# An Algorithm for Computing $p$-Adic Heights Using Monsky-Washnitzer Cohomology

William Stein

Notes for a Talk at MIT on 2004-10-15

Let $E$ be an elliptic curve over $\mathbb{Q}$ and suppose

$$P = (x, y) = \left(\frac{a}{d^2}, \frac{b}{d^3}\right) \in E(\mathbb{Q}),$$

with $a, b, d \in \mathbb{Z}$ and $\gcd(a, d) = \gcd(b, d) = 1$. The *naive height* of $P$ is

$$\tilde{h}(P) = \log \max\{|a|, d^2\},$$

and the *canonical height* of $P$ is

$$h(P) = \lim_{n\to\infty} \frac{h(2^n P)}{4^n}.$$

This definition is not good for computation, because $2^n P$ gets huge very quickly, and computing $2^n P$ exactly, for $n$ large, is not reasonable.

In [Cre97, §3.4], Cremona describes an efficient method (due mostly to Silverman) for computing $h(P)$. One defines *local heights* $\hat{h}_p : E(\mathbb{Q}) \to \mathbb{R}$, for all primes $p$, and $\hat{h}_\infty : E(\mathbb{Q}) \to \mathbb{R}$ such that

$$h(P) = \hat{h}_\infty(P) + \sum \hat{h}_p(P).$$

The local heights $\hat{h}_p(P)$ are easy to compute explicitly. For example, when $p$ is a prime of good reduction, $\hat{h}_p(P) = \max\{0, -\mathrm{ord}_p(x)\} \cdot \log(p)$.

*This paper is* **NOT** *about local heights $\hat{h}_p$, and we will not mention them any further.* Instead, this paper is about a canonical global $p$-adic height function

$$h_p : E(\mathbb{Q}) \to \mathbb{Q}_p.$$

These height functions are genuine height functions; e.g., $h_p$ is a quadratic function, i.e, $h_p(mP) = m^2 h(P)$ for all $m$. They appear when defining the $p$-adic regulators that appear in the Mazur-Tate $p$-adic analogues of the Birch and Swinnerton-Dyer conjecture.

**Acknowledgement:** Barry Mazur, John Tate, Mike Harrison, Christian Wuthrich, Nick Katz.

## 1 The $p$-Adic Height Pairing

Let $E$ be an elliptic curve over $\mathbb{Q}$ and suppose $p \geq 5$ is a prime such that $E$ has good ordinary reduction at $p$. Suppose $P \in E(\mathbb{Q})$ is a point that reduces to $0 \in E(\mathbb{F}_p)$ and to the connected component of $\mathcal{E}_{\mathbb{F}_\ell}$ at all bad primes $\ell$. We will define functions $\log_p$, $\sigma$, and $d$ below. In terms of these functions, the $p$-adic height of $P$ is

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

The function $h_p$ satisfies $h_p(nP) = n^2 h_p(P)$ for all integers $n$, so it naturally extends to a function on the full Mordell-Weil group $E(\mathbb{Q})$. Setting

$$\langle P, Q \rangle = \frac{1}{2} \cdot (h_p(P+Q) - h_p(P) - h_p(Q)),$$

we obtain a *nondegenerate* pairing on $E(\mathbb{Q})_{/\,\mathrm{tor}}$, and the $p$-adic regulator is the discriminant of this pairing (which is well defined up to sign).

Investigations into $p$-adic Birch and Swinnerton-Dyer conjectures for curves of positive rank inevitably lead to questions about such height pairings, which motivate our interest in computing it to high precision.

We now define each of the undefined quantities in (1.1). The function $\log_p : \mathbb{Q}_p^* \to \mathbb{Q}_p$ is the unique homomorphism with $\log_p(p) = 1$ that extends the homomorphism $\log_p : 1 + p\mathbb{Z}_p \to \mathbb{Q}_p$ defined by the usual power series of $\log(x)$ about 1. Thus if $x \in \mathbb{Q}_p^*$, we can compute $\log_p(x)$ using the formula

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

where $u = p^{-\operatorname{ord}_p(x)} \cdot x$.

