# Computation of $p$-Adic Heights and Log Convergence

In celebration of John Coates' 60th birthday

Barry Mazur, William Stein[1], John Tate

Received: September 9, 2005
Revised: May 2, 2006

Abstract. This paper is about computational and theoretical questions regarding $p$-adic height pairings on elliptic curves over a global field $K$. The main stumbling block to computing them efficiently is in calculating, for each of the completions $K_v$ at the places $v$ of $K$ dividing $p$, a *single quantity*: the value of the $p$-adic modular form $\mathbf{E}_2$ associated to the elliptic curve. Thanks to the work of Dwork, Katz, Kedlaya, Lauder and Monsky-Washnitzer we offer an efficient algorithm for computing these quantities, i.e., for computing the value of $\mathbf{E}_2$ of an elliptic curve. We also discuss the $p$-adic convergence rate of canonical expansions of the $p$-adic modular form $\mathbf{E}_2$ on the Hasse domain. In particular, we introduce a new notion of log convergence and prove that $\mathbf{E}_2$ is log convergent.

2000 Mathematics Subject Classification: 11F33, 11Y40, 11G50
Keywords and Phrases: $p$-adic heights, algorithms, $p$-adic modular forms, Eisenstein series, sigma-functions

## 1 Introduction

Let $p$ be an odd prime number, and $E$ an elliptic curve over a global field $K$ that has good ordinary reduction at $p$. Let $L$ be any (infinite degree) Galois extension with a continuous injective homomorphism $\rho$ of its Galois group to

[1] This material is based upon work supported by the National Science Foundation under Grant No. 0555776.

$\mathbf{Q}_p$. To the data $(E, K, \rho)$, one associates[2] a canonical (bilinear, symmetric) ($p$-adic) height pairing

$$( \ , \ )_\rho : E(K) \times E(K) \longrightarrow \mathbf{Q}_p.$$

Such pairings are of great interest for the arithmetic of $E$ over $K$, and they arise specifically in $p$-adic analogues of the Birch and Swinnerton-Dyer conjecture.[3]

The goal of this paper is to discuss some computational questions regarding $p$-adic height pairings. The main stumbling block to computing them efficiently is in calculating, for each of the completions $K_v$ at the places $v$ of $K$ dividing $p$, the value of the $p$-adic modular form $\mathbf{E}_2$ associated to the elliptic curve with a chosen Weierstrass form of good reduction over $K_v$.

We shall offer an algorithm for computing these quantities, i.e., for computing the value of $\mathbf{E}_2$ of an elliptic curve (that builds on the works of Katz and Kedlaya listed in our bibliography) and we also discuss the $p$-adic convergence rate of canonical expansions of the $p$-adic modular form $\mathbf{E}_2$ on the Hasse domain, where for $p \geq 5$ we view $\mathbf{E}_2$ as an infinite sum of classical modular forms divided by powers of the (classical) modular form $\mathbf{E}_{p-1}$, while for $p \leq 5$ we view it as a sum of classical modular forms divided by powers of $\mathbf{E}_4$.

We were led to our fast method of computing $\mathbf{E}_2$ by our realization that the more naive methods, of computing it by integrality or by approximations to it as function on the Hasse domain, were not practical, because the convergence is "logarithmic" in the sense that the $n$th convergent gives only an accuracy of $\log_p(n)$. We make this notion of log convergence precise in Part II, where we also prove that $\mathbf{E}_2$ is log convergent.

The reason why this constant $\mathbf{E}_2$ enters the calculation is because it is needed for the computation of the $p$-adic sigma function [MT91], which in turn is the critical element in the formulas for height pairings.

For example, let us consider the *cyclotomic* $p$-adic height pairing in the special case where $K = \mathbf{Q}$ and $p \geq 5$.

If $G_{\mathbf{Q}}$ is the Galois group of an algebraic closure of $\mathbf{Q}$ over $\mathbf{Q}$, we have the natural surjective continuous homomorphism $\chi : G_{\mathbf{Q}} \to \mathbf{Z}_p^*$ pinned down by the standard formula $g(\zeta) = \zeta^{\chi(g)}$ where $g \in G_{\mathbf{Q}}$ and $\zeta$ is any $p$-power root of unity. The $p$-adic logarithm $\log_p : \mathbf{Q}_p^* \to (\mathbf{Q}_p, +)$ is the unique group homomorphism with $\log_p(p) = 0$ that extends the homomorphism $\log_p : 1 + p\mathbf{Z}_p \to \mathbf{Q}_p$ defined by the usual power series of $\log(x)$ about 1. Explicitly, if $x \in \mathbf{Q}_p^*$, then

$$\log_p(x) = \frac{1}{p-1} \cdot \log_p(u^{p-1}),$$

where $u = p^{-\operatorname{ord}_p(x)} \cdot x$ is the unit part of $x$, and the usual series for log converges at $u^{p-1}$.

[2] See [MT83], [Sch82] [Sch85], [Zar90], [Col91], [Nek93], [Pla94], [IW03], and [Bes04].

[3] See [Sch82], [Sch85] [MT83], [MT87], [PR03a]. See also the important recent work of Jan Nekovář [Nek03].

The composition $(\frac{1}{p}\cdot\log_p)\circ\chi$ is a cyclotomic linear functional $G_{\mathbf{Q}}\to\mathbf{Q}_p$ which, in the body of our text, will be dealt with (thanks to class field theory) as the idele class functional that we denote $\rho_{\mathbf{Q}}^{\mathrm{cycl}}$.

Let $\mathcal{E}$ denote the Néron model of $E$ over $\mathbf{Z}$. Let $P\in E(\mathbf{Q})$ be a non-torsion point that reduces to $0\in E(\mathbf{F}_p)$ and to the connected component of $\mathcal{E}_{\mathbf{F}_\ell}$ at all primes $\ell$ of bad reduction for $E$. Because $\mathbf{Z}$ is a unique factorization domain, any nonzero point $P=(x(P),y(P))\in E(\mathbf{Q})$ can be written uniquely in the form $(a/d^2,b/d^3)$, where $a,b,d\in\mathbf{Z}$, $\gcd(a,d)=\gcd(b,d)=1$, and $d>0$. The function $d(P)$ assigns to $P$ this square root $d$ of the denominator of $x(P)$.

Here is the formula for the *cyclotomic* $p$-adic height of $P$, i.e., the value of

$$h_p(P):=-\frac{1}{2}(P,P)_p\in\mathbf{Q}_p$$

where $(\ ,\ )_p$ is the height pairing attached to $G_{\mathbf{Q}}\to\mathbf{Q}_p$, the cyclotomic linear functional described above:

$$h_p(P)=\frac{1}{p}\cdot\log_p\left(\frac{\sigma(P)}{d(P)}\right)\in\mathbf{Q}_p. \tag{1.1}$$

Here $\sigma=\sigma_p$ is the $p$-adic sigma function of [MT91] associated to the pair $(E,\omega)$. The $\sigma$-function depends only on $(E,\omega)$ and not on a choice of Weierstrass equation, and behaves like a modular form of weight $-1$, that is $\sigma_{E,c\omega}=c\cdot\sigma_{E,\omega}$. It is "quadratic" the sense that for any $m\in\mathbf{Z}$ and point $Q$ in the formal group $E^f(\mathbf{Z}_p)$, we have

$$\sigma(mQ)=\sigma(Q)^{m^2}\cdot f_m(Q), \tag{1.2}$$

where $f_m$ is the $m$th division polynomial of $E$ relative to $\omega$ (as in [MT91, App. 1]). The $\sigma$-function is "bilinear" in that for any $P,Q\in E^f(\mathbf{Z}_p)$, we have

$$\frac{\sigma(P-Q)\cdot\sigma(P+Q)}{\sigma^2(P)\cdot\sigma^2(Q)}=x(Q)-x(P). \tag{1.3}$$

See [MT91, Thm. 3.1] for proofs of the above properties of $\sigma$.

The height function $h_p$ of (1.1) extends uniquely to a function on the full Mordell-Weil group $E(\mathbf{Q})$ that satisfies $h_p(nQ)=n^2h_p(Q)$ for all integers $n$ and $Q\in E(\mathbf{Q})$. For $P,Q\in E(\mathbf{Q})$, setting

$$(P,Q)_p=h_p(P)+h_p(Q)-h_p(P+Q),$$

we obtain a pairing on $E(\mathbf{Q})$. The *$p$-adic regulator* of $E$ is the discriminant of the induced pairing on $E(\mathbf{Q})_{/\,\mathrm{tor}}$ (well defined up to sign), and we have the following standard conjecture about this height pairing.

CONJECTURE 1.1. *The cyclotomic height pairing $(\ ,\ )_p$ is nondegenerate; equivalently, the $p$-adic regulator is nonzero.*

REMARK 1.2. Height pairings attached to other $p$-adic linear functionals can be degenerate; in fact, given an elliptic curve defined over $\mathbf{Q}$ with good ordinary reduction at $p$, and $K$ a quadratic imaginary field over which the Mordell-Weil group $E(K)$ is of odd rank, the $p$-adic anticyclotomic height pairing for $E$ over $K$ is *always* degenerate.

The $p$-adic $\sigma$ function is the most mysterious quantity in (1.1). There are many ways to define $\sigma$, e.g., [MT91] contains 11 different characterizations of $\sigma$! We now describe a characterization that leads directly to an algorithm (see Algorithm 3.3) to compute $\sigma(t)$. Let

$$x(t) = \frac{1}{t^2} + \cdots \in \mathbf{Z}_p((t)) \tag{1.4}$$

be the formal power series that expresses $x$ in terms of the local parameter $t = -x/y$ at infinity. The following theorem, which is proved in [MT91], uniquely determines $\sigma$ and $c$.

THEOREM 1.3. *There is exactly one odd function $\sigma(t) = t + \cdots \in t\mathbf{Z}_p[[t]]$ and constant $c \in \mathbf{Z}_p$ that together satisfy the differential equation*

$$x(t) + c = -\frac{d}{\omega}\left(\frac{1}{\sigma}\frac{d\sigma}{\omega}\right), \tag{1.5}$$

*where $\omega$ is the invariant differential $dx/(2y + a_1x + a_3)$ associated with our chosen Weierstrass equation for $E$.*

REMARK 1.4. The condition that $\sigma$ is odd and that the coefficient of $t$ is 1 are essential.

In (1.1), by $\sigma(P)$ we mean $\sigma(-x/y)$, where $P = (x, y)$. We have thus given a complete definition of $h_p(Q)$ for any point $Q \in E(\mathbf{Q})$ and a prime $p \geq 5$ of good ordinary reduction for $E$.

### 1.1 THE $p$-ADIC $\sigma$-FUNCTION

The differential equation (1.5) leads to a slow algorithm to compute $\sigma(t)$ to any desired precision. This is Algorithm 3.3 below, which we now summarize. If we expand (1.5), we can view $c$ as a formal variable and solve for $\sigma(t)$ as a power series with coefficients that are polynomials in $c$. Each coefficient of $\sigma(t)$ must be in $\mathbf{Z}_p$, so we obtain conditions on $c$ modulo powers of $p$. Taking these together for many coefficients must eventually yield enough information to compute $c \pmod{p^n}$, for a given $n$, hence $\sigma(t) \pmod{p^n}$. This integrality algorithm is hopelessly slow in general.

Another approach to computing $\sigma$ is to observe that, up to a constant, $c$ is closely related to the value of a certain $p$-adic modular form. More precisely, suppose that $E$ is given by a (not necessarily minimal) Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.6}$$

and let $\omega = dx/(2y + a_1x + a_3)$. Let $x(t)$ be as in (1.4). Then the series

$$\wp(t) = x(t) + \frac{a_1^2 + 4a_2}{12} \in \mathbf{Q}((t)) \tag{1.7}$$

satisfies $(\wp')^2 = 4\wp^3 - g_2\wp - g_3$. In [MT91] we find[4] that

$$x(t) + c = \wp(t) - \frac{1}{12} \cdot \mathbf{E}_2(E, \omega), \tag{1.8}$$

where $\mathbf{E}_2(E, \omega)$ is the value of the Katz $p$-adic weight 2 Eisenstein series at $(E, \omega)$, and the equality is of elements of $\mathbf{Q}_p((t))$. Using the definition of $\wp(t)$ and solving for $c$, we find that

$$c = \frac{a_1^2 + 4a_2}{12} - \frac{1}{12}\mathbf{E}_2(E, \omega). \tag{1.9}$$

Thus computing $c$ is equivalent to computing the $p$-adic number $\mathbf{E}_2(E, \omega)$. Having computed $c$ to some precision, we then solve for $\sigma$ in (1.5) using Algorithm 3.1 below.

### 1.2 $p$-adic analogues of the Birch and Swinnerton-Dyer conjecture

One motivation for this paper is to provide tools for doing computations in support of $p$-adic analogues of the BSD conjectures (see [MTT86]), especially when $E/\mathbf{Q}$ has rank at least 2. For example, in [PR03b], Perrin-Riou uses her results about the $p$-adic BSD conjecture in the supersingular case to prove that $\text{Ш}(E/\mathbf{Q})[p] = 0$ for certain $p$ and elliptic curves $E$ of rank $> 1$, for which the work of Kolyvagin and Kato does not apply.

Another motivation for this work comes from the study of the fine structure of Selmer modules. Let $K$ be a number field and $\Lambda$ the $p$-adic integral group ring of the Galois group of the maximal $\mathbf{Z}_p$-power extension of $K$. Making use of fundamental results of Nekovář [Nek03] and of Greenberg [Gre03] one can construct (see [RM05]) for certain elliptic curves defined over $K$, a skew-Hermitian matrix with coefficients in $\Lambda$ from which one can read off a free $\Lambda$-resolution of the canonical Selmer $\Lambda$-module of the elliptic curve in question over $K$. To compute the entries of this matrix modulo the square of the augmentation ideal in $\Lambda$ one must know *all* the $p$-adic height pairings of the elliptic curve over $K$. Fast algorithms for doing this provide us with an important first stage in the computation of free $\Lambda$-resolutions of Selmer $\Lambda$-modules.

The paper [GJP+05] is about computational verification of the full Birch and Swinnerton-Dyer conjecture for specific elliptic curves $E$. There are many cases in which the rank of $E$ is 1 and the upper bound on $\#\text{Ш}(E/\mathbf{Q})$ coming from Kolyvagin's Euler system is divisible by a prime $p \geq 5$ that also divides a Tamagawa number. In such cases, theorems of Kolyvagin and Kato combined

[4] There is a sign error in [MT91].

with explicit computation do not give a sufficiently sharp upper bound on $\#\text{Ш}(E/\mathbf{Q})$. However, it should be possible in these cases to compute $p$-adic heights and $p$-adic $L$-functions, and use results of Kato, Schneider, and others to obtain better bounds on $\#\text{Ш}(E/\mathbf{Q})$. Wuthrich and the second author (Stein) are writing a paper on this.

