Computations About Tate-Shafarevich Groups Using Iwasawa Theory

William Stein and Christian Wuthrich

3rd February 2007

Abstract

We explain how to combine deep results from Iwasawa theory with explicit computation to obtain information about p-parts of Shafarevich-Tate groups of elliptic curves over $\mathbb{Q}$. This method provides a practical way to compute $\text{Ш}(E/\mathbb{Q})(p)$ in many cases when traditional p-descent methods are completely impractical.

1 Introduction

[1] [[1]]

[2] [[2]]

[3] [[3]]

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

$$y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \tag{1}$$

be a choice of global minimal Weierstrass equation for E. Then Mordell proved [**?**][4] [[4]] that the set of rational points $E(\mathbb{Q})$ is an abelian group of finite rank $r = \operatorname{rank}(E(\mathbb{Q}))$. Birch and Swinnerton-Dyer then conjectured that $r = \operatorname{ord}_{s=1} L(E,s)$, where $L(E,s)$ is the Hasse-Weil L-function of E (see Conjecture 2 below). We call $r_{\text{an}} = \operatorname{ord}_{s=1} L(E,s)$ the analytic rank of E.

There is no known provably correct general algorithm to compute r, but one can computationally obtain upper and lower bounds in any particular case. One way to give a lower bound on r is to search for linearly independent points of small height via the method of descent, which involves searching for points of even smaller height on a collection of auxiliary curves. Complex and p-adic Heegner points constructions can also be used in some cases to bound the rank from below. To give a computable upper bound on the rank r, apart from the case of analytic ranks 0 and 1 when Kolyvagin's work on the Euler systems of Heegner points can be applied, the only general way of obtaining an upper bound is by doing an n-descent for some integer $n > 1$. The 2-descents implemented by John Cremona [Cre97], by Denis Simon [**?**] in PARI and in MAGMA[5], and the 3 and 4 descents in Magma and described in [**?**], are particularly [[5]] powerful. But they may fail in practice to compute the exact rank due to the presence of 2 or 3-torsion elements in the Tate-Shafarevich group.

The Tate-Shafarevich group, denoted by $\text{Ш}(E/\mathbb{Q})$, is a torsion abelian group associated to $E/\mathbb{Q}$. It is the kernel of the localization map

$$0 \longrightarrow \text{Ш}(E/\mathbb{Q}) \longrightarrow \mathrm{H}^1(\mathbb{Q}, E) \longrightarrow \prod_v \mathrm{H}^1(\mathbb{Q}_v, E)$$

[1] [[William: Be sure to cite [Col04b], perrin-riou, etc.]]

[2] [[William: In sections 3–5, it would be good to have an actual short (!) illustrative example in each section.]]

[3] [[Christian: Certainly.]]

[4] [[Christian: I could not find the reference – and I am not sure if we should refer to it anyway]]

[5] [[Christian: I don't like capitalized names, maybe smallcaps ?]]

where the product runs over all places v in $\mathbb{Q}$. The arithmetic importance of this group lies in its geometric interpretation. There is a bijection from $\text{Ш}(E/\mathbb{Q})$ to the $\mathbb{Q}$-isomorphism classes of principal homogeneous spaces $C/\mathbb{Q}$ of E which have points everywhere locally. In particular, such a C is a curve of genus 1 defined over $\mathbb{Q}$ whose Jacobian is isomorphic to E. Nontrivial elements in $\text{Ш}(E/\mathbb{Q})$ correspond to curves C which defy the Hasse principle, i.e., have a point over every completion of $\mathbb{Q}$, but have no points over $\mathbb{Q}$.