The denominator $d(P)$ is the square root of the denominator of the $x$-coordinate of $P$.

The $\sigma$ function is the most mysterious quantity in (1.1), and it turns out the mystery is closely related to the difficulty of computing the $p$-adic number $\mathbb{E}_2(E, \omega)$, where $\mathbb{E}_2$ is the $p$-adic weight 2 Eisenstein series. There are *many* ways to define or characterize $\sigma$, e.g., [MT91] contains 11 different characterizations! Let

$$x(t) = \frac{1}{t^2} + \cdots \in \mathbb{Z}((t))$$

be the formal power series that expresses $x$ in terms of $t = -x/y$ locally near $0 \in E$. Then Mazur and Tate prove there is exactly one function $\sigma(t) \in t\mathbb{Z}_p[[t]]$ and constant $c \in \mathbb{Q}_p$ that satisfy the equation

$$x(t) + c = -\frac{d}{\omega}\left(\frac{1}{\sigma}\frac{d\sigma}{\omega}\right). \tag{1.2}$$

This defines $\sigma$, and, unwinding the meaning of the expression on the right, it leads to an algorithm to compute $\sigma(t)$ to any desired precision, which we now sketch.

If we expand (1.2), 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 $\mathbb{Z}_p$, so when there are denominators in the polynomials in $c$, we obtain conditions on $c$ modulo powers of $p$. Taking these together for many coefficients yields enough scraps of information to get $c \pmod{p^n}$, for some small $n$, hence $\sigma(t) \pmod{p^n}$. However, this algorithm is *extremely inefficient* and its complexity is unclear (how many coefficients are needed to compute $c$ to precision $p^n$?).

For the last 15 or 20 years, the above unsatisifactory algorithm has been the standard one for computing $p$-adic heights, e.g., when investigating $p$-adic analogues of the BSD conjecture.

*The situation changed a few weeks ago...*

# 2 Using Cohomology to Compute $\sigma$

Suppose that $E$ is an elliptic curve over $\mathbb{Q}$ given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Let $x(t)$ be the formal series as before, and set

$$\wp(t) = x(t) + (a_1^2 + 4a_2)/12 \in \mathbb{Q}((t)).$$

(The function $\wp$ satisfies $(\wp')^2 = 4\wp^3 - g_2\wp - g_3$, etc.; it's the formal analogue of the usual complex $\wp$-function.) In [MT91], Mazur and Tate prove that

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

where $\mathbb{E}_2(E, \omega)$ is the value of the Katz $p$-adic weight 2 Eisenstein series at $(E, \omega)$, and the equality is of elements of $\mathbb{Q}_p((t))$. Thus computing $c$ is equivalent to computing $\mathbb{E}_2(E, \omega)$.

This summer, Mazur, Tate, and I explored many ideas for computing $\mathbb{E}_2(E, \omega)$. Though each was interesting and promising, nothing led to a better algorithm that just computing $c$ as sketched above. Perhaps the difficult of computing $\mathbb{E}_2(E, \omega)$ is somehow at the heart of the theory?

Barry wrote to Nick Katz, who fired off the following email:

