MATHEMATICS OF COMPUTATION
VOLUME 48, NUMBER 177
JANUARY 1987, PAGES 351-370

Computation of the Néron-Tate Height on Elliptic Curves

By Heinz M. Tschöpe and Horst G. Zimmer

For Daniel Shanks on the occasion of his 70th birthday

Abstract. Using Néron's reduction theory and a method of Tate, we develop a procedure for calculating the local and global Néron-Tate height on an elliptic curve over the rationals. The procedure is illustrated by means of two examples of Silverman and is then applied to calculate the global Néron-Tate height of a series of rank-one curves of Bremner-Cassels and of a series of rank-two curves of Selmer. In the latter case, the regulator is also computed, and a conjecture of S. Lang is investigated numerically.

In dealing with the arithmetic of elliptic curves E over a global field K, the task arises of computing the Néron-Tate height on the group $E(K)$ of rational points of E over K. Solving this task in an efficient manner is important, for instance, in view of calculations concerning the Birch and Swinnerton-Dyer conjecture (see [2]) or of the conjectures of Serge Lang [6]. The purpose of this note is to suggest a procedure for performing the necessary calculations.

1. Multiplication Formulas. Let the elliptic curve E over any field K be defined by a *generalized Weierstrass equation*

$$\text{(E)} \qquad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (a_i \in K).$$

As usual, we introduce the quantities (see [10], [11])

$$b_2 = a_1^2 + 4a_2, \quad b_4 = a_1a_3 + 2a_4, \quad b_6 = a_3^2 + 4a_6,$$
$$b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2,$$
$$c_4 = b_2^2 - 24b_4, \qquad c_6 = -b_2^3 + 36b_2b_4 - 216b_6,$$

and the *discriminant*

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \neq 0,$$

as well as the *absolute invariant*

$$j = c_4^3/\Delta$$

belonging to E over K.

The fact that E is nonsingular implies the nonvanishing of the partial derivatives of the polynomial

$$F(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

Received May 19, 1986; revised June 30, 1986.
1980 *Mathematics Subject Classification*. Primary 14-04, 14H45, 14K07, 14K15; Secondary 10B10, 14G20, 14G25, 14H25.

at every rational point $P \in E(K)$:

$$\left(\frac{\partial F}{\partial x}(P), \frac{\partial F}{\partial y}(P)\right) \neq (0,0).$$

The addition law in the additive Abelian group $E(K)$ of rational points on E over K is given by the following formulas:

For $P = (x_P, y_P)$, $Q = (x_Q, y_Q) \in E(K)$, denote the sum by $P + Q = (x_{P+Q}, y_{P+Q})$. Then,

$$(1)\quad \begin{aligned} x_{P+Q} &= -(x_P + x_Q) + \left(\frac{y_P - y_Q}{x_P - x_Q}\right)^2 + a_1\left(\frac{y_P - y_Q}{x_P - x_Q}\right) - a_2, \\ y_{P+Q} &= \frac{y_P - y_Q}{x_P - x_Q}(x_P - x_{P+Q}) - a_1 x_{P+Q} - a_3 - y_P \quad \text{if } P \neq Q \end{aligned}$$

and

$$(2)\quad \begin{aligned} x_{2P} &= -2x_P + t_P^2 + a_1 t_P - a_2, \qquad y_{2P} = t_P(x_P - x_{2P}) - a_1 x_{2P} - a_3 - y_P \\ &\text{for } t_P = \frac{3x_P^2 + 2a_2 x_P + a_4 - a_1 y_P}{2y_P + a_1 x_P + a_3} \qquad \text{if } P = Q. \end{aligned}$$

Generalizing classical formulas (see [3], [4], [15]), we obtain

PROPOSITION 1. *For a rational point $P \in E(K)$ and an $r \in \mathbf{N}$, the r-fold rational point has coordinates*

$$rP = (x_{rP}, y_{rP}) = \left(\frac{\Phi_r(P)}{\Psi_r^2(P)}, \frac{\Omega_r(P)}{\Psi_r^3(P)}\right),$$

where Φ_r, Ψ_r, and $2\Omega_r$ are polynomials in x and y with coefficients in $\mathbf{Z}[a_1, a_2, a_3, a_4, a_6]$ given by the following recursion formulas:

$\Phi_1 = x, \qquad \Phi_2 = x^4 - b_4x^2 - 2b_6x - b_8,$

$\Omega_1 = y, \quad \Psi_0 = 0, \quad \Psi_1 = 1, \Psi_2 = 2y + a_1x + a_3,$

$\Psi_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8,$

$\Psi_4 = \Psi_2\left[2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + b_4b_8 - b_6^2\right]$

and for $r \geqslant 2$,

$$(3)\quad \begin{aligned} \Phi_r &= x\Psi_r^2 - \Psi_{r-1}\Psi_{r+1}, \\ 2\Psi_2\Omega_r &= \Psi_{r-1}^2\Psi_{r+2} - \Psi_{r-2}\Psi_{r+1}^2 - \Psi_2\Psi_r\left[a_1\Phi_r + a_3\Psi_r^2\right], \\ \Psi_{2r+1} &= \Psi_r^3\Psi_{r+2} - \Psi_{r-1}\Psi_{r+1}^3, \\ \Psi_2\Psi_{2r} &= \Psi_r\left[\Psi_{r-1}^2\Psi_{r+2} - \Psi_{r-2}\Psi_{r+1}^2\right]. \end{aligned}$$

Moreover, Φ_r, as a polynomial in x, has degree r^2 and leading coefficient 1, whereas Ψ_r (resp. $\Psi_2^{-1}\Psi_r$), as a polynomial in x, has degree $(r^2 - 1)/2$ (resp. $(r^2 - 4)/2$) and leading coefficient r (resp. $r/2$) provided that r is odd (resp. even). If we assign the weight 2, 3 or i to x, y or a_i, then each term of Φ_r has weight $2r^2$ and each term of

Ψ_r (resp. $\Psi_2^{-1}\Psi_r$) has weight $r^2 - 1$ (resp. $r^2 - 4$). The coefficients of Φ_r, Ψ_r, as polynomials in x, y, belong already to $\mathbf{Z}[b_2, b_4, b_6, b_8]$.

From Proposition 1, one derives the following

COROLLARY. *For $r \in \mathbf{N}$, we put $\Psi_{-r} = -\Psi_r$. Then, for $r, n \in \mathbf{N}$, we have*

$$\Psi_{rn}^2(P) = \Psi_n^{2r^2}(P)\Psi_r^2(nP) \tag{4}$$

and, more generally,

$$\Psi_{m^n}^2(P) = \prod_{\nu=1}^{n} \Psi_m^{2m^{2(n-\nu)}}(m^{\nu-1}P). \tag{4'}$$

Furthermore,

$$x_{rP} - x_{nP} = -\frac{\Psi_{r+n}(P)\Psi_{r-n}(P)}{\Psi_r^2(P)\Psi_n^2(P)}, \tag{5}$$

$$x_{rP} - x_{rQ} = (-1)^{r+1}\frac{\Psi_r(P+Q)\Psi_r(P-Q)}{\Psi_r^2(P)\Psi_r^2(Q)}(x_P - x_Q)^{r^2} \tag{6}$$

and finally, for $r \in \mathbf{N}_0$,

$$\Phi_2(2^rP) = \Phi_{2^{r+1}}(P)\Psi_{2^r}^{-8}(P), \qquad \Psi_2^2(2^rP) = \Psi_{2^{r+1}}^2(P)\Psi_{2^r}^{-8}(P). \tag{7}$$

These formulas will be needed in the sequel.