### 1.3 Sample computations

In Section 4 we illustrate our algorithms with curves of ranks $1, 2, 3, 4$ and $5$, and two twists of $X_0(11)$ of rank 2.

Acknowledgement: It is a pleasure to thank Nick Katz for feedback that led to Section 3. We would also like to thank Mike Harrison for discussions about his implementation of Kedlaya's algorithm in Magma, Kiran Kedlaya for conversations about his algorithm, Christian Wuthrich for feedback about computing $p$-adic heights, Alan Lauder for discussions about computing $\mathbf{E}_2$ in families, and Fernando Gouvea for remarks about non-overconvergence of $\mathbf{E}_2$. We would also like to thank all of the above people for comments on early drafts of the paper. Finally, we thank Jean-Pierre Serre for the proof of Lemma 6.6.

# Part I
# Heights, $\sigma$-functions, and $\mathbf{E}_2$

## 2 The Formulas

In this section we give formulas for the $p$-adic height pairing in terms of the $\sigma$ function. We have already done this over $\mathbf{Q}$ in Section 1. Let $p$ be an (odd) prime number, $K$ a number field, and $E$ an elliptic curve over $K$ with good ordinary reduction at all places of $K$ above $p$. For any non-archimedean place $w$ of $K$, let $k_w$ denote the residue class field at $w$.

### 2.1 General global height pairings

By the *idele class* $\mathbf{Q}_p$*-vector space* of $K$ let us mean

$$I(K) = \mathbf{Q}_p \otimes_{\mathbf{Z}} \left\{ \mathbf{A}_K^*/ \left( K^* \cdot \prod_{v \nmid p} \mathcal{O}_v^* \cdot \mathrm{C} \right) \right\},$$

where $\mathbf{A}_K^*$ is the group of ideles of $K$, and $\mathrm{C}$ denotes its connected component containing the identity. Class field theory gives us an identification $I(K) = \Gamma(K) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, where $\Gamma(K)$ is the Galois group of the maximal $\mathbf{Z}_p$-power extension of $K$. For every (nonarchimedean) place $v$ of $K$, there is a natural homomorphism $\iota_v : K_v^* \to I(K)$.

For $K$-rational points $\alpha, \beta \in E(K)$ we want to give explicit formulas for an element that we might call the "universal" $p$-adic height pairing of $\alpha$ and $\beta$; denote it $(\alpha, \beta) \in I(K)$. If $\rho : I(K) \to \mathbf{Q}_p$ is any linear functional, then the *$\rho$-height pairing* is a symmetric bilinear pairing

$$( \ , \ )_\rho : E(K) \times E(K) \to \mathbf{Q}_p,$$

defined as the composition of the universal pairing with the linear functional $\rho$:

$$(\alpha, \beta)_\rho = \rho(\alpha, \beta) \in \mathbf{Q}_p.$$

We define the *$\rho$-height* of a point $\alpha \in E(K)$ by:

$$h_\rho(\alpha) = -\frac{1}{2}(\alpha, \alpha)_\rho \in \mathbf{Q}_p.$$

Of course, any such (nontrivial) linear functional $\rho$ uniquely determines a $\mathbf{Z}_p$-extension, and we sometimes refer to the $\rho$-height pairing in terms of this $\mathbf{Z}_p$-extension. E.g., if $\rho$ cuts out the cyclotomic $\mathbf{Z}_p$-extension, then the $\rho$-height pairing is a normalization of the *cyclotomic height pairing* that has, for the rational field, already been discussed in the introduction.

If $K$ is quadratic imaginary, and $\rho$ is the anti-cyclotomic linear functional, meaning that it is the unique linear functional (up to normalization) that has the property that $\rho(\bar{x}) = -\rho(x)$ where $\bar{x}$ is the complex conjugate of $x$, then we will be presently obtaining explicit formulas for this anti-cyclotomic height pairing.

We will obtain a formula for $(\alpha, \beta) \in I(K)$ by defining, for every nonarchimedean place, $v$, of $K$ a "local height pairing," $(\alpha, \beta)_v \in K_v^*$. These local pairings will be very sensitive to some auxiliary choices we make along the way, but for a fixed $\alpha$ and $\beta$ the local height pairings $(\alpha, \beta)_v$ will vanish for all but finitely many places $v$; the global height is the sum of the local ones and will be independent of all the choices we have made.

## 2.2 Good representations

Let $\alpha, \beta \in E(K)$. By a *good representation* of the pair $\alpha, \beta$ we mean that we are given a four-tuple of points $(P, Q, R, S)$ in $E(K)$ (or, perhaps, in $E(K')$ where $K'/K$ is a number field extension of $K$) such that

- $\alpha$ is the divisor class of the divisor $[P] - [Q]$ of $E$, and $\beta$ is the divisor class of the divisor $[R] - [S]$,
- $P, Q, R, S$ are four distinct points,
- for each $v \mid p$ all four points $P, Q, R, S$ specialize to the same point on the fiber at $v$ of the Néron model of $E$.
- at all places $v$ of $K$ the points $P, Q, R, S$ specialize to the same component of the fiber at $v$ of the Néron model of $E$.

We will show how to erase these special assumptions later, but for now, let us assume all this, fix a choice of a good representation, $P, Q, R, S$, of $(\alpha, \beta)$ as above, and give the formulas in this case.

### 2.3 Local height pairings when $v \mid p$

Let $\sigma_v$ be the canonical $p$-adic $\sigma$-function attached to the elliptic curve $E$ over $K_v$ given in Weierstrass form. We may view $\sigma_v$ as a mapping from $E_1(K_v)$ to $K_v^*$, where $E_1(K_v)$ is the kernel of the reduction map $E(K_v) \to E(k_v)$, and $E(k_v)$ denotes the group of points on the reduction of $E$ modulo $v$. Define $(\alpha, \beta)_v \in K_v^*$ by the formula,

$$(\alpha, \beta)_v = \frac{\sigma_v(P-R)\sigma_v(Q-S)}{\sigma_v(P-S)\sigma_v(Q-R)} \ \in \ K_v^*.$$

The dependence of $\sigma$ on the Weierstrass equation is through the differential $\omega = dx/(2y + a_1 x + a_3)$, and $\sigma_{c\omega} = c\sigma_\omega$, so this depends upon the choice of $P, Q, R, S$, but does not depend on the choice of Weierstrass equation for $E$.

### 2.4 Local height pairings when $v \nmid p$

First let $x$ denote the "$x$-coordinate" in some minimal Weierstrass model for $A$ at $v$. Define for a point $T$ in $E(K_v)$ the rational number $\lambda_v(T)$ to be *zero* if $x(T) \in \mathcal{O}_v$, and to be $-\frac{1}{2}v(x(T))$ if $x(T) \notin \mathcal{O}_v$.

Next, choose a uniformizer $\pi_v$ of $K_v$ and define:

$$\tilde{\sigma}_v(T) = \pi_v^{\lambda_v(T)},$$

the square of which is in $K_v^*$. We think of $\tilde{\sigma}_v$ as a rough replacement for $\sigma_v$ in the following sense. The $v$-adic valuation of $\tilde{\sigma}_v$ is the same as $v$-adic valuation of the $v$-adic sigma function (if such a function is definable at $v$) and therefore, even if $\sigma_v$ cannot be defined, $\tilde{\sigma}_v$ is a perfectly serviceable substitute at places $v$ at which our $p$-adic idele class functionals $\rho$ are necessarily unramified, and therefore sensitive only to the $v$-adic valuation.

For $v \nmid p$, put:

$$(\alpha, \beta)_v = \frac{\tilde{\sigma}_v(P-R)\tilde{\sigma}_v(Q-S)}{\tilde{\sigma}_v(P-S)\tilde{\sigma}_v(Q-R)}.$$

The square of this is in $K_v^*$. However, note that $\pi_v^{\lambda_v(T)}$ really means $\sqrt{\pi_v}^{2\lambda_v(T)}$, for a fixed choice of $\sqrt{\pi_v}$ and that the definition of $(\alpha, \beta)_v$ is independent of the choice of square root and therefore that $(\alpha, \beta)_v$, not only its square, is in $K_v^*$.

Our local height $(\alpha, \beta)_v$, depends upon the choice of $P, Q, R, S$ and of the uniformizer $\pi_v$.

### 2.5 How the local heights change, when we change our choice of divisors

Let $\beta \in E(K)$ be represented by both $[R]-[S]$ and $[R']-[S']$. Let $\alpha \in E(K)$ be represented by $[P]-[Q]$. Moreover let both four-tuples $P, Q, R, S$ and $P, Q, R', S'$ satisfy the *good representation* hypothesis described at the beginning of Section 2.2. Since, by hypothesis, $[R]-[S]-[R']+[S']$ is linearly equivalent to zero, there is a rational function $f$ whose divisor of zeroes and poles is

$$(f) = [R]-[S]-[R']+[S'].$$

If $v$ is a nonarchimedean place of $K$ define $(\alpha,\beta)_v$ to be as defined in the previous sections using the choice of four-tuple of points $P, Q, R, S$, (and of uniformizer $\pi_v$ when $v \nmid p$). Similarly, define $(\alpha,\beta)'_v$ to be as defined in the previous sections using the choice of four-tuple of points $P, Q, R', S'$, (and of uniformizer $\pi_v$ when $v \nmid p$).

Proposition 2.1. *1. If $v \mid p$ then*

$$(\alpha,\beta)_v = \frac{f(P)}{f(Q)} \cdot (\alpha,\beta)'_v \ \in \ K_v^*.$$

*2. If $v \nmid p$ then there is a unit $u$ in the ring of integers of $K_v$ such that*

$$(\alpha,\beta)_v^2 = u \cdot \left(\frac{f(P)}{f(Q)} \cdot (\alpha,\beta)'_v\right)^2 \ \in \ K_v^*.$$

### 2.6 The global height pairing more generally

We can then form the sum of local terms to define the global height

$$(\alpha,\beta) = \quad \frac{1}{2}\sum_v \iota_v((\alpha,\beta)_v^2) \ \in \ I(K).$$

This definition is independent of any of the (good representation) choices $P, Q, R, S$ and the $\pi_v$'s made. It is independent of the choice of $\pi_v$'s because the units in the ring of integers of $K_v$ is in the kernel of $\iota_v$ if $v \nmid p$. It is independent of the choice of $P, Q, R, S$ because by the previous proposition, a change (an allowable one, given our hypotheses) of $P, Q, R, S$ changes the value of $(\alpha,\beta)$ by a factor that is a principal idele, which is sent to zero in $I(K)$.

What if, though, our choice of $P, Q, R, S$ does *not* have the property that $\alpha$ and $\beta$ reduce to the same point in the Néron fiber at $v$ for all $v \mid p$, or land in the same connected component on each fiber of the Néron model? In this case the pair $\alpha, \beta$ do not have a *good representation.* But replacing $\alpha, \beta$ by $m\cdot\alpha, n\cdot\beta$ for sufficiently large positive integers $m, n$ we can guarantee that the pair $m\cdot\alpha, n\cdot\beta$ does possess a good representation, and obtain formulas for $(\alpha,\beta)$ by:

$$(\alpha,\beta) = \frac{1}{mn}(m\cdot\alpha, n\cdot\beta).$$

Note in passing that to compute the global height pairing $(\alpha,\alpha)$ for a non-torsion point $\alpha \in E(K)$ that specializes to 0 in the Néron fiber at $v$ for all $v \mid p$, and that lives in the connected component containing the identity in all Néron fibers, we have quite a few natural choices of *good representations*. For example, for positive integers $m \neq n$, take

$$P = (m+1)\cdot\alpha;\ Q = m\cdot\alpha;\ R = (n+1)\cdot\alpha;\ S = n\cdot\alpha.$$

Then for any $p$-adic idele class functional $\rho$ the global $\rho$-height pairing $(\alpha,\alpha)_\rho$ is given by

$$\sum_{v \mid p} \rho_v \left\{ \frac{\sigma_v((m-n)\alpha)^2}{\sigma_v((m-n+1)\alpha)\cdot\sigma_v((m-n-1)\alpha)} \right\} + \sum_{v \nmid p} \rho_v \left\{ \frac{\tilde{\sigma}_v((m-n)\alpha)^2}{\tilde{\sigma}_v((m-n+1)\alpha)\cdot\tilde{\sigma}_v((m-n-1)\alpha)} \right\},$$

which simplifies to

$$(2(m-n)^2 - (m-n+1)^2 - (m-n-1)^2)\cdot\left\{ \sum_{v \mid p} \rho_v\sigma_v(\alpha) + \sum_{v \nmid p} \rho_v\tilde{\sigma}_v(\alpha) \right\}.$$

Since $(2(m-n)^2 - (m-n+1)^2 - (m-n-1)^2) = -2$ we have the formula

$$h_\rho(\alpha) = -\frac{1}{2}(\alpha,\alpha)_\rho$$

quoted earlier.

### 2.7 Formulas for the $\rho$-height

For each $v$, let $\sigma_v$ be the canonical $p$-adic $\sigma$-function of $E$ over $K_v$ given in Weierstrass form. Suppose $P \in E(K)$ is a (non-torsion) point that reduces to 0 in $E(k_v)$ for each $v \mid p$, and to the connected component of all special fibers of the Néron model of $E$. Locally at each place $w$ of $K$, we have a denominator $d_w(P)$, well defined up to units.

We have

$$h_\rho(P) = \sum_{v \mid p} \rho_v(\sigma_v(P)) - \sum_{w \nmid p} \rho_w(d_w(P)).$$

Note that $h_\rho$ is quadratic because of the quadratic property of $\sigma$ from (1.2), and the $h_\rho$-pairing is then visibly bilinear. See also property (1.3).

