MATHEMATICS OF COMPUTATION
VOLUME 51, NUMBER 183
JULY 1988, PAGES 339-358

Computing Heights on Elliptic Curves*

By Joseph H. Silverman**

Abstract. We describe how to compute the canonical height of points on elliptic curves. Tate has given a rapidly converging series for Archimedean local heights over $\mathbf{R}$. We describe a modified version of Tate's series which also converges over $\mathbf{C}$, and give an efficient procedure for calculating local heights at non-Archimedean places. In this way we can calculate heights over number fields having complex embeddings. We also give explicit estimates for the tail of our series, and present several examples.

Let E be an elliptic curve defined over a number field K, say given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1}$$

The *canonical height* on E is a quadratic form

$$\hat{h}\colon E(K) \to \mathbf{R}.$$

(For the definition and basic properties of $\hat{h}$, see [11, VIII, Section 9] or [6, Chapter VI].) The canonical height is an extremely important theoretical tool in the arithmetic theory of elliptic curves, being used for such diverse purposes as studying values of L-functions [5], numbers of integral points [12], and transcendence theory [9]. It is also important as a computational tool, such as its use in Zagier's algorithm for finding integral points up to large bounds [18]. It is thus of interest to have an efficient method for calculating the canonical height of a point.

The usual definition of $\hat{h}$ as a limit $\hat{h}(P) = \lim_{n\to\infty} 4^{-n}h(x(2^nP))$ is not practical for computation. Instead, one uses the fact that the canonical height can be written as a sum of *local heights*, one term for each distinct absolute value on K:

$$\hat{h}(P) = \sum_{v\in M_K} n_v\hat{\lambda}_v(P). \tag{2}$$

(For example, if $K = \mathbf{Q}$, then M_K can be identified with the set of rational primes together with the usual absolute value on $\mathbf{Q}$. The multiplicities n_v are chosen so that the product formula holds and so that $\hat{h}$ is independent of the choice of the field K.) The local height corresponding to a non-Archimedean absolute value is given by intersection theory in a well-known manner. (See, e.g., [2], [4] or [7, Chapter 11, Section 5].) We will describe a quick way to compute non-Archimedean local heights in Section 5.

The local height for an Archimedean absolute value is given by a transcendental function, and so efficient computation is somewhat more difficult. J. Tate [15]

Received August 20, 1987; revised October 21, 1987.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11G05, 14K07, 11D25.

*This work was partially supported by NSF grant #DMS-8612393.

** *Current address*: Mathematics Department, Brown University, Providence, RI 02912.

©1988 American Mathematical Society
0025-5718/88 $1.00 + $.25 per page

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

has given an easily computed power series which works for real absolute values. Precisely, for a given curve E and point $P = (x, y)$, he gives a sequence of easily computed numbers $c_0, c_1, \ldots$ so that

$$\hat{\lambda}_v(P) = \tfrac{1}{2}\log|x|_v + \tfrac{1}{8}\sum_{n=0}^{\infty} 4^{-n} c_n;$$

and he shows that the c_n's are bounded *provided that there are no points on* $E(K_v)$ *with x-coordinate equal to* 0. (Here K_v, the completion of K at v, is either **R** or **C**.) If $K_v = \mathbf{R}$, then one can always ensure that $0 \notin x(E(K_v))$ by making an initial shift of coordinates $x' = x + r$ for some sufficiently large integer r. Thus, for computations over **Q**, Tate's series provides an efficient computational tool, producing an error on the order of 4^{-N} if one takes N terms of the sum. It has been used in this case by a number of people (e.g., [1], [13], [16]). Unfortunately, if $K_v = \mathbf{C}$, then the shifting trick no longer works; and it is possible for Tate's series to have poor convergence properties. (See the correction to [19] for a brief discussion.)

In Section 2 we will present a revised version of Tate's series which converges in all cases. The basic idea is as follows. We start, as Tate does, computing the sequence of coefficients $c_0, c_1, \ldots$ and the series $c_0 + 4^{-1}c_1 + \cdots$. However, if some c_{n+1} is going to be large, then we replace c_n by a different (still bounded) quantity, and switch over to a new sequence $c'_{n+1}, c'_{n+2}, \ldots$. This new sequence is essentially Tate's sequence for the parameter $x' = x + 1$. We continue with the new sequence, computing $\cdots + 4^{-n-1}c'_{n+1} + 4^{-n-2}c'_{n+2} + \cdots$, until some c'_{m+1} is going to be large. Then we replace c'_m with a corrected (bounded) value and switch back to the unprimed sequence. In this way we obtain a series for $\hat{\lambda}_v(P)$ which converges regardless of whether or not $0 \in x(E(K_v))$. As with Tate's series, the error in using only N terms is on the order of 4^{-N}. We will begin in Section 2 by proving that our series converges under the assumption that the local height function exists and has certain basic properties, since this makes the proof somewhat easier. Then in Sections 3 and 4 we will go back and make all of our estimates explicit, thereby giving an a priori proof that our series converges and obtaining practical error estimates. This also yields a new proof of the existence of the local height function for complex absolute values. (Tate's original series previously gave the existence for real absolute values.)

In the final section we give several examples.

1. Generalities on Local Heights and Tate's Series. Let K be a number field, and let E/K be an elliptic curve given by a Weierstrass equation (1). Associated with (1) are the usual quantities (cf. [11, Chapter III, Section 1])

$$\begin{gathered} b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6, \\ b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ c_4 = b_2^2 - 24b_4, \qquad c_6 = -b_2^3 + 36b_2b_4 - 216b_6, \\ \Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \end{gathered} \tag{3}$$

We also have the relation

$$(2y + a_1x + a_3)^2 = 4x^3 + b_2x^2 + 2b_4x + b_6. \tag{4}$$

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

If $P = (x, y)$ is a point of E, then the duplication formula [11, III.2.3d] reads

$$x(2P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}. \tag{5}$$

Let $|\cdot|_v$ be a nontrivial absolute value on K. Néron proved that there exists a unique function

$$\hat{\lambda}_v\colon E(K_v) \setminus \{O\} \to \mathbf{R},$$

called the *local height function on E associated with the absolute value v*, having the following three properties:

$$\hat{\lambda}_v(2P) = 4\hat{\lambda}_v(P) - \log|2y + a_1x + a_3|_v \qquad \text{for all } P = (x, y) \in E(K_v) \text{ with } 2P \neq O; \tag{6}$$

$$\lim_{P \to O} (\hat{\lambda}_v(P) - \tfrac{1}{2}\log|x(P)|_v) \text{ exists,} \qquad \text{where } P \to O \text{ in the } v\text{-adic topology;} \tag{7}$$

(8) $\hat{\lambda}_v$ is bounded on any v-adic open subset of $E(K_v)$ disjoint from O.

For a proof of the existence of $\hat{\lambda}_v$, see [6, Chapter I, Section 7, Chapter III, Section 4]; and for a proof that the canonical height $\hat{h}$ is the sum of the local heights (i.e., a proof of Eq. (2)), see [6, Chapter IV, Section 6]. The explicit estimates we derive in Section 4 will provide an alternative proof of the existence of $\hat{\lambda}$.

Remark. We remark that the local height is sometimes normalized slightly differently. Specifically, the duplication formula is often given with $\frac{1}{4}\log|\Delta|_v$ added onto the right-hand side. As the reader will easily verify, if we use $\hat{\lambda}'_v$ to denote this new local height, then $\hat{\lambda}_v = \hat{\lambda}'_v + \frac{1}{12}\log|\Delta|_v$. Thus there is little practical difference in which one we compute. Further, when adding up the local heights (2) to get the canonical height, the product formula will ensure that the extra term vanishes. From a computational viewpoint, we have found it slightly less cumbersome to compute $\hat{\lambda}_v$, although it seems that for theoretical purposes, $\hat{\lambda}'_v$ is often more useful.

