Pacific Journal of Mathematics

S-INTEGER POINTS ON ELLIPTIC CURVES

ROBERT HOWARD GROSS AND JOSEPH SILVERMAN

Volume 167 No. 2 February 1995

PACIFIC JOURNAL OF MATHEMATICS
Vol. 167, No. 2, 1995

S-INTEGER POINTS ON ELLIPTIC CURVES

ROBERT GROSS AND JOSEPH SILVERMAN

We give a quantitative bound for the number of S-integral points on an elliptic curve over a number field K in terms of the number of primes dividing the denominator of the j-invariant, the degree $[K:\mathbb{Q}]$, and the number of primes in S.

Let K be a number field of degree d and M_K the set of places of K. Let E/K be an elliptic curve with quasi-minimal Weierstrass equation

$$E \quad : \quad y^2 = x^3 + Ax + B.$$

If $\Delta = 4A^3 + 27B^2$ is the discriminant of this equation, recall that quasi-minimal means that $|N_{K/\mathbb{Q}}(\Delta)|$ is minimized subject to the condition that $A, B \in \mathrm{O}_K$. Let $S \subset M_K$ be a finite set of s places containing all the archimedean ones, and denote the ring of S-integers by O_S. Let j be the j-invariant of E.

In [**11**], Silverman proved that if j is integral, then

$$\#\{P \in E(K) : x(P) \in \mathrm{O}_S\}$$

can be bounded in terms of the field K, $\#S$, and the rank of $E(K)$. More generally, Silverman proved that if the j-invariant is non-integral for at most δ places of K, then that set can be bounded in terms of the previously mentioned constants and δ. This is a special case of a conjecture of Lang asserting the existence of such a bound which is independent of δ. However, Silverman did not explicitly compute the constants involved.

In this paper, using more explicit methods, we compute the dependence of the bounds on the various constants. In particular, as a consequence of Proposition 11, we have the following

THEOREM 0.1. *For elliptic curves E/K of sufficiently large height, the number of S-integral points is at most* $2{\cdot}10^{11} d\delta(j)^{3d}(32{\cdot}10^9)^{r\delta(j)+s}$.

For elliptic curves E defined over $\mathbb{Q}$ of sufficiently large height, the number of S-integral points is at most $32 \cdot 10^{11}(32 \cdot 10^9)^{r\delta(j)+s}$.

Our method is to first bound the number of points in a set $\Gamma_S(\epsilon)$, defined in terms of local height functions, and then to relate the number of elements in that set to the set we are interested in counting.

This paper falls into three parts. Propositions 1–5 summarize the necessary facts about height functions. Propositions 6–8 are various counting results. Proposition 9 counts the size of $\Gamma_S(\epsilon)$, Proposition 10 is a technical result, and the final Proposition combines the previous results to count the number of S-integral points.

We begin with some notation. Let $d_v = [K_v : \mathbb{Q}_v]$. For a point $P \in E(K)$, the *canonical height of P* is defined by

$$\hat{h}_K(P) = \frac{1}{2} \lim_{n\to\infty} \frac{h_K(x(2^n P))}{4^n},$$

where $h_K(k) = \log H_K(k)$ and

$$H_K(k) = \prod_{v\in M_K} \max(|k|_v, 1).$$

The *absolute canonical height* is defined by $\hat{h}(P) = \hat{h}_K(P)/d$.

PROPOSITION 1. *The canonical height satisfies*

(1) $\hat{h}(P) = 0$ *if and only if P is a torsion point.*

(2) $\hat{h}$ *is a positive definite quadratic form on $E(\overline{K}) \otimes \mathbb{R}$.*

Proof. These facts are well-known. See, for example, [**10**], chapter 8. □

PROPOSITION 2. *Let $v \in M_K$. There exists a unique function λ (also denoted λ_v or $\lambda_{v,K}$), $\lambda : E(K_v) \setminus \{0\} \to \mathbb{R}$ which satisfies:*

(1) λ *is continuous.*

(2)
$$\lim_{P\to 0} \left(\lambda(P) + \frac{1}{2} v(x(P))\right) = \frac{1}{12} v(\Delta).$$

(3) *Let $P, Q \in E(K_v)$ with $P, Q, P \pm Q \neq 0$. Then*

$$\lambda(P+Q) + \lambda(P-Q) = 2\lambda(P) + 2\lambda(Q) + \frac{1}{6} v(F(P,Q))$$

where

$$F(P,Q) = \frac{(x(P) - x(Q))^6}{\Delta}.$$

The function λ further satisfies

(4) *Let L/K be a finite extension, $w \in M_L$ a place over v, $P \in E(K_v) \setminus \{0\}$. Then*

$$\lambda_{v,K}(P) = \lambda_{w,L}(P).$$

(5) *For any $\sigma \in \mathrm{Aut}(\overline{K}_v/\mathbb{Q})$,*

$$\lambda_{v,K}(P) = \lambda_{v^\sigma,K^\sigma}(P^\sigma).$$

Similarly, for any $\alpha \in \mathrm{Aut}_{K_v}(E)$,

$$\lambda(P) = \lambda(\alpha P).$$

(6) *Let $m \in \mathbb{Z}$, $P \in E(K_v)$, $mP \neq 0$. Then*

$$\lambda(mP) = m^2\lambda(P) + \frac{1}{12}v(f_m(P)),$$

where

$$f_m(P) = m^{12} \prod_{T \in E[m], T \neq 0} \frac{(x(P) - x(T))^6}{\Delta}.$$

(7)

$$\sum_{T \in E[m], T \neq 0} \lambda(T) = v(m).$$

(8) *Let $P \in E(K_v)$ with $mP \neq 0$. Then*

$$\sum_{T \in E[m]} \lambda(P+T) = \lambda(mP).$$

(9) *For any $P \in E(K) \setminus \{0\}$,*

$$\hat{h}_K(P) = \sum_{v \in M_K} d_v \lambda_v(P).$$

Proof. For existence, uniqueness, (1)–(5), and (9), see [4], chapters 1, 3, and 4. To prove (6) for $m = 2$, let $Q \to P$ in (3) and use (2)

and the addition formula. Then (6) can be proven by induction on m using (3) and the classical formula

$$F(mP,P)=\frac{f_{m+1}(P)f_{m-1}(P)}{f_m(P)^2}.$$

(See [**13**].)

The distribution relations (7) and (8) do not seem to be in the literature, though they appear in an unpublished letter of Tate to Serre (as does (6)), so we briefly sketch a proof. Using (3), (6), and the definition of f_m and F, we have

$$\begin{aligned}\sum_{T\in E[m]}&\lambda(P+T)-\lambda(mP)\\ &=\sum_{T\in E[m],T\neq 0}\left(\lambda(P+T)-\lambda(P)-\frac{1}{12}v(F(P,T))\right)-v(m)\\ &=\sum_{T\in E[m],T\neq 0}\lambda(T)-v(m).\end{aligned}$$

Therefore, this quantity $c(m)$ does not depend on P, and both (7) and (8) follow if we can show that $c(m)=0$.