Conjecture 1. (Shafarevich and Tate) *The group* $\text{Ш}(E/\mathbb{Q})$ *is finite.*

These two invariants, the rank r and the Tate-Shafarevich group $\text{Ш}(E/\mathbb{Q})$, are encoded in the Selmer groups of E. Fix a prime p, and let $E(p)$ denote the $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-module of all torsion points of E whose orders are powers of p. The Selmer group $\mathcal{S}_p(E/\mathbb{Q})$ is defined by the following exact sequence:

$$0 \longrightarrow \mathcal{S}_p(E/\mathbb{Q}) \longrightarrow \mathrm{H}^1(\mathbb{Q}, E(p)) \longrightarrow \prod_v \mathrm{H}^1(\mathbb{Q}_v, E)\,.$$

Likewise, for any positive integer m,[6] the m-Selmer group is defined by the exact sequence [[6]]

$$0 \to \mathcal{S}^{(m)}(E/\mathbb{Q}) \to \mathrm{H}^1(\mathbb{Q}, E[m]) \longrightarrow \prod_v \mathrm{H}^1(\mathbb{Q}_v, E)$$

where $E[m]$ is the subgroup of elements of order dividing m in E.

It follows from the Kummer sequence that there are short exact sequences

$$0 \longrightarrow E(\mathbb{Q})/mE(\mathbb{Q}) \longrightarrow \mathcal{S}^{(m)}(E/\mathbb{Q}) \longrightarrow \text{Ш}(E/\mathbb{Q})[m] \longrightarrow 0\,.$$

and

$$0 \longrightarrow E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \mathcal{S}_p(E/\mathbb{Q}) \longrightarrow \text{Ш}(E/\mathbb{Q})(p) \longrightarrow 0\,.$$

If the Tate-Shafarevich group is finite, then the $\mathbb{Z}_p$-corank of $\mathcal{S}_p(E/\mathbb{Q})$ is equal to the rank r of $E(\mathbb{Q})$.

The finiteness of $\text{Ш}(E/\mathbb{Q})$ is only known for curves of analytic rank 0 and 1 in which case computation of Heegner points and Kolyvagin's work on Euler systems gives an explicit computable multiple of its order. The group $\text{Ш}(E/\mathbb{Q})$ is not known to be finite for even a single elliptic curve with $r_{\text{an}} \geqslant 2$. In such cases, the best one can do using current techniques is hope to bound the p-part $\text{Ш}(E/\mathbb{Q})(p)$ of $\text{Ш}(E/\mathbb{Q})$, for specific primes p. Even this might not a priori be possible, since it is not known that $\text{Ш}(E/\mathbb{Q})(p)$ is finite. However, if it were the case that $\text{Ш}(E/\mathbb{Q})(p)$ is finite (as Conjecture 1 asserts), then this could be verified by computing Selmer groups $\mathcal{S}^{(p^n)}(E/\mathbb{Q})$ for sufficiently many n (see, e.g., [SS04]). Note that practical computation of $\mathcal{S}^{(p^n)}(E/\mathbb{Q})$ is prohibitively difficult for all but a few very small p^n.

We present in this paper two algorithms using p-adic L-functions $\mathcal{L}_p(E,T)$. They are p-adic analogs of the complex function $L(E,s)$, see section 3 for the definition. Both algorithms rely heavily on the work of Kato [Kat04] which is considered to be a major breakthrough in the direction of a proof of the p-adic version of the Birch and Swinnerton-Dyer conjecture (see section 5).

The first algorithm finds an provable upper bound for the rank r of $E(\mathbb{Q})$ by simply computing approximations to the p-adic L-series for various small primes p. Any upper bound on the vanishing of the $\mathcal{L}_p(E,T)$ at $T=0$ is known to be an upper bound on the rank r. See section 10 for details.