Tate's idea [15] is to use $1/x$ as a parameter and to apply the relation (6) repeatedly to derive a series for $\hat{\lambda}$. More precisely, let

$$\begin{aligned} t &= 1/x, \\ w &= 4t + b_2t^2 + 2b_4t^3 + b_6t^4, \\ z &= 1 - b_4t^2 - 2b_6t^3 - b_8t^4. \end{aligned} \tag{9}$$

Substituting (9) and (4) into the duplication formula (5) yields formulas for $x(2P)$ and $t(2P)$,

$$\begin{aligned} x(2P) &= \frac{x^4 z}{(2y + a_1x + a_3)^2} = \frac{z}{w}, \\ t(2P) &= \frac{1}{x(2P)} = \frac{w}{z}. \end{aligned} \tag{10}$$

The former allows us to rewrite (6) as

$$\{\hat{\lambda}(2P) - \tfrac{1}{2}\log|x(2P)|_v\} = \{\hat{\lambda}(P) - \tfrac{1}{2}\log|x(P)|_v\} + \tfrac{1}{2}\log|z(P)|_v.$$

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

Following Tate, we define a new function μ by the formula

$$\tfrac{1}{8}\mu(P) = \hat{\lambda}(P) - \tfrac{1}{2}\log|x(P)|_v. \tag{11}$$

(If $x(P) = 0$, we will formally set $\mu(P) = \infty$; while we can define $\mu(O)$ to equal $\lim_{Q\to O}\mu(Q)$, which exists by (7).) From above, μ satisfies the duplication formula

$$\mu(2P) = 4\mu(P) - 4\log|z(P)|_v \quad \text{for } P \in E(K_v) \text{ with } x(P), x(2P) \neq 0. \tag{12}$$

Now rewriting (12) as $\mu = \log|z|_v + 4^{-1}\mu \circ [2]$ and substituting it into itself repeatedly gives the formula

$$\mu(P) = \sum_{n=0}^{N} 4^{-n}\log|z(2^nP)|_v + 4^{-N}\mu(2^NP), \tag{13}$$

valid provided that $x(2^nP) \neq 0$ for $n = 0, 1, \ldots, N$. It is natural to let N tend to ∞, thereby obtaining a series for $\mu(P)$, provided that the remainder $4^{-N}\mu(2^NP)$ goes to 0. Tate describes conditions under which this limiting procedure is valid. (Notice that the sequence $z(2^nP)$, $n = 1, 2, \ldots$, is easily computed using (10) and (9).)

LEMMA 1.1. *For any $\varepsilon > 0$, let*

$$V_\varepsilon = \{Q \in E(K_v)\colon |x(Q)|_v \geq \varepsilon\} = \{Q \in E(K_v)\colon |t(Q)|_v \leq \varepsilon^{-1}\}.$$

(a) *μ is bounded on V_ε.*

(b) *$\log|z|_v$ is bounded on $\{Q \in V_\varepsilon\colon 2Q \in V_\varepsilon\}$.*

Proof (under the assumption that $\hat{\lambda}$ exists). (a) From (7) and (11), $\mu(P)$ approaches a limit as $P \to O$; so there is a constant c such that μ is bounded on V_c. (Note that $\bigcap_{c>0} V_c = \{O\}$.) On the other hand, (8) says that $\hat{\lambda}$ is bounded on $\{Q\colon c \geq |x(Q)|_v\}$, while $\log|x|_v$ is clearly bounded on $\{Q\colon c \geq |x(Q)|_v \geq \varepsilon\}$. It follows that μ is bounded on V_ε.

(b) This is immediate from (a) and the duplication formula (12). □

THEOREM 1.2 (TATE). *Suppose that there is an $\varepsilon > 0$ so that every point Q in $E(K_v)$ satisfies $|x(Q)|_v > \varepsilon$. Then for all $P \in E(K_v) \setminus \{O\}$,*

$$\hat{\lambda}(P) = \tfrac{1}{2}\log|x(P)|_v + \tfrac{1}{8}\sum_{n=0}^{\infty} 4^{-n}\log|z(2^nP)|_v.$$

Further, the error in taking only N terms of the sum is $O(4^{-N})$.

Proof. By assumption, there is an $\varepsilon > 0$ so that in the notation of Lemma 1.1, $E(K_v) = V_\varepsilon$. In particular, Lemma 1.1(a) says that $\mu(2^NP)$ is bounded independently of N. From (13) we obtain the estimate

$$\mu(P) = \sum_{n=0}^{N} 4^{-n}\log|z(2^nP)|_v + O(4^{-N}).$$

This and the definition of μ (11) give both parts of Theorem 1.2. □

Remark. Tate actually proceeds somewhat differently. He proves directly that the series in Theorem 1.2 converges and has the properties (6), (7), (8), thereby proving simultaneously that $\hat{\lambda}$ exists and is given by his series. (Always, of course,

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

under the conditions of Theorem 1.2.) In the next section we will give a modification of Tate's series which converges to $\hat{\lambda}$ with no conditions being imposed on $E(K_v)$. Then in Section 3 we will give explicit estimates for the boundedness in Lemma 1.1(b) and for some similar quantities used in our modified series. Using these, the reader may construct an a priori proof of the existence of $\hat{\lambda}$, valid for any local field K_v.

2. A Universally Convergent Series for the Local Height. Tate's series (Theorem 1.2) converges provided that $E(K_v)$ has no points with $x = 0$. More precisely, Tate's series behaves well for P unless some multiple 2^nP has small x-coordinate. Our idea is to use Tate's series until hitting some multiple with $x(2^nP)$ small. At that time, we make the substitution $x' = x + 1$. Then $x'(2^nP)$ is not small, so we start using Tate's series associated with the parameter $t' = 1/x'$. (This requires a little juggling of the nth term in Tate's series.) We proceed using the t' series until $x'(2^mP)$ is small, at which time we switch back to the t series.

In order to derive the formulas describing this switching procedure, we start with the well-known description of how the various quantities associated with a Weierstrass equation (1) change under the substitution $x' = x + 1$ (cf. [11, Chapter III, Section 1] or [14]):

$$\begin{aligned} &x' = x+1, && x = x'-1,\\ &t' = t/(1+t), && t = t'/(1-t'),\\ &b_2' = b_2 - 12, && b_6' = b_6 - 2b_4 + b_2 - 4,\\ &b_4' = b_4 - b_2 + 6, && b_8' = b_8 - 3b_6 + 3b_4 - b_2 + 3,\\ &w' = 4t' + b_2't'^2 + 2b_4't'^3 + b_6't'^4, && z' = 1 - b_4't'^2 - 2b_6't'^3 - b_8't'^4, \end{aligned} \tag{14}$$

$$t'(2P) = \frac{4t' + b_2't'^2 + 2b_4't'^3 + b_6't'^4}{1 - b_4't'^2 - 2b_6't'^3 - b_8't'^4} = \frac{w'}{z'}.$$

As with the original equation, we define μ' by

$$\tfrac{1}{8}\mu' = \hat{\lambda} - \tfrac{1}{2}\log|x'|_v; \tag{15}$$

so μ' satisfies the duplication formula

$$\mu'(2P) = 4\mu'(P) - 4\log|z'(P)|_v. \tag{16}$$

Since $\hat{\lambda}$ is independent of any shifting of x, we see that

$$\tfrac{1}{8}(\mu - \mu') = \tfrac{1}{2}\log|x'/x|_v = \tfrac{1}{2}\log|t/t'|_v.$$

Using (14), this yields

$$\mu = \mu' + 4\log|1+t|_v, \qquad \mu' = \mu + 4\log|1-t'|_v. \tag{17}$$

As indicated above, our idea is to switch back and forth between μ and μ'. To do this, we derive the following "mixed" duplication formula involving both μ and

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

μ':

$$\begin{aligned}\mu(Q) &= \log|z(Q)|_v + \tfrac{1}{4}\mu(2Q) && \text{from (12)}\\ &= \log|z(Q)|_v + \tfrac{1}{4}\{\mu'(2Q) + 4\log|1+t(2Q)|_v\} && \text{from (17)}\\ &= \log|z(Q)|_v + \log|1+w(Q)/z(Q)|_v + \tfrac{1}{4}\mu'(2Q) && \text{from (10)}\\ &= \log|z(Q)+w(Q)|_v + \tfrac{1}{4}\mu'(2Q).\end{aligned}$$

A similar calculation expresses $\mu'(Q)$ in terms of $\mu(2Q)$, giving us the two formulas

$$\begin{aligned}\mu(Q) &= \log|z(Q)+w(Q)|_v + \tfrac{1}{4}\mu'(2Q),\\ \mu'(Q) &= \log|z'(Q)-w'(Q)|_v + \tfrac{1}{4}\mu(2Q).\end{aligned} \tag{18}$$

Now repeated application of these mixed duplication formulas, together with the usual ones (10) and (14), will give a convergent series for $\hat{\lambda}$. We start with an estimate, analogous to Lemma 1.1, for the quantities $\log|z+w|_v$ and $\log|z'-w'|_v$ appearing in (18).