We begin by showing that $c(2)=0$. In (3), let P and Q be distinct non-zero two-torsion points. If we add the six choices for (P,Q), we obtain

$$\sum_{T\in E[2],T\neq 0}\lambda(T)+\frac{1}{24}\sum_{\substack{P,Q\in E[2]\\ P,Q,P-Q\neq 0}}v(F(P,Q))=0.$$

Now $c(2)=0$, because

$$\Delta=2^4\prod_{\substack{P,Q\in E[2]\\ P,Q,P-Q\neq 0}}(x(P)-x(Q)).$$

Next, let $m,n\in\mathbb{Z}$ with $(m,n)=1$. Then $E[mn]=E[m]\oplus E[n]$, so

$$\begin{aligned}\lambda(mnP)+c(mn)&=\sum_{S\in E[m]}\sum_{T\in E[n]}\lambda(P+S+T)\\ &=\lambda(mnP)+c(m)+m^2c(n).\end{aligned}$$

Hence, by symmetry

$$(m^2-1)c(n) = (n^2-1)c(m) \text{ if } (m,n) = 1.$$

Now, if m is odd, take $n = 2$ and use $c(2) = 0$ to get $c(m) = 0$. Then for any m, take $n \geq 3$ odd and prime to m to get $c(m) = 0$. □

The preceding proposition gives the formal properties of the local height function λ. The following proposition gives inequalities for λ and $\hat{h}$ whose proof depends on various explicit formulæ for λ, which can be found in [**4**], among other places.

PROPOSITION 3. *For $v \in M_K$, let*

$$\alpha(v) = \begin{cases} 1 & \text{if } v \text{ is archimedean,} \\ 0 & \text{otherwise.} \end{cases}$$

Then $\lambda = \lambda_v$ has the following properties, where the constants are absolute.

(1) *Let $P \in E(K_v) \setminus \{0\}$. Then*

$$\lambda_v(P) \geq \frac{1}{24}\min(0, v(j)) - 3\alpha(v).$$

Hence, for $P \in E(K)$ and any set $S \subset M_K$,

$$\hat{h}_K(P) \geq \sum_{v \in S} d_v \lambda_v(P) - \frac{1}{24} h_K(j) - 3d.$$

(2) *Let $P, Q \in E(K_v)$ with $P, Q, P+Q \neq 0$. Then*

$$\lambda_v(P+Q) \geq \min(\lambda_v(P), \lambda_v(Q)) + \frac{1}{8}\min(0, v(j)) - 6\alpha(v).$$

(3) *Let $P \in E(K)$ be a point of infinite order. Then*

$$\hat{h}(P) > (24 \cdot 144 \cdot 97200^2)^{-\delta(j)} \max\left(h(j), \frac{1}{d}\log\left|N_{K/\mathbb{Q}}\Delta_{E/K}\right|, 1\right),$$

where $\Delta_{E/K}$ is the minimal discriminant of E/K, and

$$\delta(j) = \#M_K^\infty + \#\{v \in M_K^0 : v(j) < 0\}$$

is essentially the number of primes in the denominator of j.

(4) *Assume that* v *has been extended in some fashion to* $\overline{K}$. *Let* $P \in E(K)\setminus\{0\}$. *Then there is a* $Q \in E(\overline{K})$ *with* $mQ = P$ *satisfying*

$$\lambda_v(Q) \geq \lambda_v(P) + \frac{m^2}{8}\min(0, v(j)) - v(m) - 6m^2\alpha(v).$$

(5) *Let* $P, Q \in E(K_v)$ *with* $P, Q, P \pm Q \neq 0$. *Then*

$$\begin{aligned} 2\lambda(P) + 2\lambda(Q) + \frac{1}{6}\max(0, -v(j)) + 12\alpha(v) & \\ \geq \frac{1}{6}\max(0, -v(F(P,Q))) & \\ \geq 2\lambda(P) - 2\lambda(Q) + \frac{1}{3}\min(0, v(j)) - 18\alpha(v). & \end{aligned}$$

Hence, for $P, Q \in E(K) \setminus \{0\}$,

$$\begin{aligned} 2\hat{h}(P) + 2\hat{h}(Q) + \frac{1}{6}h(j) + 12d \geq h\left(\frac{x(P) - x(Q)}{\Delta^{1/6}}\right) & \\ \geq 2\hat{h}(P) - 2\hat{h}(Q) - \frac{1}{3}h(j) - 18d. & \end{aligned}$$

(6) *Assume that the Weierstrass equation for* E *with discriminant* Δ *has coefficients in* O_K. *Let* $P \in E(K) \setminus \{0\}$. *Then*

$$\begin{aligned} \left|\lambda_v(P) - \frac{1}{2}\max(0, v(x(P)))\right| & \\ \leq \frac{1}{6}\max(0, -v(j)) + \frac{1}{12}|v(\Delta)| + 1.07\alpha(v) & \end{aligned}$$

and

$$\left|\hat{h}(P) - \frac{1}{2}h(x(P))\right| \leq \frac{1}{6}h(j) + \frac{1}{6}h(\Delta) + 1.07.$$

Proof. Assume first that v is archimedean. We begin with (1) and (2) in this case.

Choose an isomorphism $E(\overline{K}_v) \simeq \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$, with the point P corresponding to $u = u_1 + u_2\tau$. We may take τ in the usual fundamental domain, so that $\mathrm{Im}\tau \geq \sqrt{3}/2$. Since we may replace P by $-P$ (because $\lambda(P) = \lambda(-P)$), we may further suppose that

$0 \le u_1 \le 1$ and $0 \le u_2 \le 1/2$. If we write $q = q_\tau = e^{2\pi i\tau}$ and $q_u = e^{2\pi iu}$, then $|q| \le e^{-\pi\sqrt{3}}$.

We have

$$\lambda(P) = \lambda(u) = \frac{1}{2}B_2(u_2)v(q) + v(g_0(q_u)),$$

where

$$B_2(t) = t^2 - t + \frac{1}{6}, \qquad 0 \le t \le 1,$$

(and B_2 is extended to $\mathbb{R}$ by periodicity) and

$$g_0(t) = (t-1)\prod_{n=1}^{\infty}(1-q^nt)(1-q^nt^{-1}).$$

We have

$$-0.0655 \le \lambda(z) + \frac{1}{2}B_2(u_2)\log|q_\tau| + \log|1-q_u| \le 0.0711$$

from [**12**] and

$$-\log|q_\tau| \ge \min(v(j),0) - 2.304$$

from [**3**].

We also know that $B_2(u_2) \ge B_2(1/2) = -\frac{1}{12}$. Finally,

$$v(1-q_u) \ge -\log\left(\frac{\sqrt{3}}{2} + \frac{3}{2}\right) - \log\pi \ge -2.01.$$

Therefore,

$$\lambda(P) \ge \frac{1}{24}\min(v(j),0) - 3.$$

This proves (1).