2. Reduction Theory. Now let the elliptic curve E be defined by (E) over a complete field K with respect to a discrete normalized additive valuation v, and suppose that the corresponding residue field $\tilde{K}$ of K is perfect. We assume the equation defining E over K to be minimal with respect to the valuation v (see [11]). Reducing E modulo v yields a cubic curve

$$\tilde{y}^2 + \tilde{a}_1\tilde{x}\tilde{y} + \tilde{a}_3\tilde{y} = \tilde{x}^3 + \tilde{a}_2\tilde{x}^2 + \tilde{a}_4\tilde{x} + \tilde{a}_6 \qquad (\tilde{a}_i \in \tilde{K}) \tag{$\tilde{\mathrm{E}}$}$$

over $\tilde{K}$ with discriminant $\tilde{\Delta}$. If $\tilde{\Delta} \neq 0$, i.e., $v(\Delta) = 0$, then $\tilde{E}$ is an elliptic curve over $\tilde{K}$, and E has *good reduction* at v. If, however, $\tilde{\Delta} = 0$, i.e., $v(\Delta) > 0$, then $\tilde{E}$ is a rational curve over $\tilde{K}$, and E has *bad reduction* at v. In the latter case, E is said to have *multiplicative reduction* or *additive reduction* modulo v, according as $v(c_4) = 0$ or $v(c_4) > 0$, respectively.

Denote by $E_0(K)$ the set of points in $E(K)$ whose image under the reduction map modulo v,

$$\rho\colon E(K) \to \tilde{E}(\tilde{K}),$$

is a nonsingular point on $\tilde{E}$ over $\tilde{K}$. Then, $E_0(K)$ is a subgroup of finite index in $E(K)$. Further, the set

$$E_1(K) = \{P = (x_P, y_P) \in E(K) \mid v(x_P) \leqslant -2,\ v(y_P) \leqslant -3\}$$

is a subgroup of $E_0(K)$, and the restriction ρ_0 to $E_0(K)$ of the reduction map ρ induces an injective homomorphism of the factor group

$$\tilde{\rho}_0\colon E_0(K)/E_1(K) \to \tilde{E}_0(\tilde{K})$$

to the nonsingular part $\tilde{E}_0(\tilde{K})$ of $\tilde{E}(\tilde{K})$.

We shall use the following result (see [11]).

PROPOSITION 2. *The above groups satisfy*

$$E(K) = E_0(K) \quad \textit{if } E \textit{ has good reduction at } v,$$
$$\#(E(K)/E_0(K)) \textit{ divides } v(j) \quad \textit{if } E \textit{ has multiplicative reduction at } v,$$

and

$$\#(E(K)/E_0(K)) \leqslant 4 \quad \textit{if } E \textit{ has additive reduction at } v.$$

3. Definition of Height Functions. Now let K be a *global field*, that is, an algebraic number field or a function field of finite transcendence degree over its field of constants k. Then K possesses a complete set M_K of nonequivalent additive valuations v satisfying the *sum formula*

$$\text{(S)} \qquad \sum_{v \in M_K} \lambda_v v(c) = 0 \quad \text{for } 0 \neq c \in K$$

with some positive multiplicities $\lambda_v \in \mathbf{R}$ (cf. [7], [13]).

For an elliptic curve E over K, given by the Weierstrass equation (E), we introduce the quantities

$$\text{(8)} \qquad \mu_v = \min\{v(b_2), \tfrac{1}{2}v(b_4), \tfrac{1}{3}v(b_6), \tfrac{1}{4}v(b_8)\}.$$

Let $P = (x_P, y_P) \in E(K)$ be any rational point and $\mathcal{O} = (\infty, \infty)$ designate the point at infinity. Then we define the *local Weil height* on $E(K)$ with respect to v by setting

$$\text{(9)} \qquad d_v(P) = \begin{cases} -\frac{1}{2}\min\{\mu_v, v(x_P)\} & \text{if } P \neq \mathcal{O}, \\ -\frac{1}{2}\mu_v & \text{if } P = \mathcal{O}. \end{cases}$$

Then the *global Weil height* on $E(K)$ is simply the sum, with multiplicities, over the local Weil heights

$$d(P) = \sum_{v \in M_K} \lambda_v d_v(P)$$

(see [13]).

In order to define the global Néron-Tate height on $E(K)$, we proceed in the same way as with the global Weil height. However, before introducing the local Néron-Tate height on $E(K)$, we need some estimates.

PROPOSITION 3. *The local Weil height on $E(K)$ satisfies the following estimates*:

$$\text{(10)} \qquad \begin{aligned} \tfrac{1}{2}(6\mu_v - v(\Delta)) + 5\alpha_v \leqslant{} & d_v(P+Q) + d_v(P-Q) \\ & - 2d_v(P) - 2d_v(Q) - v(x_P - x_Q) \\ \leqslant{} & -2\alpha_v \quad \text{if } P, Q, P \pm Q \neq \mathcal{O}, \end{aligned}$$

and

$$\tag{11} \begin{aligned} \tfrac{1}{2}(6\mu_v - v(\Delta)) + 4\alpha_v \leqslant d_v(2P) - 4d_v(P) - \tfrac{1}{2}v(\Psi_2^2(P)) \\ \leqslant -\tfrac{3}{2}\alpha_v \quad \text{if } 2P \neq \mathcal{O}, \end{aligned}$$

where the constant α_v *can be chosen to be* 0 *or* $-\log 2$ *according as the valuation* v *of* K *is discrete or archimedean, respectively* (*see* [13]).

These estimates are obtained as generalizations of those given in [13], [14]. At the same time, they sharpen those cited.

Remark 1. It is interesting to note that the authors of [2] suggested that a sharpening of the estimates in [13], [14] should be possible. Proposition 3 appears to be a step in this direction.

Employing (10), the inequalities (11) can be further generalized.