LEMMA 2.1. *With notation as above, define two subsets U and U' of $E(K_v)$ by*

$$U = \{Q \in E(K_v)\colon |t(Q)|_v \le 2\}, \qquad U' = \{Q \in E(K_v)\colon |t'(Q)|_v \le 2\}.$$

(a) $E(K_v) = U \cup U'$.

(b) *There exists a constant c so that for all $Q \in E(K_v)$,*

$$\begin{aligned}&\text{(i)} && Q, 2Q \in U \Rightarrow |\log|z(Q)|_v| \le c;\\ &\text{(ii)} && Q \in U, 2Q \in U' \Rightarrow |\log|z(Q)+w(Q)|_v| \le c;\\ &\text{(iii)} && Q, 2Q \in U' \Rightarrow |\log|z'(Q)|_v| \le c;\\ &\text{(iv)} && Q \in U', 2Q \in U \Rightarrow |\log|z'(Q)-w'(Q)|_v| \le c.\end{aligned}$$

Proof. (a) Suppose that $Q \in E(K_v)$ is not in U. Then $t(Q) > 2$, so

$$|t'(Q)|_v = \left|\frac{t(Q)}{1+t(Q)}\right|_v \le \frac{1}{1-|t(Q)|_v^{-1}} \le 2.$$

Therefore $Q \in U'$.

(b) First we note that (i) and (iii) are special cases of Lemma 1.1(b). Next, to prove (ii), we apply Lemma 1.1(a), which says that $\mu(Q)$ and $\mu'(2Q)$ are bounded independently of Q (subject to $Q \in U$ and $2Q \in U'$.) Now (18) shows that

$$\log|z(Q)+w(Q)|_v = \mu(Q) - \tfrac{1}{4}\mu'(2Q)$$

is similarly bounded. This proves (ii). We leave the analogous proof of (iv) to the reader. □

We are now ready to define a sequence of real numbers $c_0, c_1, \ldots$, depending on a given point $P \in E(K_v)$, so that $\mu(P) = \sum 4^{-n}c_n$. In order to decide which of the duplication formulae (12), (16), (18) to use, we will assign to each real number c_n a Boolean value, which we denote by β_n. Thus β_n will be 0 if c_n was computed using the series for μ', and it will be 1 if c_n comes from the series for μ. (To assist in the implementation of this theorem, we also provide a pseudocode subroutine.)

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

SUBROUTINE to Calculate Local Height of P at an Archimedean Absolute Value

```
PARAMETERS needed by the subroutine
    $b_2, b_4, b_6, b_8$                        Weierstrass coefficients
    $x$                                          $x$-coordinate of point $P$
    $N$                                          # of terms of sum to compute
Calculate $b'_2, b'_4, b'_6, b'_8$               formulas given below
IF $|x| \geq \frac{1}{2}$
    $t = 1/x$                                    $P \in U$
    $\beta = 1$
ELSE                                             $P \in U', P \notin U$
    $t = 1/(x+1)$
    $\beta = 0$
END IF
$\lambda = -\frac{1}{2}\log|t|$: $n = 0$: $\mu = 0$
LOOP WHILE $n \leq N$
    IF $\beta = 1$
        Compute $w$ and $z$                      formulas given below
        IF $|w| \leq 2|z|$                       $2^nP, 2^{n+1}P \in U$
            $\mu = \mu + 4^{-n}\log|z|$
            $t = w/z$
        ELSE                                     $2^nP \in U, 2^{n+1}P \notin U$
            $\mu = \mu + 4^{-n}\log|z+w|$
            $t = w/(z+w)$
            $\beta = 1 - \beta$
        END IF
    ELSE $\boxed{\beta = 0}$
        Compute $w'$ and $z'$                    formulas given below
        IF $|w'| \leq 2|z'|$                     $2^nP, 2^{n+1}P \in U'$
            $\mu = \mu + 4^{-n}\log|z'|$
            $t = w'/z'$
        ELSE                                     $2^nP \in U', 2^{n+1}P \notin U'$
            $\mu = \mu + 4^{-n}\log|z' - w'|$
            $t = w'/(z' - w')$
            $\beta = 1 - \beta$
        END IF
    END IF
$n = n + 1$
END LOOP
$\lambda = \lambda + \frac{1}{8}\mu$
RETURN $(\lambda)$                               = local height with error $O(4^{-N})$
```

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

$b_2' = b_2 - 12$	$b_6' = b_6 - 2b_4 + b_2 - 4$
$b_4' = b_4 - b_2 + 6$	$b_8' = b_8 - 3b_6 + 3b_4 - b_2 + 3$
$w = 4t + b_2t^2 + 2b_4t^3 + b_6t^4$	$w = 4t + b_2't^2 + 2b_4't^3 + b_6't^4$
$z = 1 - b_4t^2 - 2b_6t^3 - b_8t^4$	$z = 1 - b_4't^2 - 2b_6't^3 - b_8't^4$

THEOREM 2.2. *Define a sequence of real numbers $c_{-1}, c_0, \dots$ and a sequence of Boolean values $\beta_{-1}, \beta_0, \dots$ as follows*:

$$c_{-1}, \beta_{-1} = \begin{cases} -\log|t(P)|_v, 1 & \text{if } P \in U, \\ -\log|t'(P)|_v, 0 & \text{if } P \notin U; \end{cases}$$

$$c_n, \beta_n = \begin{cases} \log|z(2^nP)|_v, 1 & \text{if } \beta_{n-1} = 1 \text{ and } 2^{n+1}P \in U, \\ \log|z(2^nP) + w(2^nP)|_v, 0 & \text{if } \beta_{n-1} = 1 \text{ and } 2^{n+1}P \notin U, \\ \log|z'(2^nP)|_v, 1 & \text{if } \beta_{n-1} = 0 \text{ and } 2^{n+1}P \in U', \\ \log|z'(2^nP) - w'(2^nP)|_v, 0 & \text{if } \beta_{n-1} = 0 \text{ and } 2^{n+1}P \notin U'. \end{cases}$$

(a) $\hat{\lambda}(P) = \frac{1}{2}c_{-1} + \frac{1}{8}\sum_{n=0}^{\infty} 4^{-n}c_n$.

(b) *More precisely,*

$$\hat{\lambda}(P) = \frac{1}{2}c_{-1} + \frac{1}{8}\sum_{n=0}^{N-1} 4^{-n}c_n + O(4^{-N})$$

for a big-O constant independent of both N and P.

Remark. An explicit expression for the $O(4^{-N})$ error term is given below in Theorem 4.2.

Proof. Using either (11) or (15), depending on whether or not $P \in U$, we see that

$$\hat{\lambda}(P) = \tfrac{1}{2}c_{-1} + \begin{cases} \frac{1}{8}\mu(P) & \text{if } P \in U, \\ \frac{1}{8}\mu'(P) & \text{if } P \notin U. \end{cases}$$

We then repeatedly apply the duplication formulas (12), (16) and (18), following the instructions provided above for producing the c_n's. After N steps, this leads to the equation

$$\hat{\lambda}(P) = \tfrac{1}{2}c_{-1} + \tfrac{1}{8}\sum_{n=0}^{N-1} 4^{-n}c_n + \begin{cases} 4^{-N}\mu(2^NP) & \text{if } \beta_N = 1, \\ 4^{-N}\mu'(2^NP) & \text{if } \beta_N = 0. \end{cases}$$

Further, one easily checks that

$$\beta_N = 1 \Rightarrow P \in U,$$
$$\beta_N = 0 \Rightarrow P \in U'.$$

(Remember that $U \cup U' = E(K_v)$ from Lemma 2.1(a).) But Lemma 1.1(a) says that $\mu(Q)$ (respectively $\mu'(Q)$) is bounded for $Q \in U$ (respectively $Q \in U'$). Hence in both cases we obtain the desired estimate, thereby proving (b). Then (a) follows immediately on letting N tend to ∞. □

3. Some Resultant Results. In this section we prove two results concerning resultants which will be used in the next section to derive explicit error estimates for our local height series. We start by computing the resultant of the two polynomials (9) which are used in Tate's series. We will sketch three quite different proofs.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

PROPOSITION 3.1. *Let $z(T)$ and $w(T)$ be the usual polynomials* (9),

$$z(T) = 1 - b_4T^2 - 2b_6T^3 - b_8T^4, \qquad w(T) = 4T + b_2T^2 + 2b_4T^3 + b_6T^4;$$

and let Δ be the discriminant of the Weierstrass equation (1), *given by formula* (3). *Then*

$$\operatorname{Res}(z(T), w(T)) = \Delta^2,$$

where $\operatorname{Res}(z(T), w(T))$ *denotes the resultant of $z(T)$ and $w(T)$.*

Proof (version 1, quick and dirty). Compute the resultant directly from the definition as an 8×8 determinant, either by hand (ugh!) or using a symbolic processor like MACSYMA.