To prove (2), let Q correspond to $z = z_1 + z_2\tau$, with $0 \le z_1, z_2 \le 1$. By symmetry, we may assume that $0 \le u_2 \le \min(z_2, 1-z_2)$. (If this is not true, then switch P and Q, and then if necessary use $-P$ and $-Q$ instead.) Then, using the above formula for λ, we have

$$\begin{aligned}\lambda(P+Q) &- \min(\lambda(P),\lambda(Q)) \\ &\ge \frac{1}{2}\left(B_2(u_2+z_2) - \max(B_2(u_2),B_2(z_2))v(q_\tau)\right) \\ &\quad + v(1-q_{u+z}) - \min(v(1-q_u),v(1-q_z)) - 0.4.\end{aligned}$$

We now proceed further. First, we observe that

$$\min_{s,t\in\mathbb{R}}(B_2(s+t)-\max(B_2(s),B_2(t)))=-\frac{1}{4}.$$

We also have

$$|1-q_{u+z}|\le|1-q_z|+|q_z||1-q_u|\le 2\max(|1-q_z|,|1-q_u|),$$

because $|q_z|\le 1$. Finally, we know that $v(q_\tau)\ge\min(v(j),0)-2.304$. Put all of these together, and we have

$$\begin{aligned}\frac{1}{2}\Big(B_2(u_2+z_2)-\max(B_2(u_2),B_2(z_2))v(q_\tau)\Big)&\\ +v(1-q_{u+z})-\min(v(1-q_u),v(1-q_z))-0.133&\\ \ge\frac{1}{8}\min(0,v(j))-6.&\end{aligned}$$

Next, suppose that v is non-archimedean. In proving (1) and (2), we may extend the ground field, so we may suppose that E has either good or split multiplicative reduction. Let

$$E(K_v)\supset E_0(K_v)\supset E_1(K_v)\supset\dots$$

be the usual filtration of $E(K_v)$ (see [**10**]). For $P\in E(K_v)$, let $i(P)$ be the largest integer i so that $P\in E_i(K_v)$. (If $P\notin E_0(K_v)$, set $i(P)=0$.) Then from [**4**], theorems III.4.3 and III.5.1, we have

$$\lambda(P)=\frac{1}{2}B_2(\beta(P))\max(0,-v(j))+i(P)v(\pi)$$

where π is a uniformiser at v, and

$$\beta: E(K_v)\to E(K_v)/E_0(K_v)\to\mathbb{Q}/\mathbb{Z}$$

is a certain homomorphism. Since $B_2(\beta)\ge -1/12$, this gives (1).

To prove (2), suppose first that either P or Q is in $E_0(K_v)$ (suppose P, for simplicity's sake). Then $\beta(P+Q)=\beta(Q)$, and $i(P+Q)\ge i(Q)$, so $\lambda(P+Q)\ge\lambda(Q)$.

On the other hand, if $P,Q\notin E_0(K_v)$, then

$$\begin{aligned}\lambda(P+Q)-\min(\lambda(P),\lambda(Q))&\\ \ge\frac{1}{2}\Big(B_2(\beta(P)+\beta(Q))&\\ -\min\{B_2(\beta(P)),B_2(\beta(Q))\}\Big)\max(0,-v(j))&\\ \ge\frac{1}{24}\min(0,v(j))&\end{aligned}$$

which is actually a stronger inequality than that stated in the proposition.

(3) can be proved by combining formulas from [**3**] and [**7**]. The proof of lemma 2.2(a) of [**3**] shows that $-\log|q| \geq \log|j(\tau)| - 2.304$, and also that $-\log|q| \geq \pi\sqrt{3} \geq 5.44$; therefore, $-\log|q| \geq \max(\log|j(\tau), 7.744) - 2.304$. Then Proposition 2.3 (with $\epsilon = 1/2$) says that if

$$\max(|\alpha|, |\beta|) \leq 1/44,$$

then

$$\lambda_v(z) \geq 1/24 \max(\log|j(\tau)|, 7.744).$$

Turning to [**7**], this says that in Lemma 2 of [**7**], if we take

$$c = \frac{1}{24}\max(\log|j(\tau)|, 7.744),$$

then the $\delta(c)$ in Lemma 2 of [**7**] equals $1/44$. The constant M in Lemma 3 of [**7**] then becomes $4 \cdot 45^2 = 8100$. The proof of the Theorem in [**7**] with $C = \frac{1}{24}\max(\log|j(\tau)|, 7.744)$ rather than $C = 1$, and with $R = \delta(j)$, says that

$$\hat{h}(nP) > \frac{1}{24}\left(\frac{1}{d}\log|N_{K/\mathbb{Q}}\Delta_{E/K}| + \max(\log|j(\tau)|, 7.744)\right)$$

and so (remembering the factor of $1/144$ mentioned at the beginning of the proof), we have

$$\hat{h}(P) \geq \frac{1}{24 \cdot 144} 97200^{-2\delta(j)} \max\left(\frac{1}{d}\log|N_{K/\mathbb{Q}}\Delta_{E/K}|, h(j), 7.744\right).$$

To prove (4), we take $Q \in E(\overline{K})$ satisfying $mQ = P$ so that $\lambda(Q)$ is maximized. Then for any $T \in E[m] \setminus \{0\}$, we have

$$\begin{aligned}\lambda(Q+T) &= \min(\lambda(Q), \lambda(Q+T)) \\ &\leq \lambda(T) - \frac{1}{8}\min(0, v(j)) + 6\alpha(v)\end{aligned}$$

from (2). Hence, from proposition 2, (8) and (7), we have

$$\begin{aligned}\lambda(P) &= \lambda(Q) + \sum_{T \in E[m], T \neq 0} \lambda(Q+T) \\ &\leq \lambda(Q) - \frac{m^2}{8}\min(0, v(j)) - 6m^2\alpha(v) - v(m).\end{aligned}$$

To show (5), begin by recalling that

$$-\frac{1}{6}v(F(P,Q)) = 2\lambda(P) + 2\lambda(Q) - \lambda(P+Q) - \lambda(P-Q)$$
$$\leq 2\lambda(P) + 2\lambda(Q) + \frac{1}{12}\max(0, -v(j)) - 6\alpha(v).$$

We also can use (1) to show that

$$2\lambda(P) + 2\lambda(Q) + \frac{1}{6}\max(0, -v(j)) + 12\alpha(v) \geq 0,$$

and therefore

$$\frac{1}{6}\max(0, -v(F(P,Q)))$$
$$\leq 2\lambda(P) + 2\lambda(Q) + \frac{1}{6}\max(0, -v(j)) + 12\alpha(v).$$

The lower bound estimate is only non-trivial if it is positive, and so we may suppose that

$$\lambda(P) \geq \lambda(Q) - \frac{1}{6}\min(0, v(j)) + 12\alpha(v).$$

We also have from (2) that

$$\lambda(Q) \geq \min(\lambda(P \pm Q), \lambda(P)) + \frac{1}{8}\min(0, v(j)) - 6\alpha(v).$$

If we combine those two, we may conclude that

$$\lambda(P \pm Q) \leq \lambda(Q) - \frac{1}{8}\min(0, v(j)) + 6\alpha(v).$$

Then

$$-\frac{1}{6}v(F(P,Q)) = 2\lambda(P) + 2\lambda(Q) - \lambda(P+Q) - \lambda(P-Q)$$
$$\geq 2\lambda(P) + 2\lambda(Q) - 2\lambda(Q) + \frac{1}{4}\min(0, v(j)) - 12\alpha(v)$$
$$\geq 2\lambda(P) + 2\lambda(Q) + \left(\frac{2}{24} + \frac{1}{4}\right)\min(0, v(j)) - 18\alpha(v)$$
$$= 2\lambda(P) + 2\lambda(Q) + \frac{1}{3}\min(0, v(j)) - 18\alpha(v).$$

As for (6), [**12**] contains the proofs of considerably stronger statements. □

Note that if $x \in K$, then x is S-integral if and only if

$$\sum_{v \in S} d_v \max(0, -v(x)) = h_K(x).$$

We actually prove a stronger result than simply bounding the number of S-integral points on E. We give a bound depending on ϵ for the number of points P on an elliptic curve whose x-coordinate $x(P)$ satisfies

$$\sum_{v \in S} d_v \max(0, -v(x(P))) \geq \epsilon h_K(x(P)).$$

Intuitively, such a point P is v-adically close to 0 for some $v \in S$.

