New York Journal of Mathematics

New York J. Math. **12** (2006) 257–268.

Small rational points on elliptic curves over number fields

Clayton Petsche

Abstract. Let E/k be an elliptic curve over a number field. We obtain some quantitative refinements of results of Hindry–Silverman, giving an upper bound for the number of k-rational torsion points, and a lower bound for the canonical height of nontorsion k-rational points, in terms of expressions depending explicitly on the degree $d = [k : \mathbb{Q}]$ of k and the Szpiro ratio σ of E/k. The bounds exhibit only polynomial dependence on both d and σ.

Contents

1. Introduction 257
2. Elliptic curves over number fields 260
3. A few preliminary lemmas 261
4. A bound on the number of small points 264
References 267

1. Introduction

Let k be a number field of degree $d = [k : \mathbb{Q}]$, and let E/k be an elliptic curve. In [12], Merel used deep facts about the arithmetic of modular curves to prove that there is a universal bound $C(d)$ depending only on d such that $|E(k)_{\mathrm{tor}}| \leq C(d)$. Quantitative refinements of Merel's theorem due to Parent [13] and Oesterlé (cf. [7]) give bounds which depend exponentially on d, but it is still unknown whether one can give a bound $C(d)$ whose growth is polynomial in d. Such a result—or a proof that no such bound is possible—would be of value, both for its intrinsic interest and for its implications in cryptography; cf. [2], [8].

In this paper we give an explicit polynomial bound on $|E(k)_{\mathrm{tor}}|$ depending on d and the Szpiro ratio σ, a certain quantity associated to the elliptic curve E/k which we will now define. Recall that the conductor $\mathfrak{f}_{E/k}$ and the minimal discriminant

Received August 3, 2005; revised August 26, 2006.
Mathematics Subject Classification. 11G05, 11G07, 11G50.
Key words and phrases. Elliptic curves, heights, torsion points, Szpiro ratio, Lang's conjecture.

ISSN 1076-9803/06

$\Delta_{E/k}$ are certain integral ideals of $\mathcal{O}_k$ that are supported on the primes at which E/k has bad reduction. The Szpiro ratio is given by

$$\sigma = \frac{\log |\mathbb{N}_{k/\mathbb{Q}}(\Delta_{E/k})|}{\log |\mathbb{N}_{k/\mathbb{Q}}(\mathfrak{f}_{E/k})|} \tag{1}$$

when E/k has at least one place of bad reduction; by convention we put $\sigma = 1$ if E/k has everywhere good reduction.

Theorem 1. *Let k be a number field of degree $d = [k : \mathbb{Q}]$, and let E/k be an elliptic curve with Szpiro ratio σ. Then*

$$|E(k)_{\mathrm{tor}}| \leq c_1 d\sigma^2 \log(c_2 d\sigma^2), \tag{2}$$

where $c_1 = 134861$ and $c_2 = 104613$.

Strictly speaking (2) is not a *uniform* bound, in that the right-hand side depends on the elliptic curve E/k. However, the result is perhaps more interesting in view of the fact that one generally expects σ to be small. More precisely, let $\Sigma(k)$ denote the set (with multiplicities) of Szpiro ratios σ of all elliptic curves E/k. A well-known conjecture of Szpiro [17] asserts that $\Sigma(k)$ is bounded, and that 6 is its largest limit point. (As pointed out by Masser [10], 6 is in fact a limit point.) An analogue of Szpiro's conjecture is known to hold in the function field case, and in the number field case it can be shown to follow from the ABC conjecture.

Note that if Szpiro's conjecture is true, then Theorem 1 gives a uniform bound on $|E(k)_{\mathrm{tor}}|$ in terms of k only. The first result showing that Szpiro's conjecture implies such a uniform bound is due to Frey; the argument was written up by Flexor–Oesterlé [4]. Also in [4], the authors treated the special case of everywhere good reduction ($\sigma = 1$), giving a bound on $|E(k)_{\mathrm{tor}}|$ that is exponential in d. In [7] Hindry–Silverman improved this to a bound of $O(d \log d)$; thus our bound (2) recovers theirs (with slightly different constants) in this special case. In the general case, Hindry–Silverman [5] have given a bound on $|E(k)_{\mathrm{tor}}|$ that is exponential in both d and σ. Thus the main interest in our bound (2) is in its explicit nature, and in the fact that it exhibits only polynomial growth in both d and σ. It is also worth mentioning here another bound of Flexor–Oesterlé from the paper [4]: they show that if there exists a place of additive reduction then $|E(k)_{\mathrm{tor}}| \leq 48d$.

Finally, it should be pointed out that our inequality (2) does not imply the full theorem of Merel, even if we allow ourselves Szpiro's conjecture, as the resulting bound would depend on the number field k. To hope for more seems doubtful; for if we let Σ_d denote the union of the sets $\Sigma(k)$ over all number fields k of degree $d = [k : \mathbb{Q}]$, then we are presented with the question of whether $\sup \Sigma_d$ is finite, and if so, how it depends on d. A similar question relating to the ABC conjecture has been investigated by Masser [11].