COROLLARY. *For any* $m \in \mathbf{N}$, *there are* (*recursively computable*) *nonnegative constants* $c_{1,m}$, $c_{2,m} \in \mathbf{R}$ *depending on* E, K, *and* v *such that, given an arbitrary point* $P \in E(K)$ *with* $mP \neq \mathcal{O}$, *we have*

$$\tag{11$'$} c_{1,m} \leqslant d_v(mP) - m^2 d_v(P) - \tfrac{1}{2}v(\Psi_m^2(P)) \leqslant c_{2,m}.$$

We are now in a position to define the local Néron-Tate height on $E(K)$ with respect to v. Let $m, n \in \mathbf{N}$ and $m \geqslant 2$. Then, for a rational point $P \in E(K)$ such that $m^n P \neq \mathcal{O}$ for each $n \in \mathbf{N}$, we define the *local Néron-Tate height* of P with respect to v by the limit formula

$$\tag{12} \delta_{v,m}(P) = \lim_{n\to\infty}\left\{\frac{d_v(m^nP)}{m^{2n}} - \frac{1}{2}\frac{v(\Psi_{m^n}^2(P))}{m^{2n}}\right\} + \frac{1}{12}v(\Delta).$$

PROPOSITION 4. *For an elliptic curve* E *defined by a Weierstrass equation* (E) *over a global field* K *and any valuation* v *of* K, *the function* $\delta_{v,m}$, *defined by* (12) *on the rational point group* $E(K)$, *exists, is independent of the choice of* $m \in \mathbf{N}$, *so that* $\delta_{v,m} = \delta_v$, *and fulfills the relations*

$$\tag{13} \delta_v(P+Q) + \delta_v(P-Q) - 2\delta_v(P) - 2\delta_v(Q) - v(x_P - x_Q) + \tfrac{1}{6}v(\Delta) = 0$$

for any two points $P = (x_P, y_P)$, $Q = (x_Q, y_Q) \in E(K)$ *such that* $P, Q, P \pm Q \neq \mathcal{O}$, *and*

$$\tag{14} \delta_v(rP) - r^2\delta_v(P) - \tfrac{1}{2}v(\Psi_r^2(P)) + \frac{r^2-1}{12}v(\Delta) = 0$$

for any $P = (x_P, y_P) \in E(K)$ *and* $r \in \mathbf{N}$ *such that* $rP \neq \mathcal{O}$.

Proof. The proof is an adaptation of the corresponding proof of the existence theorem in [14]. Indeed, one exploits (10), (11) from Proposition 3 and (11$'$) from the corollary to establish the existence of $\delta_{v,m}$. Then formulas (6) and (4) from the corollary to Proposition 1 are utilized to prove that $\delta_{v,m}$ fulfills the asserted relations

(13) and (14). Finally, the independence of $\delta_{v,m}$ on m is a consequence of the following

COROLLARY 1. *The function $\delta_{v,m}$ on $E(K)$ is related to the local Weil height on $E(K)$ through the estimate*

$$\left|\delta_{v,m}(P) - \left\{d_v(P) + \frac{1}{12}v(\Delta)\right\}\right| \leqslant c_m, \tag{15}$$

where

$$c_m = \frac{1}{m^2-1} \cdot \max\{|c_{1,m}|, |c_{2,m}|\}.$$

In fact, $\delta_{v,m} = \delta_v$ is uniquely determined by the properties (14) *and* (15) *and hence is independent of the choice of m.*

We can now define the *global Néron-Tate height* on $E(K)$ as the sum, with multiplicities, over the local Néron-Tate heights as follows (see [14]):

$$\delta(P) = \begin{cases} \sum_{v \in M_K} \lambda_v \delta_v(P) & \text{if } P \neq \mathcal{O}, \\ 0 & \text{if } P = \mathcal{O}. \end{cases} \tag{16}$$

By the sum formula (S) we then obtain on the basis of (13) and (14):

COROLLARY 2. *The global Néron-Tate height on $E(K)$ fulfills the relations*

$$\delta(P+Q) + \delta(P-Q) - 2\delta(P) - 2\delta(Q) = 0 \tag{13'}$$

and, for $r \in \mathbf{N}$,

$$\delta(rP) - r^2\delta(P) = 0. \tag{14'}$$

Remark 2. Corollary 2 shows that the global Néron-Tate height δ is a quadratic form on $E(K)$, whereas Proposition 4 implies that the local Néron-Tate height δ_v is "almost" a quadratic form on $E(K)$.

4. Computation of the Néron-Tate Height. Again, let the elliptic curve E be given by (E) over a global field K. Fix a nonarchimedean (discrete) valuation v of K. Suppose that $P = (x_P, y_P) \in E(K)$ is a rational point satisfying $v(x_P) < \mu_v$.

By Proposition 1, on choosing an $m \in \mathbf{N}$ such that $m \geqslant 2$ and $v(m) = 0$, we have

$$x_{m^nP} = \frac{\Phi_{m^n}(P)}{\Psi^2_{m^n}(P)}.$$

Now $v(x_P) < \mu_v$ together with $v(a_i) \geqslant \mu_v$ entails

$$v(\Phi_{m^n}(P)) = m^{2n}v(x_P), \qquad v(\Psi^2_{m^n}(P)) = (m^{2n}-1)v(x_P).$$

Hence

$$v(x_{m^nP}) = v(x_P).$$

Thus we obtain from the limit formula (12) and the definition (9) of d_v the asserted relation

$$\delta_v(P) = -\tfrac{1}{2}v(x_P) + \frac{1}{12}v(\Delta) = d_v(P) + \frac{1}{12}v(\Delta).$$

PROPOSITION 5. *Suppose that a rational point $P = (x_P, y_P) \in E(K)$ satisfies the inequality $v(x_P) < \mu_v$ for a nonarchimedean (discrete) valuation v of the global field K. Then the local Néron-Tate height of P essentially coincides with the local Weil height of P with respect to v; more precisely,*

$$\delta_v(P) = d_v(P) + \frac{1}{12}v(\Delta).$$

From Proposition 5 we get the following theorem, which is crucial for the calculation of the Néron-Tate height on $E(K)$.

THEOREM 1. *Let E be an elliptic curve defined by a Weierstrass equation* (E) *over an algebraic number field K. Choose a discrete normalized additive valuation v of K and suppose that the equation* (E) *is minimal with respect to v.* Then, for each nontorsion point $P \in E_0(K)$, the local Néron-Tate height of P is essentially equal to the local Weil height of P with respect to v; more precisely,*

$$\delta_v(P) = d_v(P) + \frac{1}{12}v(\Delta).$$

Proof. The theorem can be found in [9]. For the convenience of the reader, however, we give a proof.

By Proposition 5, we may confine ourselves to the case in which $v(x_P) \geqslant \mu_v$. The subcase in which $v(x_P) \geqslant \mu_v > 0$ would lead to a contradiction to the choice of $P \in E_0(K)$. Hence it remains to consider the subcase in which

$$v(x_P) \geqslant \mu_v = 0.$$

The reduction map of Section 2,

$$\tilde{\rho}_0\colon E_0(K)/E_1(K) \to \tilde{E}_0(\tilde{K}),$$

is an injective homomorphism. Since K is a number field, the residue field $\tilde{K}$ of K with respect to v is finite and hence so is the group $\tilde{E}_0(\tilde{K})$. Therefore, for any $P \in E_0(K)$, there exists a number $r \in \mathbf{N}$ such that $rP \in E_1(K)$. Choose $r \in \mathbf{N}$ minimal with this property. Then we have

$$v(x_{rP}) < \mu_v = 0.$$

From this, since $v(x_P) \geqslant \mu_v = 0$ and $v(a_i) \geqslant \mu_v = 0$, we conclude that

$$v(\Phi_r(P)) \geqslant 0 \quad \text{and} \quad v(\Psi_r(P)) > 0.$$

We claim

$$v(x_{rP}) = -v\left(\Psi_r^2(P)\right). \tag{17}$$

*The required minimal model of E is found by Tate's algorithm [11].