A more intrinsic measure of the v-adic distance to 0 is given by the local height function $\lambda_v(P)$, so we start by bounding the number of elements in the set

$$\Gamma_S(\epsilon) = \left\{ P \in E(K) : \sum_{v \in S} d_v \lambda_v(P) \geq \epsilon \hat{h}_K(P) \right\}.$$

This bound will be independent of the choice of an equation for E. Then we give an estimate for the discriminant of a quasi-minimal Weierstrass equation, and use this to prove our main result.

Set r to be the rank of E. Recall that the equation $y^2 = x^3 + Ax + B$ with discriminant $\Delta = -16(4A^3 + 27B^2)$ is *quasi-minimal* if $h_K(\Delta)$ is minimized subject to $A, B \in \mathrm{O}_K$.

Let $\xi : S \to \mathbb{R}$ be a function satisfying $\xi_v \geq 0$ and $\sum_{v \in S} \xi_v = 1$. Let

$$\Gamma_S(\epsilon, \xi) = \Big\{ P \in E(K) : P \neq 0 \text{ and}$$

$$\lambda_v(P) + \frac{1}{24} \max(0, -v(j)) + 3\alpha(v) \geq \frac{\epsilon \xi_v}{d_v} \hat{h}_K(P) \text{ for all } v \in S \Big\}.$$

Because of proposition 3(1), we know that the left-hand side of this inequality is always non-negative.

We have yet another notation before we can state our next theorem. For any integer $m > 1$, let

$$\hat{h}^{(m)}(P) = \min_{Q \in E(K)} \hat{h}(P + mQ).$$

We need to recall a quantitative version of

ROTH'S THEOREM. *Let $F(T) \in K[T]$ with degree n. Let $\alpha_1, \ldots, \alpha_n$ be the roots of $F(T)$. There are at most $4^s c_1$ elements $x \in K$ satisfying both*

$$\prod_{v \in S} \min_{1 \le i \le n} (\|x - \alpha_i\|_v, 1) \le H_K(x)^{-2.5}$$

$$h(x) \ge c_2 \max(h(\alpha_1), h(\alpha_2), \ldots, h(\alpha_n), 1),$$

where $N = [2304 \log n] + 1$, $c_1 = N - 1 + 8.5(N-1)\log(5nN(2N)!)$, and $c_2 = 28(2N)!$.

Proof. See [**2**]. □

PROPOSITION 4. *Let $1 > \epsilon > 0$. Let $m = [8/\sqrt{\epsilon}]$. Compute the constants c_1 and c_2 from Roth's Theorem with $n = 18m^2$. There are at most $2c_1 (16/\sqrt{\epsilon})^{2s+r}$ points $P \in \Gamma_S(\epsilon, \xi)$ satisfying*

$$\hat{h}(P) \ge \frac{51m^2 dc_2}{\epsilon} (\hat{h}^{(m)}(P) + h(j) + 1).$$

Proof. Choose a Weierstrass equation for E/K with coordinates x and y and discriminant Δ, and fix a 2-torsion point $T \in E[2]$. Note that the field $K(\Delta^{1/6}, T)$ has degree at most 18 over K. For $P, Q \in E(\overline{K}) \setminus \{0\}$, define

$$\phi(P, Q) = \frac{x(P) - x(Q)}{\Delta^{1/6}}.$$

We also assume that valuations in K have been extended to $\overline{K}$ in some fashion.

Let m be as in the statment of the proposition, and write $\Gamma = \Gamma_S(\epsilon, \xi)$. Split Γ up into (at most) m^{r+2} subsets according to cosets in $E(K)/mE(K)$. We may then look at those $P \in \Gamma$ which can be written as $P = mP' + R$ for a fixed R. Taking R of minimal height in its coset, we may assume that $\hat{h}^{(m)}(P) = \hat{h}(R)$. By proposition 3 (4), for each $v \in S$ we may choose an $R'_v \in E(\overline{K})$ so that $P = m(P' + R'_v)$ (and hence $mR'_v = R$) and

$$\lambda_v(P' + R'_v) \ge \lambda_v(P) + \frac{m^2}{8} \min(0, v(j)) - v(m) - 6m^2 \alpha(v).$$

Note that for fixed R, there are only m^2 choices for R'_v, so the numbers in the set $\{\phi(R'_v, T) : v \in S\}$ all satisfy a single equation over K of degree at most $18m^2$.

Now multiply the above inequality by d_v, add over $v \in S$, and use that $P \in \Gamma$. We get

$$(1) \quad \sum_{v \in S} d_v \lambda_v(P' + R'_v) \geq \epsilon \hat{h}_K(P) - \left(\frac{1}{24} + \frac{m^2}{8}\right) h_K(j) - 3d - 6dv(m) - 6m^2 d.$$

We next eliminate some trivial cases. If $P' = 0$, then $P = R$. If $P' = R'_v$ for some $v \in S$, then $P = 2R$. If $P' = -R'_v$ for some $v \in S$, then $P = 0$, which is not allowed. Hence for the given R, after discarding two possible points P, we may assume that $P' \neq 0$ and $P' \neq \pm R'_v$ for all $v \in S$.

Now suppose that $v \in S$. If $R'_v \neq 0$, then from proposition 2(2) and proposition 3(3), we have

$$\lambda_v(P' + R'_v) \leq 2\lambda_v(P') + 2\lambda_v(R'_v) + v(\phi(P', R'_v)) - \frac{1}{24}\min(0, v(j)) + 3\alpha(v),$$

while if $R'_v = 0$, then proposition 3(1) gives

$$\lambda_v(P' + R'_v) \leq 2\lambda_v(P') - \frac{1}{24}\min(0, v(j)) + 3\alpha(v).$$

Multiply by d_v, and add these inequalities over $v \in S$, and again use proposition 3(1) to conclude

$$\sum_{v \in S} d_v \lambda_v(P' + R'_v) \leq 2\hat{h}_K(P') + 2 \sum_{mR' = R} \hat{h}_K(R') + \sum_{v \in S'} d_v v(\phi(P', R'_v)) + \left(2m^2 + \frac{3}{24}\right) h_K(j) + 9d + 3m^2 d,$$

where the first sum on the right-hand side of the inequality is over all R' satisfying $mR' = R$ and S' is the set of $v \in S$ with $R'_v \neq 0$.

Hence, since $\hat{h}(R) = m^2\hat{h}(R')$, we have

$$\begin{aligned}(2)\qquad \sum_{v\in S} d_v\lambda_v(P' + R'_v) \leq & 2\hat{h}_K(P') + 2\hat{h}_K(R) \\ & + \sum_{v\in S'} d_v v(\phi(P', R'_v)) \\ & + \left(2m^2 + \frac{3}{24}\right) h_K(j) + 9d + 3m^2.\end{aligned}$$

We now can apply Roth's Theorem to study how well the numbers $\phi(R'_v, T) \in \overline{K}$ with $R'_v \neq 0$ can be approximated by the numbers $\phi(P', T) \in K(\Delta^{1/6}, T)$.