A problem somewhat related to counting rational torsion points is that of giving a lower bound on the Néron–Tate canonical height $\hat{h}(P)$, for nontorsion rational points P, depending explicitly on the relevant data associated to the elliptic curve E/k. In particular, a conjecture of Lang asserts that if $P \in E(k)$ is not a torsion point, then

$$\hat{h}(P) \geq c \log |\mathbb{N}_{k/\mathbb{Q}}(\Delta_{E/k})|, \tag{3}$$

where $c = c(k) > 0$ is a constant depending only on k. We show that one can take for c a certain expression depending explicitly on d and σ.

Theorem 2. *Let k be a number field of degree $d = [k : \mathbb{Q}]$, and let E/k be an elliptic curve with minimal discriminant $\Delta_{E/k}$ and Szpiro ratio σ. Then*

$$\hat{h}(P) \geq c(d,\sigma) \log |\mathbb{N}_{k/\mathbb{Q}}(\Delta_{E/k})| \tag{4}$$

for all nontorsion points $P \in E(k)$, where

$$c(d,\sigma) = \frac{1}{10^{15} d^3 \sigma^6 \log^2(c_2 d \sigma^2)}, \tag{5}$$

and $c_2 = 104613$.

A consequence of Theorem 2 is that Szpiro's conjecture implies Lang's conjecture; this fact was originally proved by Hindry–Silverman [5], who showed that (3) holds with a value of c depending exponentially on d and σ. Thus again the main interest in (4) is in the fact that $c(d,\sigma)$ exhibits only polynomial decay in d and σ. Compare with the results of David [3], who uses methods from transcendence theory to obtain a similar bound.

Let us now briefly summarize our approach, in which we extend the methods of Hindry–Silverman [7] to include a treatment of the places of bad reduction. Denote by $\mathcal{M}_k$ the set of all places of k, and given $v \in \mathcal{M}_k$, let k_v be the completion of k at v. Let $\hat{h} : E(\bar{k}) \to [0, +\infty)$ denote the Néron–Tate canonical height, and recall that given a point $P \in E(k) \setminus \{O\}$, we have the local decomposition $\hat{h}(P) = \sum_{v \in \mathcal{M}_k} \frac{d_v}{d} \lambda_v(P)$, where $d_v = [k_v : \mathbb{Q}_v]$ is the local degree and $\lambda_v : E(k_v) \setminus \{O\} \to \mathbb{R}$ is the appropriately normalized Néron local height function (cf. [16], §VI.1). Given a set $Z = \{P_1, \ldots, P_N\} \subset E(k)$ of N distinct small rational points, we estimate the height-discriminant sum

$$\Lambda(Z) = \frac{1}{N^2} \sum_{1 \leq i,j \leq N} \hat{h}(P_i - P_j), \tag{6}$$

from above globally via the parallelogram law, and from below locally using the decomposition $\Lambda(Z) = \sum_{v \in \mathcal{M}_k} \frac{d_v}{d} \Lambda_v(Z)$, where

$$\Lambda_v(Z) = \frac{1}{N^2} \sum_{\substack{1 \leq i,j \leq N \\ i \neq j}} \lambda_v(P_i - P_j). \tag{7}$$

In order to obtain the necessary archimedean estimates we follow [7], using the pigeonhole principle to pass to a subset of Z of positive density, all of whose points are close to each other in $E(k_v)$ at a particular archimedean place v. At the nonarchimedean places we give an analytic lower bound on $\Lambda_v(Z)$ in terms of the valuation of the minimal discriminant (cf. Lemma 4 below). Although we will not specifically require this interpretation in the present paper, this inequality can be viewed as a quantitative form of a local equidistribution principle for small points, as developed in [1]. Finally, it is worth noting that we do not decompose the minimal discriminant into "small power" and "large power" parts as Hindry–Silverman do in [5]. Instead, we assemble the local information at the different places of bad reduction into global information by a simple application of Jensen's inequality.

Acknowledgements. The author would like to express his gratitude to Matt Baker for his many valuable suggestions, and to the anonymous referee, who offered several insightful comments on the content and the exposition of this paper.

2. Elliptic curves over number fields

In this section we fix some notation, and we review some of the relevant facts concerning elliptic curves over number fields.

Let $\mathcal{O}_k$ be the ring of integers of a number field k, and denote by $\mathcal{M}_k^\infty$ and $\mathcal{M}_k^0$ the set of all archimedean and nonarchimedean places of k respectively. For each place $v \in \mathcal{M}_k$ we will select the normalized absolute value $|\ |_v$ that, when restricted to $\mathbb{Q}$, coincides with one of the usual archimedean or p-adic absolute values. Given a place $v \in \mathcal{M}_k^0$ lying over the rational prime p, let $\mathcal{O}_v$ and $\mathcal{M}_v$ be the ring of integers and maximal ideal in k_v respectively. Let $\mathfrak{p}_v = \mathcal{O}_k \cap \mathcal{M}_v$ denote the prime ideal of $\mathcal{O}_k$ corresponding to the place v, and let $\pi_v \in \mathcal{M}_v$ be a uniformizer. Thus $|\mathbb{N}_{k/\mathbb{Q}}(\mathfrak{p}_v)| = |\mathcal{O}_v/\mathcal{M}_v| = p^{f_v}$ and $|\pi_v|_v = p^{-1/e_v}$, where f_v and e_v are the residual degree and ramification index, respectively. Recall that $d_v = [k_v : \mathbb{Q}_p] = e_v f_v$.