By Proposition 5, Formula (14) of Proposition 4, and the definition (9) of d_v, this claim yields the asserted identity

$$\delta_v(P) = \frac{1}{r^2}\left\{\delta_v(rP) - \frac{1}{2}v\big(\Psi_r^2(P)\big) + \frac{r^2-1}{12}v(\Delta)\right\}$$
$$= d_v(P) + \frac{1}{12}v(\Delta)$$

since $v(x_P) \geqslant \mu_v = 0$.

To prove (17) it suffices to show that

$$v(\Phi_r(P)) = 0. \tag{18}$$

This is accomplished by verifying (18), first for the lower $r \in \mathbf{N}$ and then for general $r \in \mathbf{N}$.

Let $r = 2$.
If $v(3x_P^2 + 2a_2x_P + a_4 - a_1y_P) > 0$ we would get a contradiction to the assumption that $P \in E_0(K)$. Hence it is enough to consider $v(3x_P^2 + 2a_2x_P + a_4 - a_1y_P) = 0$. But then the asserted relation (18) follows directly from the formula (2) for x_{2P} and Proposition 1.

Let $r = 3$.
By the minimal choice of r, we have

$$v\big(\Psi_2(P)\big) = 0 \quad \text{and} \quad v\big(\Psi_3(P)\big) > 0.$$

Now the decomposition formula (which can be verified without trouble)

$$\Psi_4(P) = \Psi_2(P)\big[\Psi_3(P)\big(6x_P^2 + b_2x_P + b_4\big) - \Psi_2^4(P)\big]$$

yields $v(\Psi_4(P)) = 0$, and hence the relation from Proposition 1,

$$\Phi_3(P) = x_P\Psi_3^2(P) - \Psi_2(P)\Psi_4(P),$$

leads to the identity $v(\Phi_3(P)) = 0$, as asserted in (18).

Finally, let $r \geqslant 4$.
Again, by the choice of r, we have

$$v\big(\Psi_2(P)\big) = v\big(\Psi_3(P)\big) = \cdots = v\big(\Psi_{r-1}(P)\big) = 0 \quad \text{and}$$
$$v\big(\Psi_r(P)\big) > 0.$$

Then Formula (5) from the corollary to Proposition 1 yields

$$v\big(x_{2P} - x_P\big) = 0 \quad \text{and} \quad v\big(x_{(r-1)P} - x_P\big) > 0,$$

so that another consequence of Formula (5), viz.,

$$\Psi_{r+1}(P) = -\big[\big(x_{(r-1)P} - x_P\big) + \big(x_P - x_{2P}\big)\big]\frac{\Psi_{r-1}^2(P)\Psi_2^2(P)}{\Psi_{r-3}(P)},$$

leads to $v(\Psi_{r+1}(P)) = 0$. Now the identity from Proposition 1,

$$\Phi_r(P) = x_P\Psi_r^2(P) - \Psi_{r-1}(P)\Psi_{r+1}(P),$$

reveals that $v(\Phi_r(P)) = 0$, as asserted in (18). This proves Theorem 1.

Remark 3. Theorem 1 makes it possible to calculate the local Néron-Tate height $\delta_v(P)$ with respect to all discrete valuations v of the number field K for all nontorsion points $P \in E(K)$.

This is true because Proposition 2 tells us that a suitable multiple rP of P belongs to $E_0(K)$. Then we apply Theorem 1 to calculate $\delta_v(rP)$ and use Formula (14) from Proposition 4 to get the desired value of $\delta_v(P)$ itself.**

Remark 4. Torsion points $P \in E(K)$ are of no interest in this connection since their global Néron-Tate height is $\delta(P) = 0$.

It remains to show how to compute the local Néron-Tate height δ_v for archimedean valuations v of the number field K. From (4′) in the corollary to Proposition 1, we get the formula

$$(4'') \qquad \frac{1}{2}\frac{v\left(\Psi_{m^n}^2(P)\right)}{m^{2n}} = \sum_{\nu=1}^{m} \frac{1}{2}\frac{v\left(\Psi_m^2(m^{\nu-1}P)\right)}{m^{2\nu}},$$

which proves to be useful in the sequel.

Now, since we are interested here only in the case of $K = \mathbf{Q}$, the field of rational numbers, we confine ourselves to considering its completion $K_\infty = \mathbf{Q}_\infty = \mathbf{R}$ with respect to the ordinary absolute value $v = v_\infty = -\log|\ |$. Then Tate's method is best suited for calculating δ_{v_∞} (see [12]).

THEOREM 2. *Let E be an elliptic curve defined by a Weierstrass equation* (E) *over the field* $\mathbf{R}$ *of real numbers and denote by $v_\infty = -\log|\ |$ the ordinary additive archimedean valuation of* $\mathbf{R}$. *Take an open subgroup Γ of $E(\mathbf{R})$ such that all $P = (x_P, y_P) \in \Gamma$ satisfy $x_P \neq 0$.*** *For $P \in \Gamma$ such that $2^nP \neq \mathcal{O}$ for all $n \in \mathbf{N}$, define the entities T_n, W_n, and Z_n by putting*

$$T_0 = \frac{1}{x_P}, \qquad T_{n+1} = \frac{W_n}{Z_n} \quad \textit{for } n \in \mathbf{N}_0,$$

where

$$W_n = 4T_n + b_2T_n^2 + 2b_4T_n^3 + b_6T_n^4, \qquad Z_n = 1 - b_4T_n^2 - 2b_6T_n^3 - b_8T_n^4.$$

Let

$$\mu(P) = \sum_{n=0}^{\infty} \frac{\log|Z_n|}{2^{2n}}, \qquad \lambda(P) = \frac{1}{2}\log|x_P| + \frac{1}{8}\mu(P).$$

Then the local Néron-Tate height of P with respect to v_∞ is

$$\delta_{v_\infty}(P) = \lambda(P) - \frac{1}{12}\log|\Delta|.$$

Proof. See [12]. However, the assertion of Theorem 2 also follows from

PROPOSITION 6. *In the situation of Theorem* 2 *we have for $n \in \mathbf{N}_0$,*

$$T_n = \frac{1}{x_{2^nP}}, \quad W_n = \frac{\Psi_2^2(2^nP)}{x_{2^nP}^4}, \quad Z_n = \frac{\Phi_2(2^nP)}{x_{2^nP}^4}.$$

** *Added in proof.* Joe Silverman, whom we wish to thank for some valuable hints, told us that he has carried out similar height computations (unpublished) avoiding, however, the use of Proposition 2 by employing Tate's local formulas (see [14]).

***Hence Γ is either $E(\mathbf{R})$ or the identity component of $E(\mathbf{R})$ according as $E(\mathbf{R})$ is connected or disconnected.

Proof. The proof is carried out easily by means of the formulas (7) in the corollary to Proposition 1.

Remark 5. The simplest way of finding a subgroup Γ of $E(\mathbf{R})$ of the type desired in Theorem 2 is by applying a birational transformation to (E) to obtain a model (E′) such that $b_6' < 0$. Then $\Gamma = E'(\mathbf{R})$ itself will do.