We know that with at most $4^s c_1$ exceptions (where c_1 is taken from the statement of Roth's Theorem), either

$$\sum_{v\in S'} d_v \max(v(\phi(P', R'_v)), 0) < 2.5h_K(\phi(P', T))$$

or

$$h(\phi(P', T)) < c_2 \max_{v\in S'}(h(\phi(R'_v, T)), 1),$$

where c_2 is again taken from the statement of the theorem.

If we apply Proposition 3(5) to the first inequality, and note that $\hat{h}(T) = 0$, we have

$$(3)\qquad \sum_{v\in S'} d_v v(\phi(P', R'_v)) < 5\hat{h}_K(P') + \frac{1}{2}h_K(j) + 30d,$$

while the same proposition applied to the second inequality gives

$$2\hat{h}(P') - \frac{1}{3}h(j) - 18d < c_2\left(2\hat{h}(R') + \frac{1}{6}h(j) + 12d + 1\right).$$

We may use the facts that $\hat{h}(R) = m^2\hat{h}(R'_v)$ and $c_2 \geq 2$ to simplify this inequality to

$$(4)\qquad \hat{h}(P') < \frac{c_2}{2}\left(\frac{\hat{h}(R)}{m^2} + \frac{1}{2}h(j) + 30d + 1\right).$$

Now $\hat{h}$ is positive semi-definite, and $P = mP' + R$, so we have

$$2m^2\hat{h}(P') + 2\hat{h}(R) \geq \hat{h}(P) \geq \frac{m^2}{2}\hat{h}(P') - \hat{h}(R).$$

If we combine this with (1), (2), (3), and (4), we get either

$$\begin{aligned}
\epsilon\hat{h}_K(P) &\le 7\hat{h}_K(P') + 2\hat{h}_K(R) + 4m^2h_K(j) + 51dm^2 \\
&\le \frac{14}{m^2}\hat{h}(P) + 3\hat{h}_K(R) + 4m^2h_K(j) + 51dm^2 \\
\left(\epsilon - \frac{14}{m^2}\right) &\le 3\hat{h}_K(R) + 4m^2h_K(j) + 51dm^2 \\
\hat{h}_K(P) &\le \frac{4}{3\epsilon}\left(3\hat{h}_K(R) + 4m^2h_K(j) + 51dm^2\right) \\
&\le \frac{81m^2}{\epsilon}(\hat{h}_K(R) + h_K(j) + d)
\end{aligned}$$

(using $\epsilon - 14/m^2 > 3\epsilon/4$), or

$$\begin{aligned}
\hat{h}(P) &\le 2m^2\hat{h}(P') + 2\hat{h}(R) \\
&\le c_2m^2\left(\frac{\hat{h}(R)}{m^2} + \frac{1}{2}h(j) + 30d + 1\right) + 2\hat{h}(R) \\
&\le (c_2+2)\hat{h}(R) + \frac{c_2m^2}{2}h(j) + 31dc_2m^2 \\
&\le 31dc_2m^2(\hat{h}(R) + h(j) + 1)
\end{aligned}$$

with at most 4^sc_1 exceptions.

We also note that $\phi(P', T)$ determines P' up to ± 1.

Note that the number of exceptions must be multiplied by m^{r+2} to account for the initial choice of a coset in $E(K)/mE(K)$. □

Next, we show that the elements of $\Gamma_S(\epsilon, \xi)$ satisfy a type of orthogonality relation with respect to the canonical height.

PROPOSITION 5. *Let $P, Q \in \Gamma_S(\epsilon, \xi)$ with $P \neq Q$. Then*

$$\hat{h}(P - Q) \ge \epsilon \min(\hat{h}(P), \hat{h}(Q)) - \frac{5}{24}h(j) - 9.$$

Proof.

$$\begin{aligned}
\hat{h}_K(P - Q) &\ge \sum_{v\in S} d_v\lambda_v(P - Q) - \frac{1}{24}h_K(j) - 3d \\
&\ge \sum_{v\in S} d_v \min(\lambda_v(P), \lambda_v(Q)) - \frac{1}{6}h_K(j) - 9d \\
&\ge \sum_{v\in S} \xi_v\epsilon \min(\hat{h}_K(P), \hat{h}_K(Q)) - \frac{5}{24}h_K(j) - 9d
\end{aligned}$$

which is the desired result since $\sum \xi_v = 1$. □

We also need a bound on the torsion subgroup of $E(K)$. For $K = \mathbb{Q}$, there is Mazur's deep result [**5**] that $|E(K)_{\text{tors}}| \leq 16$, and there are recent generalizations of this work by Kamienny and Mazur to certain extensions of $\mathbb{Q}$. However, lacking the general result needed, we content ourselves with the following weaker but elementary estimate.

PROPOSITION 6. *$|E(K)_{\text{tors}}| < 32768(\delta(j))^{3d}$ where $\delta(x)$ is $|M_K^\infty| + |\{v \in M_K^0 : v(x) < 0\}|$, which is essentially the number of primes in the denominator of x.*

Proof. Let $p_1 = 2$, $p_2 = 3$, ... be the sequence of rational primes, and let v_1, v_2, ... be places of K lying over p_1, p_2, ... By assumption, $v_n(j) \geq 0$ for two integers $n = n_1, n_2$ with $1 \leq n \leq \delta(j) + 2$, so E has either good or additive reduction at those v_n. Since prime-to-p_n torsion injects into the special fibre of the Néron model at v_n, trivial estimates for the number of points over finite fields yields

$$|E(K)_{\text{prime-to-}p_n \text{ torsion}}| \leq 4N_{K/\mathbb{Q}}v_n \leq 4p_n^d$$

(where we have used the fact that for additive reduction, the special fiber has at most 4 components). Hence,

$$|E(K)_{\text{tors}}| \leq 16(p_{n_1}p_{n_2})^d \leq 32768(\delta(j))^{3d},$$

where the last inequality uses the bound $p_n \leq 2n \log n$. □

Of course, it is not difficult to greatly improve the bound given in the Proposition, but we are content to give a bound with an explicit dependence on d and $\delta(j)$.

The next tool is essentially the result known as "reduction to simultaneous approximation" (see [**11**], for example). There is a slight added complication because the local height functions might be negative.