## 2.8 Cyclotomic $p$-adic heights

The idele class $\mathbf{Q}_p$-vector space $I(\mathbf{Q})$ attached to $\mathbf{Q}$ is canonically isomorphic to $\mathbf{Q}_p \otimes \mathbf{Z}_p^*$. Composition of this canonical isomorphism with the mapping $1 \times \frac{1}{p}\log_p$ induces an isomorphism

$$\rho_{\mathrm{cycl}}^{\mathbf{Q}} : I(\mathbf{Q}) = \mathbf{Q}_p \otimes \mathbf{Z}_p^* \xrightarrow{\cong} \mathbf{Q}_p.$$

For $K$ any number field, consider the homomorphism on idele class $\mathbf{Q}_p$-vector spaces induced by the norm $N_{K/\mathbf{Q}} : I(K) \to I(\mathbf{Q})$, and define

$$\rho_{\mathrm{cycl}}^{K} : I(K) \to \mathbf{Q}_p$$

as the composition

$$\rho_{\mathrm{cycl}}^{K} = \rho_{\mathrm{cycl}}^{\mathbf{Q}} \circ N_{K/\mathbf{Q}}.$$

By the *cyclotomic height pairing* for an elliptic curve $E$ over $K$ (of good ordinary reduction at all places $v$ of $K$ above $p$) we mean the $\rho_{\mathrm{cycl}}^{K}$-height pairing $E(K) \times E(K) \to \mathbf{Q}_p$. We put

$$h_p(P) = h_{\rho_{\mathrm{cycl}}^{K}}(P)$$

for short. Here is an explicit formula for it.

$$h_p(P) = \frac{1}{p} \cdot \left( \sum_{v|p} \log_p(N_{K_v/\mathbf{Q}_p}(\sigma_v(P))) - \sum_{w\nmid p} \mathrm{ord}_w(d_w(P)) \cdot \log_p(\# k_w) \right).$$

If we assume that $P$ lies in a sufficiently small (finite index) subgroup of $E(K)$ (see [Wut04, Prop. 2]), then there will be a global choice of denominator $d(P)$, and the formula simplifies to

$$h_p(P) = \frac{1}{p} \cdot \log_p \left( \prod_{v|p} N_{K_v/\mathbf{Q}_p} \left( \frac{\sigma_v(P)}{d(P)} \right) \right).$$

## 2.9 Anti-cyclotomic $p$-adic heights

Let $K$ be a quadratic imaginary field in which $p$ splits as $(p) = \pi \cdot \bar{\pi}$. Suppose $\rho : \mathbf{A}_K^*/K^* \to \mathbf{Z}_p$ is a nontrivial *anti-cyclotomic* idele class character, meaning that if $\mathbf{c} : \mathbf{A}_K^*/K^* \to \mathbf{A}_K^*/K^*$ denotes the involution of the idele class group induced by complex conjugation $x \mapsto \bar{x}$ in $K$, then $\rho \cdot \mathbf{c} = -\rho$. Then the term

$$\sum_{v \ | \ p} \rho_v(\sigma_v(P))$$

in the formula for the $\rho$-height at the end of Section 2.7 is just

$$\sum_{v \ | \ p} \rho_v(\sigma_v(P)) = \rho_\pi(\sigma_\pi(P)) - \rho_\pi(\sigma_\pi(\bar{P})),$$

so we have the following formula for the $\rho$-height of $P$:

$$h_\rho(P) = \rho_\pi(\sigma_\pi(P)) - \rho_\pi(\sigma_\pi(\bar{P})) - \sum_{w \nmid p} \rho_w(d_w(P)).$$

Remark 2.2. The Galois equivariant property of the $p$-adic height pairing implies that if $P$ is a $\mathbf{Q}$-rational point, its anti-cyclotomic height is 0. Specifically, let $K/k$ be any Galois extension of number fields, with Galois group $G = \mathrm{Gal}(K/k)$. Let $V = V(K)$ be the $\mathbf{Q}_p$-vector space (say) defined as $(G_K)^{\mathrm{ab}} \otimes \mathbf{Q}_p$, so that $V$ is naturally a $G$-representation space. Let $E$ be an elliptic curve over $k$ and view the Mordell-Weil group $E(K)$ as equipped with its natural $G$-action. Then (if $p$ is a good ordinary prime for $E$) we have the $p$-adic height pairing

$$\langle P, Q\rangle \in V,$$

for $P, Q \in E(K)$ and we have Galois equivariance,

$$\langle g \cdot P, g \cdot Q\rangle = g \cdot \langle P, Q\rangle,$$

for any $g$ in the Galois group.

Put $k = \mathbf{Q}$, $K/k$ a quadratic imaginary field. Then $V$ is of dimension two, with $V = V^+ \oplus V^-$ each of the $V^\pm$ being of dimension one, with the action of complex conjugation, $g \in G$ on $V^\pm$ being given by the sign; so that $V^+$ corresponds to the cyclotomic $\mathbf{Z}_p$-extension and $V^-$ corresponds to the anticyclotomic $\mathbf{Z}_p$- extension. In the notation above, the anticyclotomic height of $P$ and $Q$ is just $\langle g \cdot P, g \cdot Q\rangle^-$ where the superscript $-$ means projection to $V^-$. Suppose that $P \in E(\mathbf{Q})$, so that $g \cdot P = P$. Then we have by Galois equivariance

$$\langle P, P\rangle^- = \langle g \cdot P, g \cdot P\rangle^- = -\langle P, P\rangle^-,$$

so $\langle P, P\rangle^- = 0$. More generally, the anticyclotomic height is zero as a pairing on either $E(K)^+ \times E(K)^+$ or $E(K)^- \times E(K)^-$ and can only be nonzero on $E(K)^+ \times E(K)^-$. If $E(K)$ is of odd rank, then the ranks of $E(K)^+$ and $E(K)^-$ must be different, which obliges the pairing on $E(K)^+ \times E(K)^-$ to be either left-degenerate or right-degenerate (or, of course, degenerate on both sides). Rubin and the first author conjecture that it is nondegenerate on one side (the side, of course having smaller rank); for more details see, e.g., [MR04, Conj. 11].

## 3 The Algorithms

Fix an elliptic curve $E$ over $\mathbf{Q}$ and a good ordinary prime $p \geq 5$. In this section we discuss algorithms for computing the cyclotomic $p$-adic height of elements of $E(\mathbf{Q})$.

### 3.1 Computing the $p$-adic $\sigma$-function

First we explicitly solve the differential equation (1.5). Let $z(t)$ be the formal logarithm on $E$, which is given by $z(t) = \int \frac{\omega}{dt} = t + \cdots$ (here the symbol $\int$

means formal integration with 0 constant term). There is a unique function $F(z) \in \mathbf{Q}((z))$ such that $t = F(z(t))$. Set $x(z) = x(F(z))$. Rewrite (1.5) as

$$x(z) + c = -\frac{d}{\omega}\left(\frac{d\log(\sigma)}{\omega}\right). \tag{3.1}$$

A crucial observation is that

$$x(z) + c = \frac{1}{z^2} - \frac{a_1^2 + 4a_2}{12} + c + \cdots;$$

in particular, the coefficient of $1/z$ in the expansion of $g(z) = x(z) + c$ is 0.

Since $z = \int(\omega/dt)$ we have $dz = (\omega/dt)dt = \omega$, hence $dz/\omega = 1$, so

$$-\frac{d}{\omega}\left(\frac{d\log(\sigma)}{\omega}\right) = -\frac{dz}{\omega}\frac{d}{dz}\left(\frac{d\log(\sigma)}{\omega}\right) = -\frac{d}{dz}\left(\frac{d\log(\sigma)}{dz}\right). \tag{3.2}$$

Write $\sigma(z) = z\sigma_0(z)$ where $\sigma_0(z)$ has nonzero constant term. Then

$$-\frac{d}{dz}\left(\frac{d\log(\sigma)}{dz}\right) = \frac{1}{z^2} - \frac{d}{dz}\left(\frac{d\log(\sigma_0)}{dz}\right). \tag{3.3}$$

Thus combining (3.1)–(3.3) and changing sign gives

$$\frac{1}{z^2} - x(z) - c = \frac{d}{dz}\left(\frac{d\log(\sigma_0)}{dz}\right).$$

This is particularly nice, since $g(z) = \frac{1}{z^2} - x(z) - c \in \mathbf{Q}[[z]]$. We can thus solve for $\sigma_0(z)$ by formally integrating twice and exponentiating:

$$\sigma_0(z) = \exp\left(\int\int g(z)dzdz\right),$$

where we choose the constants in the double integral to be 0, so $\int\int g = 0 + 0z + \cdots$. Using (1.8) we can rewrite $g(z)$ in terms of $e_2 = \mathbf{E}_2(E,\omega)$ and $\wp(z)$ as

$$g(z) = \frac{1}{z^2} - (x(z) + c) = \frac{1}{z^2} - \wp(z) + \frac{e_2}{12}.$$

Combining everything and using that $\sigma(z) = z\sigma_0(z)$ yields

$$\sigma(z) = z \cdot \exp\left(\int\int\left(\frac{1}{z^2} - \wp(z) + \frac{e_2}{12}\right)dzdz\right),$$

Finally, to compute $\sigma(t)$ we compute $\sigma(z)$ and obtain $\sigma(t)$ as $\sigma(z(t))$.

We formalize the resulting algorithm below.

Algorithm 3.1 (The Canonical $p$-adic Sigma Function). Given an elliptic curve $E$ over $\mathbf{Q}$, a good ordinary prime $p$ for $E$, and an approximation $e_2$ for $\mathbf{E}_2(E,\omega)$, this algorithm computes an approximation to $\sigma(t) \in \mathbf{Z}_p[[t]]$.

1. [Compute Formal Log] Compute the formal logarithm $z(t) = t + \cdots \in \mathbf{Q}((t))$ using that
$$z(t) = \int \frac{dx/dt}{2y(t) + a_1 x(t) + a_3}, \qquad \text{(0 constant term)} \tag{3.4}$$
where $x(t) = t/w(t)$ and $y(t) = -1/w(t)$ are the local expansions of $x$ and $y$ in terms of $t = -x/y$, and $w(t) = \sum_{n \geq 0} s_n t^n$ is given by the following explicit inductive formula (see, e.g., [Blu, pg. 18]):
$$s_0 = s_1 = s_2 = 0, \qquad s_3 = 1, \qquad \text{and for } n \geq 4,$$
$$s_n = a_1 s_{n-1} + a_2 s_{n-2} + a_3 \sum_{i+j=n} s_i s_j + a_4 \sum_{i+j=n-1} s_i s_j + a_6 \sum_{i+j+k=n} s_i s_j s_k.$$
2. [Reversion] Using a power series "reversion" (functional inverse) algorithm, find the unique power series $F(z) \in \mathbf{Q}[[z]]$ such that $t = F(z)$. Here $F$ is the reversion of $z$, which exists because $z(t) = t + \cdots$.
3. [Compute $\wp$] Compute $\alpha(t) = x(t) + (a_1^2 + 4a_2)/12 \in \mathbf{Q}[[t]]$, where the $a_i$ are as in (1.6). Then compute the series $\wp(z) = \alpha(F(z)) \in \mathbf{Q}((z))$.
4. [Compute $\sigma(z)$] Set $g(z) = \dfrac{1}{z^2} - \wp(z) + \dfrac{e_2}{12} \in \mathbf{Q}_p((z))$, and compute
$$\sigma(z) = z \cdot \exp\left( \int \int g(z) dz dz \right) \in \mathbf{Q}_p[[z]].$$
5. [Compute $\sigma(t)$] Set $\sigma(t) = \sigma(z(t)) \in t \cdot \mathbf{Z}_p[[t]]$, where $z(t)$ is the formal logarithm computed in Step 1. Output $\sigma(t)$ and terminate.

### 3.2 Computing $\mathbf{E}_2(E, \omega)$ using cohomology

This section is about a fast method of computation of $\mathbf{E}_2(E, \omega)$ for individual ordinary elliptic curves, "one at a time". The key input is [Kat73, App. 2] (see also [Kat76]), which gives an interpretation of $\mathbf{E}_2(E, \omega)$ as the "direction" of the unit root eigenspace (cf. formula A.2.4.1 of [Kat73, App. 2]) of Frobenius acting on the one-dimensional de Rham cohomology of $E$.

Concretely, consider an elliptic curve $E$ over $\mathbf{Z}_p$ with good ordinary reduction. Assume that $p \geq 5$. Fix a Weierstrass equation for $E$ of the form $y^2 = 4x^3 - g_2 x - g_3$, The differentials $\omega = dx/y$ and $\eta = x dx/y$ form a $\mathbf{Z}_p$-basis for the first $p$-adic de Rham cohomology group $\mathrm{H}^1$ of $E$, and we wish to compute the matrix $F$ of absolute Frobenius with respect to this basis. Frobenius is $\mathbf{Z}_p$-linear, since we are working over $\mathbf{Z}_p$; if we were working over the Witt vectors of $\mathbf{F}_q$, then Frobenius would only be semi-linear.

We explicitly calculate $F$ (to a specified precision) using Kedlaya's algorithm, which makes use of Monsky-Washnitzer cohomology of the affine curve $E - \mathcal{O}$. Kedlaya designed his algorithm for computation of zeta functions of hyperelliptic curves over finite fields. An intermediate step in Kedlaya's algorithm is computation of the matrix of absolute Frobenius on $p$-adic de Rham cohomology, via Monsky-Washnitzer cohomology. For more details see [Ked01] and [Ked03]. For recent formulations and applications of fast algorithms to compute Frobenius eigenvalues, see [LW02].

Now that we have computed $F$, we deduce $\mathbf{E}_2(E,\omega)$ as follows. The unit root subspace is a direct factor, call it $U$, of $\mathrm{H}^1$, and we know that a complementary direct factor is the $\mathbf{Z}_p$ span of $\omega$. We also know that $F(\omega)$ lies in $p\,\mathrm{H}^1$, and this tells us that, mod $p^n$, the subspace $U$ is the span of $F^n(\eta)$. Thus if for each $n$, we write $F^n(\eta) = a_n\omega + b_n\eta$, then $b_n$ is a unit (congruent (mod $p$) to the $n$th power of the Hasse invariant) and $\mathbf{E}_2(E,\omega) \equiv -12a_n/b_n \pmod{p^n}$. Note that $a_n$ and $b_n$ are the entries of the second column of the matrix $F^n$.

Algorithm 3.2 (Evaluation of $\mathbf{E}_2(E,\omega)$). Given an elliptic curve over $\mathbf{Q}$ and a good ordinary prime $p \geq 5$, this algorithm approximates $\mathbf{E}_2(E,\omega) \in \mathbf{Z}_p$ modulo $p^n$.

1. [Invariants] Let $c_4$ and $c_6$ be the $c$-invariants of a minimal model of $E$. Set
$$a_4 = -\frac{c_4}{2^4\cdot 3} \qquad \text{and} \qquad a_6 = -\frac{c_6}{2^5\cdot 3^3}.$$
2. [Kedlaya] Apply Kedlaya's algorithm to the hyperelliptic curve $y^2 = x^3 + a_4x + a_6$ (which is isomorphic to $E$) to obtain the matrix $F$ (modulo $p^n$) of the action of absolute Frobenius on the basis
$$\omega = \frac{dx}{y}, \qquad \eta = \frac{x\,dx}{y}.$$
We view $F$ as acting from the left.
3. [Iterate Frobenius] Compute the second column $\begin{pmatrix} a \\ b \end{pmatrix}$ of $F^n$, so $\mathrm{Frob}^n(\eta) = a\omega + b\eta$.
4. [Finished] Output $-12a/b$ (which is a number modulo $p^n$, since $b$ is a unit).

