(P,t_Q)} = 0, \tag{2.4}$$

which proves the lemma. □

Our purposes will only require that we deal with $\log d(P,t_Q)$ in asymptotic settings, so we can get away with using the notation $d(P,Q) := d(P,t_Q)$ for some choice of $t_Q$, without worrying about the precise dependence on $t_Q$.

The next lemma states that the logarithm of the distance between two points is asymtotically invariant under any finite unramified map. Later in our main proof, we will apply this lemma to the map $P \mapsto mP + R$ for some fixed integer $m$ and point $R \in C(\mathbb{Q})$.

**Lemma 2.2.** *Let $\varphi : C \to C$ be a finite unramified map defined over $\mathbb{Q}$. For any $Q \in C(\mathbb{R})$,*

$$\lim_{\substack{P\in C(\mathbb{R})\\ P\to Q}} \frac{\log d(\varphi(P),\varphi(Q))}{\log d(P,Q)} = 1.$$

*Proof.* Define $t_Q, t_{\varphi(Q)} \in \mathbb{R}(C)$ by

$$t_Q : R \mapsto \frac{x(R-Q)}{y(R-Q)} \quad\text{and}\quad t_{\varphi(Q)} : R \mapsto \frac{x(R-\varphi(Q))}{y(R-\varphi(Q))}. \tag{2.5}$$

Note that $t_Q$ and $t_{\varphi(Q)}$ vanish to order 1 at $Q$ and $\varphi(Q)$, respectively. Indeed, at the point at infinity $\mathcal{O}$, the rational function $x$ has a pole of order 2, while $y$ has a pole of order 3.

Since $\varphi$ is unramified, it has no branch points when viewed in the complex-analytic perspective, i.e., as a self-map on the Riemann surface $C$. Thus, there exists a (sufficiently small) open neighborhood $U$ of $Q$ such that $\varphi$ restricted to $U$ is injective, so that $U$ and $\varphi(U)$ are analytically isomorphic Riemann surfaces by the map $\varphi$. Since $t_Q$ and $t_{\varphi(Q)}$ each vanish to order 1 at $Q$ and $\varphi(Q)$ respectively, it follows that

$$\rho := \frac{t_{\varphi(Q)} \circ \varphi}{t_Q}$$

is a meromorphic function on $U$ with neither a zero nor a pole at $Q$. So, as $P \to Q$, the following holds when $P$ is sufficiently close to $Q$:

$$\frac{\log d(\varphi(P),\varphi(Q))}{\log d(P,Q)} = \frac{\log |t_{\varphi(Q)}(\varphi(P))|}{\log |t_Q(P)|} = \frac{\log |t_Q(P)\cdot \rho(P)|}{\log |t_Q(P)|} = 1 + \frac{\log |\rho(P)|}{\log |t_Q(P)|}.$$

We thus see that

$$\lim_{\substack{P\in C(\mathbb{R})\\ P\to Q}} \frac{\log d(\varphi(P),\varphi(Q))}{\log d(P,Q)} = 1 + \lim_{\substack{P\in C(\mathbb{R})\\ P\to Q}} \frac{\log |\rho(P)|}{\log |t_Q(P)|}. \tag{2.6}$$

$\rho$ has neither a zero or a pole at $Q$, so $|\rho|$ is bounded away from 0 and $\infty$ near $Q$. On the other hand, as $P \to Q$, we have that $|t_Q(P)| \to 0$, and so $\log |t_Q(P)| \to -\infty$. Thus,

$$\lim_{\substack{P\in C(\mathbb{R})\\ P\to Q}} \frac{\log |\rho(P)|}{\log |t_Q(P)|} = 0, \tag{2.7}$$

which proves the lemma. □

## 3. Height Bounds for Rational Points on $C$

We define the height of a point $P \in C(\mathbb{Q})$ as follows:

$$H_x(P) := \begin{cases} H(x(P)) & \text{if } P \neq \mathcal{O} \\ 1 & \text{if } P = \mathcal{O}. \end{cases}$$

In fact, any rational function $f$ over $\mathbb{Q}$ defines a morphism $C \to \mathbb{P}^1$ over $\mathbb{Q}$, and pulling back the usual height function on $\mathbb{P}^1(\overline{\mathbb{Q}})$ defines a corresponding height function $H_f(P) := H(f(P))$ on $C(\overline{\mathbb{Q}})$. In particular, we have taken $f = x$ in the above definition.