Proof (version 2, elegant but a lot of machinery). Consider the projective scheme $\mathscr{E}$ given by the equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

over the ring $\mathscr{R} = \mathbf{Z}[a_1, a_2, a_3, a_4, a_6, \Delta^{-1}]$, where b_2, b_4, b_6, b_8 and Δ are given by (3). Then $\mathscr{E}$ is a group scheme over $\mathscr{R}$ (see, for example, [3, §7]), and the doubling map $[2]\colon \mathscr{E} \to \mathscr{E}$ is a finite morphism which descends to a finite morphism $\phi\colon \mathbf{P}^1_{\mathscr{R}} \to \mathbf{P}^1_{\mathscr{R}}$ (i.e., $\phi \circ [X, Z] = [X, Z] \circ [2]$). The map ϕ is given by $[1, T] \to [z(T), w(T)]$. Since ϕ is finite, the resultant of $z(T)$ and $w(T)$ must be a *unit* in $\mathscr{R}$. Therefore,

$$\operatorname{Res}(z(T), w(T)) = \pm\Delta^r$$

for some integer r. To find r and the proper sign, one can explicitly calculate the special case $a_1 = a_2 = a_3 = a_4 = 0$, $a_6 = A$, which gives a very sparse 8×8 matrix to compute. (Alternatively, assigning weights $wt(a_i) = i$, it is easy to see that Δ and $\operatorname{Res}(z, w)$ are homogeneous of weights 12 and 24, respectively; so $r = 2$ is immediate.)

Proof (version 3, straightforward calculation). Let $f(x) = 4x^3 + b_2x^2 + b_4x + b_6$. Then the doubling formula (5) can be written as

$$x \circ [2] = \frac{(\frac{1}{4}f'(x))^2 - (a_2 + 2x)f(x)}{f(x)} = \frac{x^4z(1/x)}{x^4w(1/x)}.$$

(This is easily derived from the geometric definition of the group law [11, Chapter III, Section 2].) If we factor $f(x)$ as $4(x - \alpha)(x - \beta)(x - \gamma)$, then the roots of $w(T)$ are 0, α^{-1}, β^{-1} and γ^{-1}. A standard formula for the resultant ([17, Section 5.9]) gives

$$\begin{aligned}\operatorname{Res}(w(T), z(T)) &= b_6^4 \cdot z(0) \cdot z(\alpha^{-1}) \cdot z(\beta^{-1}) \cdot z(\gamma^{-1}) \\ &= b_6^4 \cdot 1 \cdot \alpha^{-4}(\tfrac{1}{4}f'(\alpha))^2 \cdot \beta^{-4}(\tfrac{1}{4}f'(\beta))^2 \cdot \gamma^{-4}(\tfrac{1}{4}f'(\gamma))^2 \\ &= 4^{-6}(b_6/\alpha\beta\gamma)^4(f'(\alpha)f'(\beta)f'(\gamma))^2.\end{aligned}$$

Note that $b_6 = -4\alpha\beta\gamma$. Further,

$$f'(\alpha)f'(\beta)f'(\gamma) = \tfrac{1}{4}\operatorname{Disc}(f) = -4\Delta.$$

(The first equality is [17, Section 5.9], the second follows from [17, Section 5.7] and (3).) Substituting these in above gives the desired result. □

It is clear that if two polynomials have distinct roots, then they cannot be simultaneously small. The following standard sort of result quantifies this observation. For lack of a suitable reference, we sketch a proof.

Notation. For $F(X) = \sum A_iX^i \in \mathbf{C}[X]$, let $|F| = \max\{|A_i|\}$.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

LEMMA 3.2. *Let* $F(X), G(X) \in \mathbf{C}[X]$, $\deg(F) = m$, $\deg(G) = n$. *Then for all* $x \in \mathbf{C}$,

$$\max\left\{\frac{|F(x)|}{|F|}, \frac{|G(x)|}{|G|}\right\} \geq \frac{|\mathrm{Res}(F,G)|}{2^{mn}|F|^n|G|^m} \min\left\{\frac{1}{2^m(m+1)^{n-1}}, \frac{1}{2^n(n+1)^{m-1}}\right\}.$$

Proof. By homogeneity, it suffices to prove the lemma for monic polynomials. (Note that $\mathrm{Res}(c_1F, c_2G) = c_1^n c_2^m \mathrm{Res}(F,G)$.) Write

$$F(X) = \sum A_i X^i = \prod (X - \alpha_j), \qquad G(X) = \sum B_i X^i = \prod (X - \beta_j).$$

Let $x \in \mathbf{C}$. Switching F and G and relabeling the roots if necessary, we may assume that

$$\min_{1 \leq j \leq m} |x - \alpha_j| \geq \min_{1 \leq j \leq n} |x - \beta_j| = |x - \beta_1|. \tag{19}$$

There is a formula for the resultant [17, Section 5.9] of the form

$$\mathrm{Res}(F,G) = \prod_{j=1}^{n} F(\beta_j). \tag{20}$$

For any $z \in \mathbf{C}$, let $|z,1|$ denote the maximum of $|z|$ and 1. We have the trivial bound

$$|F(x)| \leq (m+1)|F|\,|x,1|^m \quad \text{for all } x \in \mathbf{C}; \tag{21}$$

and in [7, Chapter 3, Lemma 2.1] we find the estimate

$$\prod_{j=1}^{n} |\beta_j, 1| \leq 2^n |G|. \tag{22}$$

Using these, we calculate

$$\begin{aligned} |F(\beta_1)| &= |\mathrm{Res}(F,G)| \Big/ \prod_{j=2}^{n} |F(\beta_j)| \quad \text{using (20)} \\ &\geq |\mathrm{Res}(F,G)| \Big/ \prod_{j=2}^{n} (m+1)|F|\,|\beta_j,1|^m \quad \text{using (21)} \\ &\geq |\mathrm{Res}(F,G)|/((m+1)|F|)^{n-1} 2^{mn} |G|^m \quad \text{using (22).} \end{aligned} \tag{23}$$

Finally,

$$\begin{aligned} |F(x)| &\geq \prod_{j=1}^{m} \tfrac{1}{2}|x - \alpha_j| + \tfrac{1}{2}\{|\beta_1 - \alpha_j| - |x - \beta_1|\} \quad \text{triangle inequality} \\ &\geq \prod_{j=1}^{m} \tfrac{1}{2}|\beta_1 - \alpha_j| \quad \text{from (19)} \\ &= 2^{-m}|F(\beta_1)|. \end{aligned}$$

Combining this with (23) gives the desired result. □

4. Explicit Error Estimates. We now use the estimates from the last section to give an explicit bound for the tail of the series in Theorem 2.2. Although this bound will not be sharp, we will see below that from a computational viewpoint there is little reason to search for a sharp bound. (See the remark following the statement of Theorem 4.2.) We begin by reproving Lemma 2.1 with specific values in place of the undetermined constants. As usual, let b_2, b_4, b_6, b_8 and Δ be the quantities (3) associated with the Weierstrass equation (1).