Let E/k be an elliptic curve, and let j_E denote its j-invariant. The conductor and minimal discriminant of E/k are the integral ideals

$$\mathfrak{f}_{E/k} = \prod_{v \in \mathcal{M}_k^0} \mathfrak{p}_v^{\eta_v}, \text{ and } \Delta_{E/k} = \prod_{v \in \mathcal{M}_k^0} \mathfrak{p}_v^{\delta_v} \tag{8}$$

of $\mathcal{O}_k$, respectively, where the exponents η_v and δ_v are given as follows. Fix a place $v \in \mathcal{M}_k^0$, and define $\delta_v = \mathrm{ord}_v(\Delta_v)$, where $\Delta_v \in \mathcal{O}_v$ denotes the discriminant of a minimal Weierstrass equation for E/k_v; thus $|\Delta_v|_v = |\pi_v|_v^{\delta_v}$. The exponent η_v of the conductor has a rather complicated Galois-theoretic definition (cf. [16], §IV.10); alternatively, it can be characterized by Ogg's formula

$$\delta_v = \eta_v + m_v - 1, \tag{9}$$

where m_v is the number of components on the special fiber of the minimal proper regular model of E/k_v (cf. [16], §IV.11). An immediate consequence of (9) is that $\eta_v \leq \delta_v$, from which we deduce the lower bound $\sigma \geq 1$ on the Szpiro ratio.

Let $E_0(k_v)$ denote the subgroup of $E(k_v)$ consisting of those points whose reduction (with respect to a minimal Weierstrass equation for E/k_v) is nonsingular, and let

$$c_v = |E(k_v)/E_0(k_v)| \tag{10}$$

be the cardinality of the quotient. It is well-known that the set $E_0(k_v)$, and thus also the number c_v, do not depend on the choice of the minimal Weierstrass equation used to define them.

Finally, we recall that the various data discussed above are governed by the reduction type of E/k_v. To be precise, if E/k_v has good reduction then $\delta_v = \eta_v = 0$ and $c_v = 1$; if E/k_v has split multiplicative reduction then $\eta_v = 1$ and $c_v = \delta_v$; and finally, in all other cases we have $c_v \leq 4$. For proofs of these assertions see [16], §IV.9.

Following Rumely (cf. [14] §2.4), it will be useful to decompose the nonarchimedean Néron local height function $\lambda_v : E(k_v) \setminus \{O\} \to \mathbb{R}$ into a sum

$$\lambda_v(P - Q) = i_v(P, Q) + j_v(P, Q), \tag{11}$$

where i_v is a nonnegative arithmetic intersection term, and j_v is bounded (cf. also [1]). These functions are most naturally described by first passing to a finite extension K_v of k_v over which E achieves either good or split multiplicative reduction (cf. [15], Prop. VII.5.4). Recall that the absolute value $|\ |_v$ extends uniquely to K_v, and that the Néron local height function is invariant under this finite extension (cf. [16], Thm. VI.1.1). We now consider the cases of integral and nonintegral j-invariant separately:

Case 1: $|j_E|_v \leq 1$. Then j_v is identically zero and $\lambda_v(P-Q) = i_v(P,Q)$.

Case 2: $|j_E|_v > 1$. We have maps

$$E(k_v) \hookrightarrow E(K_v) \xrightarrow{\sim} K_v^\times/q^{\mathbb{Z}} \to \mathbb{R}/\mathbb{Z}, \tag{12}$$

where $q \in K_v^\times$ with $|q|_v = |1/j_E|_v < 1$; here the first map is inclusion, the second map is the isomorphism afforded by Tate's uniformization theory [18], and the third map is given by $u \mapsto \log|u|_v/\log|q|_v$. Let r denote the composition of the three maps in (12). Then

$$j_v(P,Q) = \frac{1}{2}\mathbf{B}_2(r(P-Q))\log|j_E|_v,$$

where

$$\mathbf{B}_2(t) = (t-[t])^2 - \frac{1}{2}(t-[t]) + \frac{1}{6} = \frac{1}{2\pi^2}\sum_{m\in\mathbb{Z}\setminus\{0\}}\frac{1}{m^2}e^{2\pi imt}$$

is the periodic second Bernoulli polynomial. If $r(P) \neq r(Q)$ then $i_v(P,Q) = 0$. On the other hand if $r(P) = r(Q)$, then we can select representatives $u(P)$, $u(Q) \in K_v^\times/q^{\mathbb{Z}}$ for P and Q under the Tate isomorphism such that $|u(P)|_v = |u(Q)|_v$; in this case

$$i_v(P,Q) = -\log|1-u(P)/u(Q)|_v.$$

Finally, we note for future reference that $E_0(k_v) = \ker(r)$; in other words, a point $P \in E(k_v)$ has nonsingular reduction if and only if $r(P) = 0$.

3. A few preliminary lemmas

We begin with a purely group theoretical counting lemma.