It is convenient to have a notion of height that works additively rather than multiplicatively, so we also define a logarithmic version of the above definition:

$$h_x(P) := \log H_x(P).$$

It is natural to ask how this notion of height behaves in the context of the group law. To this end, we introduce the following height estimates, which are used in the proof of Mordell-Weil and will also be necessary for our proof.

**Lemma 3.1.** (a) *For a fixed point $Q \in C(\mathbb{Q})$, there is a constant $\kappa_0$, depending only on $Q$ and $C$, such that*

$$h_x(P+Q) \le 2h_x(P) + \kappa_0 \qquad \text{for all } P \in C(\mathbb{Q})$$

(b) *There is a constant $\kappa$, depending only on $C$, such that*

$$h_x(2P) \ge 4h_x(P) - \kappa \qquad \text{for all } P \in C(\mathbb{Q})$$

*Proof.* See [2, Lemma 3.2] and [2, Lemma 3.3] for an elementary proof. See [1, VIII.6.4] for a proof that the result holds even when one replaces $h_x$ with $h_f$ for any $f \in \mathbb{Q}(C)$ that is even, i.e., $f \circ [-1] = f$, where $[-1] \in \mathrm{End}(C)$ is defined by $P \mapsto -P$. □

The next height bound we will need is the following reinterpretation of Roth's theorem.

**Proposition 3.2.** *Suppose $Q \in C(\overline{\mathbb{Q}})$ is an accumulation point of $C(\mathbb{Q})$ in the topology defined by the valuation $\infty$. Then,*

$$\liminf_{\substack{P \in C(\mathbb{Q}) \\ P \to Q}} \frac{\log d(P,Q)}{h_x(P)} \geq -2,$$

*Proof.* Since $Q$ is an accumulation point of $C(\mathbb{Q})$, we have $x(Q) \in \mathbb{P}^1(\mathbb{R})$. Let $f = 1/x$ if $x(Q) = \infty$ and $f = x$ otherwise; note that this definition works because $H_{1/x} = H_x$. Then, $f(Q) \in \mathbb{R}$, so $P \mapsto f(P) - f(Q)$ is a function in $\mathbb{R}(C)$ that vanishes at $Q$. Let $e \geq 1$ denote the order of vanishing. Then, we can write

$$d(P,Q) = \min\{|f(P) - f(Q)|^{1/e}, 1\}. \tag{3.1}$$

It follows that for an arbitrary $\tau \in \mathbb{R}$, we have

$$\begin{aligned}
\liminf_{\substack{P \in C(\mathbb{Q}) \\ P \to Q}} \frac{\log d(P,Q)}{h_x(P)} &= \frac{1}{e} \cdot \liminf_{\substack{P \in C(\mathbb{Q}) \\ P \to Q}} \frac{\log |f(P) - f(Q)|}{h_x(P)} \\
&= \frac{1}{e} \cdot \liminf_{\substack{P \in C(\mathbb{Q}) \\ P \to Q}} \frac{\log(H_x(P)^\tau |f(P) - f(Q)|) - \tau \cdot h_x(P)}{h_x(P)} \\
&= \frac{1}{e} \cdot \liminf_{\substack{P \in C(\mathbb{Q}) \\ P \to Q}} \left[ \frac{\log(H_x(P)^\tau |f(P) - f(Q)|)}{h_x(P)} - \tau \right].
\end{aligned}$$

Let $\tau = 2 + \varepsilon$ for an arbitrary $\varepsilon > 0$. Then, by Roth's theorem (Theorem 1.2), we have

$$H_x(P)^\tau |f(P) - f(Q)| \geq 1$$

for all but finitely many $P \in C(\mathbb{Q})$. Moreover, $h_x(P) > 0$ for all but finitely many $P \in C(\mathbb{Q})$, which overall implies that

$$\liminf_{\substack{P \in C(\mathbb{Q}) \\ P \to Q}} \frac{\log(H_x(P)^\tau |f(P) - f(Q)|)}{h_x(P)} \geq 0, \tag{3.2}$$

from which we have

$$\liminf_{\substack{P \in C(\mathbb{Q}) \\ P \to Q}} \frac{\log d(P,Q)}{h_x(P)} \geq -\frac{2+\varepsilon}{e} \geq -2 - \varepsilon. \tag{3.3}$$

Since $\varepsilon > 0$ was arbitrary, the lemma follows. □

## 4. The Main Proof

Using our lemmas from the previous section, we will prove the following result, from which we can prove Theorem 1.4 and thereby prove Siegel's theorem (Theorem 1.1).