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

LEMMA 4.1. *Let U and U' be the sets described in Lemma* 2.1 *and define the quantity H by*

$$H = \max\{4, |b_2|, 2|b_4|, 2|b_6|, |b_8|\}.$$

Let $Q \in E(K_v)$. Then

$$\text{(i)} \qquad Q, 2Q \in U \Rightarrow |\Delta|_v^2/2^{28}H^8 \le |z(Q)|_v \le 2^6 H;$$

$$\text{(ii)} \qquad Q \in U, 2Q \in U' \Rightarrow |\Delta|_v^2/2^{28}H^8 \le |z(Q)+w(Q)|_v \le 2^7 H;$$

$$\text{(iii)} \qquad Q, 2Q \in U' \Rightarrow |\Delta|_v^2/2^{60}H^8 \le |z'(Q)|_v \le 2^{10} H;$$

$$\text{(iv)} \qquad Q \in U', 2Q \in U \Rightarrow |\Delta|_v^2/2^{60}H^8 \le |z'(Q)-w'(Q)|_v \le 2^{11} H.$$

Proof. First we apply Lemma 3.2 to the polynomials $w(t)$ and $z(t)$, using Proposition 3.1 for the value of their resultant. Since $|w| \ge 1$ and $|z| \ge 1$, it follows that for all $t \in \mathbf{C}$,

$$\max\{|w(t)|_v, |z(t)|_v\} \ge \frac{|\Delta|_v^2}{2^{16}H^4H^4} \min\left\{\frac{1}{2^4 5^3}, \frac{1}{2^4 5^3}\right\} \ge \frac{|\Delta|_v^2}{2^{27}H^8}. \tag{24}$$

(i) Let $t = t(Q)$. By assumption, $Q \in U$, so $|t|_v \le 2$. This gives the trivial estimate

$$|z(Q)|_v = |1 - b_4t^2 - 2b_6t^3 - b_8t^4|_v \le 4H|t,1|_v^4 \le 2^6 H. \tag{25}$$

On the other hand, since $2Q \in U$, we have $|t(2Q)|_v \le |w(Q)/z(Q)|_v \le 2$. Now using (24) gives

$$|z(Q)|_v \ge \tfrac{1}{2}\max\{|z(Q)|_v, |w(Q)|_v\} \ge |\Delta|_v^2/2^{28}H^8.$$

(ii) Since $Q \in U$, we again get the estimate (25), and by a similar calculation, $|w(Q)|_v \le 2^6 H$. This gives the upper bound

$$|z(Q)+w(Q)|_v \le |z(Q)|_v + |w(Q)|_v \le 2^7 H.$$

Next, since $2Q \in U'$, we have

$$2 \ge |t'(2Q)|_v = \left|\frac{t(2Q)}{1+t(2Q)}\right|_v = \left|\frac{w(Q)}{z(Q)+w(Q)}\right|_v,$$

so

$$|z(Q)+w(Q)|_v \ge \tfrac{1}{2}|w(Q)|_v.$$

Now using this, a trivial estimate and (24), we obtain

$$\begin{aligned} |z(Q)+w(Q)|_v &\ge \max\{|z(Q)+w(Q)|_v, \tfrac{1}{2}|w(Q)|_v\} \\ &\ge \tfrac{1}{2}\max\{|z(Q)|_v, |w(Q)|_v\} \\ &\ge |\Delta|_v^2/2^{28}H^8. \end{aligned}$$

(iii) and (iv). These are proven in exactly the same manner as (i) and (ii), but with H replaced by

$$\begin{aligned} H' &= \max\{4, |b_2'|_v, 2|b_4'|_v, 2|b_6'|_v, |b_8'|_v\} \\ &\le \max\{4, |b_2|_v + 12, |b_4|_v + |b_2|_v + 6, |b_6|_v + 2|b_4|_v + |b_2|_v + 4, \\ &\qquad\qquad |b_8|_v + 3|b_6|_v + 3|b_4|_v + |b_2|_v + 3\} \\ &\le 16H. \end{aligned}$$

Substituting 2^4H for H in the bounds for (i) and (ii) gives (iii) and (iv). □

We are now ready for our main error analysis.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

THEOREM 4.2. *Let $\{c_n\}$ be the sequence described in Theorem* 2.2.

(a) *For all* $n \geq 0$,

$$\log | |\Delta|_v^2 / 2^{60} H^8 | \leq c_n \leq \log(2^{11} H).$$

(b) *Define the error term* $R(N)$ *by*

$$\hat{\lambda}_v(P) = \tfrac{1}{2} c_{-1} + \tfrac{1}{8} \sum_{n=0}^{N-1} 4^{-n} c_n + R(N).$$

Then

$$\tfrac{1}{6} \cdot 4^{-N} \cdot \log | |\Delta|_v^2 / 2^{60} H^8 | \leq R(N) \leq \tfrac{1}{6} \cdot 4^{-N} \cdot \log(2^{11} H).$$

(c) *In order to make* $|R(N)|$ *less than* $\frac{1}{2} \cdot 10^{-d}$ (*i.e., to calculate* $\hat{\lambda}$ *to* d *decimal places*), *it suffices to take*

$$N \geq \tfrac{5}{3} d + \tfrac{1}{2} + \tfrac{3}{4} \log(7 + \tfrac{4}{3} \log H + \tfrac{1}{3} \log \max\{1, |\Delta|_v^{-1}\}).$$

Example 4.3. Suppose that we wish to calculate $\hat{\lambda}_v(P)$ to 50 decimal places for a curve whose coefficients satisfy $H \leq 10^{100}$ and $|\Delta|_v \geq 10^{-100}$. Then part (c) of the theorem says that it suffices to take 89 terms in the series $\sum 4^{-n} c_n$. Suppose now that by a more careful analysis we were able to replace the bounds $\Delta^2 / 2^{60} H^8$ and $2^{11} H$ in Lemma 4.1 by just H. (It seems very unlikely that this large an improvement is even possible.) Then the estimate in Theorem 4.2(c) could be replaced by

$$N \geq \tfrac{5}{3} d + \tfrac{1}{2} + \tfrac{3}{4} \log \tfrac{1}{8} \log H;$$

and this means that in the problem just posed we would only need to use 87 terms to compute $\hat{\lambda}_v(P)$ to 50 decimal places. Thus, for the purpose of giving error estimates for our series, there seems little point in bothering to improve the coarse bounds in Lemma 4.1. (Of course, for other applications, such as giving explicit estimates for the difference of the canonical and Weil heights, more accurate bounds are important. See, for example, [16, Section 3].)

Proof of Theorem 4.2. (a) Comparing the description of the sequence $\{c_n\}$ in Theorem 2.2 with the conditions (i)–(iv) in Lemma 4.1 above, we see that $\exp(c_n)$ satisfies one of the inequalities (i)–(iv). Taking logarithms gives the desired result.

(b) From the definition of $R(N)$,

$$R(N) = \tfrac{1}{8} \sum_{n=N}^{\infty} 4^{-n} c_n \leq \tfrac{1}{8} \left(\sum_{n=N}^{\infty} 4^{-n} \right) \sup_{n \geq N} \{c_n\} = \tfrac{1}{8} \cdot \tfrac{4}{3} \cdot 4^{-N} \cdot \sup_{n \geq N} \{c_n\}.$$

Similarly, $R(N) \geq \frac{1}{6} \cdot 4^{-N} \cdot \inf\{c_n\}$. Substituting in the estimate for c_n obtained in (a) yields something stronger than (b).

(c) Using (b), we see that it suffices to take N satisfying

$$N \geq (\log_4 10) d + \tfrac{1}{2} + \log_4 \tfrac{1}{6} \log \max\{2^{11} H, 2^{60} H^8 / |\Delta|_v^2\}.$$

An elementary calculation shows that this is weaker than the condition imposed by (c). □

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

5. Local Height for Non-Archimedean Valuations. Suppose now that $v \in M_K$ is a non-Archimedean absolute value, and let

$$\mathrm{ord}_v \colon K_v^* \xrightarrow{\text{onto}} \mathbf{Z}$$

be the corresponding normalized valuation. Thus, if the residue field at v has order q_v, then

$$\log|x|_v = -\frac{1}{[K_v : \mathbf{Q}_v]} \mathrm{ord}_v(x) \log(q_v) \quad \text{for all } x \in K_v^*.$$

(See, e.g., [7, Chapter 1, Section 2].)