## 2.1 Katz's Email

```
Date: Thu, 8 Jul 2004 13:53:13 -0400
From: Nick Katz <nmk@Math.Princeton.EDU>
Subject: Re: convergence of the Eisenstein series of weight two
To: mazur@math.harvard.edu, nmkatz@Math.Princeton.EDU
Cc: tate@math.utexas.edu, was@math.harvard.edu

It seems to me you want to use the interpretation of P as the
```

```
"direction of the unit root subspace", that should make it fast to
compute. Concretely, suppose we have a pair (E, \omega) over Z_p, and
to fix ideas p is not 2 or 3.  Then we write a Weierstrass eqn for E,
y^2 = 4x^3 - g_2x - g_3, so that \omega is dx/y, and we denote by \eta
the differential xdx/y. Then \omega and \eta form a Z_p basis of
H^1_DR = H^1_cris, and the key step is to compute the matrix of
absolute Frobenius (here Z_p linear, the advantage of working over
Z_p: otherwise if over Witt vectors of an F_q, only \sigma-linear).
[This calculation goes fast, because the matrix of Frobenius lives
over the entire p-adic moduli space, and we are back in the glory days
of Washnitzer-Monsky cohomology (of the open curve E - {origin}).]

        Okay, now suppose we have computed the matrix of Frob in the
basis \omega, \eta. The unit root subspace is a direct factor, call
it U, of the H^1, and we know that a complimentary direct factor is
Fil^1 := the Z_p span of \omega. We also know that Frob(\omega) lies
in pH^1, and this tells us that, mod p^n, U is the span of
Frob^n(\eta). What this means concretely is that if we write,
for each n,

   Frob^n(\eta) = a_n\omega + b_n\eta,

then b_n is a unit (cong mod p to the n'th power of the Hasse
invariant) and that P is something like the ratio a_n/b_n (up to a
sign and a factor 12 which i don't recall offhand but which is in my
Antwerp appendix and also in my "p-adic interp. of real
anal. Eis. series" paper).

        So in terms of speed of convergence, ONCE you have Frob, you
have to iterate it n times to calculate P mod p^n. Best, Nick
```

## 2.2 The Algorithms

The following algorithms culminate in an algorithm for computing $h_p(P)$ that incorporates Katz's ideas with the discussion elsewhere in this paper. I have computed $\sigma$ and $h_p$ in numerous cases using the algorithm described below, and using my implementations of the "integrality" algorithm described above and also Wuthrich's algorithm, and the results match. The analysis of some of the necessary precision is not complete. I also have not analyzed the complexity.

The first algorithm computes $\mathbb{E}_2(E, \omega)$.

**Algorithm 2.1 (Evaluation of $\mathbb{E}_2(E, \omega)$).** Given an elliptic curve over $\mathbb{Q}$ and prime $p$, this algorithm computes $\mathbb{E}_2(E, \omega) \in \mathbb{Q}_p$ (to precision $O(p^n)$ say) . We assume that Kedlaya's algorithm is available for computing a presentation of the $p$-adic Monsky-Washnitzer cohomology of $E - \{(0, 0)\}$ with Frobenius action.

1. Let $c_4$ and $c_6$ be the $c$-invariants of a minimal model of $E$. Set
$$a_4 \leftarrow -\frac{c_4}{2^4 \cdot 3} \qquad \text{and} \qquad a_6 \leftarrow -\frac{c_6}{2^5 \cdot 3^3}.$$
2. Apply Kedlaya's algorithm to the hyperelliptic curve $y^2 = x^3 + a_4 x + a_6$ (which is isomorphic to $E$) to obtain the matrix $M$ of the action of absolute Frobenius on the basis
$$\omega = \frac{dx}{y}, \qquad \eta = \frac{xdx}{y}$$
to precision $O(p^n)$. (We view $M$ as acting from the left.)
3. We know $M$ to precision $O(p^n)$. Compute the $n$th power of $M$ and let $\begin{pmatrix} a \\ b \end{pmatrix}$ be the second column of $M^n$. Then $\mathrm{Frob}^n(\eta) = a\omega + b\eta$
4. Output $M$ and $-12a/b$ (which is $\mathbb{E}_2(E, \omega)$), then terminate.

The next algorithm uses the above algorithm to compute $\sigma(t)$.

**Algorithm 2.2 (The Canonical $p$-adic Sigma Function).** Given an elliptic curve $E$ and a good ordinary prime $p$, this algorithm computes $\sigma(t) \in \mathbb{Z}_p[[t]]$ modulo $(p^n, t^m)$ for any given positive integers $n, m$. (I have *not* figured out exactly what precision each object below must be computed to.)