Lemma 3. *Let G_0 be a subgroup of a group G with finite index $c = [G:G_0]$, and let Z be a finite subset of G with cardinality N. Then*

$$|\{(x,y) \in Z\times Z \mid xy^{-1} \in G_0\}| \geq \frac{N^2}{c}. \tag{13}$$

Proof. Denote by G/G_0 the set of right-cosets of G_0, and for each $C \in G/G_0$ let $N_C = |Z \cap C|$. Note that $xy^{-1} \in G_0$ if and only if both x and y lie in the same

right-coset. It follows that the number on the left-hand side of (13) is

$$\begin{aligned}\sum_{\substack{(x,y)\in Z\times Z\\ xy^{-1}\in G_0}} 1 &= \sum_{C\in G/G_0} N_C^2\\ &= \sum_{C\in G/G_0}\left\{\left(N_C-\frac{N}{c}\right)^2+\frac{2N_CN}{c}-\frac{N^2}{c^2}\right\}\\ &\geq \frac{2N}{c}\sum_{C\in G/G_0} N_C-\frac{N^2}{c^2}\sum_{C\in G/G_0}1\\ &= \frac{N^2}{c}.\end{aligned}$$

□

The following lower bound on the nonarchimedean local sum (7) is a variant of [6], Proposition 1.2. To be precise, our bound (14) is given in terms of the valuation of the minimal discriminant, rather than the valuation of the j-invariant as in [6], a distinction that is only relevant at the places of additive reduction.

Lemma 4. *Let E/k be an elliptic curve, let v be a nonarchimedean place of k, and let $\Delta_v \in \mathcal{O}_v$ be the discriminant of a minimal Weierstrass equation for E/k_v. If $Z=\{P_1,\dots,P_N\}\subset E(k_v)$ is a set of N distinct k_v-rational points, then*

$$\Lambda_v(Z) \geq \left(\frac{1}{c_v^2}-\frac{1}{N}\right)\frac{1}{12}\log|1/\Delta_v|_v. \tag{14}$$

Proof. First, note that

$$\log^+|j_E|_v \leq \log|1/\Delta_v|_v, \tag{15}$$

with equality if and only if E/k_v has good or multiplicative reduction (cf. [15], Prop. VII.5.1). Also, the Néron local height function satisfies the lower bound $\lambda_v(P)\geq \frac{1}{12}\log|1/\Delta_v|_v$ for points $P\in E_0(k_v)\setminus\{O\}$ (cf. [16], Thm. VI.4.1). It follows from this and the decomposition (11) that

$$i_v(P,Q)\geq \frac{1}{12}(\log|1/\Delta_v|_v-\log^+|j_E|_v)\geq 0$$

for $P-Q\in E_0(k_v)\setminus\{O\}$. As i_v is nonnegative, it follows that

$$\sum_{\substack{1\leq i,j\leq N\\ i\neq j}} i_v(P_i,P_j)\geq (M-N)\frac{1}{12}(\log|1/\Delta_v|_v-\log^+|j_E|_v), \tag{16}$$

where M is the number of ordered pairs $(P_i,P_j)\in Z\times Z$ with $P_i-P_j\in E_0(k_v)$. By Lemma 3 we have the lower bound $M\geq N^2/c_v$, which in combination with (16) yeilds

$$\frac{1}{N^2}\sum_{\substack{1\leq i,j\leq N\\ i\neq j}} i_v(P_i,P_j)\geq \left(\frac{1}{c_v}-\frac{1}{N}\right)\frac{1}{12}(\log|1/\Delta_v|_v-\log^+|j_E|_v). \tag{17}$$

We will now show that

$$\frac{1}{N^2}\sum_{\substack{1\leq i,j\leq N\\ i\neq j}} j_v(P_i,P_j)\geq \left(\frac{1}{c_v^2}-\frac{1}{N}\right)\frac{1}{12}\log^+|j_E|_v. \tag{18}$$

For if $|j_E|_v \leq 1$ then both sides of (18) are zero. On the other hand, assume that $|j_E|_v > 1$. Since the map r is trivial on the identity component $E_0(k_v)$, it is well-defined on the quotient $E(k_v)/E_0(k_v)$, which has cardinality c_v. Therefore $r(E(k_v)) \subseteq \langle 1/c_v \rangle \subset \mathbb{R}/\mathbb{Z}$, and we conclude that $e^{2\pi i m r(P_j)} = 1$ for all $P_j \in Z \subset E(k_v)$, whenever $c_v \mid m$. It follows that

$$\begin{aligned}
(19) \qquad \sum_{\substack{1\leq i,j\leq N\\ i\neq j}} j_v(P_i,P_j) &= \sum_{1\leq i,j\leq N} j_v(P_i,P_j) - \frac{N}{12}\log|j_E|_v \\
&= \frac{\log|j_E|_v}{4\pi^2} \sum_{m\in\mathbb{Z}\setminus\{0\}} \frac{1}{m^2} \left| \sum_{1\leq j\leq N} e^{2\pi i m r(P_j)} \right|^2 - \frac{N}{12}\log|j_E|_v \\
&\geq \frac{N^2\log|j_E|_v}{4\pi^2} \sum_{m\in c_v\mathbb{Z}\setminus\{0\}} \frac{1}{m^2} - \frac{N}{12}\log|j_E|_v \\
&= \frac{N^2\log|j_E|_v}{12c_v^2} - \frac{N}{12}\log|j_E|_v,
\end{aligned}$$

which implies (18).