PROPOSITION 7. *$|\Gamma_S(\epsilon)| \leq 4^s \max_\xi \left|\Gamma_S\left(\frac{\epsilon}{2}, \xi\right)\right|$, where the maximum is taken over all functions $\xi : S \to \mathbb{R}$ satisfying $\xi_v \geq 0$ and $\sum \xi_v = 1$.*

Proof. For $P \in \Gamma_S(\epsilon)$ with $\hat{h}_K(P) > 0$, let

$$\phi_v(P) = d_v \frac{\lambda_v(P) + \frac{1}{24}\max(0, -v(j)) + 3\alpha(v)}{\hat{h}_K(P)}.$$

We know that $\phi_v(P) \geq 0$ by proposition 3(1). Using the definition of $\Gamma_S(\epsilon)$, we have

$$\sum_{v \in S} \phi_v(P) \geq \frac{\sum_{v \in S} d_v \lambda_v(P)}{\hat{h}_K(P)} \geq \epsilon.$$

Therefore, if we write $[x]$ for the greatest integer less than or equal to x, we have

$$\sum_{v \in S} \left[\frac{2\phi_v(P)s}{\epsilon} \right] \geq \sum_{v \in S} \left(\frac{2\phi_v(P)s}{\epsilon} - 1 \right) \geq s,$$

so we may choose integers $a_v(P)$ satisfying

$$0 \leq a_v(P) \leq \frac{2\phi_v(P)s}{\epsilon}$$

and

$$\sum_{v \in S} a_v(P) = s.$$

If we set $\xi_v = a_v(P)/s$, then $P \in \Gamma_S(\epsilon/2, \xi)$. Note also that if $\hat{h}_K(P) = 0$, then $P \in \Gamma_S(\epsilon/2, \xi)$ for any choice of ξ. We have therefore shown that $\Gamma_S(\epsilon)$ is contained in the union of $\Gamma_S(\epsilon/2, \xi)$ for those ξ which have the form $\xi_v = a_v/s$ for some function $a : S \to \mathbb{Z}$ satisfying $a_v \geq 0$ and $\sum_{v \in S} a_v = s$. There are exactly $\binom{2s-1}{s-1}$ such functions a, which gives the desired result. □

We state the next counting result in an abstract fashion. We have chosen this method of presentation to clarify the role that the various constants play in the theorem.

PROPOSITION 8. *Let Γ be a finitely generated abelian group of rank r. Let $t = \#\Gamma_{\text{tors}}$. Let $h : \Gamma \to \mathbb{R}$ be a "distance function" which satisfies:*

(1) *$h(P) \geq 0$, and $h(P) = 0$ if and only if $P \in \Gamma_{\text{tors}}$.*

(2) *$h(qP) = q^2 h(P)$ for all positive integers q.*

(3) *$h(P \pm Q) \leq c(h(P) + h(Q))$ for a fixed constant $c \geq 1$.*

Define $h^{(m)}(P) = \min_{Q \in \Gamma} h(P + mQ)$. Let W be a subset of Γ and consider the following two conditions on W:

$$(*) \qquad \begin{aligned} &h(P - Q) \geq A \min(h(P), h(Q)) - B \text{ for all } P, Q \in W, \\ &P - Q \notin \Gamma_{\text{tors}} \end{aligned}$$

where $A \leq c$.

$$(**) \qquad h(P) \leq Ch^{(m)}(P) + D \text{ for all } P \in W.$$

Let

$$\lambda = \min\{h(P) : P \in \Gamma, P \notin \Gamma_{\text{tors}}\}.$$

Then for any $\delta > 0$,

$$\#\{P \in W : \delta > h(P)\} \leq t\left(\left(\frac{2c\delta}{\lambda}\right)^{1/2} + 1\right)^r.$$

If in addition, W *satisfies* $(*)$, *then for every* $\delta \geq \gamma \geq 2B/A$, *we have*

$$\#\{P \in W : \delta > h(P) \geq \gamma\} \leq t\left(\log \frac{3\delta}{\gamma}\right)\left(\frac{17c^4}{A}\right)^{r/2}.$$

If we then ask also that W *satisfy* $(**)$, *then*

$$\#\{P \in W : h(P) \geq 2B/A\} \leq t\left(\log \frac{6BC + 3AD}{2B}\right)\left(m\left(\frac{17c^4}{A}\right)^{1/2}\right)^r.$$

Proof. This is essentially proved in [**11**], Lemma 1.2. □

PROPOSITION 9. *For any elliptic curve* E/K, *the set*

$$\Gamma_S(\epsilon) = \left\{P \in E(K) : P \neq 0 \text{ and } \sum_{v \in S} d_v \lambda_v(P) \geq \epsilon \hat{h}_K(P)\right\}$$

has at most

$$10^{11} d(\delta(j))^{3d}\left(\frac{16 \cdot 10^9}{\epsilon}\right)^{r\delta(j)+s}$$

elements.

Proof. We essentially use Proposition 8 to bound the size of $\Gamma_S(\epsilon, \xi)$, and then finish by using Proposition 7.

To apply Proposition 8, begin by noticing that the constant c may be taken to be 2, and $t \leq 32768\delta(j)^{3d}$. We have $A = \epsilon$ (note that $A < c$), and $B = 5/24h(j) + 9$, from Proposition 5. Using the

remaining part of Proposition 8 requires breaking $\Gamma_S(\epsilon, \xi)$ into three pieces. Let

$$W_1 = \left\{ P \in \Gamma_S(\epsilon,\xi) : \hat{h}(P) < \frac{5}{12\epsilon} h(j) + \frac{18}{\epsilon} \right\}$$

$$W_2 = \left\{ P \in \Gamma_S(\epsilon,\xi) : \frac{5}{12\epsilon} h(j) + \frac{18}{\epsilon} \right.$$
$$\left. \leq \hat{h}(P) < \frac{51m^2dc_2}{\epsilon} \left(\hat{h}^{(m)}(P) + h(j) + 1 \right) \right\}$$

$$W_3 = \left\{ P \in \Gamma_S(\epsilon,\xi) : \hat{h}(P) \geq \frac{51m^2dc_2}{\epsilon} \left(\hat{h}^{(m)}(P) + h(j) + 1 \right) \right\}$$

where m and c_2 are taken from Proposition 4. Then we know that $n = 18m^2 \leq 1200/\epsilon$, $N < 20000/\epsilon^{1/3}$, and a rough estimate gives $c_1 < 3.5 \cdot 10^{10}/\epsilon^{1/2}$ and $c_2 < 28 \cdot (40000/\epsilon^{1/3})^{40000/\epsilon^{1/3}}$.

Note that W_3 is non-empty only if the rank of E is at least 1, so in bounding the size of that set, we may assume $r \geq 1$. Proposition 4 now says that

$$|W_3| \leq 2c_1 \left(\frac{16}{\sqrt{\epsilon}} \right)^{2s+r} \leq 7 \cdot 10^{10} \left(\frac{256}{\epsilon} \right)^{s+r\delta(j)}.$$

Next, for $P, Q \in W_2$, $P \neq Q$, Proposition 5 gives

$$\hat{h}(P-Q) \geq \epsilon \min(h(P), h(Q)) - \frac{5}{24} h(j) - 9,$$

while by definition, every $P \in W_2$ satisfies

$$\hat{h}(P) < \frac{51m^2dc_2}{\epsilon} \hat{h}^{(m)}(P) + \frac{51m^2dc_2}{\epsilon} (h(j) + 1).$$

We now have condition $(**)$ of Proposition 8, if we set

$$C = \frac{51m^2dc_2}{\epsilon} < \frac{4000dc_2}{\epsilon^2}$$

and

$$D = \frac{51m^2dc_2}{\epsilon} (h(j) + 1) < \frac{4000dc_2}{\epsilon^2} (h(j) + 1).$$

Therefore,

$$\begin{aligned}|W_2| &\leq 32768\delta(j)^{3d}\left(\log\frac{6BC+3\epsilon D}{2\epsilon B}\right)\left(m\left(\frac{17\cdot 16}{\epsilon}\right)^{1/2}\right)^r \\ &\leq 32768\delta(j)^{3d}\log\frac{50000dc_2}{\epsilon^3}\left(\frac{160}{\epsilon}\right)^r \\ &\leq 2\cdot 10^{10}d\delta(j)^{3d}\left(\frac{160}{\epsilon}\right)^{r\delta(j)+s}.\end{aligned}$$