1. Using Algorithm 2.1, compute $e_2 = \mathbb{E}_2(E, \omega) \in \mathbb{Z}_p$ to precision $O(p^n)$.
2. Compute the formal power series $x = x(t) \in \mathbb{Q}[[t]]$ associated to the formal group of $E$ to precision $O(t^m)$.
3. Compute the formal logarithm $z(t) \in \mathbb{Q}((t))$ to precision $O(t^m)$ using that $z(t) = \displaystyle\int \frac{dx/dt}{(2y(t) + a_1 x(t) + a_3)}$, where $x(t) = t/w(t)$ and $y(t) = -1/w(t)$ are the formal $x$ and $y$ functions, and $w(t)$ is given by the explicit inductive formula in [Sil92, Ch. 7]. (Here $t = -x/y$ and $w = -1/y$ and we can write $w$ as a series in $t$.)
4. Using a power series "reversion" (functional inverse) algorithm (see e.g., Mathworld), find the power series $F(z) \in \mathbb{Q}[[z]]$ such that $t = F(z)$. Here $F$ is the reversion of $z$, which exists because $z(t) = t + \cdots$.
5. Set $\wp(t) \leftarrow x(t) + (a_1^2 + 4a_2)/12 \in \mathbb{Q}[[t]]$ (to precision $O(t^m)$), where the $a_i$ are the coefficients of the Weierstrass equation of $E$. Then compute the series $\wp(z) = \wp(F(z)) \in \mathbb{Q}((z))$.
6. Set $g(z) \leftarrow \dfrac{1}{z^2} - \wp(z) + \dfrac{e_2}{12} \in \mathbb{Q}_p((z))$. (Note: The theory suggests the last term should be $-e_2/12$ but the calculations do not work unless I use the above formula. Maybe there are two normalizations of $E_2$ in the literature?)
7. Set $\sigma(z) \leftarrow z \cdot \exp\left( \displaystyle\int \int g(z) \, \mathrm{d}z \, \mathrm{d}z \right) \in \mathbb{Q}_p[[z]]$.
8. Set $\sigma(t) \leftarrow \sigma(z(t)) \in t \cdot \mathbb{Z}_p[[t]]$, where $z(t)$ is the formal logarithm computed above. Output $\sigma(t)$ and terminate.

**Remark 2.3.** The trick of changing from $\wp(t)$ to $\wp(z)$ is essential so that we can solve a certain differential equation using just operations with power series.

The final algorithm uses $\sigma(t)$ to compute the $p$-adic height.

**Algorithm 2.4 ($p$-adic Height).** Given an elliptic curve $E$ over $\mathbb{Q}$, a good ordinary prime $p$, and an element $P \in E(\mathbb{Q})$, this algorithm computes the $p$-adic height $h_p(P) \in \mathbb{Q}_p$ to precision $O(p^n)$. (I will ignore the precision below, though this must be not be ignored for the final version of this paper.)

1. [Prepare Point] Compute an integer $m$ such that $mP$ reduces to $0 \in E(\mathbb{F}_p)$ and to the connected component of $\mathcal{E}_{\mathbb{F}_\ell}$ at all bad primes $\ell$. For example, $m$ could be the least common multiple of the Tamagawa numbers of $E$ and $\#E(\mathbb{F}_p)$. Set $Q \leftarrow mP$ and write $Q = (x, y)$.
2. [Denominator] Let $d$ be the positive integer square root of the denominator of $x$.
3. [Compute $\sigma$] Compute $\sigma(t)$ using Algorithm 2.2, and set $s \leftarrow \sigma(-x/y) \in \mathbb{Q}_p$.
4. [Logs] Compute $h_p(Q) \leftarrow \dfrac{1}{p}\log_p\left(\dfrac{s}{d}\right)$, and $h_p(P) \leftarrow \dfrac{1}{m^2} \cdot h_p(Q)$. Output $h_p(P)$ and terminate.

# 3 Future Directions

Suppose $E_t$ is an elliptic curves over $\mathbb{Q}(t)$. It might be extremely interesting to obtain formula for $\mathbb{E}_2(E_t)$ as something like (?) a power series in $\mathbb{Q}_p[[t]]$. This might shed light on the analytic behavior of the $p$-adic modular form $\mathbb{E}_2$, and on Tate's recent surprising experimental observations about the behavior of the $(1/j)$-expansion of $\mathbb{E}_2$.