**Theorem 4.1.** *Suppose $C$ has infinitely many rational points. Then, for $Q \in C(\overline{\mathbb{Q}})$,*

$$\lim_{\substack{P \in C(\mathbb{Q}) \\ h_x(P) \to \infty}} \frac{\log d(P,Q)}{h_x(P)} = 0.$$

*Proof.* Note that $d(P,Q) \leq 1$, meaning $\log d(P,Q) \leq 0$. Moreover, $h_x(P) > 0$ for all but finitely many $P \in C(\mathbb{Q})$, which overall implies that

$$\limsup_{\substack{P \in C(\mathbb{Q}) \\ h_x(P) \to \infty}} \frac{\log d(P,Q)}{h_x(P)} \leq 0. \tag{4.1}$$

It thus suffices to show that

$$L := \liminf_{\substack{P \in C(\mathbb{Q}) \\ h_x(P) \to \infty}} \frac{\log d(P,Q)}{h_x(P)}$$

is greater than or equal to 0. To this end, let $\{P_i\}_{i \in \mathbb{N}}$ be a sequence of distinct points in $C(\mathbb{Q})$ with $h_x(P_i) \to \infty$ such that $\log d(P,Q)/h_x(P)$ approaches the infimum, i.e.,

$$\lim_{i \to \infty} \frac{\log d(P_i,Q)}{h_x(P_i)} = L. \tag{4.2}$$

If the points $P_i$ are bounded away from $Q$ in distance, then $\log d(P_i,Q)$ is bounded away from $-\infty$ while $h_x(P_i) \to \infty$, so $\log d(P_i,Q)/h_x(P_i) \to 0$. So, we only need to consider the case where the points $P_i$ are not bounded away from $Q$ in distance. Then, by replacing $\{P_i\}_{i \in \mathbb{N}}$ with a subsequence that approaches $Q$ in the limit, we can assume that the distance $d(P_i,Q) \to 0$.

Let $n$ be an arbitrary positive integer, and let $m = 2^n$. Recall that $C(\mathbb{Q})/mC(\mathbb{Q})$ is finite by the weak Mordell-Weil theorem (Theorem 1.3). Thus, some coset of the quotient group, say $R + mC(\mathbb{Q})$ for some $R \in C(\mathbb{Q})$, contains infinitely many of the points $P_i$ that are approaching $Q$. Replacing $\{P_i\}_{i \in \mathbb{N}}$ with this subsequence, we can assume that the points $P_i$ are all contained in this coset $R + mC(\mathbb{Q})$. Then, we can write

$$P_i = mP_i' + R$$

for some points $\{P_i'\}_{i \in \mathbb{N}} \subset C(\mathbb{Q})$.

We now check that the following height estimate holds:

$$\begin{aligned} m^2 h_x(P_i') = 2^{2n} h_x(P_i') &\leq h_x(2^n P_i') + \left( \sum_{j=0}^{n-1} 2^{2j} \right) \kappa \\ &= h_x(P_i - R) + \left( \sum_{j=0}^{n-1} 2^{2j} \right) \kappa \\ &\leq 2h_x(P_i) + \kappa_0 + \left( \sum_{j=0}^{n-1} 2^{2j} \right) \kappa, \end{aligned}$$

where we have used Lemma 3.1(b) inductively $n$ times for the first inequality and used Lemma 3.1(a) for the second inequality. Summarizing, we get

$$\frac{m^2}{2} h_x(P_i') - \lambda(n) \leq h_x(P_i) \tag{4.3}$$

for some constant $\lambda(n)$ depending only on $C$ and $n$.