Finally, for the non-torsion points $P \in E(K)$, we have the lower bound for $h(P)$ given by Proposition 3(3), namely

$$\hat{h}(P) > (24\cdot 144\cdot 97200^2)^{-\delta(j)}\max(h(j),1).$$

Hence, we may apply Proposition 8 to

$$\left\{P\in E(K) : \hat{h}(P) < \frac{5}{24\epsilon}h(j)+\frac{18}{\epsilon}\right\}$$

(a set which contains W_1), we have

$$\begin{aligned}&|W_1| \\ &\leq 32768\delta(j)^{3d}\left(\left(\left(\frac{5}{6\epsilon}h(j)+\frac{72}{\epsilon}\right)\left(\frac{24\cdot 144\cdot 97200^2}{\max(h(j),1)}\right)^{\delta(j)}\right)^{1/2}+1\right)^r \\ &\leq 32768\delta(j)^{3d}\left(\frac{80}{\epsilon}\sqrt{244\cdot 144\cdot 97200^2}\right)^r \leq 32768\delta(j)^{3d}\left(\frac{2\cdot 10^9}{\epsilon}\right)^r.\end{aligned}$$

We may finally combine all of these to get the bound

$$|\Gamma_S(\epsilon,\xi)| \leq 10^{11}d\delta(j)^{3d}\left(\frac{2\cdot 10^9}{\epsilon}\right)^{s+r\delta(j)}.$$

Now we can obtain the bound

$$|\Gamma_S(\epsilon)| \leq 10^{11}d\delta(j)^{3d}\left(\frac{16\cdot 10^9}{\epsilon}\right)^{s+r\delta(j)}$$

by applying proposition 7. □

We are nearly in a position to prove our main result bounding uniformly the number of S-integral solutions to a quasi-minimal

equation for an elliptic curve. But first, we must study how far a quasi-minimal Weierstrass equation can fail to be globally minimal. We adopt the notation that $\Delta_1, \Delta_2, \ldots$ denote the discriminants of the Weierstrass equations (1), (2), etc.

PROPOSITION 10. *A quasi-minimal Weierstrass equation*

$$y^2 = x^3 + Ax + B \tag{1}$$

for E/K satisfies

$$\begin{aligned} h_K(\Delta_1) < \log &\left|N_{K/\mathbb{Q}}\Delta_{E/K}\right| \\ &+ 6\log|D_K| \\ &+ d(60d^2\log 6d)^d\left(\frac{2}{\sqrt{3}}\right)^{d(d-1)/2}(R_K+1). \end{aligned}$$

Proof. The obstruction to finding a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2}$$

which is globally minimal over O_K is given by an ideal class $A_{E/K} \in \mathrm{Pic}(\mathrm{O}_K)$ satisfying $\Delta_{E/K} \in A_{E/K}^{-12}$. Furthermore, if $a \in A_{E/K}$ is an *integral* ideal, then there is an equation (2) with $a_i \in \mathrm{O}_K$ and

$$(\Delta_2) = a^{12}\Delta_{E/K}.$$

(See [**10**]). Minkowski's theorem now says that we can find an integral ideal a in the class $A_{E/K}$ satisfying

$$\left|N_{K/\mathbb{Q}}a\right| \le \left(\frac{4}{\pi}\right)^{r_2}\left(\frac{d!}{d^d}\right)\sqrt{|D_K|} \le \sqrt{|D_K|}.$$

Hence, there is an equation (2) with $a_i \in \mathrm{O}_K$ and

$$\left|N_{K/\mathbb{Q}}\Delta_2\right| \le D_K^6\left|N_{K/\mathbb{Q}}\Delta_{E/K}\right|.$$

Next, the standard substitutions

$$\begin{aligned} X &= 36x + 3a_1^2 + 12a_2 \\ Y &= 216y + 108a_1x + 108a_3 \end{aligned}$$

transforms the equation (2) into an equation

$$Y^2 = X^3 - 27c_4X - 54c_6 \tag{3}$$

with $c_4, c_6 \in \mathbb{Z}[a_1, \ldots, a_6]$ and

$$\Delta_3 = 6^{12}\Delta_2.$$

Thus,

$$\left|N_{K/\mathbb{Q}}\Delta_3\right| \leq 6^{12d} D_K^6 \left|N_{K/\mathbb{Q}}\Delta_{E/K}\right|.$$

Finally, replacing X and Y with $u^{-2}X$ and $u^{-3}Y$ respectively for some unit $u \in \mathrm{O}_K^\times$, we get a new equation with discriminant Δ_4 which satisfies

$$\Delta_4 = u^{12}\Delta_3.$$

Therefore, all we need to show is that for any $\Delta \in \mathrm{O}_K$ and any $n \geq 1$, there is a unit $u \in \mathrm{O}_K^\times$ so that

$$h_K(u^n\Delta) \leq \log\left|N_{K/\mathbb{Q}}\Delta\right| + \gamma n R_K.$$

This is in [**8**] Proposition 2(b), save that the second term on the right hand side of the inequality is not given explicitly. However, from the proof, one sees that it is less than

$$n \sum_{v \in M_K^\infty} \sum_{i=1}^{t} |v(u_i)| = 2n \sum_{i=1}^{t} h_K(u_i),$$

where $\{u_1, \ldots, u_t\}$ is any basis for $\mathrm{O}_K^\times$/torsion. Now, following the argument in [**9**], equation (1), we can choose a basis $u_1, \ldots, u_t$ so that

$$\prod_{i=1}^{t} h(u_i) < \left(\frac{2}{\sqrt{3}}\right)^{t(t-1)/2} \left(\frac{\sqrt{t}}{d}\right)^t R_K \leq \left(\frac{2}{\sqrt{3}}\right)^{d(d-1)/2} R_K.$$

On the other hand, [**1**] shows that

$$H_K(\alpha) \geq 1 + \frac{1}{30d^2 \log 6d}$$

if α is not a root of unity, and therefore

$$h_K(u_i) \geq \frac{1}{60d^2 \log 6d}.$$

Therefore,

$$\sum_{i=1}^{t} h_K(u_i) \leq t(60d^2 \log 6d)^{t-1} \prod_{i=1}^{t} h_K(u_i).$$

□

PROPOSITION 11. *Let*

$$y^2 = x^3 + Ax + B$$

be a quasi-minimal Weierstrass equation for an elliptic curve E/K. Let $\epsilon > 0$ be a constant. Suppose that

$$\max\left(h_K(j), \log\left|N_{K/\mathbb{Q}}\Delta_{E/K}\right|\right) \geq 6d(60d^2 \log 6d)^d \left(\frac{2}{\sqrt{3}}\right)^{d(d-1)/2} \max\left(R_K, \log|D_K|, 1\right).$$

Then the set

$$\left\{P \in E(K) : \sum_{v \in S} d_v \max(0, -v(x(P))) \geq \epsilon h_K(x(P))\right\}$$

contains at most

$$2 \cdot 10^{11} d\delta(j)^{3d} \left(\frac{32 \cdot 10^9}{\epsilon}\right)^{r\delta(j)+s}$$

points. (If $K = \mathbb{Q}$, then the $\delta(j)^{3d}$ factor may be replaced with a simpler constant.)