In the *special case* of $K = \mathbf{Q}$ we are interested in, the set $M_{\mathbf{Q}}$ consists in the p-adic valuations v_p corresponding to the primes p of $\mathbf{Q}$ and the additive valuation $v_\infty = -\log|\ |$ corresponding to the unique archimedean absolute value $|\ |$ on $\mathbf{Q}$. Of course, the multiplicities in the sum formula (S) are all $\lambda_v = 1$.

5. Examples. We are now in a position to calculate the Néron-Tate height δ on the group $E(K)$ of rational points on an elliptic curve E over the rational number field $K = \mathbf{Q}$. To this end, we use the defining formula (16) for δ with multiplicities $\lambda_v = 1$ to reduce the computation of δ to that of the local Néron-Tate heights δ_v on $E(K)$. For discrete valuations v of $\mathbf{Q}$, the height δ_v is calculated by means of Theorem 1 in accordance with Remark 3, and for the archimedean absolute value $v_\infty = -\log|\ |$, the calculation of δ_{v_∞} is performed on the basis of Theorem 2.

(i) *Examples of Silverman*. We illustrate our procedure by verifying the height calculations of Silverman [9].

(A)
$$E\colon y^2 + 21xy + 494y = x^3 + 26x^2,$$
$$P = (0,0) \in E(\mathbf{Q}),$$
$$\Delta = -2^{13} \cdot 13^3 \cdot 19^2.$$

Silverman obtains

$$\delta(P) = 0.010{,}492, \ldots .$$

We have

(a)
$$\delta_{v_\infty}(P) = 0.038{,}612{,}393, \ldots,$$

(b)
$$P \notin E_0(\mathbf{Q}) \quad \text{for } p = 2, 13 \text{ and } 19; \text{ and}$$
$$\delta_{v_p}(P) = 0 \quad \text{for all primes } p \neq 2, 13 \text{ or } 19.$$

Now

$$13P \in E_0(\mathbf{Q}) \quad \text{for } p = 2,$$
$$3P \in E_0(\mathbf{Q}) \quad \text{for } p = 13,$$
$$2P \in E_0(\mathbf{Q}) \quad \text{for } p = 19.$$

One computes

$$\Psi_2(P) = 2 \cdot 13 \cdot 19, \quad \Psi_3(P) = 2^3 \cdot 13^3 \cdot 19^2, \quad \Psi_{13}(P) = -2^{80} \cdot 13^{56} \cdot 19^{42}$$

and

$$x_{2P} = -2 \cdot 13, \quad x_{3P} = -2 \cdot 19, \quad x_{13P} = -2^4 \cdot 5 \cdot 13 \cdot 19.$$

This leads to

$$\delta_{v_2}(13P) = \frac{37}{12}\ln 2, \quad \delta_{v_{13}}(3P) = \frac{1}{4}\ln 13, \quad \delta_{v_{19}}(2P) = \frac{1}{6}\ln 19.$$

Hence, by (14) of Proposition 4,

$$\delta_{v_2}(P) = \frac{97}{156}\ln 2, \quad \delta_{v_{13}}(P) = -\frac{1}{12}\ln 13, \quad \delta_{v_{19}}(P) = -\frac{1}{12}\ln 19.$$

By (16) this adds up to

$$\delta(P) = 0.010{,}492{,}061, \ldots .$$

(B)

$$E\colon y^2 + 11xy + 80y = x^3 + 8x^2,$$
$$P = (0,0) \in E(\mathbf{Q}),$$
$$\Delta = -2^{11} \cdot 5^2 \cdot 19.$$

Silverman gets

$$\delta(P) = 0.010{,}284, \ldots$$

and we obtain similarly to (A)

$$\delta(P) = 0.010{,}284{,}005, \ldots .$$

(ii) *The Bremner-Cassels Curves.* Our procedure turns out to be particularly useful for calculating the global Néron-Tate height on the elliptic curves

$$E_p\colon y^2 = x^3 + px$$

for primes p of **Q** such that $p \equiv 5 \pmod 8$, as they were considered by Bremner and Cassels [1]. The authors exhibit points $P \in E(\mathbf{Q})$ of infinite order on 43 curves of this type, where

$$P = (x_P, y_P) \quad \text{with } x_P = \frac{r^2}{s^2}, \qquad y_P = \frac{r \cdot t}{s^3} \quad \text{for } r, s, t \in \mathbf{Z}$$

such that

$$\text{g.c.d.}(r,s) = 1; \quad r, t \not\equiv 0 \pmod p; \quad \text{and}$$
$$r \equiv t \equiv 1 \pmod 2, \quad s \equiv 0 \pmod 2.$$

One easily checks that $P \in E_0(\mathbf{Q})$ for all primes p of **Q** and all points $P \in E(\mathbf{Q})$ displayed in [1]. (Notice that $2y_P$ and $3x_P^2 + p$ are relatively prime.) This leads to

PROPOSITION 7. *For the points $P \in E_p(\mathbf{Q})$ of infinite order on the Bremner-Cassels curves in* [1], *the Néron-Tate height is*

$$\delta(P) = \delta_{v_\infty}(P) + \frac{1}{12}\ln|\Delta| + \ln|s|.$$

(iii) *Modular Elliptic Curves.* In [16, pp. 75–113], N. M. Stephens and J. Davenport list 68 modular elliptic curves E of rank 1 with a rational point $P \in E(\mathbf{Q})$ of infinite order. We computed the Néron-Tate heights of these points P.† Comparison of the Néron-Tate height of the generator of the 63rd curve in their table with the Néron-Tate height of the point in Silverman's second example (see (i) (B) above) shows that the two values agree. It turns out, as one easily checks, that the corresponding two curves are birationally isomorphic (see Table 1).

† We have compared the height values in our Table 1 with those in a corresponding (unpublished) table of Silverman containing up to six digits behind the period. They agree (except for the sixth digits of the curves 58A, 61A, 135A, 153A, 189C and for the fifth and sixth digit of the curve 185D).