## 3.3 Computing $\mathbf{E}_2(E,\omega)$ using integrality

The algorithm in this section is more elementary than the one in Section 3.2, and is directly motivated by Theorem 1.3. In practice it is very slow, except if $p$ is small (e.g., $p = 5$) and we only require $\mathbf{E}_2(E,\omega)$ to very low precision. Our guess is that it should be exponentially hard to compute a quantity using a log convergent series for it, and that this "integrality" method is essentially the same as using log convergent expansions.

Let $c$ be an indeterminate and in view of (1.9), write $e_2 = -12c + a_1^2 + 4a_2 \in \mathbf{Q}[c]$. If we run Algorithm 3.1 with this (formal) value of $e_2$, we obtain a series $\sigma(t,c) \in \mathbf{Q}[c][[t]]$. For each prime $p \geq 5$, Theorem 1.3 implies that there is a unique choice of $c_p \in \mathbf{Z}_p$ such that $\sigma(t,c_p) = t + \cdots \in t\mathbf{Z}_p[[t]]$

is odd. Upon fixing a prime $p$, we compute the coefficients of $\sigma(t,c)$, which are polynomials in $\mathbf{Q}[c]$; integrality of $\sigma(t,c_p)$ then imposes conditions that together must determine $c_p$ up to some precision, which depends on the number of coefficients that we consider. Having computed $c_p$ to some precision, we recover $\mathbf{E}_2(E,\omega)$ as $-12c_p+a_1^2+4a_2$. We formalize the above as an algorithm.

Algorithm 3.3 (Integrality). Given an elliptic curve over $\mathbf{Q}$ and a good ordinary prime $p \geq 5$, this algorithm approximates the associated $p$-adic $\sigma$-function.

1. [Formal Series] Use Algorithm 3.1 with $e_2 = -12c + a_1^2 + 4a_2$ to compute $\sigma(t) \in \mathbf{Q}[c][[t]]$ to some precision.
2. [Approximate $c_p$] Obtain constraints on $c$ using that the coefficients of $\sigma$ must be in $\mathbf{Z}_p$. These determine $c$ to some precision. (For more details see the example in Section 4.1).

### 3.4 Computing cyclotomic $p$-adic heights

Finally we give an algorithm for computing the cyclotomic $p$-adic height $h_p(P)$ that combines Algorithm 3.2 with the discussion elsewhere in this paper. We have computed $\sigma$ and $h_p$ in numerous cases using the algorithm described below, and implementations of the "integrality" algorithm described above, and the results match.

Algorithm 3.4 (The $p$-adic Height). Given an elliptic curve $E$ over $\mathbf{Q}$, a good ordinary prime $p$, and a non-torsion element $P \in E(\mathbf{Q})$, this algorithm approximates the $p$-adic height $h_p(P) \in \mathbf{Q}_p$.

1. [Prepare Point] Compute a positive integer $m$ such that $mP$ reduces to $\mathcal{O} \in E(\mathbf{F}_p)$ and to the connected component of $\mathcal{E}_{\mathbf{F}_\ell}$ at all bad primes $\ell$. For example, $m$ could be the least common multiple of the Tamagawa numbers of $E$ and $\#E(\mathbf{F}_p)$. Set $Q = mP$ and write $Q = (x,y)$.
2. [Denominator] Let $d$ be the positive integer square root of the denominator of $x$.
3. [Compute $\sigma$] Approximate $\sigma(t)$ using Algorithm 3.1 together with either Algorithm 3.2 or Algorithm 3.3, and set $s = \sigma(-x/y) \in \mathbf{Q}_p$.
4. [Height] Compute $h_p(Q) = \dfrac{1}{p}\log_p\left(\dfrac{s}{d}\right)$, then $h_p(P) = \dfrac{1}{m^2}\cdot h_p(Q)$. Output $h_p(P)$ and terminate.

## 4 Sample Computations

We did the calculations in this section using SAGE [SJ05] and Magma [BCP97]. In particular, SAGE includes an optimized implementation due to J. Balakrishnan, R. Bradshaw, D. Harvey, Y. Qiang, and W. Stein of our algorithm for computing $p$-adic heights for elliptic curves over $\mathbf{Q}$. This implementation includes further tricks, e.g., for series manipulation, which are not described in this paper.

### 4.1 The rank one curve of conductor 37

Let $E$ be the rank 1 curve $y^2 + y = x^3 - x$ of conductor 37. The point $P = (0,0)$ is a generator for $E(\mathbf{Q})$. We illustrate the above algorithms in detail by computing the $p$-adic height of $P$ for the good ordinary prime $p = 5$. The steps of Algorithm 3.4 are as follows:

1. [Prepare Point] The component group of $\mathcal{E}_{\mathbf{F}_{37}}$ is trivial. The group $E(\mathbf{F}_5)$ has order 8 and the reduction of $P$ to $E(\mathbf{F}_5)$ also has order 8, so let
$$Q = 8P = \left(\frac{21}{25}, -\frac{69}{125}\right).$$
2. [Denominator] We have $d = 5$.
3. [Compute $\sigma$] We illustrate computation of $\sigma(t)$ using both Algorithm 3.2 and Algorithm 3.3.
   (a) [Compute $\sigma(t,c)$] We use Algorithm 3.1 with $e_2 = 12c - a_1^2 - 4a_2$ to compute $\sigma$ as a series in $t$ with coefficients polynomials in $c$, as follows:
      i. [Compute Formal Log] Using the recurrence, we find that
      $$w(t) = t^3 + t^6 - t^7 + 2t^9 - 4t^{10} + 2t^{11} + 5t^{12} - 5t^{13} + 5t^{14} + \cdots$$
      Thus
      $$x(t) = t^{-2} - t + t^2 - t^4 + 2t^5 - t^6 - 2t^7 + 6t^8 - 6t^9 - 3t^{10} + \cdots$$
      $$y(t) = -t^{-3} + 1 - t + t^3 - 2t^4 + t^5 + 2t^6 - 6t^7 + 6t^8 + 3t^9 + \cdots$$
      so integrating (3.4) we see that the formal logarithm is
      $$z(t) = t + \frac{1}{2}t^4 - \frac{2}{5}t^5 + \frac{6}{7}t^7 - \frac{3}{2}t^8 + \frac{2}{3}t^9 + 2t^{10} - \frac{60}{11}t^{11} + 5t^{12} + \cdots$$
      ii. [Reversion] Using reversion, we find $F$ with $F(z(t)) = t$:
      $$F(z) = z - \frac{1}{2}z^4 + \frac{2}{5}z^5 + \frac{1}{7}z^7 - \frac{3}{10}z^8 + \frac{2}{15}z^9 - \frac{1}{28}z^{10} + \frac{54}{385}z^{11} + \cdots$$
      iii. [Compute $\wp$] We have $a_1 = a_2 = 0$, so
      $$\alpha(t) = x(t) + (a_1^2 + 4a_2)/12 = x(t),$$
      so
      $$\wp(z) = x(F(z)) = z^{-2} + \frac{1}{5}z^2 - \frac{1}{28}z^4 + \frac{1}{75}z^6 - \frac{3}{1540}z^8 + \cdots$$
      Note that the coefficient of $z^{-1}$ is 0 and all exponents are even.

iv. [Compute $\sigma(t,c)$] Noting again that $a_1 = a_2 = 0$, we have

$$\begin{aligned} g(z,c) &= \frac{1}{z^2} - \wp(z) + \frac{12c - a_1^2 - 4a_2}{12} \\ &= c - \frac{1}{5}z^2 + \frac{1}{28}z^4 - \frac{1}{75}z^6 + \frac{3}{1540}z^8 - \frac{1943}{3822000}z^{10} + \cdots \end{aligned}$$

Formally integrating twice and exponentiating, we obtain

$$\begin{aligned} \sigma(z,c) &= z \cdot \exp\left(\int\int g(z,c)dzdz\right) \\ &= z \cdot \exp\Big(\frac{c}{2} \cdot z^2 - \frac{1}{60}z^4 + \frac{1}{840}z^6 - \frac{1}{4200}z^8 + \frac{1}{46200}z^{10} \\ &\qquad - \frac{1943}{504504000}z^{12} + \cdots\Big) \\ &= z + \frac{1}{2}cz^3 + \left(\frac{1}{8}c^2 - \frac{1}{60}\right)z^5 + \left(\frac{1}{48}c^3 - \frac{1}{120}c + \frac{1}{840}\right)z^7 + \\ &\qquad \left(\frac{1}{384}c^4 - \frac{1}{480}c^2 + \frac{1}{1680}c - \frac{1}{10080}\right)z^9 + \cdots \end{aligned}$$

Finally,

$$\begin{aligned} \sigma(t) = \sigma(z(t)) = t + \frac{1}{2}ct^3 + \frac{1}{2}t^4 + \left(\frac{1}{8}c^2 - \frac{5}{12}\right)t^5 + \frac{3}{4}ct^6 + \\ \left(\frac{1}{48}c^3 - \frac{73}{120}c + \frac{103}{120}\right)t^7 + \cdots \end{aligned}$$

(b) [Approximate] The first coefficient of $\sigma(t)$ that gives integrality information is the coefficient of $t^7$. Since

$$\frac{1}{48}c^3 - \frac{73}{120}c + \frac{103}{120} \in \mathbf{Z}_5,$$

multiplying by 5 we see that

$$\frac{5}{48}c^3 - \frac{73}{24}c + \frac{103}{24} \equiv 0 \pmod 5.$$

Thus

$$c \equiv \frac{103}{24} \cdot \frac{24}{73} \equiv 1 \pmod 5.$$

The next useful coefficient is the coefficient of $t^{11}$, which is

$$\frac{1}{3840}c^5 - \frac{169}{2880}c^3 + \frac{5701}{6720}c^2 + \frac{127339}{100800}c - \frac{40111}{7200}$$

Multiplying by 25, reducing coefficients, and using integrality yields the congruence

$$10c^5 + 5c^3 + 20c^2 + 2c + 3 \equiv 0 \pmod{25}.$$

Writing $c = 1+5d$ and substituting gives the equation $10d+15 \equiv 0 \pmod{25}$, so $2d+3 \equiv 0 \pmod 5$. Thus $d \equiv 1 \pmod 5$, hence $c = 1+5+O(5^2)$. Repeating the procedure above with more terms, we next get new information from the coefficient of $t^{31}$, where we deduce that $c = 1+5+4\cdot 5^2+O(5^3)$.

Using Algorithm 3.2: Using Kedlaya's algorithm (as implemented in [BCP97]) we find almost instantly that

$$\mathbf{E}_2(E,\omega) = 2+4\cdot 5+2\cdot 5^3+5^4+3\cdot 5^5+2\cdot 5^6+5^8+3\cdot 5^9+4\cdot 5^{10}+\cdots.$$

Thus

$$c = \frac{1}{12}\mathbf{E}_2(E,\omega) = 1+5+4\cdot 5^2+5^3+5^4+5^6+4\cdot 5^7+3\cdot 5^8+2\cdot 5^9+4\cdot 5^{10}+\cdots,$$

which is consistent with what we found above using integrality.

4. [Height] For $Q = (x,y) = 8(0,0)$ as above, we have

$$s = \sigma\left(-\frac{x}{y}\right) = \sigma\left(\frac{35}{23}\right) = 4\cdot 5+5^2+5^3+5^4+\cdots,$$

so

$$\begin{aligned} h_5(Q) &= \frac{1}{5}\cdot \log_5\left(\frac{s}{5}\right) = \frac{1}{5}\cdot\log_5(4+5+5^2+5^3+2\cdot 5^5+\cdots) \\ &= 3+5+2\cdot 5^3+3\cdot 5^4+\cdots. \end{aligned}$$

Finally,

$$h_5(P) = \frac{1}{8^2}\cdot h_5(Q) = 2+4\cdot 5+5^2+2\cdot 5^3+2\cdot 5^4+\cdots.$$

Remark 4.1. A *very* good check to see whether or not any implementation of the algorithms in this paper is really correct, is just to make control experiments every once in a while, by computing $h(P)$ and then comparing it with $h(2P)/4$, $h(3P)/9$, etc. In particular, compute $h(P)-h(nP)/n^2$ for several $n$ and check that the result is $p$-adically small. We have done this in many cases for the implementation used to compute the tables in this section.

### 4.2 Curves of ranks 1, 2, 3, 4, and 5

#### 4.2.1 Rank 1

The first (ordered by conductor) curve of rank 1 is the curve with Cremona label 37A, which we considered in Section 4.1 above.

| $p$ | $p$-adic regulator of 37A |
|---|---|
| 5 | $1 + 5 + 5^2 + 3 \cdot 5^5 + 4 \cdot 5^6 + O(5^7)$ |
| 7 | $1 + 7 + 3 \cdot 7^2 + 7^3 + 6 \cdot 7^4 + 2 \cdot 7^5 + 4 \cdot 7^6 + O(7^7)$ |
| 11 | $7 + 9 \cdot 11 + 7 \cdot 11^2 + 8 \cdot 11^3 + 9 \cdot 11^4 + 2 \cdot 11^5 + 7 \cdot 11^6 + O(11^7)$ |
| 13 | $12 \cdot 13 + 5 \cdot 13^2 + 9 \cdot 13^3 + 10 \cdot 13^4 + 4 \cdot 13^5 + 2 \cdot 13^6 + O(13^7)$ |
| 23 | $20 + 10 \cdot 23 + 18 \cdot 23^2 + 16 \cdot 23^3 + 13 \cdot 23^4 + 4 \cdot 23^5 + 15 \cdot 23^6 + O(23^7)$ |
| 29 | $19 + 4 \cdot 29 + 26 \cdot 29^2 + 2 \cdot 29^3 + 26 \cdot 29^4 + 26 \cdot 29^5 + 17 \cdot 29^6 + O(29^7)$ |
| 31 | $15 + 10 \cdot 31 + 13 \cdot 31^2 + 2 \cdot 31^3 + 24 \cdot 31^4 + 9 \cdot 31^5 + 8 \cdot 31^6 + O(31^7)$ |
| 41 | $30 + 2 \cdot 41 + 23 \cdot 41^2 + 15 \cdot 41^3 + 27 \cdot 41^4 + 8 \cdot 41^5 + 17 \cdot 41^6 + O(41^7)$ |
| 43 | $30 + 30 \cdot 43 + 22 \cdot 43^2 + 38 \cdot 43^3 + 11 \cdot 43^4 + 29 \cdot 43^5 + O(43^6)$ |
| 47 | $11 + 37 \cdot 47 + 27 \cdot 47^2 + 23 \cdot 47^3 + 22 \cdot 47^4 + 34 \cdot 47^5 + 3 \cdot 47^6 + O(47^7)$ |
| 53 | $26 \cdot 53^{-2} + 30 \cdot 53^{-1} + 20 + 47 \cdot 53 + 10 \cdot 53^2 + 32 \cdot 53^3 + O(53^4)$ |

Note that when $p = 53$ we have $\#E(\mathbf{F}_p) = p$, i.e., $p$ is anomalous.