REMARKS. Note that for any given field K, there are only finitely many elliptic curves E/K with bounded $\log N_{K/\mathbb{Q}}|\Delta_{E/K}|$ and $h_K(j)$, so the above estimate will apply for almost every elliptic curve over a fixed field K.

It would be interesting to produce similar bounds to those above that depend only on d and not D_K.

Taking $\epsilon = 1$ gives precisely the S-integral points. Thus,

$$|\{P \in E(K) : x(P) \in \mathrm{O}_S\}| \leq 2 \cdot 10^{11} d\delta(j)^{3d}(32 \cdot 10^9)^{r\delta(j)+s}$$

for all but finitely many E/K. In particular, we may take $K = \mathbb{Q}$, replace the $\delta(j)^{3d}$ term with 16, and conclude that for all but finitely many elliptic curves $E/\mathbb{Q}$, we have

$$|\{P \in E(\mathbb{Q}) : x(P) \in \mathbb{Z}_S\}| \le 32 \cdot 10^{11}(32 \cdot 10^9)^{r\delta(j)+s}.$$

Proof. We assume that E/K satisfies the hypotheses of the proposition. Let

$$\Gamma_x = \left\{ P \in E(K) : \sum_{v \in S} d_v \max(0, -v(x(P))) \ge \epsilon h_K(x(P)) \right\}.$$

Let $\Delta = -16(4A^3 + 27B^2)$ be the discriminant of the equation. For any $P \in \Gamma_x$, we know from Proposition 3(6) that

$$\sum_{v \in S} d_v \lambda_v(P) \ge \epsilon \hat{h}_K(P) - \frac{1}{3} h_K(j) - \frac{1}{3} h_K(\Delta) - 1.07d.$$

Now Proposition 10 and the assumptions in the theorem give

$$\begin{aligned}
\sum_{v \in S} d_v \lambda_v(P) &\ge \epsilon \hat{h}_K(P) - \frac{1}{3} h_K(j) \\
&\quad - \frac{1}{3} \left(\log \left| N_{K/\mathbb{Q}} \Delta_{E/K} \right| + 6 \log D_K + \right. \\
&\qquad \left. d(60d^2 \log 6d)^d \left(\frac{2}{\sqrt{3}} \right)^{\frac{d(d-1)}{2}} \right) (R_K + 1) \\
&\quad - 1.07d \\
&\ge \epsilon \hat{h}_K(P) - 4 \max(h_K(j), \log \left| N_{K/\mathbb{Q}} \Delta_{E/K} \right|, d),
\end{aligned}$$

and therefore

$$\begin{aligned}
\Gamma_x \subseteq \Gamma_S(\epsilon/2) \cup \Bigg\{ & P \in E(K) : \hat{h}(P) \\
& \le \frac{2}{\epsilon} \max \left(h(j), \frac{1}{d} \log \left| N_{K/\mathbb{Q}} \Delta_{E/K} \right|, 1 \right) \Bigg\}.
\end{aligned}$$

But we know that

$$\left| \Gamma_S \left(\frac{\epsilon}{2} \right) \right| \le 10^{11} d \delta(j)^{3d} \left(\frac{32 \cdot 10^9}{\epsilon} \right)^{r\delta(j)+s},$$

and we can apply Proposition 8 to conclude that

$$\left|\left\{P \in E(K) : \hat{h}(P) \leq \frac{2}{\epsilon} \max\left(h(j), \frac{1}{d}\log\left|N_{K/\mathbb{Q}}\Delta_{E/K}\right|, 1\right)\right\}\right| \leq 32768\delta(j)^{3d}\left(\frac{2\cdot 10^7}{\epsilon}\right)^{r\delta(j)+s},$$

and so

$$|\Gamma_x| \leq 2\cdot 10^{11} d\delta(j)^{3d}\left(\frac{32\cdot 10^9}{\epsilon}\right)^{r\delta(j)+s}.$$

The factor of $\delta(j)^{3d}$ arises solely from the estimate on $|E(K)_{\text{tors}}|$, and so if $K = \mathbb{Q}$, it may be replaced by 16. □

We thank the referee for many helpful comments and suggestions.

References

[1] P. E. Blanksby and H. L. Montgomery, *Algebraic integers near the unit circle*, Acta Arith., **18** (1971), 355-369.

[2] Robert Gross, *A Note on Roth's Theorem*, J. Number Theory, **36** (1990), 127-132.

[3] M. Hindry and J. Silverman, *The canonical height and integral points on elliptic curves*, Invent. math., **93** (1988), 419-450.

[4] Serge Lang, *Elliptic Curves: Diophantine Analysis*, Springer-Verlag, New York, 1978.

[5] Barry Mazur, *Modular curves and the Eisenstein ideal*, IHES Publ. Math., **47** (1976), 33-186.

[6] Joseph Silverman, *Integer points and the rank of Thue elliptic curves*, Inv. Math., **66** (1982), 395-404.

[7] ———, *Lower bound for the canonical height on elliptic curves*, Duke Math. J., **48** (1982), 633-648.

[8] ———, *Representations of integers by binary forms and the rank of the Mordell-Weil group*, Inv. Math., **74** (1983), 281-292.

[9] ———, *An inequality relating the regulator and discriminant of a number field*, J. Number Theory, **19** (1984), 437-442.

[10] ———, *The Arithmetic of Elliptic Curves*, Graduate texts in Mathematics 106, Springer-Verlag, New York, 1986.

[11] ———, *A quantitative version of Siegel's theorem: Integral points on elliptic curves and Catalan curves*, J. Reine Angew. Math., **378** (1987), 60-100.

[12] ———, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp., **55** (1990), 723-743.

[13] H. Zimmer, *Quasifunctions on elliptic curves over local fields*, J. Reine Angew. Math., **307/308** (1979), 221-246.

Received October 1, 1992.

BOSTON COLLEGE
CHESTNUT HILL, MA 02167-3806
E-mail address: gross@bcvms.bc.edu

AND

BROWN UNIVERSITY
PROVIDENCE, RI 02912-0001
E-mail address: joseph_silverman@brown.edu

PACIFIC JOURNAL OF MATHEMATICS

Volume 167 No. 2 February 1995

Existence of shortest directed networks in $\mathbb{R}^2$ 201
MANUEL ALFARO GARCIA

Hecke characters of singular Drinfel'd modules 215
SUNGHAN BAE

Factorization method for a bimeromorphic morphism 231
JOSE PEREZ BLANCO

L^p estimates for operators associated to flat curves without the Fourier transform 243
ANTHONY CARBERY, JAMES THOMAS VANCE, JR., STEPHEN WAINGER, DAVID K. WATSON and JAMES WRIGHT

S-integer points on elliptic curves 263
ROBERT HOWARD GROSS and JOSEPH SILVERMAN

On metrics defined by modules 289
JAMES ALLISTER JENKINS

Conditional Wiener integrals. II 293
CHULL PARK and DAVID LEE SKOUG

On a Plancherel formula for certain discrete, finitely generated, torsion-free nilpotent groups 313
CAROLYN PFEFFER JOHNSTON

Desingularizations of some unstable orbit closures 327
MARK STEPHEN REEDER

Determining multiplicities of half-integral weight newforms 345
THOMAS RICHARD SHEMANSKE and LYNNE WALLING

Generation of integral orthogonal groups over dyadic local fields 385
FEI XU

0030-8730(1995)167:2;1-D