The second algorithm, which is discussed in section 11, gives a new method for computing bounds on the order of $\text{Ш}(E/\mathbb{Q})(p)$, for specific primes p. We will exclude $p=2$, since traditional descent methods work well at $p=2$, and Iwasawa theory is not as well developed for $p=2$. We also exclude some primes p like those for which E has additive reduction, since much of the theory we rely on has not been developed in this case yet (see section 3.6 and 11).[7] [[7]]

This second algorithm uses again the p-adic L-functions $\mathcal{L}_p(E,t)$, but also requires that the full Mordell-Weil group $E(\mathbb{Q})$ is known. Its output, if it yields some, is a

[6] [[Christian: sorry, I changed n to m]]

[7] [[Christian: we say more about the cartan cases ?]]

proven upper bound on the order of $Ш(E/\mathbb{Q})(p)$, in particular it will prove the finiteness of the p-primary part of the Tate-Shafarevich group. But it will not be able to give any information about the structure of $Ш(E/\mathbb{Q})(p)$ as an abelian group or any information on its elements. For such finer results on the Tate-Shafarevich group, there is currently no other general method than to use p^n-descents as described above.[8] The computability of the upper bound on $\#Ш(E/\mathbb{Q})(p)$ relies on several conjectures, such as the finiteness of $Ш(E/\mathbb{Q})(p)$ and the conjectures 3 and 4 on the non-degeneracy of the p-adic height on E. Under the assumption of the so-called main conjecture of Iwasawa theory (see section 7), the result of the algorithm is known to be equal to the order of $Ш(E/\mathbb{Q})(p)$. There are several cases when this conjecture is known to hold by Greenberg and Vatsal in [GV00], by Grigorov in [Gri05], and in a forthcoming paper by Skinner and Urban. [[8]]

Note that both algorithms can possibly be implemented also to give bounds on the rank $E(K)$ and bounds on $\#Ш(E/K)(p)$ for number fields K which are abelian extensions of $\mathbb{Q}$.

[9] [[9]]

Acknowledgments. Ralph Greenberg, Robert Pollack

2 The Birch and Swinnerton-Dyer conjecture

If Conjecture 2 below were true, it would yield an algorithm to compute both the rank r and the order of $Ш(E/\mathbb{Q})$.

Let E be an elliptic curve over $\mathbb{Q}$, and let $L(E, s)$ be the Hasse-Weil L-function associated to the $\mathbb{Q}$-isogeny class of E. According to [**?**] (which completes work initiated in [**?**][10]), the function $L(E, s)$ is holomorphic on the whole complex plane. Let ω_E be the invariant differential $dx/(2y + a_1x + a_3)$ of a minimal Weierstrass equation (1) of E. We write $\Omega_E = \int_{E(\mathbb{R})} \omega_E \in \mathbb{R}_{>0}$ for the Néron period of E. [[10]]

Conjecture 2. (Birch and Swinnerton-Dyer)

1. *The order of vanishing of the Hasse-Weil function $L(E, s)$ at $s = 1$ is equal to the rank $r = \operatorname{rank}(E(\mathbb{Q}))$.*
2. *The leading term $L^*(E, 1)$ of the Taylor expansion of $L(E, s)$ at $s = 1$ satisfies*

$$\frac{L^*(E,1)}{\Omega_E} = \frac{\prod_v c_v \cdot \#Ш(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{\mathrm{tors}})^2} \cdot \mathrm{Reg}(E/\mathbb{Q}) \tag{2}$$

where the Tamagawa numbers are denoted by c_v and $\mathrm{Reg}(E/\mathbb{Q})$ is the regulator of E, i.e., the discriminant of the Néron-Tate canonical height pairing on $E(\mathbb{Q})$.

Note that the conjecture (2) is invariant under isogenies defined over $\mathbb{Q}$ (see Cassels [Cas65]).

Proposition 1. *If Conjecture 2 is true, then there is an algorithm to compute r and $\#Ш(E/\mathbb{Q})$.*

Proof. The proof is well known, but we repeat it here since it illustrates several key ideas. By naively searching for points in $E(\mathbb{Q})$ we obtain a lower bound on r, which is closer and closer to the true rank r, the longer we run the search. At some point this lower bound will equal r, but without using further information we do not know when that will occur. As explained, e.g., in [Cre97], we can for any k compute $L^{(k)}(E, 1)$ to any desired precision. Such computations yield upper bounds on r_{an}. In particular, if we compute $L^{(k)}(E, 1)$ and it is nonzero (to the precision of our computation), then $r_{\mathrm{an}} < k$. Eventually this method will also converge to give an upper bound on r_{an},

[8] [[Christian: maybe you can add here something about visibility.]]