### 4.3 Rank 2

The first curve of rank 2 is the curve 389A of conductor 389. The $p$-adic regulators of this curve are as follows:

| $p$ | $p$-adic regulator of 389A |
|---|---|
| 5 | $1 + 2 \cdot 5 + 2 \cdot 5^2 + 4 \cdot 5^3 + 3 \cdot 5^4 + 4 \cdot 5^5 + 3 \cdot 5^6 + O(5^7)$ |
| 7 | $6 + 3 \cdot 7^2 + 2 \cdot 7^3 + 6 \cdot 7^4 + 7^5 + 2 \cdot 7^6 + O(7^7)$ |
| 11 | $4 + 7 \cdot 11 + 6 \cdot 11^2 + 11^3 + 9 \cdot 11^4 + 10 \cdot 11^5 + 3 \cdot 11^6 + O(11^7)$ |
| 13 | $9 + 12 \cdot 13 + 10 \cdot 13^2 + 5 \cdot 13^3 + 5 \cdot 13^4 + 13^5 + 9 \cdot 13^6 + O(13^7)$ |
| 17 | $4 + 8 \cdot 17 + 15 \cdot 17^2 + 11 \cdot 17^3 + 13 \cdot 17^4 + 16 \cdot 17^5 + 6 \cdot 17^6 + O(17^7)$ |
| 19 | $3 + 5 \cdot 19 + 8 \cdot 19^2 + 16 \cdot 19^3 + 13 \cdot 19^4 + 14 \cdot 19^5 + 11 \cdot 19^6 + O(19^7)$ |
| 23 | $17 + 23 + 22 \cdot 23^2 + 16 \cdot 23^3 + 3 \cdot 23^4 + 15 \cdot 23^5 + O(23^7)$ |
| 29 | $9 + 14 \cdot 29 + 22 \cdot 29^2 + 29^3 + 22 \cdot 29^4 + 29^5 + 20 \cdot 29^6 + O(29^7)$ |
| 31 | $1 + 17 \cdot 31 + 4 \cdot 31^2 + 16 \cdot 31^3 + 18 \cdot 31^4 + 21 \cdot 31^5 + 8 \cdot 31^6 + O(31^7)$ |
| 37 | $28 + 37 + 11 \cdot 37^2 + 7 \cdot 37^3 + 3 \cdot 37^4 + 24 \cdot 37^5 + 17 \cdot 37^6 + O(37^7)$ |
| 41 | $20 + 26 \cdot 41 + 41^2 + 29 \cdot 41^3 + 38 \cdot 41^4 + 31 \cdot 41^5 + 23 \cdot 41^6 + O(41^7)$ |
| 43 | $40 + 25 \cdot 43 + 15 \cdot 43^2 + 18 \cdot 43^3 + 36 \cdot 43^4 + 35 \cdot 43^5 + O(43^6)$ |
| 47 | $25 + 24 \cdot 47 + 7 \cdot 47^2 + 11 \cdot 47^3 + 35 \cdot 47^4 + 3 \cdot 47^5 + 9 \cdot 47^6 + O(47^7)$ |

### 4.4 Rank 3

The first curve of rank 3 is the curve 5077A of conductor 5077. The $p$-adic regulators of this curve are as follows:

| $p$ | $p$-adic regulator of 5077A |
|---|---|
| 5 | $5^{-2} + 5^{-1} + 4 + 2 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + 4 \cdot 5^4 + 2 \cdot 5^5 + 5^6 + O(5^7)$ |
| 7 | $1 + 3 \cdot 7 + 3 \cdot 7^2 + 4 \cdot 7^3 + 4 \cdot 7^5 + O(7^7)$ |
| 11 | $6 + 11 + 5 \cdot 11^2 + 11^3 + 11^4 + 8 \cdot 11^5 + 3 \cdot 11^6 + O(11^7)$ |
| 13 | $2 + 6 \cdot 13 + 13^3 + 6 \cdot 13^4 + 13^5 + 4 \cdot 13^6 + O(13^7)$ |
| 17 | $11 + 15 \cdot 17 + 8 \cdot 17^2 + 16 \cdot 17^3 + 9 \cdot 17^4 + 5 \cdot 17^5 + 11 \cdot 17^6 + O(17^7)$ |
| 19 | $17 + 9 \cdot 19 + 10 \cdot 19^2 + 15 \cdot 19^3 + 6 \cdot 19^4 + 13 \cdot 19^5 + 17 \cdot 19^6 + O(19^7)$ |
| 23 | $7 + 17 \cdot 23 + 19 \cdot 23^3 + 21 \cdot 23^4 + 19 \cdot 23^5 + 22 \cdot 23^6 + O(23^7)$ |
| 29 | $8 + 16 \cdot 29 + 11 \cdot 29^2 + 20 \cdot 29^3 + 9 \cdot 29^4 + 8 \cdot 29^5 + 24 \cdot 29^6 + O(29^7)$ |
| 31 | $17 + 11 \cdot 31 + 28 \cdot 31^2 + 3 \cdot 31^3 + 17 \cdot 31^5 + 29 \cdot 31^6 + O(31^7)$ |
| 43 | $9 + 13 \cdot 43 + 15 \cdot 43^2 + 32 \cdot 43^3 + 28 \cdot 43^4 + 18 \cdot 43^5 + 3 \cdot 43^6 + O(43^7)$ |
| 47 | $29 + 3 \cdot 47 + 46 \cdot 47^2 + 4 \cdot 47^3 + 23 \cdot 47^4 + 25 \cdot 47^5 + 37 \cdot 47^6 + O(47^7)$ |

For $p = 5$ and $E$ the curve 5077A, we have $\#E(\mathbf{F}_5) = 10$, so $a_p \equiv 1 \pmod 5$, hence $p$ is anamolous.

### 4.5 Rank 4

Next we consider the curve of rank 4 with smallest known conductor ($234446 = 2 \cdot 117223$):

$$y^2 + xy = x^3 - x^2 - 79x + 289.$$

Note that computation of the $p$-adic heights is just as fast for this curve as the above curves, i.e., our algorithm for computing heights is insensitive to the conductor, only the prime $p$ (of course, computing the Mordell-Weil group could take much longer if the conductor is large).

| $p$ | $p$-adic regulator of rank 4 curve |
|---|---|
| 5 | $2 \cdot 5^{-2} + 2 \cdot 5^{-1} + 3 \cdot 5 + 5^2 + 4 \cdot 5^3 + 4 \cdot 5^4 + 3 \cdot 5^5 + 3 \cdot 5^6 + O(5^7)$ |
| 7 | $6 \cdot 7 + 4 \cdot 7^2 + 5 \cdot 7^3 + 5 \cdot 7^5 + 3 \cdot 7^6 + O(7^7)$ |
| 11 | $5 + 10 \cdot 11 + 5 \cdot 11^2 + 11^3 + 3 \cdot 11^5 + 11^6 + O(11^7)$ |
| 13 | $12 + 2 \cdot 13 + 4 \cdot 13^2 + 10 \cdot 13^3 + 3 \cdot 13^4 + 5 \cdot 13^5 + 7 \cdot 13^6 + O(13^7)$ |
| 17 | $15 + 8 \cdot 17 + 13 \cdot 17^2 + 5 \cdot 17^3 + 13 \cdot 17^4 + 7 \cdot 17^5 + 14 \cdot 17^6 + O(17^7)$ |
| 19 | $14 + 16 \cdot 19 + 15 \cdot 19^2 + 6 \cdot 19^3 + 10 \cdot 19^4 + 7 \cdot 19^5 + 13 \cdot 19^6 + O(19^7)$ |
| 23 | $3 + 15 \cdot 23 + 15 \cdot 23^2 + 12 \cdot 23^4 + 20 \cdot 23^5 + 7 \cdot 23^6 + O(23^7)$ |
| 29 | $25 + 4 \cdot 29 + 18 \cdot 29^2 + 5 \cdot 29^3 + 27 \cdot 29^4 + 23 \cdot 29^5 + 27 \cdot 29^6 + O(29^7)$ |
| 31 | $21 + 26 \cdot 31 + 22 \cdot 31^2 + 25 \cdot 31^3 + 31^4 + 3 \cdot 31^5 + 14 \cdot 31^6 + O(31^7)$ |
| 37 | $34 + 14 \cdot 37 + 32 \cdot 37^2 + 25 \cdot 37^3 + 28 \cdot 37^4 + 36 \cdot 37^5 + O(37^6)$ |
| 41 | $33 + 38 \cdot 41 + 9 \cdot 41^2 + 35 \cdot 41^3 + 25 \cdot 41^4 + 15 \cdot 41^5 + 30 \cdot 41^6 + O(41^7)$ |
| 43 | $14 + 34 \cdot 43 + 12 \cdot 43^2 + 26 \cdot 43^3 + 32 \cdot 43^4 + 26 \cdot 43^5 + O(43^6)$ |
| 47 | $43 + 47 + 17 \cdot 47^2 + 28 \cdot 47^3 + 40 \cdot 47^4 + 6 \cdot 47^5 + 7 \cdot 47^6 + O(47^7)$ |

### 4.6 Rank 5

Next we consider the curve of rank 5 with smallest known conductor, which is the prime 19047851. The curve is

$$y^2 + y = x^3 - 79x + 342$$

| $p$ | $p$-adic regulator of rank 5 curve |
|---|---|
| 5 | $2 \cdot 5 + 5^2 + 5^3 + 2 \cdot 5^4 + 5^5 + 5^6 + O(5^7)$ |
| 7 | $2 + 6 \cdot 7 + 4 \cdot 7^2 + 3 \cdot 7^3 + 6 \cdot 7^4 + 2 \cdot 7^5 + 4 \cdot 7^6 + O(7^7)$ |
| 11 | $10 + 11 + 6 \cdot 11^2 + 2 \cdot 11^3 + 6 \cdot 11^4 + 7 \cdot 11^5 + 5 \cdot 11^6 + O(11^7)$ |
| 13 | $11 + 8 \cdot 13 + 3 \cdot 13^2 + 4 \cdot 13^3 + 10 \cdot 13^4 + 5 \cdot 13^5 + 6 \cdot 13^6 + O(13^7)$ |
| 17 | $4 + 11 \cdot 17 + 4 \cdot 17^2 + 5 \cdot 17^3 + 13 \cdot 17^4 + 5 \cdot 17^5 + 2 \cdot 17^6 + O(17^7)$ |
| 19 | $11 + 7 \cdot 19 + 11 \cdot 19^2 + 7 \cdot 19^3 + 9 \cdot 19^4 + 6 \cdot 19^5 + 10 \cdot 19^6 + O(19^7)$ |
| 23 | $14 + 14 \cdot 23 + 20 \cdot 23^2 + 6 \cdot 23^3 + 19 \cdot 23^4 + 9 \cdot 23^5 + 15 \cdot 23^6 + O(23^7)$ |
| 29 | $3 + 5 \cdot 29 + 20 \cdot 29^3 + 21 \cdot 29^4 + 18 \cdot 29^5 + 11 \cdot 29^6 + O(29^7)$ |
| 31 | $4 + 26 \cdot 31 + 11 \cdot 31^2 + 12 \cdot 31^3 + 3 \cdot 31^4 + 15 \cdot 31^5 + 22 \cdot 31^6 + O(31^7)$ |
| 37 | $3 + 20 \cdot 37 + 11 \cdot 37^2 + 17 \cdot 37^3 + 33 \cdot 37^4 + 5 \cdot 37^5 + O(37^7)$ |
| 41 | $3 + 41 + 35 \cdot 41^2 + 29 \cdot 41^3 + 22 \cdot 41^4 + 27 \cdot 41^5 + 25 \cdot 41^6 + O(41^7)$ |
| 43 | $35 + 41 \cdot 43 + 43^2 + 11 \cdot 43^3 + 32 \cdot 43^4 + 11 \cdot 43^5 + 18 \cdot 43^6 + O(43^7)$ |
| 47 | $25 + 39 \cdot 47 + 45 \cdot 47^2 + 25 \cdot 47^3 + 42 \cdot 47^4 + 13 \cdot 47^5 + O(47^6)$ |

Note that the regulator for $p = 5$ is not a unit, and $\#E(F_5) = 9$. This is the only example of a regulator in our tables with positive valuation.

# Part II
# Computing expansions for $\mathbf{E}_2$ in terms of classical modular forms

We next study convergence of $\mathbf{E}_2$ in the general context of $p$-adic and overconvergent modular forms. Coleman, Gouvea, and Jochnowitz prove in [CGJ95] that $\mathbf{E}_2$ is *transcendental* over the ring of overconvergent modular forms, so $\mathbf{E}_2$ is certainly non-overconvergent. However, $\mathbf{E}_2$ is *log convergent* in a sense that we make precise in this part of the paper.

## 5 Questions about rates of convergence

Fix $p$ a prime number, which, in this section, we will assume is $\geq 5$. We only consider modular forms of positive even integral weight, on $\Gamma_0(M)$ for some $M$, and with Fourier coefficients in $\mathbf{C}_p$. By a *classical modular form* we will mean one with these properties, and by a *Katz modular form* we mean a $p$-adic modular form in the sense of Katz ([Kat73]), again with these properties, i.e., of integral weight $k \geq 0$, of tame level $N$ for a positive integer $N$ prime to $p$, and with Fourier coefficients in $\mathbf{C}_p$. A *p-integral modular form* is a modular form with Fourier coefficients in $\mathbf{Z}_p$. Note that throughout Sections 5 and 6, all our modular forms can be taken to be with coefficients in $\mathbf{Q}_p$.

If $f$ is a classical, or Katz, modular form, we will often simply identify the form $f$ with its Fourier expansion, $f = \sum_{n\geq 0} c_f(n)q^n$. By $\mathrm{ord}_p(f)$ we mean the greatest lower bound of the non-negative integers $\mathrm{ord}_p(c_f(n))$ for $n \geq 0$. The valuation $\mathrm{ord}_p$ on $\mathbf{C}_p$ here is given its natural normalization, i.e., $\mathrm{ord}_p(p) = 1$.

We say two $p$-integral modular forms are *congruent* modulo $p^n$, denoted

$$f \equiv g \pmod{p^n},$$

if their corresponding Fourier coefficients are congruent modulo $p^n$. Equivalently, $f \equiv g \pmod{p^n}$ if $\mathrm{ord}_p(f - g) \geq n$.

Recall the traditional notation,

$$\sigma_{k-1}(n) = \sum_{0\,<\,d\,\mid\,n} d^{k-1},$$

and put $\sigma(n) = \sigma_1(n)$.