TABLE 1

1 .)	a1 = 0	a2 = 0	a3 = 1	a4 =-1	a6 = 0
37A	P = (0 ; 0)				
	global height: .02555570412				
2 .)	a1 = 0	a2 = 1	a3 = 1	a4 = 0	a6 = 0
43A	P = (0 ; 0)				
	global height: .031408253544				
3 .)	a1 = 1	a2 =-1	a3 = 1	a4 = 0	a6 = 0
53A	P = (0 ; 0)				
	global height: .046490742319				
4 .)	a1 = 0	a2 =-1	a3 = 1	a4 =-2	a6 = 2
57E	P = (2 ; 1)				
	global height: .018787296368				
5 .)	a1 = 1	a2 =-1	a3 = 0	a4 =-1	a6 = 1
58A	P = (0 ; 1)				
	global height: .02121015392				
6 .)	a1 = 1	a2 = 0	a3 = 0	a4 =-2	a6 = 1
61A	P = (1 ; 0)				
	global height: .039593865681				
7 .)	a1 = 1	a2 = 0	a3 = 0	a4 =-1	a6 = 0
65A	P = (-1 ; 1)				
	global height: .187757				
8 .)	a1 = 0	a2 = 0	a3 = 1	a4 = 2	a6 = 0
77F	P = (2 ; 3)				
	global height: .049013989632				
9 .)	a1 = 1	a2 = 1	a3 = 1	a4 =-2	a6 = 0
79A	P = (0 ; 0)				
	global height: .048832105054				
10 .)	a1 = 1	a2 = 0	a3 = 1	a4 =-2	a6 = 0
82A	P = (0 ; 0)				
	global height: .112353462459				
11 .)	a1 = 1	a2 = 1	a3 = 1	a4 = 1	a6 = 0
83A	P = (0 ; 0)				
	global height: .088646147057				
12 .)	a1 = 0	a2 = 0	a3 = 0	a4 =-4	a6 = 4
88A	P = (2 ; 2)				
	global height: .020132182168				
13 .)	a1 = 1	a2 = 1	a3 = 1	a4 =-1	a6 = 0
89C	P = (0 ; 0)				
	global height: .056052440615				
14 .)	a1 = 0	a2 = 0	a3 = 1	a4 = 1	a6 = 0
91A	P = (0 ; 0)				
	global height: .071196075334				
15 .)	a1 = 0	a2 = 1	a3 = 1	a4 =-7	a6 = 5
91B	P = (-1 ; 3)				
	global height: .529622543205				
16 .)	a1 = 0	a2 = 0	a3 = 0	a4 =-1	a6 = 1
92C	P = (1 ; 1)				
	global height: .024904198649				
17 .)	a1 = 1	a2 =-1	a3 = 1	a4 =-2	a6 = 0
99A	P = (0 ; 0)				
	global height: .151285692281				

TABLE 1 (*continued*)

No.	Curve	a1	a2	a3	a4	a6	P	global height
18 .)	101A	0	1	1	-1	-1	(-1 ; 0)	.082351726475
19 .)	102E	1	1	0	-2	0	(-1 ; 2)	.07162694647
20 .)	106A	1	1	0	-7	5	(2 ; 1)	.034456340202
21 .)	112K	0	1	0	0	4	(0 ; 2)	.119959949363
22 .)	117A	1	-1	1	4	6	(0 ; 2)	.56516781309
23 .)	118A	1	1	0	1	1	(0 ; 1)	.043953097838
24 .)	121D	0	-1	1	-7	10	(4 ; 5)	.04489257808
25 .)	122A	1	0	1	2	0	(1 ; 1)	.060421607704
26 .)	123A	0	1	1	-10	10	(1 ; 1)	.420260708766
27 .)	124B	0	1	0	-2	1	(1 ; 1)	.260265346941
28 .)	128C	0	1	0	1	1	(0 ; 1)	.216165582287
29 .)	129E	0	-1	1	-19	39	(1 ; 4)	.04997957634
30 .)	130E	1	0	1	-33	68	(2 ; 2)	.585232076797
31 .)	131A	0	-1	1	1	0	(0 ; 0)	.108047599334
32 .)	136A	0	1	0	-4	0	(-2 ; 2)	.115753996413
33 .)	138E	1	1	0	-1	1	(0 ; 1)	.08868409567
34 .)	141E	0	1	1	-12	2	(-3 ; 4)	.017243387509

TABLE 1 (*continued*)

```
35 .)  a1 = 0    a2 =-1    a3 = 1    a4 =-1    a6 = 0
141I   P = ( 0 ; 0 )
       global height: .099247618232

36 .)  a1 = 1    a2 = 1    a3 = 0    a4 =-1    a6 =-1
142E   P = (-1 ; 1 )
       global height: .090456855492

37 .)  a1 = 1    a2 =-1    a3 = 1    a4 =-12   a6 = 15
142F   P = ( 1 ; 1 )
       global height: .016894571319

38 .)  a1 = 1    a2 =-1    a3 = 1    a4 =-3    a6 = 2
145A   P = ( 0 ; 1 )
       global height: .292228814932

39 .)  a1 = 0    a2 =-1    a3 = 0    a4 =-5    a6 = 1
148A   P = (-1 ; 2 )
       global height: .048120589701

40 .)  a1 = 0    a2 = 1    a3 = 0    a4 =-1    a6 = 3
152A   P = (-1 ; 2 )
       global height: .032707434794

41 .)  a1 = 0    a2 = 0    a3 = 1    a4 = 6    a6 = 27
153A   P = ( 5 ; 13 )
       global height: .056444869251

42 .)  a1 = 0    a2 = 0    a3 = 1    a4 =-3    a6 = 2
153C   P = ( 0 ; 1 )
       global height: .034740140542

43 .)  a1 = 0    a2 =-1    a3 = 1    a4 =-1    a6 = 1
155C   P = ( 1 ; 0 )
       global height: .092071961309

44 .)  a1 = 0    a2 =-1    a3 = 0    a4 =-5    a6 = 6
156E   P = ( 1 ; 1 )
       global height: .073707206024

45 .)  a1 = 1    a2 = 1    a3 = 0    a4 =-3    a6 = 1
158D   P = ( 0 ; 1 )
       global height: .03958438143

46 .)  a1 = 1    a2 =-1    a3 = 1    a4 =-9    a6 = 9
158E   P = (-1 ; 4 )
       global height: .019495140155

47 .)  a1 = 1    a2 =-1    a3 = 0    a4 =-6    a6 = 8
162K   P = ( 2 ; 0 )
       global height: .152967441934

48 .)  a1 = 0    a2 = 0    a3 = 1    a4 =-2    a6 = 1
163A   P = ( 1 ; 0 )
       global height: .094954616249

49 .)  a1 = 1    a2 = 1    a3 = 0    a4 =-6    a6 = 4
166A   P = ( 0 ; 2 )
       global height: .044978395458

50 .)  a1 = 0    a2 = 0    a3 = 1    a4 = 6    a6 = 0
171A   P = ( 2 ; 4 )
       global height: .112983434413

51 .)  a1 = 0    a2 = 1    a3 = 0    a4 =-13   a6 = 15
172A   P = ( 2 ; 1 )
       global height: .380069831503
```

TABLE 1 (*continued*)