It would also be interesting to do yet more computations in support of $p$-adic analogues of the BSD conjectures of [MTT86], especially when $E/\mathbb{Q}$ has large rank. Substantial theoretical work has been done toward these $p$-adic conjectures, and this work may be useful to algorithms for computing information about Shafarevich-Tate and Selmer groups of elliptic curves. For example, in [PR03], Perrin-Riou uses her results about the $p$-adic BSD conjecture in the supersingular case to prove that $Ш(E/\mathbb{Q})[p] = 0$ for certain $p$ and elliptic curves $E$ of rank $> 1$, for which the work of Kolyvagin and Kato does not apply. Mazur and Rubin (with my computational input) are also obtaining results that could be viewed as fitting into this program.

I would like to optimize the implementation of the algorithm. Probably the most time-consuming step is computation of $\mathbb{E}_2(E, \omega)$ using Kedlaya's algorithm. My current implementation uses Michael Harrison's implementation of Kedlaya's algorithm for $y^2 = f(x)$, with $f(x)$ of arbitrary degree. Perhaps implementing just what is needed for $y^2 = x^3 + ax + b$ might be more efficient. Also, Harrison tells me his implementation isn't nearly as optimized as it might be.

It might be possible to compute $p$-adic heights on Jacobians of hyperelliptic curves.

Formulate everything above over number fields, and extend to the case of additive reduction.

Supersingular reduction?

## 4 Examples

The purpose of this section is to show you how to use the MAGMA package I wrote for computing with $p$-adic heights, and give you a sense for how fast it is.

```
> function EC(s) return EllipticCurve(CremonaDatabase(),s); end function;
> E := EC("37A");
> Attach("padic_height.m");
> P := good_ordinary_primes(E,100); P;
[ 5, 7, 11, 13, 23, 29, 31, 41, 43, 47, 53, 59, 61, 67, 71, 73,
79, 83, 89, 97 ]
> for p in P do time print p, regulator(E,p,10); end for;
5 22229672 + O(5^11)
Time: 0.040
7 317628041 + O(7^11)
...
89 15480467821870438719 + O(89^10)
Time: 1.190
97 -11195795337175141289 + O(97^10)
Time: 1.490

> E := EC("389A");
> P := good_ordinary_primes(E,100); P;
[ 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61,
67, 71, 73, 79, 83, 89, 97 ]
> for p in P do time print p, regulator(E,p,10); end for;
5 -3871266 + O(5^11)
Time: 0.260
7 483898350 + O(7^11)
...
89 9775723521676164462 + O(89^10)
Time: 1.330
97 -13688331881071698338 + O(97^10)
Time: 1.820

> E := EC("5077A");
> P := good_ordinary_primes(E,100); P;
[ 5, 7, 11, 13, 17, 19, 23, 29, 31, 43, 47, 53, 59, 61, 67, 71,
73, 79, 83, 89, 97 ]
> for p in P do time print p, regulator(E,p,10); end for;
5 655268*5^-2 + O(5^7)
Time: 0.800
7 -933185758 + O(7^11)
...
89 -3325438607428779200 + O(89^10)
```

```
Time: 1.910
97 -5353586908063282167 + O(97^10)
Time: 2.010

--------

> E := EC("37A");
> time regulator(E,5,50);
115299522541340178416234094637464047 + O(5^51)
Time: 1.860
> Valuation(115299522541340178416234094637464047 - 22229672,5);
9

> time regulator(E,97,50);
-5019271523950156862996295340254565181870308222348277984940964806\
     97957622583267105973403430183075091 + O(97^50)
Time: 31.7
```

## References


[Cre97] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997, Complete text available at http://www.maths.nott.ac.uk/personal/jec/book/.

[MT91] B. Mazur and J. Tate, *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 MR830037 (87e:11076)

[PR03] Bernadette Perrin-Riou, *Arithmétique des courbes elliptiques à réduction supersingulière en p*, Experiment. Math. **12** (2003), no. 2, 155–186. MR MR2016704

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