[9] [[Christian: add an overview over the sections?]]

[10] [[Christian: I think that is what you meant]]

though again without further information we do not know when our computed upper bound on r_{an} equals to the true value of r_{an}. However, if we know Conjecture 2, we know that $r = r_{\text{an}}$, hence at some point the lower bound on r computed using point searches, will equal the upper bound on r_{an} computed using the L-series. At this point, by Conjecture 2 we know the true value of r.

Once r is known, one can compute $E(\mathbb{Q})$ via a point search (and saturation [**?**][11]), [[11]]
hence we can approximate $\text{Reg}(E/\mathbb{Q})$ to any desired precision. All other quantities in (2) can also be approximated to any desired precision. Solving for $\#Ш(E/\mathbb{Q})$ in 2 and computed all other quantities to large enough precision to determine $\#Ш(E/\mathbb{Q})$ then determines $\#Ш(E/\mathbb{Q})$, as claimed. □

[12] We wish to emphasize that this algorithm would only produce the order of [[12]]
$Ш(E/\mathbb{Q})$ but no information about its structure as an abelian group.

The algorithm presented at the end of this article will mimic the ideas of the proof of this proposition, but instead of working with the complex L-function it will be in a p-adic setting.

3 The p-adic L-function

We will assume for the rest of this article that E does not admit complex multiplication
(CM), [13] though CM curves are an area of active research for these methods ([**?**, **?**]).[14] [[13]]

In order to formulate a p-adic analogue of the conjecture of Birch and Swinnerton-
Dyer, one needs first a p-adic version of the analytic function $L(E, s)$. Mazur and [[14]]
Swinnerton-Dyer [MSD74] have found such a function. We refer to [MTT86] for details on the construction and the historic references.

Let $\pi\colon X_0(N) \longrightarrow E$ be the modular parametrization of E and let c_π be the Manin constant, i.e., the positive integer satisfying $c_\pi \cdot \pi^*\omega_E = 2\pi i f(\tau)d\tau$ with f the newform associated to E. Manin conjectured that $c_\pi = 1$, and much work has been done toward
this conjecture ([**?**, **?**]).[15] [[15]]

Given a rational number r, consider the image $\pi_*(\{r\})$ in $H_1(E,\mathbb{R})$ of the path joining r to $i\infty$ in the upper half plane. Define

$$\lambda^+(r) = \frac{c_\pi}{2}\cdot\left(\int_{\pi_*(\{r\})}\omega_E + \int_{\pi_*(\{-r\})}\omega_E\right) = \pi i\cdot\left(\int_r^{i\infty} f(\tau)\,d\tau + \int_{-r}^{i\infty} f(\tau)\,d\tau\right)$$

There is a basis $\{\gamma_+, \gamma_-\}$ of $H_1(E,\mathbb{Z})$ such that $\int_{\gamma_+}\omega_E$ is equal to Ω_E if $E(\mathbb{R})$ is connected and to $\frac{1}{2}\,\Omega_E$ otherwise. By a theorem of Manin [Man72], we know that $\lambda^+(r)$ belongs to $\mathbb{Q}\cdot\Omega_E$. We define the modular symbol $[r]^+ \in \mathbb{Q}$ to be

$$[r]^+ \cdot \Omega_E = \lambda^+(r)$$

for all $r \in \mathbb{Q}$. In particular we have $[0]^+ = L(E, 1)\cdot\Omega_E^{-1}$. The quantity $[r]^+$ can be computed either algebraically using modular symbols and linear algebra ([Cre97]) or numerically, by approximating both Ω_E using the Gauss arithmetic-geometry mean and $\lambda^+(r)$ by summing a rapidly convergent series, and bounding the denominator of
$\lambda^+(r)/\Omega_E$ using results about modular symbols.[16][17] [[16]]

