Computing p-Adic Cyclotomic Heights

William Stein

Notes for a Talk at Harvard on 2004-12-08

Contents

1 Introduction

Let E be an elliptic curve over $\mathbb{Q}$ given by a minimal Weierstrass equation 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, $\hat{h}_p(P) = \max\{0, -\operatorname{ord}_p(x)\} \cdot \log(p)$.

This talk is **NOT** *about local heights $\hat{h}_p$, and we will not mention them any further.* Instead, this talk 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 p-adic analogues of the Birch and Swinnerton-Dyer conjecture, in work of Mazur, Tate, Teitelbaum, Greenberg, Schneider, Perrin-Riou and many other people.

Acknowledgement: Discussions with Mike Harrison, Nick Katz, and Christian Wuthrich.
This is joint work with Barry Mazur and John Tate.

2 The p-Adic Cyclotomic 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 ℓ. We will define functions $\log_p$, σ, and d below. In terms of these functions, the p-adic height of P is

$$h_p(P) = \frac{1}{p} \cdot \log_p\left(\frac{\sigma(P)}{d(P)}\right) \in \mathbb{Q}_p. \tag{2.1}$$

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

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

we obtain a 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). We have the following standard conjecture about this height pairing.

Conjecture 2.1. *The pairing $\langle -, -\rangle_p$ is nondegenerate.*

Investigations into p-adic analogues of the Birch and Swinnerton-Dyer conjecture for curves of positive rank inevitably lead to questions about this height pairings, which motivate our interest in computing it.

We now define each of the undefined quantities in (2.1). The function $\log_p : \mathbb{Q}_p^* \to \mathbb{Q}_p$ is the unique group homomorphism with $\log_p(p) = 0$ 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 have

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

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

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

The σ function is the most mysterious quantity in (2.1), 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 σ, 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 $c \in \mathbb{Z}_p$ that satisfy the equation

$$x(t) + c = -\frac{d}{\omega}\left(\frac{1}{\sigma}\frac{d\sigma}{\omega}\right). \tag{2.2}$$

This defines σ, 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 (2.2), 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 eventually yields enough information to get $c \pmod{p^n}$, for a given n, hence $\sigma(t) \pmod{p^n}$. However, this algorithm is *extremely inefficient* and its complexity is unclear. Cristian Wuthrich, who has probably done more computations with this method than anyone else (and has a nice PARI implementation), told me the following in email (Oct 2004):

> "I believe that in the integrality algorithm, approximately p^n coefficients of the sigma function have to be computed to get c up to p^n (which gives the height up to p^{n+1}). i.e. it is hopelessly ineffective for $p > 100$."

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.

Due to a fortuitous combination of events, the situation recently improved...

3 Using Cohomology to Compute σ

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

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

One can show that the function $\wp$ satisfies $(\wp')^2 = 4\wp^3 - g_2\wp - g_3$, etc.; it's the 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, ω), and the equality is of elements of $\mathbb{Q}_p((t))$. Thus computing the mysterious c is equivalent to computing the p-adic number $\mathbb{E}_2(E, \omega) \in \mathbb{Z}_p$.

"The" weight 2 Eisenstein appears in many ways. In the context of clssical modular forms, the function

$$E_2(z) = 1 - 24\sum_{n=1}^{\infty} \sigma_1(n)q^n$$

is holomorphic on $\mathfrak{h}$, but is not a modular form of level 1. There exists a nonzero constant A such that

$$F_2(z) = E_2(z) + \frac{A}{\pi y} \qquad\qquad y = \mathrm{Im}(z)$$

is not holomorphic, but one can show that it transforms like a modular form of level 1 and weight 2. Thus for any integer $N > 1$, the difference

$$F_2(z) - NF_2(Nz) = E_2(z) - NE_2(Nz)$$

is a modular form for $\Gamma_0(N)$. However, in the context of Katz's p-adic modular forms (i.e., functions on pairs (E, ω)), there is a p-adic Eisenstein series $\mathbb{E}_2$ of level 1. It's q-expansion is

$$\mathbb{E}_2(\mathrm{Tate}(q), \omega_{\mathrm{can}}) = 1 - 24\sum_{n=1}^{\infty} \sigma_1(n)q^n,$$

where Tate(q) is the Tate curve over $\mathbb{Q}_p$ with parameter q and ω_{can} is the canonical nonvanishing differential on the Tate curve.

This summer, Mazur, Tate, and I explored many ideas for computing $\mathbb{E}_2(E,\omega)$ explicitly, where E is a curve with good ordinary reduction at p. Perhaps the difficulty of computing $\mathbb{E}_2(E,\omega)$ is somehow intrinsic to the theory?

3.1 Katz's Email

This section contains an email that Nick Katz sent out in response to a query from Barry Mazur. It is the basis of the algorithm we will describe later.

```
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
```

(I have edited the email below, to better fit the style of these notes.)