52 .)	175A	a1 = 0	a2 =-1	a3 = 1	a4 =-148	a6 = 748	P = (7 ; 2)	global height: .332314998542
53 .)	175C	a1 = 0	a2 =-1	a3 = 1	a4 =-33	a6 = 93	P = (-3 ; 12)	global height: .046286666901
54 .)	176A	a1 = 0	a2 =-1	a3 = 0	a4 = 3	a6 = 1	P = (1 ; 2)	global height: .087531915126
55 .)	184B	a1 = 0	a2 =-1	a3 = 0	a4 =-4	a6 = 5	P = (2 ; 1)	global height: .051533618406
56 .)	184C	a1 = 0	a2 =-1	a3 = 0	a4 = 0	a6 = 1	P = (0 ; 1)	global height: .061565455601
57 .)	185A	a1 = 0	a2 =-1	a3 = 1	a4 =-5	a6 = 6	P = (0 ; 2)	global height: .055139483611
58 .)	185B	a1 = 1	a2 = 0	a3 = 1	a4 =-4	a6 =-3	P = (3 ; 2)	global height: .712632645336
59 .)	185D	a1 = 0	a2 = 1	a3 = 1	a4 =-156	a6 = 700	P = (4 ; 12)	global height: .057028352204
60 .)	189A	a1 = 0	a2 = 0	a3 = 1	a4 =-3	a6 = 0	P = (-1 ; 1)	global height: .031606094417
61 .)	189C	a1 = 0	a2 = 0	a3 = 1	a4 =-24	a6 = 45	P = (-3 ; 9)	global height: .931621776106
62 .)	190C	a1 = 1	a2 = 1	a3 = 0	a4 = 2	a6 = 2	P = (1 ; 2)	global height: .065910740941
63 .)	190D	a1 = 1	a2 =-1	a3 = 1	a4 =-48	a6 = 147	P = (13 ; 33)	global height: .010284005728
64 .)	192Q	a1 = 0	a2 =-1	a3 = 0	a4 =-4	a6 =-2	P = (3 ; 2)	global height: .675801867206
65 .)	196A	a1 = 0	a2 =-1	a3 = 0	a4 =-2	a6 = 1	P = (0 ; 1)	global height: .043017725483
66 .)	197A	a1 = 0	a2 = 0	a3 = 1	a4 =-5	a6 = 4	P = (1 ; 0)	global height: .069433995882
67 .)	198I	a1 = 1	a2 =-1	a3 = 0	a4 =-18	a6 = 4	P = (-1 ; 5)	global height: .097521495699
68 .)	200C	a1 = 0	a2 = 1	a3 = 0	a4 =-3	a6 =-2	P = (-1 ; 1)	global height: .146605513301

6. Lang's Conjectures. Silverman [9] used his above-cited examples of rank-one elliptic curves E over $\mathbf{Q}$ to estimate the constants c_1, c_2 in S. Lang's Conjecture 2 (see [6]) about lower bounds for the Néron-Tate height δ on nontorsion points in $E(\mathbf{Q})$. We wish to carry through a similar estimation with respect to Lang's Conjecture 3 (see [6]) for Selmer's [8] rank-two elliptic curves E over $\mathbf{Q}$.

In Section 3, Remark 2, we observed that the Néron-Tate height δ is a quadratic form on the rational point group $E(\mathbf{Q})$. This property of δ is tantamount to the fact that the function

$$\beta(P,Q) = \tfrac{1}{2}\{\delta(P+Q) - \delta(P) - \delta(Q)\}$$

TABLE 2

```
a1 = 0     a2 = 0     a3 = 0     a4 = 0     a6 = -388800

P1 = ( 76 / 1 ; 224 / 1 )

P2 = ( 124 / 1 ; 1232 / 1)

The transformation with (r;s;t;u) = ( 0 ; 0 ; 0 ; 2 ) leads to

a1 =  0    a2 =  0    a3 =  0    a4 =  0    a6 = -6075
--------------------------------------------------------------
P1=( 19 / 1 ; 28 / 1 )

p        the local height                    decimal

2        ( 1 / 3 )*ln( 2 )                   .231049060186
3        ( 13 / 12 )*ln( 3 )                 1.190163312723
5        ( 1 / 3 )*ln( 5 )                   .536479304144
∞                                            -.220039705773

The global height is   1.73765197128
--------------------------------------------------------------
P2=( 31 / 1 ; 154 / 1 )

p        the local height                    decimal

2        ( 1 / 3 )*ln( 2 )                   .231049060186
3        ( 13 / 12 )*ln( 3 )                 1.190163312723
5        ( 1 / 3 )*ln( 5 )                   .536479304144
∞                                            -.068619441325

The global height is   1.889072235727
--------------------------------------------------------------
P1+P2=( 241 / 4 ;-3689 / 8 )

p        the local height                    decimal

2        ( 4 / 3 )*ln( 2 )                   .924196240746
3        ( 13 / 12 )*ln( 3 )                 1.190163312723
5        ( 1 / 3 )*ln( 5 )                   .536479304144
∞                                            .18319182537

The global height is   2.834030682983
--------------------------------------------------------------
Regulator : 3.125459338543
```

TABLE 2 (*continued*)

```
a1 = 0     a2 = 0     a3 = 0     a4 = 0     a6 = -26142912

P1 = ( 26572 / 9 ; 4329280 / 27 )

P2 = ( 61516 / 25 ; 15244064 / 125 )

The transformation with (r;s;t;u) = ( 0 ; 0 ; 0 ; 2 ) leads to

a1 =  0    a2 =  0    a3 =  0    a4 =  0    a6 = -408483

----------------------------------------------------------------

P1=( 6643 / 9 ; 541160 / 27 )

p        the local height                     decimal

2        ( 1 / 3 )*ln( 2 )                    .231049060186
3        ( 25 / 12 )*ln( 3 )                  2.288775601391
41       ( 1 / 3 )*ln( 41 )                   1.237857355568
∞                                             .673826315477

The global height is  4.431508332622

----------------------------------------------------------------

P2=( 15379 / 25 ; 1905508 / 125 )

p        the local height                     decimal

2        ( 1 / 3 )*ln( 2 )                    .231049060186
3        ( 13 / 12 )*ln( 3 )                  1.190163312723
5        ( 1 / 1 )*ln( 5 )                    1.609437912434
41       ( 1 / 3 )*ln( 41 )                   1.237857355568
∞                                             .588854192712

The global height is  4.857361833623

----------------------------------------------------------------

P1+P2=( 133393 / 784 ; 46655225 / 21952 )

p        the local height                     decimal

2        ( 7 / 3 )*ln( 2 )                    1.617343421306
3        ( 13 / 12 )*ln( 3 )                  1.190163312723
7        ( 1 / 1 )*ln( 7 )                    1.945910149055
41       ( 1 / 3 )*ln( 41 )                   1.237857355568
∞                                             .039300793087

The global height is  6.030575031739

----------------------------------------------------------------

Regulator : 18.87131764437
```

for $P, Q \in E(\mathbf{Q})$ represents a symmetric bilinear form on $E(\mathbf{Q})$. If E has rank two over $\mathbf{Q}$ and $P = P_1$, $Q = P_2$ are two basis points of $E(\mathbf{Q})$, the quantity

$$R = \left|\det\left(\beta\left(P_i, P_j\right)\right)_{i,j=1,2}\right| \in \mathbf{R}$$

is called the *regulator* of the elliptic curve E over $\mathbf{Q}$. In addition to the Néron-Tate height of the basis points P_1, P_2 of the rank-two curves E in Selmer's tables [8], we have also computed their regulator R. More detailed information about Selmer's curves is to be found in [6]. To begin with, we list in detail two examples, namely the curves with $A = 30$ and $A = 246$ in [8] (see Table 2).

In analogy to Silverman [9], we now use these Selmer curves to estimate the constants in Lang's Conjecture 3. Suppose E over $\mathbf{Q}$ is given in Weierstrass normal form

$$(\mathrm{E}) \qquad y^2 = x^3 + ax + b \qquad (a, b \in \mathbf{Z}).$$

Following Lang [6], we define the *height* of E over $\mathbf{Q}$ to be the number

$$H(E) = \max\{|a|^3, |b|^2\},$$

so that approximately

$$h(E) = -\log H(E) \approx 6\mu_{v_\infty},$$

where again $v_\infty = -\log|\ |$ denotes the additive archimedean valuation of $\mathbf{Q}$. Let N stand for the *conductor* of E over $\mathbf{Q}$ (see [11]).