Let $E_k = -b_k/2k + \sum_{n=0}^{\infty} \sigma_{k-1}(n)q^n$ be the Eisenstein series of even weight $k \geq 2$, and denote by $\mathcal{E}_k$ the "other natural normalization" of the Eisenstein series,

$$\mathcal{E}_k = 1 - \frac{2k}{b_k} \cdot \sum_{n=0}^{\infty} \sigma_{k-1}(n)q^n,$$

for $k \geq 2$. We have

$$\mathcal{E}_{p-1} \equiv 1 \pmod{p}.$$

(Note that $\mathcal{E}_k$ is the $q$-expansion of the Katz modular form that we denote by $\mathbf{E}_k$ elsewhere in this paper.)

For $k > 2$ these are classical modular forms of level 1, while the Fourier series $E_2 = -1/24 + \sum_{n=0}^{\infty} \sigma(n)q^n$, and the corresponding $\mathcal{E}_2$, are not; nevertheless, they may all be viewed as Katz modular forms of tame level 1.

Put

$$\sigma^{(p)}(n) = \sum_{0\,<\,d\,\mid\,n;\ (p,d)=1} d,$$

so that we have:

$$\sigma(n) = \sigma^{(p)}(n) + p\sigma^{(p)}(n/p) + p^2\sigma^{(p)}(n/p^2) + \cdots \tag{5.1}$$

where the convention is that $\sigma^{(p)}(r) = 0$ if $r$ is not an integer.

Let $V = V_p$ be the operator on power series given by the rule:

$$V\left(\sum_{n\geq 0} c_n q^n\right) = \sum_{n\geq 0} c_n q^{pn}.$$

If $F = \sum_{n\geq 0} c_n q^n$ is a classical modular form of weight $k$ on $\Gamma_0(M)$, then $V(F)$ is (the Fourier expansion of) a classical modular form of weight $k$ on $\Gamma_0(Mp)$ (cf. [Lan95, Ch. VIII]).

The Fourier series

$$E_2^{(p)} = (1 - pV)E_2 = \frac{p-1}{24} + \sum \sigma_1^{(p)}(n)q^n$$

is, in contrast to $E_2$, a classical modular form (of weight 2 on $\Gamma_0(p)$) and we can invert the formula of its definition to give the following equality of Fourier series:

$$E_2 = \sum_{\nu \geq 0} p^\nu V^\nu E_2^{(p)}, \tag{5.2}$$

this equality being, for the corresponding Fourier coefficients other than the constant terms, another way of phrasing (5.1).

Definition 5.1 (Convergence Rate). We call a function $\alpha(\nu)$ taking values that are either positive integers or $+\infty$ on integers $\nu = 0, \pm 1, \pm 2, \ldots$ a *convergence rate* if $\alpha(\nu)$ is a non-decreasing function such that $\alpha(\nu) = 0$ for $\nu \leq 0$, $\alpha(\nu+\mu) \leq \alpha(\nu) + \alpha(\mu)$, and $\alpha(\nu)$ tends to $+\infty$ as $\nu$ does.

A simple nontrivial example of a convergence rate is

$$\alpha(\nu) = \begin{cases} 0 & \text{for } \nu \leq 0, \\ \nu & \text{for } \nu \geq 0. \end{cases}$$

If $\alpha(\nu)$ is a convergence rate, put $T\alpha(\nu) = \alpha(\nu - 1)$; note that $T\alpha(\nu)$ is also a convergence rate ($T$ translates the graph of $\alpha$ one to the right). Given a collection $\{\alpha_j\}_{j \in J}$ of convergence rates, the "max" function $\alpha(\nu) = \max_{j \in J} \alpha_j(\nu)$ is again a convergence rate.

Definition 5.2 ($\alpha$-Convergent). Let $\alpha$ be a convergence rate. A Katz modular form $f$ is *$\alpha$-convergent* if there is a function $a : \mathbf{Z}_{\geq 0} \to \mathbf{Z}_{\geq 0}$ such that

$$f = \sum_{\nu=0}^{\infty} p^{a(\nu)} f_\nu \mathcal{E}_{p-1}^{-\nu} \tag{5.3}$$

with $f_\nu$ a classical $p$-integral modular form (of weight $k + \nu(p-1)$ and level $N$) and $a(\nu) \geq \alpha(\nu)$ for all $\nu \geq 0$.

If $\alpha' \leq \alpha$ are convergence rates and a modular form $f$ is *$\alpha$-convergent* then it is also *$\alpha'$-convergent*. As formulated, an expansion of the shape of (5.3) for a given $f$ is not unique but [Kat73] and [Gou88] make a certain sequence of choices that enable them to get canonical expansions of the type (5.3), dependent on those initial choices. Specifically, let $M_{\text{classical}}(N, k, \mathbf{Z}_p)$ denote the $\mathbf{Z}_p$-module of classical modular forms on $\Gamma_0(N)$ of weight $k$ and with Fourier coefficients in $\mathbf{Z}_p$. Multiplication by $\mathcal{E}_{p-1}$ allows one to identify $M_{\text{classical}}(N, k, \mathbf{Z}_p)$ with a saturated $\mathbf{Z}_p$-lattice in $M_{\text{classical}}(N, k+p-1, \mathbf{Z}_p)$. (The lattice is saturated because multiplication by $E_{p-1}(\text{mod } p)$ is injective, since it is the identity map on $q$-expansions.) *Fix*, for each $k$, a $\mathbf{Z}_p$-module,

$$C(N, k+p-1, \mathbf{Z}_p) \subset M_{\text{classical}}(N, k+p-1, \mathbf{Z}_p)$$

that is complementary to $\mathcal{E}_{p-1}\cdot M_{\text{classical}}(N,k,\mathbf{Z}_p)\subset M_{\text{classical}}(N,k+p-1,\mathbf{Z}_p)$. Requiring the classical modular forms $f_\nu$ of the expansion (5.3) to lie in these complementary submodules, i.e., $f_\nu \in C(N,k+\nu(p-1),\mathbf{Z}_p)$ for all $\nu$, pins down the expansion uniquely. Let us call an expansion of the form

$$f=\sum_{\nu=0}^{\infty} p^{a(\nu)} f_\nu \mathcal{E}_{p-1}^{-\nu}$$

pinned down by a choice of complementary submodules as described above a *Katz expansion* of $f$.

A *classical* $p$-integral modular form is, of course, $\alpha$-convergent for every $\alpha$. For any given convergence rate $\alpha$, the $\alpha$-convergent Katz modular forms of tame level $N$ are closed under multiplication, and the collection of them forms an algebra over the ring of classical modular forms of level $N$ (with Fourier coefficients in $\mathbf{Z}_p$). Any Katz $p$-integral modular form is $\alpha$-convergent, for some convergence rate $\alpha$ (see [Gou88]).

Proposition 5.3. *A Katz $p$-integral modular form $f$ of weight $k$ and tame level $N$ as above is $\alpha$-convergent if and only if the Fourier series of $f\mathcal{E}_{p-1}^{\nu}$ is congruent to the Fourier series of a classical $p$-integral modular form (of weight $k+\nu(p-1)$ and level $N$) modulo $p^{\alpha(\nu+1)}$ for every integer $\nu\geq 0$.*

*Proof.* We use the $q$-expansion principle. Specifically, if $G_\nu$ is a classical modular form such that $f\mathcal{E}_{p-1}^{\nu}\equiv G_\nu \pmod{p^{\alpha(\nu+1)}}$ then $g_\nu = p^{-\alpha(\nu+1)}(f\mathcal{E}_{p-1}^{\nu}-G_\nu)$ is again a Katz modular form, and we can produce the requisite $\alpha$-convergent Katz expansion by inductive consideration of these $g_\nu$'s. (Note that the other implication is trivial. Also note our running hypothesis that $p\geq 5$.) □

In view of this, we may define, for any $f$ as in Proposition 5.3, the function $a_f(\nu)$ (for $\nu\geq 0$) as follows: $a_f(0)=0$, and for $\nu\geq 1$, $a_f(\nu)$ is the largest integer $a$ such that $f\mathcal{E}_{p-1}^{\nu-1}$ is congruent to a classical $p$-integral modular form (of weight $k+(\nu-1)(p-1)$ and level $N$) modulo $p^a$.

Corollary 5.4. *The Katz $p$-integral modular form $f$ is $\alpha$-convergent for any convergence rate $\alpha$ that is majorized by the function $a_f$. (I.e., for which $\alpha(\nu)\leq a_f(\nu)$ for all $\nu\geq 0$.)*

Definition 5.5 (Overconvergent of Radius $r$). Let $r\in\mathbf{Q}$ be a positive rational number. A Katz $p$-integral modular form $f$ of tame level $N$ is *overconvergent of radius $r$* if and only if it is $\alpha$-convergent for some function $\alpha$ such that $\alpha(\nu)\geq r\cdot\nu$ for all $\nu$, and $\alpha(\nu)-r\cdot\nu$ tends to infinity with $\nu$.

Remarks 5.6. It is convenient to say, for two function $\alpha(\nu)$ and $\alpha'(\nu)$, that

$$\alpha(\nu)\ \ggg\ \alpha'(\nu)$$

if $\alpha(\nu)\geq\alpha'(\nu)$ and $\alpha(\nu)-\alpha'(\nu)$ tends to infinity with $\nu$. So, we may rephrase the above definition as saying that $f$ is overconvergent with radius $r$ if it is

$\alpha$-convergent with $\alpha(\nu) \gg r \cdot \nu$. The above definition is equivalent to the definition of [Kat73, Gou88] except for the fact that the word *radius* in these references does not denote the rational number $r$ above, but rather a choice of $p$-adic number whose $\mathrm{ord}_p$ is $r$. We may think of our manner of phrasing the definition as being a *definition by Katz expansion convergence rate* as opposed to what one might call the *definition by rigid analytic geometric behavior*, meaning the equivalent, and standard, formulation (cf. [Kat73]) given by considering $f$ as a rigid analytic function on an appropriate extension of the Hasse domain in the (rigid analytic space associated to) $X_0(N)$.

Definition 5.7 ((Precisely) Log Convergent). A Katz $p$-integral modular form $f$ is *log-convergent* if $c \cdot \log(\nu) \le a_f(\nu)$ for some positive constant $c$ and all but finitely many $\nu$ (equivalently: if it is $\alpha$-convergent for $\alpha(\nu) = c \cdot \log(\nu)$ for some positive constant $c$). We will say that $f$ is *precisely log-convergent* if there are positive constants $c, C$ such that $c \cdot \log(\nu) \le a_f(\nu) \le C \cdot \log(\nu)$ for all but finitely many $\nu$.

Remark 5.8. As in Definition 5.1 above, we may think of this manner of phrasing the definition as being a *definition by Katz expansion convergence rate*. This seems to us to be of some specific interest in connection with the algorithms that we present in this article for the computation of $\mathbf{E}_2$. For more theoretical concerns, however, we think it would be interesting to give, if possible, an equivalent *definition by rigid analytic geometric behavior*: is there some explicit behavior at the "rim" of the Hasse domain that characterizes log-convergence?

Proposition 5.9. *Let $p \ge 5$. Let $f$ be a Katz $p$-integral modular form of weight $k$ and tame level $N$ that admits an expansion of the type*

$$f = \sum_{\nu=0}^{\infty} p^\nu \mathcal{F}_\nu \mathcal{E}_{p-1}^{-\nu}$$

*where, for all $\nu \ge 0$, $\mathcal{F}_\nu$ is a classical $p$-integral modular form (of weight $k + \nu(p-1)$) on $\Gamma_0(p^{\nu+1})$. Then $f$ is log-convergent and*

$$\liminf_{n\to\infty} \frac{a_f(n)}{\log(n)} \ge \frac{1}{\log(p)}.$$

*Proof.* The classical modular form $\mathcal{F}_\nu$ on $\Gamma_0(p^{\nu+1})$ is an overconvergent Katz modular form of radius $r$ for any $r$ such that $r < \frac{1}{p^{\nu-1}(p+1)}$ (cf. [Kat73], [Gou88, Cor. II.2.8]). Let

$$\mathcal{F}_\nu = \sum_{\mu=0}^{\infty} f_\mu^{(\nu)} \mathcal{E}_{p-1}^{-\mu}$$

be its Katz expansion. So,

$$\mathrm{ord}_p(f_\mu^{(\nu)}) \;\gg\; \left(\frac{1}{p^{\nu-1}(p+1)} - \epsilon_{\mu,\nu}\right) \cdot \mu$$

for any choice of positive $\epsilon_{\mu,\nu}$. We have

$$f = \sum_{\nu=0}^{\infty} p^{\nu} \sum_{\mu=0}^{\infty} f_{\mu}^{(\nu)} \mathcal{E}_{p-1}^{-(\mu+\nu)},$$

or (substituting $\gamma = \mu + \nu$)

$$f = \sum_{\gamma=0}^{\infty} \left\{ \sum_{\nu=0}^{\gamma} p^{\nu}\ f_{\gamma-\nu}^{(\nu)} \right\} \mathcal{E}_{p-1}^{-\gamma}.$$

Putting $G_\gamma = \sum_{\nu=0}^{\gamma} p^{\nu}\ f_{\gamma-\nu}^{(\nu)}$ we may write the above expansion as

$$f = \sum_{\gamma=0}^{\infty} G_\gamma \mathcal{E}_{p-1}^{-\gamma},$$

and we must show that

$$\mathrm{ord}_p(G_\gamma) \geq c \cdot \log(\gamma)$$

for some positive constant $c$.

For any $\nu \leq \gamma$ we have

$$\mathrm{ord}_p\left(p^{\nu}\ f_{\gamma-\nu}^{(\nu)}\right)\ \geqq\ \nu + \left(\frac{1}{p^{\nu-1}(p+1)} - \epsilon_{\gamma-\nu,\nu}\right)(\gamma - \nu).$$

We need to find a lower bound for the minimum value achieved by the right-hand side of this equation. To prepare for this, first note that at the extreme value $\nu = 0$ we compute $\mathrm{ord}_p(\ f_\gamma^{(0)}) \geq \left(\frac{p}{(p+1)} - \epsilon_{\gamma,0}\right) \cdot \gamma$, and to study the remaining cases, $\nu = 1, \ldots, \gamma$, we look at the function

$$R(t) = t + \left(\frac{1}{p^{t-1}(p+1)}\right)(\gamma - t)$$

in the range $1 \leq t \leq \gamma$. This, by calculus, has a unique minimum at $t = t_\gamma \in (1, \gamma)$ given by the equation

$$\frac{p+1}{p} \cdot p^{t_\gamma} = \log(p) \cdot (\gamma - t_\gamma) + 1. \tag{5.4}$$

Define $e_\gamma = t_\gamma - \log_p(\gamma)$ and substituting, we get:

$$p^{e_\gamma} = \frac{p\log(p)}{p+1} - \frac{p\log(p)}{p+1}\frac{e_\gamma}{\gamma} + A_\gamma \tag{5.5}$$

where $A_\gamma$ goes to zero, as $\gamma$ goes to $\infty$.