It seems to me you want to use the interpretation of $P = \mathbb{E}_2$ as the "*direction of the unit root subspace*"; that should make it fast to compute. Concretely, suppose we have a pair (E,ω) over $\mathbb{Z}_p$, and to fix ideas p is not 2 or 3. Then we write a Weierstrass equation for E,

$$y^2 = 4x^3 - g_2x - g_3,$$

so that $\omega = dx/y$, and we denote by η the differential xdx/y. Then ω and η form a $\mathbb{Z}_p$ basis of

$$\mathrm{H}^1 = \mathrm{H}^1_{\mathrm{dR}},$$

and the key step is to compute the matrix of absolute Frobenius. Here this map is $\mathbb{Z}_p$-linear, since we are working over $\mathbb{Z}_p$; otherwise, if we were working over the Witt vectors of an $\mathbb{F}_q$, the map would only be σ-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 $E - \mathcal{O}$).

Okay, now suppose we have computed the matrix of Frob in the basis ω, η. The unit root subspace is a direct factor, call it U, of the H^1, and we know that a complimentary direct factor is the $\mathbb{Z}_p$ span of ω. We also know that Frob(ω) lies in $p\,\mathrm{H}^1$, and this tells us that, mod p^n, the subspace U is the span of Frob$^n(\eta)$. What this means concretely is that if we write, for each n,

$$\mathrm{Frob}^n(\eta) = a_n\omega + b_n\eta,$$

then b_n is a unit (congruent modulo p to the nth power of the Hasse invariant) and that P is $-12a_n/b_n$. See my Antwerp appendix and also my paper *p-adic interpolation of real analytic Eisenstein series.*

So in terms of speed of convergence, *once* you have Frob, you have to iterate it n times to calculate $P \pmod{p^n}$.

3.2 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 talk. I have computed σ 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. Tate has also done several computations of h_p using other methods, and again the results match. Note: The analysis of some of the necessary precision is not complete below.

Kedlaya's algorithm is an algorithm for computing zeta functions of hyperelliptic curves over finite fields. An intermediate step in his algorithm is computation of the matrix of absolute Frobenius on p-adic de Rham cohomology. In Kedlaya's papers, he determines the precision of various objects needed to compute this matrix to a given precision.

The first algorithm computes the value $\mathbb{E}_2(E, \omega)$ using Kedlaya's algorithm and the method suggested by Katz in the email above.

Algorithm 3.1 (Evaluation of $\mathbb{E}_2(E, \omega)$). Given an elliptic curve over $\mathbb{Q}$ and prime p, this algorithm computes $\mathbb{E}_2(E, \omega) \in \mathbb{Q}_p$. We assume that Kedlaya's algorithm is available for computing a presentation of the p-adic Monsky-Washnitzer cohomology of $E - \{\mathcal{O}\}$ with Frobenius action.

1. 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. 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 nth 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 Algorithm 3.1 to compute $\sigma(t)$.

Algorithm 3.2 (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.

1. Using Algorithm 3.1, compute $e_2 = \mathbb{E}_2(E, \omega) \in \mathbb{Z}_p$ to precision $O(p^n)$.

2. Compute the formal expansion of $x = x(t) \in \mathbb{Q}[[t]]$ in terms of the local parameter $t = -x/y$ at infinity to precision $O(t^m)$.

3. Compute the formal logarithm $z(t) = t + \cdots \in \mathbb{Q}((t))$ to precision $O(t^m)$ using that
$$z(t) = \int \frac{dx/dt}{(2y(t) + a_1 x(t) + a_3)},$$
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, find the unique 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 $\wp(t) = x(t) + (a_1^2 + 4a_2)/12 \in \mathbb{Q}[[t]]$ (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 $g(z) = \dfrac{1}{z^2} - \wp(z) + \dfrac{e_2}{12} \in \mathbb{Q}_p((z))$. [Warning: The theory suggests the last term should be $-e_2/12$ but the calculations do not work unless I use the above formula. There are probably two normalizations of E_2 in the references.]

7. Set $\sigma(z) = z \cdot \exp\left(\int \int g(z)\,\mathrm{dz}\,\mathrm{dz}\right) \in \mathbb{Q}_p[[z]]$.

8. Set $\sigma(t) = \sigma(z(t)) \in t \cdot \mathbb{Z}_p[[t]]$, where $z(t)$ is the formal logarithm computed above. Output $\sigma(t)$ and terminate.

Remark 3.3. 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 3.4 (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 $O(p^n)$.

1. [Prepare Point] Compute an integer m such that mP reduces to $\mathcal{O} \in E(\mathbb{F}_p)$ and to the connected component of $\mathcal{E}_{\mathbb{F}_\ell}$ at all bad primes ℓ. For example, m could be the least common multiple of the Tamagawa numbers of E and $\#E(\mathbb{F}_p)$. 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 σ] Compute $\sigma(t)$ using Algorithm 3.2, and set $s = \sigma(-x/y) \in \mathbb{Q}_p$.

4. [Logs] Compute $h_p(Q) = \dfrac{1}{p}\log_p\left(\dfrac{s}{d}\right)$, and $h_p(P) = \dfrac{1}{m^2} \cdot h_p(Q)$. Output $h_p(P)$ and terminate.