Let E/K be an elliptic curve given by a Weierstrass equation (1), and let $P = (x, y) \in E(K)$. We wish to compute $\hat{\lambda}_v(P)$, the local height of P at v. The first step is to replace (1) by an equation which is minimal at v (cf. [11, Chapter VII, Section 1]). An efficient way to do this is given by an algorithm of Laska [8]. (As formulated in [8], Laska's algorithm gives a global minimal Weierstrass equation, provided that K has class number 1. However, it is not hard to modify Laska's routine so as to produce an equation which is minimal for all $v \notin S$, where S is any set of places such that the ring of S-integers in K is a PID.) An alternative method for finding a minimal equation is to use the algorithm of Tate [14], but this is somewhat more complicated. (In fairness, it should be pointed out that Tate's algorithm also gives the reduction type and conductor of E at v, so it is in no way superseded by Laska's algorithm.) For the remainder of this section we will assume without further comment that the Weierstrass equation (1) is minimal at v.

If the reduction $\tilde{E}$ of E at v is nonsingular, then the local height is given by the simple formula

$$\hat{\lambda}_v(P) = \max\{0, -\tfrac{1}{2}\log|x|_v\}; \tag{26}$$

and more generally, this formula holds provided $\tilde{P}$ is a nonsingular point of $\tilde{E}$. (See [6, Chapter III, Theorem 4.3] for the proof when $\tilde{E}$ is smooth. However, the proof given in [6] works whenever $\tilde{P}$ is nonsingular. For general facts about the reduction of elliptic curves, see [11, Chapter VII].) $\tilde{P}$ will be nonsingular if and only if one of the partial derivatives of (1) at P does not vanish modulo v. Thus,

$$\begin{aligned} &\mathrm{ord}_v(3x^2 + 2a_2x + a_4 - a_1y) \le 0 \quad \text{or} \quad \mathrm{ord}_v(2y + a_1x + a_3) \le 0 \\ &\qquad\qquad\qquad\qquad \Rightarrow \hat{\lambda}_v(P) = \max\{0, -\tfrac{1}{2}\log|x|_v\}. \end{aligned} \tag{27}$$

Next suppose that E has multiplicative reduction at v. Referring to Tate's algorithm [14], this occurs if $\mathrm{ord}_v(\Delta) \ge 1$ and $\mathrm{ord}_v(c_4) = 0$. Let $N = \mathrm{ord}_v(\Delta)$. Then $E(K_v)/E_0(K_v)$ is cyclic of order N; and if P lies in the nth component (with $0 \le n < N$), then

$$\hat{\lambda}_v(P) = \frac{n(N-n)}{2N^2} \log|\Delta|_v. \tag{28}$$

(Here, $E_0(K_v)$ is the subset of $E(K_v)$ consisting of those points whose reduction is nonsingular. For a proof of (28), see [6, Chapter III, Theorem 5.1].) Our problem now is to compute n. Notice that (28) is invariant under the substitution $n \to N-n$, which corresponds to $P \to -P$. Further, we already know $\hat{\lambda}_v(P)$ from (26) if $n = 0$. We may thus assume that $0 < n \le \frac{1}{2}N$. An easy way to compute n is provided by the following lemma, which first appeared in the author's thesis [10].

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

LEMMA 5.1. *With notation as above,*

$$n = \min\{\mathrm{ord}_v(2y + a_1x + a_3), \tfrac{1}{2}\mathrm{ord}_v(\Delta)\}.$$

Proof. We substitute the formula (28) for P and $2P$ into the duplication formula for the local height (6). If $0 < n < \frac{1}{2}N$, then $\hat{\lambda}_v(2P)$ is given by (28) with $2n$ in place of n, so we obtain

$$\frac{2n(N-2n)}{2N^2}\log|\Delta|_v = 4\frac{n(N-n)}{2N^2}\log|\Delta|_v - \log|2y + a_1x + a_3|_v.$$

A little bit of algebra now yields

$$n = \frac{\log|2y + a_1x + a_3|_v}{\log|\Delta|_v}N = \mathrm{ord}_v(2y + a_1x + a_3).$$

Similarly, if $n = \frac{1}{2}N$, then $2P \in E_0(K_v)$, so (26) says that $\hat{\lambda}_v(2P) \geq 0$. Using this and (28) in (6) gives

$$\begin{aligned} 0 &\leq 4\frac{(N/2)(N-(N/2))}{2N^2}\log|\Delta|_v - \log|2y + a_1x + a_3|_v \\ &= \tfrac{1}{2}\log|\Delta|_v - \log|2y + a_1x + a_3|_v. \end{aligned}$$

Hence,

$$\mathrm{ord}_v(2y + a_1x + a_3) = \frac{\log|2y + a_1x + a_3|_v}{\log|\Delta|_v}\mathrm{ord}_v(\Delta) \geq \tfrac{1}{2}\mathrm{ord}_v(\Delta) = n.$$

(Note that $\log|\Delta|_v < 0$.) This completes the proof of Lemma 5.1. □

It remains to deal with the case that E has additive reduction at v and $\tilde{P}$ is singular. One approach is to compute successively nP for $n = 1, 2, 3, 4$, one of which is guaranteed to lie in $E_0(K_v)$. Then one can use (26) to compute $\hat{\lambda}_v(nP)$, and thence (6) and similar formulas to recover $\hat{\lambda}_v(P)$. This approach (with the relevant formulas) is given in [16]. For variety, we will describe a somewhat different approach which we feel is slightly more efficient. (Of course, if one has already implemented the group law on E, then it is probably just as easy to use [16]. However, we note that in the case of multiplicative reduction, this method may necessitate computing a large multiple of P; so for multiplicative reduction it is certainly preferable to use (28) in conjunction with Lemma 5.1.)

The algorithm we devise will depend on the duplication formula (6) and the corresponding triplication formula. To ease notation, we let

$$\begin{aligned} &\psi_2 = 2y + a_1x + a_3, \\ &\psi_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8. \end{aligned} \tag{29}$$

Thus, ψ_2 vanishes at the 2-torsion points of E, and ψ_3 vanishes at the 3-torsion points. The local height then satisfies the following two relations:

$$\hat{\lambda}_v(2P) = 4\hat{\lambda}_v(P) - \log|\psi_2(P)|_v, \tag{30}$$

$$\hat{\lambda}_v(3P) = 9\hat{\lambda}_v(P) - \log|\psi_3(P)|_v. \tag{31}$$

Suppose now that E has additive reduction at v and that $P \notin E_0(K_v)$. Referring to a table of reduction types such as given in [11, Table 15.1] or [14], we see that $\tilde{E}$ is one of the types III, IV, I_M^*, IV* or III*. From general theory (cf. [7] or [4]) one finds

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

that $\hat{\lambda}_v(P)$ is determined by the image of P in the finite group $\Phi \overset{\text{def}}{=} E(K_v)/E_0(K_v)$; and further, $\hat{\lambda}_v(-P) = \hat{\lambda}_v(P)$. We now consider three cases.

Case 1. $3P \in E_0(K_v)$. We must have type IV or IV* reduction, with $\Phi = \mathbf{Z}/3\mathbf{Z}$. Since P and $-2P$ have the same images in Φ, it follows that $\hat{\lambda}_v(2P) = \hat{\lambda}_v(P)$. Further, since $3P \in E_0(K_v)$, (26) says that $\hat{\lambda}_v(3P) \geq 0$. Substituting these facts into (30) and (31) and solving for $\hat{\lambda}_v(P)$ yields

$$\hat{\lambda}_v(P) = \tfrac{1}{3}\log|\psi_2(P)|_v \geq \tfrac{1}{9}\log|\psi_3(P)|_v. \tag{32}$$

Case 2. $2P \in E_0(K_v)$. In this case we have one of the reduction types III, III*, I_M^*; and P and $3P$ have the same image in Φ. Therefore, $\hat{\lambda}_v(3P) = \hat{\lambda}_v(P)$ and, since $2P \in E_0(K_v)$, $\hat{\lambda}_v(2P) \geq 0$. Substituting into (30) and (31) and solving gives

$$\hat{\lambda}_v(P) = \tfrac{1}{8}\log|\psi_3(P)|_v \geq \tfrac{1}{4}\log|\psi_2(P)|_v. \tag{33}$$

We now note that the inequalities in (32) and (33) cannot both hold. ($x(P)$ is v-integral since $P \notin E_0(K_v)$, and $\psi_2(P)$ is not a v-adic unit (27), so $|\psi_2(P)|_v < 1$ and $|\psi_3(P)|_v \leq 1$.) Hence we can use these inequalities to distinguish between the two cases.