If $e_\gamma$ is positive we get that

$$p^{e_\gamma} \leq \frac{p\log(p)}{p+1} + A_\gamma$$

and so $e_\gamma$ is bounded from above, independent of $\gamma$, while if $e_\gamma = -d_\gamma$ with $d_\gamma$ positive, we have

$$\frac{1}{p^{d_\gamma}} = \frac{p\log(p)}{p+1} + \frac{p\log(p)}{p+1}\frac{d_\gamma}{\gamma} + A_\gamma.$$

Recall that since $t_\gamma > 0$ we also have $d_\gamma < \log_p(\gamma)$, so that the right hand side of the displayed equation tends to $\frac{p\log(p)}{p+1}$ as $\gamma$ goes to $\infty$, so the equation forces $d_\gamma$ to be bounded from above, as $\gamma$ tends to $\infty$.

This discussion gives:

Lemma 5.10. *The quantity $|t_\gamma - \log_p(\gamma)|$ is bounded independent of $\gamma$.*

Substituting $t_\gamma = \log_p(\gamma) + e_\gamma$ in the defining equation for $R(t)$ and noting the boundedness of $|e_\gamma|$, we get that $|R(t_\gamma) - \log_p(\gamma)|$ is bounded as $\gamma$ goes to $\infty$, thereby establishing our proposition.

□

Corollary 5.11. *For all $p \geq 5$, the Katz modular form $f = E_2$ is log-convergent and*

$$\liminf_{n\to\infty} \frac{a_f(n)}{\log(n)} \geq \frac{1}{\log(p)}.$$

*Proof.* The modular forms $V^\nu E_2^{(p)}$ are classical modular forms on $\Gamma_0(p^{\nu+1})$ and therefore formula (5.1) exhibits $E_2$ as having a Katz expansion of the shape of (5.3). Proposition 5.9 then implies the corollary. □

Remark 5.12. Is $E_2$ *precisely* log-convergent? The minimal $c$ (cf. Definition 5.7) that can be taken in the log-convergence rate for $f = E_2$ is $\limsup_{n\to\infty}(a_f(n)/\log(n))$. Is this minimal $c$ equal to $1/\log(p)$? It is for $p = 5$, as we will show in Section 6. The previous discussion tells us that, as a kind of generalization of the well-known congruence

$$E_2\mathcal{E}_{p-1} \equiv E_{p+1} \pmod{p},$$

we have that for any $\epsilon > 0$, and all but finitely many $\nu$, there are classical modular forms $\mathcal{G}_\nu$ of level 1 and weight $2 + \nu(p-1)$ such that

$$E_2\mathcal{E}_{p-1}^\nu \equiv \mathcal{G}_\nu \pmod{p^{\lfloor (1-\epsilon)\log_p(\nu)\rfloor}}.$$

Let $\theta = qd/dq$ denote the standard shift operator; so that if $f = \sum_{n\geq 0} c_n q^n$, then $\theta(f) = \sum_{n\geq 0} nc_n q^n$. We have $\mathrm{ord}_p(\theta(f)) \geq \mathrm{ord}_p(f)$. The operator $\theta$ preserves Katz modular forms, and *almost* preserves classical modular forms in the sense that if $f$ is a classical modular form of weight $k \geq 2$ then so is $F = \theta(f) - kfE_2/12$ (cf. [Kat73]). Note, also, that $\mathrm{ord}_p(F) \geq \mathrm{ord}_p(f)$.

Corollary 5.13. *The operator $\theta$ preserves log-convergent Katz modular forms.*

*Proof.* Let $f$ be a log-convergent Katz $p$-integral modular form of weight $k$, of tame conductor $N$ with a Katz expansion,

$$f = \sum_{\nu=0}^{\infty} p^{a(\nu)} f_\nu \mathcal{E}_{p-1}^{-\nu} \tag{5.6}$$

where $a(\nu) \geq c \cdot \log(\nu)$ for some positive $c$, and the $f_\nu$'s are classical $p$-integral modular forms on $\Gamma_0(N)$. Let $F_\nu = \theta(f_\nu) - (k + \nu(p-1)) f_\nu E_2/12$ (which is a classical modular form of weight $k + 2 + \nu(p-1)$ on $\Gamma_0(N)$). Put

$$G = \theta(E_{p-1}) - \frac{p-1}{12} \mathcal{E}_{p-1} E_2.$$

Apply the derivation $\theta$ to (5.6) to get

$$\theta(f) = \sum_{\nu=0}^{\infty} p^{a(\nu)} \Big\{ (F_\nu + (k + \nu(p-1)) f_\nu E_2/12) \mathcal{E}_{p-1}^{-\nu} - \nu f_\nu \mathcal{E}_{p-1}^{-\nu-1} \left( G + \frac{p-1}{12} \mathcal{E}_{p-1} E_2 \right) \Big\}.$$

or:

$$\theta(f) = A + BE_2 - C - DE_2,$$

where

$$\begin{aligned}
A &= \sum_{\nu=0}^{\infty} p^{a(\nu)} F_\nu \mathcal{E}_{p-1}^{-\nu}, \\
B &= \sum_{\nu=0}^{\infty} p^{a(\nu)} (k + \nu(p-1)) f_\nu/12) \mathcal{E}_{p-1}^{-\nu}, \\
C &= \sum_{\nu=0}^{\infty} p^{a(\nu)} \nu f_\nu G \mathcal{E}_{p-1}^{-\nu-1}, \\
D &= \sum_{\nu=0}^{\infty} p^{a(\nu)} \frac{p-1}{12} \nu f_\nu \mathcal{E}_{p-1}.
\end{aligned}$$

Now $A, B, C, D$ are all log-convergent, as is $E_2$ by Corollary 5.11. Therefore so is $\theta(f)$. □

## 6 Precise log convergence of $E_2$ for $p = 2, 3, 5$

In this section we assume $p = 2$, 3 or 5 and let $P, Q, R$ denote the Eisenstein series of level 1 of weights $2, 4, 6$, respectively, normalized so that the constant term in its Fourier expansion is 1. Let $f$ be a Katz form of tame level 1 and weight $k$. Write $k = 4d + 6e$, with $d$ an integer $\geq -1$ and $e = 0$ or 1. Then $fQ^{-d}R^{-e}$ is a Katz form of weight 0, that is, a Katz function. Since 0 is the only supersingular value of $j$ for $p = 2, 3, 5$, a Katz function has an expansion in powers of $j^{-1}$ convergent everywhere on the disc $|j^{-1}| \le 1$. Hence, putting $z = j^{-1}$, we can write

$$f = Q^d R^e \sum_{n=0}^{\infty} c_f(n) z^n = \sum_{n=0}^{\infty} R^e \Delta^n Q^{-3n+d}.$$

with $c_f(n) \in \mathbf{Q}_p$ and $c_f(n) \to 0$ as $n \to \infty$. Let

$$C_{f,p}(N) = \min_{n>N} (\mathrm{ord}_p(c_f(n))).$$

Theorem 6.1. *For $p = 5$, we have $C_{f,5}(N) = a_f(3N + 1 - d)$, for all large $N$.*

*Proof.* Notice that for $p = 5$, $\mathcal{E}_{p-1} = Q$. Let $\nu = 3N + 1 - d$ for large $N$. Then

$$Q^{\nu-1} f = \sum_{n=0}^{N} c(n) R^e \Delta^n Q^{3(N-n)} + R^e Q^d \sum_{n>N} c(n) z^n = F + G,$$

say. We have $\mathrm{ord}_5(G) = \min_{n>N}(\mathrm{ord}_5(c(n)) = C_{f,5}(N)$. [5]

Since $F$ is a classical modular form of weight $12N + 6e$ it follows from the definition of $a_f$ that $a_f(\nu) \ge C_{f,5}(N)$. On the other hand, since $\{R^e \Delta^n Q^{3(N-n)} : 0 \le n \le N\}$ is a basis for the space of classical modular forms of weight $12N + 6e$, it is clear that for any such classical form $F'$, the difference $Q^{\nu-1} f - F'$ is a 5-adic Katz form which can be written as $R^e Q^{3N} g$ with $g$ a Katz function whose $z$-expansion coefficients are $c(n)$ for $n > N$. Thus $\mathrm{ord}_5(Q^{\nu-1} f - F') \le C_{f,5}(N)$. □

We have defined $f$ to be log convergent if

$$\liminf_{n\to\infty} \frac{a_f(n)}{\log(n)} > 0,$$

and to be precisely log convergent if in addition

$$\limsup_{n\to\infty} \frac{a_f(n)}{\log(n)} < \infty.$$

Lemma 6.2. *Suppose $h(n)$ and $H(n)$ are nondecreasing funcions defined for all sufficiently large positive integers $n$. If for some integers $r > 0$ and $s$ we have $H(N) = h(rN + s)$ for all sufficiently large integers $N$, then*

$$\liminf_{n\to\infty} \frac{h(n)}{\log(n)} = \liminf_{N\to\infty} \frac{H(N)}{\log(N)},$$

[5] To justify this claim we extend our definition of $\mathrm{ord}_p$ from the ring of Katz forms with Fourier coefficients in $\mathbf{Z}$ to the ring $\mathbf{Z}_p[[q]]$ of all formal power series with coefficients in $\mathbf{Z}$. Moreover, since $z \in q + q^2\mathbf{Z}_p[[q]]$, we have $\mathbf{Z}_p[[q]] = \mathbf{Z}_p[[z]]$, and for a formal series $g = \sum a_n q^n = \sum b^n z^n$, we have $\mathrm{ord}_p(g) = \min(\mathrm{ord}_p(a_n)) = \min(\mathrm{ord}_p(b_n))$. Also (Gauss Lemma) the rule $\mathrm{ord}(g_1 g_2) = \mathrm{ord}(g_1) + \mathrm{ord}(g_2)$ holds. Since $\mathrm{ord}_5(R) = \mathrm{ord}_5(Q) = 0$, it follows that $\mathrm{ord}_5(G) = C_{f,5}(N)$ as claimed.

*and*

$$\limsup_{n\to\infty}\frac{h(n)}{\log(n)}=\limsup_{N\to\infty}\frac{H(N)}{\log(N)}.$$

*Proof.* We use the fact that $\frac{\log(rx+s)}{\log(x)}\to 1$ as $x\to\infty$. For $n$ and $N$ related by

$$rN+s\le n\le r(N+1)+s$$

we have

$$\frac{h(n)}{\log(n)}\le\frac{h(r(N+1)+s}{\log(rN+s)}=\frac{H(N+1)}{\log(N+1)}\cdot\frac{\log(N+1)}{\log(rN+s)}.$$

Similarly,

$$\frac{h(n)}{\log(n)}\ge\frac{h(rN+s}{\log(r(N+1)+s)}=\frac{H(N)}{\log(N)}\cdot\frac{\log(N)}{\log(r(N+1)+s)}.$$

This proves the lemma, because the second factor of the right hand term in each line approaches 1 as $N$ goes to infinity. □

Theorem 6.1 and Lemma 6.2 show that for $p=5$ we can replace $a_f$ by $C_f$ in the definition of log convergent and precisely log convergent. Therefore we define log convergent and precisely log convergent for $p=2$ and $p=3$ by using $C_{f,p}$ as a replacement for $a_f$.

Theorem 6.3. *For $p=2,3$ or $5$, the weight 2 Eisenstein series $P=\mathbf{E}_2$ is precisely log convergent. In fact,*

$$\lim_{n\to\infty}\frac{C_{P,p}(n)}{\log(n)}=\frac{1}{\log(p)}.$$

During the proof of this theorem we write $c(n)=c_P(n)$ and $C_p(n)=C_{P,p}$.

The cases $p=2,3$ follow immediately from results of Koblitz (cf. [Kob77]). Koblitz writes $P=\sum a_n j^{-n}\frac{qdj}{jdq}$. Since $dj/j=-dz/z$, and as we will see later in this proof, $qdz/zdq=R/Q$, Koblitz's $a_n$ is the negative of our $c(n)$, hence $\mathrm{ord}_p(c(n))=\mathrm{ord}_p(a_n)$. Koblitz shows that if we let $l_p(n)=1+\lfloor\log(n)/\log(p)\rfloor$, the number of digits in the expression of $n$ in base $p$, and let $s_p(n)$ denote the sum of those digits, then $\mathrm{ord}_2(c(n))=l_2(n)+3s_2(n)$ and $\mathrm{ord}_3(c(n))=l_3(n)+s_3(n)$. From this it is an easy exercise to show

$$C_2(n)=\lfloor\log(n+1)/\log(2)\rfloor+4\quad\text{and}\quad C_3(n)=\lfloor(\log(n+1)/\log(3)\rfloor+2,$$

formulas from which cases $p=2$ and $p=3$ of the theorem are evident.

Investigating the case $p=5$ we found experimentally with a PARI program that the following conjecture holds for $n<1029$.

Conjecture 6.4. *We have $\mathrm{ord}_5(c(n))\ge l_5(2n)$, with equality if $n$ written in base 5 contains only the digits 0,1 or 2, but no 3 or 4.*

It is easy to see that Conjecture 6.4 implies that

$$\limsup_{n\to\infty} \frac{C_5(n)}{\log(n)} = \frac{1}{\log(5)}.$$

We already know from Corollary 5.11 that

$$\liminf_{n\to\infty} \frac{a_P(n)}{\log(n)} \geq \frac{1}{\log(5)}.$$

By Lemma 6.2, this is equivalent to

$$\liminf_{n\to\infty} \frac{C_{P,5}(n)}{\log(n)} \geq \frac{1}{\log(5)}.$$

Hence to finish the proof of Theorem 6.3, we need only prove

$$\limsup_{n\to\infty} \frac{C_{P,5}(n)}{\log(n)} \leq \frac{1}{\log(5)}. \tag{6.1}$$

To prove (6.1) it is enough to prove that Conjecture 6.4 holds for $n = 5^m$, that is, $\mathrm{ord}_5(c(n)) = m+1$. Indeed that equality implies that $C_5(n) \leq m+1$ for $n < 5^m$ and, choosing $m$ such that $5^{m-1} \leq n < 5^m$, shows that for every $n$ we have $C_5(n) \leq m+1 \leq \log(n)/\log(5) + 2$.

To prove $\mathrm{ord}_5(c(n)) = m+1$ we use two lemmas.

Lemma 6.5. *We have* $\frac{PQ}{R} - 1 = 3\frac{zdQ}{Qdz}$.