For a given $T \in C(\overline{\mathbb{Q}})$, there are precisely $m^2$ points $S \in C(\overline{\mathbb{Q}})$ that satisfy $mS = T$. We call these points $S$ the *$m$-th roots* of $T$. Since $mP_i' + R = P_i \to Q$, we have that $mP_i' \to Q - R$. Thus, the sequence $\{P_i'\}_{i \in \mathbb{N}}$ necessarily has an accumulation point (in the

$\infty$-adic topology) at some $m$-th root $Q'$ of $Q-R$. So, replacing $\{P_i'\}_{i\in\mathbb{N}}$ with a subsequence, we can assume that

$$P_i' \to Q' \quad \text{and} \quad Q = mQ' + R.$$

The map $P \mapsto mP+R$ is a finite unramified map, so by Lemma 2.2, it follows from $P_i' \to Q'$ that

$$\lim_{i\to\infty} \frac{\log d(P_i, Q)}{\log d(P_i', Q')} = 1.$$

Combining this with (4.3), we have

$$L = \lim_{i\to\infty} \frac{\log d(P_i, Q)}{h_x(P_i)} \geq \lim_{i\to\infty} \frac{\log d(P_i', Q')}{\frac{m^2}{2} h_x(P_i') - \lambda(n)}, \tag{4.4}$$

where the inequality is reversed because the logarithm of our distance function is always nonpositive. Here, we have from Lemma 3.2 that

$$\liminf_{i\to\infty} \frac{\log d(P_i', Q')}{h_x(P_i')} \geq -2.$$

So, overall we have

$$L \geq \liminf_{i\to\infty} \frac{\dfrac{2\log d(P_i', Q')}{h_x(P_i')}}{m^2 - \dfrac{2\lambda(n)}{h_x(P_i')}} \geq \liminf_{i\to\infty} \frac{-4}{m^2 - \dfrac{2\lambda(n)}{h_x(P_i')}} = -\frac{4}{m^2} = -\frac{4}{2^{2n}}, \tag{4.5}$$

where we have used the fact that $h_x(P_i') \to \infty$.

The above holds for any positive integer $n$, so taking $n \to \infty$ gives $L \geq 0$. □

*Proof of 4.1 ⇒ 1.4.* Label the rational points of $C'$ as $\{P_i\}_{i\in\mathbb{N}}$ in order of nondecreasing height of the $x$-coordinate, and write $x(P_i) = a_i/b_i$ in lowest terms. We first apply Theorem 4.1 to $Q = \mathcal{O}$. It is clear that the rational function $x$ has precisely two zeros (counting multiplicity) and no poles in the affine part of $C(\overline{\mathbb{Q}})$, so $x$ must have a pole of order 2 at $\mathcal{O}$. It follows that $1/x$ has a zero of order 2 at $\mathcal{O}$, which means that we can write

$$d(P, Q) = \min\left\{ \left( \frac{1}{|x(P)|} \right)^{1/2}, 1 \right\}, \tag{4.6}$$

so that

$$\log d(P_i, Q) = \frac{1}{2} \min\{\log|b_i| - \log|a_i|, 0\}.$$

Thus, by Theorem 4.1,

$$\lim_{i\to\infty} \frac{\frac{1}{2}\min\{\log|b_i| - \log|a_i|, 0\}}{\max\{\log|a_i|, \log|b_i|\}} = 0,$$

or equivalently,

$$\lim_{i\to\infty} \frac{\min\{\log|b_i| - \log|a_i|, 0\}}{\max\{\log|a_i|, \log|b_i|\}} = 0. \tag{4.7}$$

Now, we apply Theorem 4.1 again, this time taking $Q \in C(\overline{\mathbb{Q}})$ to be one of the two zeros (counting multiplicity) of $x$. Similarly as before, we can write

$$d(P, Q) = \min\{|x(P)|^{1/e}, 1\}, \tag{4.8}$$

where $e \in \{1, 2\}$ denotes the order of vanishing at $Q$. So, we have

$$\log d(P_i, Q) = \frac{1}{e} \min\{\log |a_i| - \log |b_i|, 0\}.$$

Just as before, we apply Theorem 4.1 to obtain

$$\lim_{i \to \infty} \frac{\min\{\log |a_i| - \log |b_i|, 0\}}{\max\{\log |a_i|, \log |b_i|\}} = 0. \tag{4.9}$$

We now partition our indexing sequence $\mathbb{N}$ into disjoint sets $\mathcal{I}_1$ and $\mathcal{I}_2$, where $\mathcal{I}_1$ is comprised of $i \in \mathbb{N}$ such that $|a_i| \geq |b_i|$, and $\mathcal{I}_2$ is comprised of $i \in \mathbb{N}$ such that $|a_i| < |b_i|$.