Finally, by the decomposition (11) and the lower bounds (17) and (18), and using the inequality (15), we have

$$\begin{aligned}
\Lambda_v(Z) &= \frac{1}{N^2} \sum_{\substack{1\leq i,j\leq N\\ i\neq j}} (i_v(P_i,P_j) + j_v(P_i,P_j)) \\
&\geq \left(\frac{1}{c_v^2} - \frac{1}{c_v}\right)\frac{1}{12}\log^+|j_E|_v + \left(\frac{1}{c_v} - \frac{1}{N}\right)\frac{1}{12}\log|1/\Delta_v|_v \\
&\geq \left(\frac{1}{c_v^2} - \frac{1}{c_v}\right)\frac{1}{12}\log|1/\Delta_v|_v + \left(\frac{1}{c_v} - \frac{1}{N}\right)\frac{1}{12}\log|1/\Delta_v|_v \\
&= \left(\frac{1}{c_v^2} - \frac{1}{N}\right)\frac{1}{12}\log|1/\Delta_v|_v,
\end{aligned}$$

which completes the proof. □

The following archimedean analogue of Lemma 4 is a quantitative refinement of a result due to Elkies (cf. [9], §VI.); for a detailed proof see [1], Appendix A.

Lemma 5. *Let E/k be an elliptic curve with j-invariant j_E, and let $Z \subset E(k)$ be a set of N distinct k-rational points. If v is an archimedean place of k, then*

$$(20) \qquad \Lambda_v(Z) \geq -\frac{\log N}{2N} - \frac{1}{12N}\log^+|j_E|_v - \frac{16}{5N}.$$

In order to obtain the necessary nonarchimedean estimates we will require the following lemma due to Hindry–Silverman (cf. Lemma 1 of [7] and Proposition 2.3 of [5]). Let $j : \mathbb{H} = \{\tau \in \mathbb{C} \mid \Im(\tau) > 0\} \to \mathbb{C}$ denote the modular j-function, and let $L = \mathbb{Z} + \tau\mathbb{Z}$ be a normalized lattice with $\tau \in \mathbb{H}$; thus $j(\tau)$ is the j-invariant of the elliptic curve $\mathbb{C}/L$. Let $\lambda : (\mathbb{C}/L) \setminus \{0\} \to \mathbb{R}$ denote the Néron function, as given in [16], §VI.3.

Lemma 6 (Hindry–Silverman)**.** *If $z = r_1 + r_2\tau \in \mathbb{C} \setminus \{0\}$, where $r_1, r_2 \in \mathbb{R}$ and $\max\{|r_1|, |r_2|\} \leq 1/24$, then*

$$\lambda(z) \geq \frac{1}{288} \max\{1, \log|j(\tau)|\}.$$

Finally, we will require the following inequality, the proof of which is elementary and given in [1], §6.

Lemma 7. *Let $N \geq 1$ satisfy the bound $N \leq A \log N + B$ for constants $A > 0, B \geq 0$. Then $N \leq (\frac{e}{e-1})(A \log A + B)$.*

4. A bound on the number of small points

In this section we will prove the results stated in the introduction, which are both consequences of the following bound on the number of small rational points.

Proposition 8. *Let k be a number field of degree $d = [k : \mathbb{Q}]$, and let E/k be an elliptic curve with Szpiro ratio σ. Then*

$$\left| \left\{ P \in E(k) \;\middle|\; \hat{h}(P) \leq \frac{\log|\mathbb{N}_{k/\mathbb{Q}}(\Delta_{E/k})|}{2^{13}3d\sigma^2} \right\} \right| \leq c_1 d\sigma^2 \log(c_2 d\sigma^2), \tag{21}$$

where $c_1 = 134861$ and $c_2 = 104613$.

Proof. To ease notation we will henceforth suppress the subscripts on the notations $\mathbb{N}_{k/\mathbb{Q}}$, $\Delta_{E/k}$, and $\mathfrak{f}_{E/k}$. Let S denote the set on the left-hand side of (21), and let N denote the largest integer satisfying $|S| \geq 24^2(N-1)+1$; thus $|S| \leq 24^2 N$. We will show that

$$N \leq (148 d\sigma^2) \log N + 971 d\sigma^2. \tag{22}$$

Assuming for now that this holds, it follows by Lemma 7 that

$$\begin{aligned} N &\leq \Big(\frac{e}{e-1}\Big)(148 d\sigma^2 \log(148 d\sigma^2) + 971 d\sigma^2) \\ &= \Big(\frac{e}{e-1}\Big) 148 d\sigma^2 \log(148 e^{971/148} d\sigma^2). \end{aligned}$$

In view of this and the fact that $|S| \leq 24^2 N$, the bound (21) follows immediately.

It now remains only to prove (22). Let v_0 be an archimedean place of k, chosen so that $|j_E|_{v_0} = \max_{v|\infty}(|j_E|_v)$. We then have a corresponding embedding $\sigma : E(k) \hookrightarrow \mathbb{C}/L$, where $L = \mathbb{Z} + \tau\mathbb{Z}$ is a normalized lattice, and $|j(\tau)| = |j_E|_{v_0}$. If $\lambda : (\mathbb{C}/L) \setminus \{0\} \to \mathbb{R}$ denotes the Néron function on the complex torus, then $\lambda_{v_0} = \lambda \circ \sigma$.