Case 3. $2P, 3P \notin E_0(K_v)$. The only possibility is reduction type I_M^* with M odd, $\Phi = \mathbf{Z}/4\mathbf{Z}$, and the image of P generating Φ. Then P and $-3P$ have the same image in Φ, so $\hat{\lambda}_v(3P) = \hat{\lambda}_v(P)$. Substituting into (31) gives the same value for $\hat{\lambda}_v(P)$ as in Case 2,

$$\hat{\lambda}_v(P) = \tfrac{1}{8}\log|\psi_3(P)|_v.$$

Unfortunately, the inequality in (33) is no longer true. However, one can verify in this case (e.g., by using Tate's algorithm [14]) that

$$\mathrm{ord}_v\psi_2(P) = \tfrac{1}{2}(M+3) \quad \text{and} \quad \mathrm{ord}_v\psi_3(P) = M+4.$$

Hence the inequality in (32) does not hold; so in all cases we can use the inequality in (32) to decide whether $\hat{\lambda}_v(P)$ is given by (32) or (33).

Combining all of the above discussion, we obtain the following algorithm for computing the local height at a non-Archimedean place. (We also include pseudocode implementing this algorithm.)

THEOREM 5.2 (Local Height at Non-Archimedean Valuations). *Let E/K be an elliptic curve given by a Weierstrass equation* (1) *which is minimal at v, and let $P \in E(K_v)$. Also let ψ_2 and ψ_3 be the functions on E defined by* (29).

(a) *If*

$$\mathrm{ord}_v(3x^2 + 2a_2x + a_4 - a_1y) \leq 0 \quad \textit{or} \quad \mathrm{ord}_v(2y + a_1x + a_3) \leq 0,$$

then ($P \in E_0(K_v)$)

$$\hat{\lambda}_v(P) = \max\{0, -\tfrac{1}{2}\log|x(P)|_v\}.$$

(b) *Otherwise, if*

$$\mathrm{ord}_v(c_4) = 0,$$

then (*multiplicative reduction*)

$$N = \mathrm{ord}_v\Delta, \qquad n = \min\{\mathrm{ord}_v\psi_2(P), \tfrac{1}{2}\mathrm{ord}_v\Delta\},$$

$$\hat{\lambda}_v(P) = \frac{n(N-n)}{2N^2}\log|\Delta|_v.$$

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

(c) *Otherwise, if*

$$\operatorname{ord}_v \psi_3(P) \geq 3 \operatorname{ord}_v \psi_2(P),$$

then (*additive reduction of type* IV *or* IV*)

$$\hat{\lambda}_v(P) = \tfrac{1}{3} \log |\psi_2(P)|_v.$$

(d) *Otherwise* (*additive reduction of type* III, III*, *or* I$^*_M$)

$$\hat{\lambda}_v(P) = \tfrac{1}{8} \log |\psi_3(P)|_v.$$

SUBROUTINE to Calculate Local Height of P at a Non-Archimedean Absolute Value v

```
PARAMETERS needed by the subroutine
    $a_1, a_2, a_3, a_4, a_6$                          $\boxed{\textit{Minimal}\text{ Weierstrass coefficients}}$
    $x, y$                                             $\boxed{x, y\text{-coordinates of point } P}$
 Calculate $b_2, b_4, b_6, b_8, c_4, \Delta$           $\boxed{\text{see formulas (3)}}$
 $N = \operatorname{ord}_v(\Delta)$
 $A = \operatorname{ord}_v(3x^2 + 2a_2x + a_4 - a_1y)$
 $B = \operatorname{ord}_v(2y + a_1x + a_3)$
 $C = \operatorname{ord}_v(3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8)$
IF $A \leq 0$ OR $B \leq 0$                            $\boxed{P \in E_0(K_v)}$
    $\Lambda = \max\{0, -\frac{1}{2}\operatorname{ord}_v(x)\}$
ELSE IF $\operatorname{ord}_v(c_4) = 0$                $\boxed{\text{Type I}_N}$
    $n = \min\{B, \frac{1}{2}N\}$
    $\Lambda = -n(N-n)/2N$
ELSE IF $C \geq 3B$                                    $\boxed{\text{Types IV, IV}^*}$
    $\Lambda = -\frac{1}{3}B$
ELSE                                                   $\boxed{\text{Types III, III}^*,\ \text{I}^*_M}$
    $\Lambda = -\frac{1}{8}C$
END IF
RETURN $(\Lambda \log(q_v)/[K_v : \mathbf{Q}_v])$      $\boxed{= \hat{\lambda}_v(P)}$
```

6. Computing the Canonical Height: Examples. The canonical height $\hat{h}$ on an elliptic curve E defined over a number field K can be computed as the sum of local heights as described by Eq. (2), which we repeat here for reference:

$$\hat{h}(P) = \sum_{v \in M_K} n_v \hat{\lambda}_v(P).$$

To make this formula precise, we must specify the multiplicities n_v and the normalization of the absolute values in M_K (which affect the definition of $\hat{\lambda}_v$ via the duplication formula (7)). Let $M_{\mathbf{Q}}$ be the usual set of absolute values on $\mathbf{Q}$,

$$|p|_p = 1/p, \qquad |x|_\infty = \max\{x, -x\},$$

and let M_K be the set of all possible extensions to K of elements of $M_{\mathbf{Q}}$. This defines M_K; and then for $v \in M_K$, we set

$$n_v = [K_v : \mathbf{Q}_v]/[K : \mathbf{Q}].$$

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

We now use the algorithms given earlier (Theorems 2.2 and 5.2) to compute the canonical height for several specific examples.

Example 1. Let E be the elliptic curve

$$E\colon y^2+y=x^3-x^2.$$

As is well known, $E(\mathbf{Q})\cong\mathbf{Z}/5\mathbf{Z}$. (The reader may recognize that E is the modular curve $X_1(11)$.) We now look at E over the field $K=\mathbf{Q}(\sqrt{-2})$ and note that $E(K)$ contains the point

$$P=(2+\sqrt{-2},1+2\sqrt{-2})\in E(K).$$

We also compute

$$\Delta=-11=-(3+\sqrt{-2})(3-\sqrt{-2}),\qquad c_4=16=(\sqrt{-2})^8.$$

Since

$$(2y+1)(P)=3+4\sqrt{-2}\not\equiv 0 \pmod{3\pm\sqrt{-2}},$$

and $x(P)$ is integral (i.e., in $\mathbf{Z}[\sqrt{-2}]$), we see from Theorem 5.2 that $\hat{\lambda}_v(P)=0$ for all non-Archimedean $v\in M_K$.

It remains to compute $\hat{\lambda}_\infty(P)$, where ∞ is the (unique) Archimedean absolute value in M_K. We have done this by implementing the algorithm described in Theorem 2.2. In order to obtain 50 decimals of accuracy, Theorem 4.2 says to take $H=4$ (as specified in Lemma 4.1) and use N terms of the series, with

$$N\geq\tfrac{5}{3}\cdot 50+\tfrac{1}{2}+\tfrac{3}{4}\log(7+\tfrac{4}{3}\log H)=85.46\ldots.$$

Since we need less than 100 terms of the series, it suffices to calculate each term to (say) 55 decimals to avoid round-off errors in the final answer. Having done this calculation, we obtain the value

$$\hat{\lambda}_\infty(P)=0.45754773287523276736211210741423654346576029814695\ldots.$$

(As an aside, we remark that the algorithm started with $\beta=1$, switched to $\beta=0$ after 11 terms, and stayed there for the remainder of the computation.)