*Proof.* Let $\theta$ denote the classical operator $qd/dq$. From the formula $\Delta = q\prod_{n\geq 1}(1-q^n)^{24}$ we get by logarithmic differentiation the classical formula

$$\frac{\theta\Delta}{\Delta} = P.$$

From $z = 1/j = \Delta/Q^3$ we get by logarithmic differentiation that

$$\frac{\theta z}{z} = \frac{\theta\Delta}{\Delta} - 3\frac{\theta Q}{Q} = P - 3\frac{\theta Q}{Q}.$$

By a formula of Ramanujan (cf. [Ser73, Thm. 4]) we have

$$3\frac{\theta Q}{Q} = P - \frac{R}{Q}.$$

Substituting gives

$$\frac{\theta z}{z} = \frac{R}{Q},$$

and dividing the next to last equation by the last proves the lemma. □

Lemma 6.6. *Let* $F = \sum_{n\geq 1}\sigma_3(n)q^n$, *so that* $Q = 1 + 240F$. *Then* $F \equiv \sum_{m\geq 0}(z^{5^m} + z^{2\cdot 5^m}) \pmod 5$.

*Proof.* Guessing this result by computer experiment, we asked Serre for a proof. He immediately supplied two, one of which is the following. During the rest of this proof all congruences are understood to be modulo 5. Since $F = z + 3z^2 + \cdots$, the statement to be proved is equivalent to $F - F^5 \equiv z + 3z^2$. Using the trivial congruence $Q \equiv 1$ and the congruence $P \equiv R$ (the case $p = 5$ of a congruence of Swinnerton-Dyer, (cf. [Ser73, Thm. 5]), we note that

$$z = \Delta/Q^3 \equiv \Delta = (Q^3 - R^2)/1728 \equiv 2 - 2R^2.$$

The case $p = 5, k = 4$ of formula (**) in section 2.2 of [Ser73] reads $F - F^5 \equiv \theta^3 R$. By Ramanujan's formula

$$\theta R = (PR - Q^2)/2 \equiv 3R^2 - 3,$$

one finds that indeed

$$\theta^3 R \equiv 2R^4 - R^2 - 1 \equiv z + 3z^2,$$

which proves Lemma 6.6. □

Let $F = \sum_{n\geq 1} b(n)z^n$. By Lemma 6.6, $b(5^m)$ and $b(2\cdot 5^m)$ are not divisible by 5. Therefore the $5^m$th and $2\cdot 5^m$th coefficients of $zdF/dz = \sum_{n\geq 1} nb(n)z^n$ are divisible exactly by $5^m$. By Lemma 6.5 we have

$$\sum_{n\geq 1} c(n)z^n = \frac{PQ}{R} - 1 = 3\frac{zdQ}{Qdz} = 3\frac{240zdF}{(1+240F)dz}.$$

This shows that $\mathrm{ord}_5(c(5^m)) = \mathrm{ord}_5(c(2\cdot 5^m)) = m + 1$ thereby completing the proof of Theorem 6.3.

Remark 6.7. For $p = 2$ or 3 a simple analogue of Lemma 6.6 holds, namely $F \equiv \sum_{m\geq 0} z^{p^m} \pmod p$. This can be used to obtain Koblitz's result for the very special case $n = p^m$.

## 7 Discussion

### 7.1 Log convergence

The running hypothesis in Section 5 is that $p \geq 5$, but in Section 6 we considered only $p = 2, 3, 5$. In dealing with the different primes, our discussion changes strikingly, depending on the three slightly different cases:

(1) $p = 2, 3$

(2) $p = 5$

(3) $p \geq 5$

For (7.1), in Section 6 we used expansions in powers of $z = 1/j$ to give a careful analysis of convergence rates, and in contrast, the general discussion of Section 5 *must* keep away from those cases $p = 2, 3$, in order to maintain the formulation that it currently has. The prime $p = 5$ is in a very fortunate position because it can be covered by the general discussion a la (7.1); but we have also given a precise "power series in $1/j$" treatment of $p = 5$. These issues suggest four questions:

1. Is there any relationship between the convergence rate analysis we give, and computation-time estimates for the actual algorithms?

2. We have produced an algebra of log-convergent modular forms, and it has at least one new element that the overconvergent forms do not have, namely $\mathbf{E}_2$. Moreover, it is closed under the action of $\theta$, i.e., "Tate twist". Are there other interesting Hecke eigenforms in this algebra that we should know about? Going the other way, are there any Hecke eigenforms that are *not* log-convergent? Is there something corresponding to the "eigencurve" (it would have to be, at the very least, a surface) that $p$-adically interpolates log-convergent eigenforms? Is a limit (in the sense of $\mathrm{ord}_p$'s of Fourier coefficients) of log-convergent eigenforms again log-convergent? For this last question to make sense, we probably need to know the following:

3. Is there a rigid-analytic growth type of definition (growth at the rim of the Hasse domain) that characterizes log-convergence, just as there is such a definition characterizing overconvergence?

4. Almost certainly one could treat the case $p = 7$ by expansions in powers of $1/(j - 1728) = \Delta/R^2$ in the same way that we did $p = 5$ with powers of $1/j = \Delta/Q^3$. The case $p = 13$ might be more interesting.

### 7.2 Uniformity in the algorithms

We are most thankful to Kiran Kedlaya and Alan Lauder for some e-mail communications regarding an early draft of our article. The topic they address is the extent to which the algorithms for the computation of $\mathbf{E}_2$ of an elliptic curve are "uniform" in the elliptic curve, and, in particular, whether one can get fast algorithms for computing $\mathbf{E}_2$ of specific families of elliptic curves. In this section we give a brief synopsis of their comments.

A "reason" why $\mathbf{E}_2$ should turn out not to be overconvergent is that Katz's formula relates it to the direction of the unit-root subspace in one-dimensional de Rham cohomology, and that seems only to make (at least naive) sense in the ordinary case (and not for points in a supersingular disc, not even ones close to the boundary).

Nevertheless, part of the algorithm has good uniformity properties.

1. *Calculating the matrix of Frobenius:* One can calculate the matrix of Frobenius for, say, all elliptic curves in the Legendre family (or any one-parameter family) and the result is overconvergent everywhere, so this should be relatively efficient. This can be done either by the algorithm developed by Kedlaya, or also using the Gauss-Manin connection, as in Lauder's work, which is probably faster. An approach to computing the "full" Frobenius matrix "all at once" for elliptic curves in the Legendre family has been written up and implemented in Magma by Ralf Gerkmann: See [Ger05] for the paper and program. Lauder's paper [Lau03] also discusses Kedlaya's algorithm "all at once" for a one-parameter family of hyperelliptic curves using the Gauss-Manin connection.

2. *Extracting the unit root subspace in de Rham cohomology:* To compute $\mathbf{E}_2$ for an individual elliptic curve, one can specialize the Frobenius matrix and extract the unit root. But extracting only the unit root part over the entire family at once would involve non-overconvergent series, and consequently might be slow. The *unit root zeta function*, which encodes the unit root of Frobenius over a family of ordinary elliptic curves, has been very well studied by Dwork and Wan (cf. [Wan99]).

### 7.3 Other future projects

1. Explicitly compute anticyclotomic $p$-adic heights, and apply this to the study of universal norm questions that arise in [RM05].

2. Further investigate Kedlaya's algorithm with a parameter in connection with log convergence and computation of heights.

3. Determine if the equality $\lim_{n\to\infty} a_P(n)/\log(n) = 1/\log(p)$ holds for all primes $p$, as it does for $p = 5$ by Theorem 6.3.

## References

[Bes04] Amnon Besser, *The p-adic height pairings of Coleman-Gross and of Nekovář*, Number theory, CRM Proc. Lecture Notes, vol. 36, Amer. Math. Soc., Providence, RI, 2004, pp. 13–25. MR 2076563 (2005f:11130)

[Blu] Antonia W. Bluher, *A Leisurely Introduction to Formal Groups and Elliptic Curves,* `http://www.math.uiuc.edu/algebraic-number-theory/0076/`.

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24 (1997), no. 3–4, 235–265, Computational algebra and number theory (London, 1993). MR 1 484 478

[Col91] Robert F. Coleman, *The universal vectorial bi-extension and p-adic heights*, Invent. Math. 103 (1991), no. 3, 631–650. MR 1091621 (92k:14021)

[CGJ95] Robert F. Coleman, Fernando Q. Gouvêa, and Naomi Jochnowitz, *$E_2$, $\Theta$, and overconvergence*, Internat. Math. Res. Notices (1995), no. 1, 23–41 (electronic). MR 1317641 (96d:11047)

[Ger05] Ralf Gerkmann, `http://www.mathematik.uni-mainz.de/~gerkmann/ellcurves.html`, (2005).

[Gre03] Ralph Greenberg, *Galois theory for the Selmer group of an abelian variety*, Compositio Math. 136 (2003), no. 3, 255–297. MR 1977007 (2004c:11097)

[GJP+05] G. Grigorov, A. Jorza, S. Patrikis, C. Patrascu, and W. Stein, *Verification of the Birch and Swinnerton-Dyer Conjecture for Specific Elliptic Curves*, (Submitted) `http://modular.fas.harvard.edu/papers/bsdalg/` (2005).

[Gou88] F. Q. Gouvêa, *Arithmetic of p-adic modular forms*, Springer-Verlag, Berlin, 1988. MR 91e:11056

[IW03] Adrian Iovita and Annette Werner, *p-adic height pairings on abelian varieties with semistable ordinary reduction*, J. Reine Angew. Math. 564 (2003), 181–203. MR 2021039 (2004j:11066)

[SJ05] William Stein and David Joyner, *Sage: System for algebra and geometry experimentation*, Communications in Computer Algebra (SIGSAM Bulletin) (July 2005), `http://sage.sourceforge.net/`.

[Kat73] Nicholas M. Katz, *p-adic properties of modular schemes and modular forms*, Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 69–190. Lecture Notes in Mathematics, Vol. 350. MR 0447119 (56 #5434)

[Kat76] ———, *p-adic interpolation of real analytic Eisenstein series*, Ann. of Math. (2) 104 (1976), no. 3, 459–571. MR 0506271 (58 #22071)

[Ked01] Kiran S. Kedlaya, *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, J. Ramanujan Math. Soc. 16 (2001), no. 4, 323–338. MR 1877805 (2002m:14019)

[Ked03] K. S. Kedlaya, *Errata for: "Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology" [J. Ramanujan Math. Soc.* 16 *(2001), no. 4, 323–338*, J. Ramanujan Math. Soc. 18 (2003), no. 4, 417–418, Dedicated to Professor K. S. Padmanabhan. MR 2 043 934

[Kob77] Neil Koblitz, 2-*adic and* 3-*adic ordinals of the (1/j)-expansion coefficients for the weight 2 Eisenstein series, Bull. L.M.S. 9 (1977), 188-192.*

[Lan95] S. Lang, *Introduction to modular forms*, Springer-Verlag, Berlin, 1995, With appendixes by D. Zagier and W. Feit, Corrected reprint of the 1976 original.

[Lau03] A. G. B. Lauder, *Rigid cohomology and p-adic point counting*, to appear in a special issue of J. de Thorie des Nombres de Bordeaux, `http://www.maths.ox.ac.uk/~lauder/`.

[LW02] A. G. B. Lauder and D. Wan, *Counting rational points on varieties over finite fields of small characteristic*, to appear in an MSRI Computational Number Theory Proceedings (October, 2002).

[MR04] Barry Mazur and Karl Rubin, *Pairings in the arithmetic of elliptic curves*, Modular curves and abelian varieties, Progr. Math., vol. 224, Birkhäuser, Basel, 2004, pp. 151–163. MR MR2058649 (2005g:11095)

[MT83] B. Mazur and J. Tate, *Canonical height pairings via biextensions*, Arithmetic and geometry, Vol. I, Progr. Math., vol. 35, Birkhäuser Boston, Boston, MA, 1983, pp. 195–237. MR 717595 (85j:14081)

[MT87] ______, *Refined conjectures of the "Birch and Swinnerton-Dyer type"*, Duke Math. J. 54 (1987), no. 2, 711–750. MR 899413 (88k:11039)

[MT91] ______, *The p-adic sigma function*, Duke Math. J. 62 (1991), no. 3, 663–688. MR 93d:11059

[MTT86] B. Mazur, J. Tate, and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. 84 (1986), no. 1, 1–48. MR 830037 (87e:11076)

[Nek93] Jan Nekovář, *On p-adic height pairings*, Séminaire de Théorie des Nombres, Paris, 1990–91, Progr. Math., vol. 108, Birkhäuser Boston, Boston, MA, 1993, pp. 127–202. MR 1263527 (95j:11050)

[Nek03] ______, *Selmer Complexes*, 2003, see `http://www.math.jussieu.fr/~nekovar/pu/`.

[Pla94] Andrew Plater, *Supersingular p-adic height pairings on elliptic curves*, Arithmetic geometry (Tempe, AZ, 1993), Contemp. Math., vol. 174, Amer. Math. Soc., Providence, RI, 1994, pp. 95–105. MR 1299736 (95h:11056)

[PR03a] Bernadette Perrin-Riou, *Arithmétique des courbes elliptiques à réduction supersingulière en $p$*, Experiment. Math. 12 (2003), no. 2, 155–186. MR 2016704 (2005h:11138)

[PR03b] ______, *Arithmétique des courbes elliptiques à réduction supersingulière en $p$*, Experiment. Math. 12 (2003), no. 2, 155–186. MR 2016704

[RM05] K. Rubin and B. Mazur, *Organizing the arithmetic of elliptic curves*, in preparation.

[Sch82] Peter Schneider, *$p$-adic height pairings. I*, Invent. Math. 69 (1982), no. 3, 401–409. MR 679765 (84e:14034)

[Sch85] ______, *$p$-adic height pairings. II*, Invent. Math. 79 (1985), no. 2, 329–374. MR 778132 (86j:11063)

[Ser73] J-P. Serre, *Congruences et formes modulaires [d'après H. P. F. Swinnerton-Dyer]*, Séminaire Bourbaki, 24e année (1971/1972), Exp. No. 416 (Berlin), Springer, 1973, pp. 319–338. Lecture Notes in Math., Vol. 317.

[Sil92] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.

[Wan99] Daqing Wan, *Dwork's conjecture on unit root zeta functions*, Ann. of Math. (2) 150 (1999), no. 3, 867–927. MR MR1740990 (2001a:11108)

[Wut04] Christian Wuthrich, *On $p$-adic heights in families of elliptic curves*, J. London Math. Soc. (2) 70 (2004), no. 1, 23–40. MR 2064750

[Zar90] Yuri G. Zarhin, *$p$-adic heights on abelian varieties*, Séminaire de Théorie des Nombres, Paris 1987–88, Progr. Math., vol. 81, Birkhäuser Boston, Boston, MA, 1990, pp. 317–341. MR 1042777 (91f:11043)

Barry Mazur
Department of Mathematics
Harvard University
mazur@math.harvard.edu

John Tate
Department of Mathematics
University of Texas at Austin
tate@math.utexas.edu

William A. Stein
Department of Mathematics
University of California at San Diego
wstein@ucsd.edu