Suppose that $\mathcal{I}_1$ is infinite. Then, index $\mathcal{I}_1$ in increasing order to write it as a subsequence $\{j_k\}_{k \in \mathbb{N}}$. From (4.7), we have

$$\lim_{k \to \infty} \frac{\log |b_{j_k}| - \log |a_{j_k}|}{\log |a_{j_k}|} = 0. \tag{4.10}$$

or equivalently,

$$\lim_{k \to \infty} \frac{\log |b_{j_k}|}{\log |a_{j_k}|} = 1.$$

Taking the reciprocal, we get

$$\lim_{k \to \infty} \frac{\log |a_{j_k}|}{\log |b_{j_k}|} = 1.$$

Now, suppose that $\mathcal{I}_2$ is infinite (note that it is possible for $\mathcal{I}_1$ and $\mathcal{I}_2$ to both be infinite). As before, index $\mathcal{I}_2$ in increasing order to write it as a subsequence $\{\ell_k\}_{k \in \mathbb{N}}$. Using (4.9), we have

$$\lim_{k \to \infty} \frac{\log |a_{\ell_k}| - \log |b_{\ell_k}|}{\log |b_{\ell_k}|} = 0, \tag{4.11}$$

or equivalently,

$$\lim_{k \to \infty} \frac{\log |a_{\ell_k}|}{\log |b_{\ell_k}|} = 1,$$

which agrees with the result regarding $\mathcal{I}_1$.

By the above considerations, it overall follows that

$$\lim_{i \to \infty} \frac{\log |a_i|}{\log |b_i|} = 1.$$

□

As shown in Section 1, the above proof of Theorem 1.4 is sufficient to prove Siegel's theorem (Theorem 1.1) that $C'$ has finitely many integral points. However, for the sake of completeness, we also provide a direct proof of Theorem 1.1 below. The main idea of this proof is that if $C'$ were to have infinitely many integral points, then they would approach the point at infinity too quickly, contradicting Theorem 4.1.

*Proof of 4.1 ⇒ 1.1.* For the sake of a contradiction, suppose that $C'$ has infinitely many integral points. As before, label the rational points of $C'$ as $\{P_i\}_{i \in \mathbb{N}}$ in order of nondecreasing height of the $x$-coordinate, and write $x(P_i) = a_i/b_i$ in lowest terms. Let $\{P_{j_k}\}_{k \in \mathbb{N}} \subset \{P_i\}_{i \in \mathbb{N}}$

be the subsequence formed by the integral points. Then, $|a_{j_k}| \geq |b_{j_k}| = 1$ for all sufficiently large $k \in \mathbb{N}$. Setting $Q = \mathcal{O}$ as in (4.6), we have for sufficiently large $k$ that

$$\log d(P_{j_k}, Q) = \log \left( \min \left\{ \left( \frac{1}{|x(P_{j_k})|} \right)^{1/2}, 1 \right\} \right) = -\frac{1}{2} \log |a_{j_k}|. \tag{4.12}$$

But $h_x(P_{j_k}) = \log |a_{j_k}|$ for sufficiently large $k$, so it follows that $d(P_{j_k}, Q)/h_x(P_{j_k}) \to -1/2$ as $k \to \infty$, which contradicts Theorem 4.1. Therefore, $C'$ has finitely many integral points. □

## Acknowledgments

The author would like to thank Professor Xiaoheng (Jerry) Wang for numerous helpful discussions and valuable suggestions on the exposition.

## References

[1] Joseph H. Silverman, *The arithmetic of elliptic curves*, Second, Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094 (2010i:11005)
[2] Joseph H. Silverman and John T. Tate, *Rational points on elliptic curves*, Second, Undergraduate Texts in Mathematics, Springer, Cham, 2015. MR3363545
[3] Evan Warner, *Elliptic curves seminar: Siegel's theorem*, 2010.

Department of Mathematics, Princeton University, Princeton, NJ 08544
*E-mail address*: pspark@math.princeton.edu