4 Future Directions

In this section we discuss various directions for future investigation.

4.1 Log Convergence

Suppose E_t is an elliptic curves over $\mathbb{Q}(t)$. It might be interesting to obtain formula for $\mathbb{E}_2(E_t)$ as an element of $\mathbb{Q}_p((t))$. This might shed light on the analytic behavior of the p-adic modular form $\mathbb{E}_2$, and on Tate's recent experimental observations about the behavior of the $(1/j)$-expansion of the weight 0 modular function $\mathbb{E}_2 E_4/E_6$. More precisely, Tate computed the expansion of $\mathbb{E}_2 E_4/E_6$ in powers of $1/j$ for $p = 2, 3, 5$, and observed very slow convergence. The rest of this section is very closely based on an email from Tate about his observation.

Here's a very small result concerning the p-adic nature of $\mathbb{E}_2$ for $p = 2, 3, 5$. For the primes $p \leq 5$ we can test the convergence of a weight 0 level 1 p-adic modular function f (with poles only at infinity) by expanding in powers of $z = 1/j$. Say $f = \sum_{n=1}^{\infty} a_n z^n$. If $f = zdg/dz$ for some formal series $g = \sum b_n z^n$ with p-integral coefficients b_n, then $a_n = nb_n$, so for example $a_{p^m} = p^m b_{p^m}$ is divisible by p^m, which is a tiny hint of f having "logarithmic" p-adic convergence.

Theorem 4.1. *The form*

$$f = \frac{E_2 E_4}{E_6} - 1$$

has this property, with $g = 3\log(E_4)$ divisible by 720 in $\mathbb{Z}_2$, $\mathbb{Z}_3$ and $\mathbb{Z}_5$.

I leave the proof as an exercise. The idea is that by well-known formulas, if $P = E_2$, $Q = E_4$, and $R = E_6$, then

$$q\frac{dg}{dq} = 3q\frac{d\log(Q)}{dq} = 3q\frac{dQ}{Qdq} = P - \frac{R}{Q}$$

and

$$q\frac{dz}{zdq} = \frac{R}{Q}.$$

Now divide the first equality by the second to get the result. Note that for $p = 2$ and 3, the result for $n = p^m$ seems just right. For $f = PQ/R$, it gives

$$v_2(a_{2^m}) \geq m + v_2(720) = m + 4,$$

and similarly

$$v_3(a_{3^m}) \geq m + 2,$$

and those inequalities are equalities for 2^m and $3^m < 200$.

For the record, in case it might give a clue to what is going on, experimentally we have, for $n < 200$:

$$v_2(a_n) = l_2(n) + 3s_2(n),$$

where $l_2(n) = 1 + \lfloor \log_2(n) \rfloor$ and $s(n)$ is the sum of the digits of n written in base 2. Similarly for $n < 200$,

$$v_3(a_n) = l_3(n) + s_3(n).$$

For $p = 5$ it seems that at least $v_5(a_n) \geq l_5(n)$; in fact, even

$$v_5(a_n) \geq l_5(2n),$$

with likely equality for $2n = 5^m - 1$ and $5^m + 1$.

4.2 Connections with p-adic Birch and Swinnerton-Dyer

It would also be interesting to do many 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 have been involved with Andrei Jorza and Stephen Patrikas on a project to verify the full Birch and Swinnerton-Dyer conjecture for all elliptic curves of conductor ≤ 1000 and rank ≤ 1. There are many examples in which the rank is 1 and the upper bound coming from Kolyvagin's Euler system is divisible by a prime $p \geq 7$, which also divides a Tamagawa number. The results of Kolyvagin and Kato do not give a sufficiently tight upper bound on $Ш(E/\mathbb{Q})$. However, discussions with Greenberg, Pollack, Grigorov, and Perrin-Riou have convinced me that it might be possible in many cases to do appropriate computations of p-adic heights and derivatives of p-adic L-functions, combined with results of Kato and Schneider, and obtain a sufficiently strong upper bounds on $\#Ш(E/\mathbb{Q})$.

4.3 Optimization

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. (Michael Harrison was a Coates student who was in industry for many years, and is now back.)

Perhaps implementing just what is needed for elliptic curves from Kedlaya's algorithm would be more efficient. Also, Harrison tells me his implementation isn't nearly as optimized as it might be.

4.4 Natural Generalizations

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

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

3. What about when p is a prime of supersingular reduction?

5 Examples

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

```
> function EC(s) return EllipticCurve(CremonaDatabase(),s); end function;
> E := EC("37A");
> Attach("kedlaya.m");        // get this from me
> Attach("padic_height.m");   // get this from me
> 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);
1152995225413401784162340946374640047 + O(5^51)
Time: 1.860
> Valuation(1152995225413401784162340946374640047 - 22229672,5);
9
> time regulator(E,97,50);
-501927152395015686299629534025456518187030822234827798494096480 6\
     979576225832671059734034301830750 91 + 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.