Divide the torus $\mathbb{C}/L$ into the 24^2 parallelograms

$$P_{m_1,m_2} = \Big\{ z = r_1 + r_2\tau \;\Big|\; \frac{m_1 - 1}{24} \leq r_1 \leq \frac{m_1}{24} \quad \text{and} \quad \frac{m_2 - 1}{24} \leq r_2 \leq \frac{m_2}{24} \Big\},$$

where $1 \leq m_1, m_2 \leq 24$. By the pigeonhole principle there exists a set $Z = \{P_1, \ldots, P_N\} \subseteq S$ of N distinct points such that $\sigma(Z)$ is contained in one of the 24^2 parallelograms. In particular, it follows that the difference $\sigma(P_i) - \sigma(P_j)$ between any two points in $\sigma(Z)$ must lie in one of the four parallelograms P_{m_1,m_2}, $m_1, m_2 \in \{1, 24\}$. Therefore, by Lemma 6 we have $\lambda_{v_0}(P_i - P_j) \geq \frac{1}{288} \max\{1, \log|j_E|_{v_0}\}$ for all such pairs.

It follows from the above considerations that

$$\Lambda_{v_0}(Z) \geq \frac{(N-1)}{288N} \max\{1, \log|j_E|_{v_0}\}; \tag{23}$$

and by Lemma 5 and the maximality of $|j_E|_{v_0}$, we have

$$\begin{aligned} \sum_{\substack{v|\infty \\ v\neq v_0}} \frac{d_v}{d}\Lambda_v(Z) &\geq -\sum_{\substack{v|\infty \\ v\neq v_0}} \frac{d_v}{d}\left\{\frac{\log N}{2N} + \frac{1}{12N}\log^+|j_E|_v + \frac{16}{5N}\right\} \\ &\geq -\frac{\log N}{2N} - \frac{1}{12N}\log^+|j_E|_{v_0} - \frac{16}{5N}. \end{aligned} \tag{24}$$

If $N \leq 24d$, then (22) plainly holds; so we may henceforth assume that $N \geq 24d+1$. Then combining the estimates (23) and (24) we have

$$\begin{aligned} \sum_{v\in\mathcal{M}_k^\infty} \frac{d_v}{d}\Lambda_v(Z) &\geq -\frac{\log N}{2N} - \frac{16}{5N} \\ &\quad + \frac{1}{N}\left\{\frac{(N-1)d_{v_0}}{288d} - \frac{1}{12}\right\}\max\{1, \log|j_E|_{v_0}\} \\ &\geq -\frac{\log N}{2N} - \frac{16}{5N} + \frac{1}{N}\left\{\frac{N-1}{288d} - \frac{1}{12}\right\} \\ &= -\frac{\log N}{2N} - \frac{197}{60N} + \frac{(N-1)}{288dN}. \end{aligned} \tag{25}$$

We now turn to the lower bounds on $\Lambda_v(Z)$ at the nonarchimedean places; in particular we will show that

$$\sum_{v\in\mathcal{M}_k^0} \frac{d_v}{d}\Lambda_v(Z) \geq \frac{1}{12d}\Big(\frac{1}{16\sigma^2} - \frac{1}{N}\Big)\log|\mathbb{N}(\Delta)|. \tag{26}$$

First, if E/k has everywhere good reduction then (26) plainly holds, since in that case $\log|\mathbb{N}(\Delta)| = 0$ and the left-hand side is nonnegative by Lemma 4. So we may assume that the set $\mathcal{M}_k^{\mathrm{br}} = \{v \in \mathcal{M}_k^0 \mid E/k_v \text{ has bad reduction}\}$ is nonempty.

At this point we will require Jensen's inequality: if $\{w_v\}$ is a finite set of positive weights with $\sum_v w_v = W$, if $x_v > 0$ for all v, and if $\phi(x)$ is a convex function for $x > 0$, then

$$\sum_v w_v\phi(x_v) \geq W\phi\left(\frac{1}{W}\sum_v w_v x_v\right). \tag{27}$$

Applying this with $\phi(x) = 1/x$, with $\{w_v = \eta_v \log|\mathbb{N}(\mathfrak{p}_v)| \mid v \in \mathcal{M}_k^{\mathrm{br}}\}$ as our weights (thus $W = \log|\mathbb{N}(\mathfrak{f})|$), and with $x_v = \eta_v c_v^2/\delta_v$, we have

$$\sum_{v\in\mathcal{M}_k^{\mathrm{br}}} \frac{\delta_v}{c_v^2}\log|\mathbb{N}(\mathfrak{p}_v)| \geq W\left(\frac{1}{W}\sum_{v\in\mathcal{M}_k^{\mathrm{br}}} \frac{\eta_v^2 c_v^2}{\delta_v}\log|\mathbb{N}(\mathfrak{p}_v)|\right)^{-1} \geq W^2\left(\sum_{v\in\mathcal{M}_k^{\mathrm{br}}} 16\delta_v\log|\mathbb{N}(\mathfrak{p}_v)|\right)^{-1} = \frac{(\log\mathbb{N}(\mathfrak{f}))^2}{16\log|\mathbb{N}(\Delta)|}. \tag{28}$$

The first inequality in (28) is Jensen's, and the second follows from the inequality

$$\frac{\eta_v^2 c_v^2}{\delta_v} \leq 16\delta_v \tag{29}$$

for $v \in \mathcal{M}_k^{\mathrm{br}}$. (To see this, recall that if E/k_v has split multiplicative reduction then $\delta_v = c_v$ and $\eta_v = 1$, and (29) holds; while otherwise $\eta_v \leq \delta_v$ and $c_v \leq 4$, and (29) follows in this case as well.)