Then we enunciate, in the case of rank-two curves,

LANG'S CONJECTURE 3. There is a basis $\{P_1, P_2\}$ of $E(\mathbf{Q})$ modulo torsion such that $\delta(P_1) \leqslant \delta(P_2)$ and

$$\delta(P_1) \leqslant c_1 H(E)^{1/24} \cdot N^{\varepsilon(N)/2} \cdot \log N \cdot (2/\sqrt{3})^{1/2},$$
$$\delta(P_2) \leqslant c_2 H(E)^{1/12} \cdot N^{\varepsilon(N)} \cdot \log N \cdot c$$

for some positive real constants c, c_1, c_2, where

$$\lim_{N\to\infty} \varepsilon(N) = 0.$$

Now the constants c_1 and c_2 in Lang's Conjecture 3 satisfy the inequalities

$$c_1 \geqslant \left(\frac{H(E)^{1/24} \cdot N^{\varepsilon(N)/2} \cdot \log N \cdot (2/\sqrt{3})^{1/2}}{\delta(P_1)}\right)^{-1},$$

$$c_2 \geqslant \left(\frac{H(E)^{1/12} \cdot N^{\varepsilon(N)} \cdot \log N \cdot c}{\delta(P_2)}\right)^{-1}.$$

On choosing $c = 1$ and putting, in analogy to the example on p. 166 of [6],

$$\varepsilon(N) = (\log N \cdot \log\log N)^{-1/2},$$

we obtain for the constants c_1 and c_2 the estimates††

$$c_1 \geqslant 0.021{,}784, \ldots, \qquad c_2 \geqslant 0.002{,}709, \ldots.$$

Here we let E range over the rank-two curves in [8] and take the maximal values for c_1 and c_2, which are attained at the curves with $A = 246$ and $A = 30$, respectively. For the sake of completeness, we include here the numerical estimates of the constants c_1 and c_2 for all values of A in Selmer's table [8] in order to show how c_1 and c_2 oscillate as A varies (see Table 3).

†† This estimation is based on the assumption that the points in Selmer's table [8] are of minimal height. We wish to thank M. Reichert for verifying this on a Siemens PC MX-2 for Selmer's curves with $A = 30$, 37, 65, 91, 110, 124, 126, 163, 182, 217, 254, 342, 468 and 469. Only for $A = 254$, the point $P_1 + P_2$ is to be taken instead of P_2 since it has a slightly smaller height value.

TABLE 3

19	0.00513126	0.00110389
30	0.0192703	0.00270903
37	0.00483937	0.000962382
65	0.00345923	0.00182501
86	0.00629273	0.00227975
91	0.0036522	0.000438337
110	0.012277	0.00153855
124	0.00374265	0.00174993
126	0.00433063	0.00114267
127	0.00414683	0.000940948
132	0.0183099	0.00244798
153	0.0105335	0.00111188
163	0.00458141	0.000483074
182	0.00445021	0.000517017
183	0.00524747	0.00199503
201	0.00511671	0.00120915
203	0.0095474	0.00116455
209	0.00721788	0.000812224
210	0.0126048	0.00121204
217	0.00308153	0.000319989
218	0.00327199	0.00201074
219	0.00500126	0.00171349
246	0.0217843	0.00193905
254	0.00531365	0.000936257
271	0.00370666	0.000782067
273	0.00472123	0.000663038
282	0.0182864	0.00183782
309	0.00457362	0.00227242
335	0.00274443	0.00165495
342	0.00352578	0.00103604
345	0.0142214	0.00141568
348	0.0175728	0.0019122
370	0.00282848	0.00117946
379	0.0038473	0.000711233
390	0.0111818	0.000859068
397	0.00349161	0.000596949
399	0.0042891	0.000624869
407	0.00267502	0.00118686
420	0.0121164	0.00107526
433	0.00518512	0.000522935
435	0.0139496	0.00147541
436	0.00482868	0.00160066
446	0.0041804	0.00145041
453	0.00415706	0.00168546
462	0.0108269	0.000877993
468	0.00388973	0.00098101
469	0.00339982	0.000304454
477	0.00744997	0.00111861
497	0.00531293	0.000907821
498	0.0171181	0.0014825

Fachbereich 9 Mathematik
Universität des Saarlandes
D-6600 Saarbrücken, West Germany

1. A. BREMNER & J. W. S. CASSELS, "On the equation $Y^2 = X^2(X + p)$," *Math. Comp.*, v. 42, 1984, pp. 257–264.

2. J. P. BUHLER, B. H. GROSS & D. B. ZAGIER, "On the conjecture of Birch and Swinnerton-Dyer for an ellliptic curve of rank 3," *Math. Comp.*, v. 44, 1985, pp. 473–481.

3. J. W. S. CASSELS, "Diophantine equations with special reference to elliptic curves," *J. London Math. Soc.*, v. 41, 1966, pp. 193–291.

4. H. G. FOLZ, *Ein Beschränktheitssatz für die Torsion von 2-defizienten elliptischen Kurven über algebraischen Zahlkörpern*, Ph.D. Thesis, Saarbrücken, 1985.

5. S. LANG, *Elliptic Curves: Diophantine Analysis*, Springer-Verlag, Berlin and New York, 1978.

6. S. LANG, "Conjectured Diophantine estimates on elliptic curves," *Progr. Math.*, v. 35, 1983, pp. 155–171.

7. S. LANG, *Fundamentals of Diophantine Geometry*, Springer-Verlag, Berlin and New York, 1983.

8. E. SELMER, "The Diophantine equation $ax^3 + by^3 + cz^3$," *Acta Math.*, v. 85, 1951, pp. 203–362.

9. J. H. SILVERMAN, "Lower bound for the canonical height on elliptic curves," *Duke Math. J.*, v. 48, 1981, pp. 633–648.

10. J. T. TATE, "The arithmetic of elliptic curves," *Invent. Math.*, v. 23, 1974, pp. 179–206.

11. J. T. TATE, "Algorithm for finding the type of a singular fibre in an elliptic pencil," in *Modular Functions of One Variable* IV, Lecture Notes in Math., vol. 476, Springer-Verlag, Berlin and New York, 1975, pp. 33–52.

12. J. T. TATE, Letter to J.-P. Serre, Oct. 1, 1979.

13. H. G. ZIMMER, "On the difference of the Weil height and the Néron-Tate height," *Math. Z.*, v. 147, 1976, pp. 35–51.

14. H. G. ZIMMER, "Quasifunctions on elliptic curves over local fields," *J. Reine Angew. Math.*, v. 307/308, 1979, pp. 221–246.

15. H. G. ZIMMER, "Torsion points on elliptic curves over a global field," *Manuscripta Math.*, v. 29, 1979, pp. 119–145.

16. *Modular Functions of One Variable* IV (B. J. Birch & W. Kuyk, eds.), Lecture Notes in Math., vol. 476, Springer-Verlag, Berlin and New York, 1975.