Finally we note that

$$n_\infty=[K_\infty\colon\mathbf{Q}_\infty]/[K\colon\mathbf{Q}]=[\mathbf{C}\colon\mathbf{R}]/[K\colon\mathbf{Q}]=1,$$

so

$$\hat{h}(P)=\hat{\lambda}_\infty(P)=0.45754773287523276736211210741423654346576029814695\ldots.$$

Example 2. Let E be the elliptic curve

$$E\colon y^2+4y=x^3+6ix,$$

which we consider over the field $K=\mathbf{Q}(i)$, where $i=\sqrt{-1}$. We compute for E the usual quantities (3),

$$b_2=0,\quad b_4=-i(1+i)^4 3,\quad b_6=(1+i)^8,\quad b_8=-(1+i)^4 3^2,$$
$$c_4=-(1+i)^{10}3^2,\qquad \Delta=-(1+i)^{16}3^3(1-2i).$$

It is clear that the equation for E is minimal at all primes except possibly $(1+i)$, since Δ has order less than 12 except at $(1+i)$. But b_8 only has order 4 at $(1+i)$, so the equation is minimal at $(1+i)$ also.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

We will compute the canonical height of the point

$$P = (0,0) \in E(K).$$

First we note that $(2y+4)(P) = 4$ is not divisible by 3 or $1-2i$, so Theorem 5.2 gives

$$\hat{\lambda}_{(3)}(P) = \hat{\lambda}_{(1-2i)}(P) = 0.$$

Next,

$$(2y+4)(P) = 4 \equiv 0 \pmod{1+i} \quad \text{and} \quad (3x^2+6i) = 6i \equiv 0 \pmod{1+i},$$

so we continue the algorithm specified by Theorem 5.2. Since $c_4 \equiv 0 \pmod{1+i}$, the reduction type is additive. We compute

$$\psi_2(P) = a_3 = 4 = -(1+i)^4, \qquad \psi_3(P) = b_8 = -(1+i)^4 3^2,$$
$$\operatorname{ord}_{(1+i)}(\psi_3(P)) = 4 < 12 = 3\operatorname{ord}_{(1+i)}(\psi_2(P)).$$

Therefore

$$\hat{\lambda}_{(1+i)}(P) = \tfrac{1}{8}\log|\psi_3(P)|_{(1+i)} = \tfrac{1}{8}\log|-(1+i)^4 3^2|_{(1+i)} = -\tfrac{1}{4}\log 2.$$

Next we use the series in Theorem 2.2 to compute $\hat{\lambda}_\infty(P)$ for the Archimedean place ∞ of K, obtaining

$$\hat{\lambda}_\infty(P) = 0.5101849952\ldots$$

accurate to 10 decimals.

Finally, we note that $n_\infty = 1$ and $n_{(1+i)} = 1$. Now putting everything together gives the estimate

$$\hat{h}(P) = \hat{\lambda}_\infty(P) + \hat{\lambda}_{(1+i)}(P) = 0.3368982000\ldots.$$

Example 3. Let E and K be as in Example 2, and let

$$Q = \left(-\frac{9}{4}, \frac{-32+27i}{8}\right) \in E(K).$$

Then

$$(2y+4)(Q) = \frac{-16+27i}{4} = \frac{(1-2i)(14+i)}{(1+i)^4},$$
$$(3x^2+6i)(Q) = \frac{243+96i}{16} = \frac{3(1+2i)(6+i)(4-5i)}{(1+i)^8}.$$

Thus,

$$(2y+4)(Q) \not\equiv 0 \pmod 3 \quad \text{and} \quad (3x^2+6i)(Q) \not\equiv 0 \pmod{1-2i},$$

so

$$\hat{\lambda}_{(3)}(Q) = \hat{\lambda}_{(1-2i)}(Q) = 0 \quad \text{and} \quad \hat{\lambda}_{(1+i)}(Q) = \tfrac{1}{2}\log|-\tfrac{9}{4}|_{(1+i)} = \log 2.$$

Using the series from Theorem 2.2, we compute

$$\hat{\lambda}_\infty(Q) = 0.6544456195\ldots,$$

and so

$$\hat{h}(Q) = \hat{\lambda}_\infty(Q) + \hat{\lambda}_{(1+i)}(Q) = 1.3475928001\ldots.$$

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

Notice that $\hat{h}(Q) \approx 4\hat{h}(P)$; and sure enough, one can easily check that $Q = 2P$. (Of course, if we had noticed this originally, then there would have been no need to compute $\hat{h}(Q)$ separately!)

Example 4. We conclude by computing the canonical height of the point over $\mathbf{Q}$ with the smallest known $\hat{h}(P)/\log|\Delta|$ ratio. (This ratio figures prominently in a conjecture of S. Lang [6, p. 92] and occurs naturally in the counting arguments of [12].) This example illustrates how the algorithm in Theorem 5.2 works for multiplicative reduction. (Compare with the procedure used in [16], which requires computing the denominator of the x-coordinate of $13P$.)

Let $E/\mathbf{Q}$ be the elliptic curve

$$E\colon y^2 + 21xy + 494y = x^3 + 26x^2,$$

and let $P = (0, 0) \in E(\mathbf{Q})$. Using Theorem 2.2, we compute

$$\hat{\lambda}_\infty(P) = 1.921499008\ldots.$$

Next, we have

$$\Delta = -6497214464 = -2^{13}13^3 19^2, \qquad c_4 = 48049.$$

Further,

$$(3x^2 + 2a_2x + a_4 - a_1y)(P) = 0 \quad \text{and} \quad (2y + a_1x + a_3)(P) = 494 = 2 \cdot 13 \cdot 19;$$

while c_4 is prime to $2 \cdot 13 \cdot 19$. Examining Theorem 5.2, we see that E has multiplicative reduction at 2, 13 and 19; and P is not in $E_0(\mathbf{Q}_p)$ for these three primes. Using the formulas in Theorem 5.2(b), we calculate

		$n =$	$\hat{\lambda}_p(P) =$
p	$N = \mathrm{ord}_p\Delta$	$\min\{\mathrm{ord}_p a_3, \frac{1}{2}N\}$	$(n(N-n)/2N^2)\log\lvert\Delta\rvert_p$
2	13	1	$-\frac{6}{13}\log 2 = -0.319914083\ldots$
13	3	1	$-\frac{1}{3}\log 13 = -0.854983119\ldots$
19	2	1	$-\frac{1}{4}\log 19 = -0.736109745\ldots$
∞	–	–	$= 1.921499008\ldots$

$$\hat{h}(P) = 0.010492061\ldots$$

Mathematics Department
Boston University
111 Cummington Street
Boston, Massachusetts 02215

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

2. D. COX & S. ZUCKER, "Intersection numbers of sections of elliptic surfaces," *Invent. Math.*, v. 53, 1979, pp. 1–44.

3. P. DELIGNE, "Courbes Elliptiques: Formulaire (d'après J. Tate)," in *Modular Functions of One Variable IV*, Lecture Notes in Math., vol. 476, Springer-Verlag, Berlin and New York, 1975, pp. 53–74.

4. B. H. GROSS, "Local heights on curves," in *Arithmetic Geometry*, Springer-Verlag, Berlin and New York, 1986, pp. 327–340.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use

5. B. H. GROSS & D. B. ZAGIER, "Heegner points and derivatives of L-series," *Invent. Math.*, v. 84, 1986, 225-320.

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

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

8. M. LASKA, "An algorithm for finding a minimal Weierstrass equation for an elliptic curve," *Math. Comp.*, v. 38, 1982, pp. 257–260.

9. D. MASSER & G. WÜSTHOLZ, "Fields of large transcendence degree generated by values of elliptic functions," *Invent. Math.*, v. 72, 1983, pp. 407–464.

10. J. H. SILVERMAN, *The Néron-Tate Height on Elliptic Curves*, Ph.D. thesis, Harvard, 1981.

11. J. H. SILVERMAN, *The Arithmetic of Elliptic Curves*, Graduate Text 106, Springer, New York, 1986.

12. J. H. SILVERMAN, "A quantitative version of Siegel's theorem," *J. Reine Angew. Math.*, v. 378, 1987, pp. 60–100.

13. J. H. SILVERMAN, Elliptic Curve Calculator v. 5.05, a program for the Apple Macintosh computer, 1987.

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

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

16. H. M. TSCHÖPE & H. G. ZIMMER, "Computation of the Néron-Tate height on elliptic curves," *Math. Comp.*, v. 48, 1987, pp. 351–370.

17. B. L. VAN DER WAERDEN, *Algebra*, 7th ed., Ungar, New York, 1970.

18. D. B. ZAGIER, "Large integral points on curves," *Math. Comp.*, v. 48, 1987, pp. 425–436.

19. H. G. ZIMMER, "Quasifunctions on elliptic curves over local fields," *J. Reine Angew. Math.*, v. 307/308, 1979, pp. 221–246; "Corrections and remarks concerning quasifunctions on elliptic curves," *J. Reine Angew. Math.*, v. 343, 1983, pp. 203–211.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use