Finally, combining (14) and (28) and noting that $d_v \log|1/\Delta_v|_v = \delta_v \log|\mathbb{N}(\mathfrak{p}_v)|$, we have

$$\begin{aligned}\sum_{v\in\mathcal{M}_k^0}\frac{d_v}{d}\Lambda_v(Z) &\geq \sum_{v\in\mathcal{M}_k^{\mathrm{br}}}\frac{d_v}{d}\left(\frac{1}{c_v^2}-\frac{1}{N}\right)\frac{1}{12}\log|1/\Delta_v|_v\\ &= \frac{1}{12d}\sum_{v\in\mathcal{M}_k^{\mathrm{br}}}\left(\frac{1}{c_v^2}-\frac{1}{N}\right)\delta_v\log|\mathbb{N}(\mathfrak{p}_v)|\\ &\geq \frac{1}{12d}\left(\frac{(\log|\mathbb{N}(\mathfrak{f})|)^2}{16\log|\mathbb{N}(\Delta)|}-\frac{1}{N}\log|\mathbb{N}(\Delta)|\right)\\ &= \frac{1}{12d}\left(\frac{1}{16\sigma^2}-\frac{1}{N}\right)\log|\mathbb{N}(\Delta)|,\end{aligned}$$

which is (26).

We are now ready to combine these local estimates. By the parallelogram law we have the global upper bound

$$\Lambda(Z) \leq \frac{4}{N}\sum_{j=1}^{N}\hat{h}(P_j) \leq \frac{\log|\mathbb{N}(\Delta)|}{2^{11}3d\sigma^2} \tag{30}$$

on the sum defined in (6), by the upper bound on $\hat{h}(P)$ for $P \in S$. Therefore by (25) and (26) we have

$$\begin{aligned}\frac{\log|\mathbb{N}(\Delta)|}{2^{11}3d\sigma^2} &\geq \Lambda(Z)\\ &= \sum_{v\in\mathcal{M}_k}\frac{d_v}{d}\Lambda_v(Z)\\ &\geq -\frac{\log N}{2N}-\frac{197}{60N}+\frac{(N-1)}{288dN}+\frac{1}{12d}\left(\frac{1}{16\sigma^2}-\frac{1}{N}\right)\log|\mathbb{N}(\Delta)|.\end{aligned} \tag{31}$$

If E/k has everywhere good reduction then, then $\sigma = 1$ and $\log|\mathbb{N}(\Delta)| = 0$, and thus (31) becomes

$$0 \geq -\frac{\log N}{2N} - \frac{197}{60N} + \frac{(N-1)}{288dN}. \tag{32}$$

It follows that $N \leq 144d\log N + 945.6d + 1 \leq 144d\log N + 946.6d$, and (22) holds in this case. On the other hand, suppose that $\mathcal{M}_k^{\mathrm{br}}$ is nonempty. If $N \leq 2^9\sigma^2$, then (22) holds, so we may assume that $N > 2^9\sigma^2$. The bound (31) implies that

$$\begin{aligned} 0 &\geq -\frac{\log N}{2N} - \frac{197}{60N} + \frac{1}{12d}\left(\frac{1}{16\sigma^2} - \frac{1}{N}\right)\log|\mathbb{N}(\Delta)| - \frac{\log|\mathbb{N}(\Delta)|}{2^{11}3d\sigma^2} \\ &\geq -\frac{\log N}{2N} - \frac{197}{60N} + \frac{1}{12d}\left(\frac{1}{2^4\sigma^2} - \frac{1}{2^9\sigma^2} - \frac{1}{2^9\sigma^2}\right)\log|\mathbb{N}(\Delta)| \\ &= -\frac{\log N}{2N} - \frac{197}{60N} + \frac{5}{2^{10}d\sigma^2}\log|\mathbb{N}(\Delta)| \\ &\geq -\frac{\log N}{2N} - \frac{197}{60N} + \frac{5\log 2}{2^{10}d\sigma^2}, \end{aligned} \tag{33}$$

since $\log|\mathbb{N}(\Delta)| \geq \log 2$. We deduce that

$$\begin{aligned} N &\leq \left\{\frac{2^9 d\sigma^2}{5\log 2}\right\}\log N + \frac{197\cdot 2^{10}d\sigma^2}{60\cdot 5\log 2} \\ &< (148d\sigma^2)\log N + 971d\sigma^2. \end{aligned} \tag{34}$$

Thus (22) holds in this case as well, and the proof of Proposition 8 is complete. □

Proof of Theorems 1 and 2. Again, let S denote the set on the left-hand side of (21). Theorem 1 follows trivially from Proposition 8, since $E(k)_{\mathrm{tor}} \subseteq S$. To see that Theorem 2 follows, let $P \in E(k)$ be a nontorsion point, and let M be the largest integer such that $\hat{h}((M-1)P) \leq (\log|\mathbb{N}_{k/\mathbb{Q}}(\Delta_{E/k})|)/2^{13}3d\sigma^2$. Then the first M multiples $O, P, 2P, \ldots, (M-1)P$ of P are contained in the set S, and therefore $M \leq c_1 d\sigma^2\log(c_2 d\sigma^2)$ by Proposition 8. On the other hand, by the maximality of M we have $M^2\hat{h}(P) = \hat{h}(MP) > (\log|\mathbb{N}_{k/\mathbb{Q}}(\Delta_{E/k})|)/2^{13}3d\sigma^2$. Therefore

$$\begin{aligned} \hat{h}(P) &> M^{-2}\frac{\log|\mathbb{N}_{k/\mathbb{Q}}(\Delta_{E/k})|}{2^{13}3d\sigma^2} \\ &\geq c(d,\sigma)\log|\mathbb{N}_{k/\mathbb{Q}}(\Delta_{E/k})|, \end{aligned}$$

where $c(d,\sigma)$ is given by (5). □

References

[1] Baker, Matthew; Petsche, Clayton. Global discrepancy and small points on elliptic curves. *Int. Math. Res. Not.* **61** (2005), 3791–3834. MR2205235.

[2] Cheng, Qi; Uchiyama, Shigenori. Nonuniform polynomial time algorithm to solve decisional Diffie–Hellman problem in finite fields under conjecture. *Topics in cryptology—CT-RSA 2002*, 290–299, Lecture Notes in Comput. Sci., 2271, *Springer, Berlin*, 2002. MR2048688, Zbl 1048.94009.

[3] David, Sinnou. Points de petite hauteur sur les courbes elliptiques. *J. Number Theory.* **64** (1997), no. 1, 104–129. MR1450488 (98k:11067), Zbl 0873.11035.

[4] Flexor, Marguerite; Oesterlé, Joseph. Sur les points de torsion des courbes elliptiques. Séminaire sur les Pinceaux de Courbes Elliptiques (Paris, 1988). *Astérisque* No. 183, (1990), 25–36. MR1065153 (91g:11057), Zbl 0737.14004.

[5] Hindry, Marc; Silverman, Joseph H. The canonical height and integral points on elliptic curves. *Invent. Math.* **93** (1988), no. 2, 419–450. MR0948108 (89k:11044), Zbl 0657.14018.

[6] Hindry, Marc; Silverman, Joseph H. On Lehmer's conjecture for elliptic curves. *Séminaire de Théorie des Nombres, Paris* 1988–1989, 103–116, Progr. Math., 91, *Birkhäuser Boston, Boston, MA*, 1990. MR1104702 (92e:11062), Zbl 0741.14013.

[7] Hindry, Marc; Silverman, Joseph H. Sur le nombre de points de torsion rationnels sur une courbe elliptique. *C. R. Acad. Sci. Paris Sér. I Math.* **329** (1999), no. 2, 97–100. MR1710502 (2000g:11047), Zbl 0993.11028.

[8] Koblitz, Neal; Menezes, Alfred J. Obstacles to the torsion-subgroup attack on the decision Diffie–Hellman problem. *Math. Comp.* **73** (2004), no. 248, 2027–2041 (electronic). MR2059749 (2006i:94055), Zbl 1064.94013.

[9] Lang, Serge. Introduction to Arakelov Theory. With an appendix by Paul Vojta: Diophantine inequalities and Arakelov theory. *Springer-Verlag, New York*, 1988. MR0969124 (89m:11059), Zbl 0667.14001.

[10] Masser, David W. Note on a conjecture of Szpiro. Séminaire sur les Pinceaux de Courbes Elliptiques (Paris, 1988). *Astérisque* No. 183, (1990), 19–23. MR1065152 (91g:11058), Zbl 0742.14027.

[11] Masser, David W. On *abc* and discriminants. *Proc. Amer. Math. Soc.* **130** (2002), no. 11, 3141–3150 (electronic). MR1912990 (2003d:11050), Zbl 1030.11011.

[12] Merel, Loic. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.* **124** (1996), no. 1-3, 437–449. MR1369424 (96i:11057), Zbl 0936.11037.

[13] Parent, Pierre. Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. *J. Reine Angew. Math.* **506** (1999), 85–116. MR1665681 (99k:11080), Zbl 0919.11040.

[14] Rumely, Robert. Capacity theory on algebraic curves. Lecture Notes in Mathematics, 1378. *Springer-Verlag, Berlin*, 1989. MR1009368 (91b:14018), Zbl 0679.14012.

[15] Silverman, Joseph H. *The arithmetic of elliptic curves*. Graduate Texts in Mathematics, 106. *Springer-Verlag, New York*, 1986. MR0817210 (87g:11070), Zbl 0585.14026.

[16] Silverman, Joseph H. Advanced topics in the arithmetic of elliptic curves. Graduate Texts in Mathematics, 151. *Springer-Verlag, New York*, 1994. MR1312368 (96b:11074), Zbl 0911.14015.

[17] Szpiro, Lucien. Discriminant et conducteur des courbes elliptiques. Séminaire sur les Pinceaux de Courbes Elliptiques (Paris, 1988). *Astérisque* No. 183, (1990), 7–18. MR1065151 (91g:11059), Zbl 0742.14026.

[18] Tate, John. A review of non-Archimedean elliptic functions. *Elliptic curves, modular forms, and Fermat's last theorem* (Hong Kong, 1993), 162–184, Ser. Number Theory, I, *Int. Press, Cambridge, MA*, 1995. MR1363501 (97d:11096), Zbl 1071.11508.

DEPARTMENT OF MATHEMATICS, THE UNIVERSITY OF GEORGIA, ATHENS, GA 30602-7403
clayton@math.uga.edu

This paper is available via http://nyjm.albany.edu/j/2006/12-16.html.