Let p be a prime of semistable reduction. We write[18] a_p for the trace of Frobenius. [[17]]
Suppose first that E has good reduction at p. Then $N_p = p + 1 - a_p$ is the number of points on $\tilde{E}(\mathbb{F}_p)$. Let $X^2 - a_p \cdot X + p$ be the characteristic polynomial of Frobenius and

[11] [[Christian: I think I know what you mean, but I don't know a reference for it]]

[12] [[Christian: added]]

[13] [[Christian: I don't think we will need the abbreviation]]

[14] [[Christian: These are two articles I partly read, there are certainly many others, but I don't think it is necessary to include more]]

[15] [[Christian: I guess you though of these two]]

[16] [[William: This is probably way too vague – I'm being lazy.]]

[17] [[Christian: I think it would be good if you could say a little bit more. I simply used the magma implementation, but I always wondered if there is a faster or better way to compute the modular symbols. p-adically, I mean. Maybe you wish to add a paragraph on the computations of modular symbols ?]]

[18] The context should make it clear if we speak about a_p or a_2 and a_3 as in (1).

let $\alpha \in \bar{\mathbb{Q}}_p$ be a root of this polynomial such that $\mathrm{ord}_p(\alpha) < 1$. There are two different possible choices if E has supersingular reduction and there is a single possibility for primes where E has good ordinary reduction. Now if E has multiplicative reduction at p, then a_p is 1 if it is split multiplicative and a_p is -1 if it is non-split multiplicative reduction. In either multiplicative case, we have to take $\alpha = a_p$.

Define a measure on $\mathbb{Z}_p^\times$ with values in $\mathbb{Q}(\alpha)$ by

$$\mu_\alpha(a + p^k\mathbb{Z}_p) = \frac{1}{\alpha^k} \cdot \left[\frac{a}{p^k}\right]^+ - \frac{1}{\alpha^{k+1}} \cdot \left[\frac{a}{p^{k-1}}\right]^+$$

for any $k \geqslant 1$ and $a \in \mathbb{Z}_p^\times$. Given a continuous character χ on $\mathbb{Z}_p^\times$ with values in the completion $\mathbb{C}_p$ of the algebraic closure of $\mathbb{Q}_p$, we may integrate χ against μ_α. Any invertible element x of $\mathbb{Z}_p^\times$ can be written as $\omega(x) \cdot \langle x \rangle$ where $\omega(x)$ is a $(p-1)$st root of unity and $\langle x \rangle$ belongs to $1 + 2p\mathbb{Z}_p$. We define the analytic p-adic L-function by

$$L_\alpha(E, s) = \int_{\mathbb{Z}_p^\times} \langle x \rangle^{s-1} \, d\mu_\alpha(x) \qquad \text{for all } s \in \mathbb{Z}_p.$$

where by $\langle x \rangle^{s-1}$ we mean $\exp_p((s-1) \cdot \log_p(\langle x \rangle))$. The function $L_\alpha(E, s)$ extends to a locally analytic function in s on the disc defined by $|s - 1| < 1$ (see § 13 in [MTT86]).

Let ${}_\infty G$ be the Galois group of the cyclotomic extension $\mathbb{Q}(\mu_{p^\infty})$ obtained by adjoining to $\mathbb{Q}$ all p-power roots of unity. By κ we denote the cyclotomic character ${}_\infty G \longrightarrow \mathbb{Z}_p^\times$. Because the cyclotomic character is an isomorphism, choosing a topological generator γ in $\Gamma = {}_\infty G^{4(p-1)}$ amounts to picking an element $\kappa(\gamma)$ in $1 + 2p\mathbb{Z}_p^\times$. With this choice, we may convert the function $L_\alpha(E, s)$ into a p-adic power series in $T = \kappa(\gamma)^{s-1} - 1$. We write $\mathcal{L}_\alpha(E, T)$ for this series in $\mathbb{Q}_p(\alpha)[\![T]\!]$. We have

$$\mathcal{L}_\alpha(E, T) = \int_{\mathbb{Z}_p^\times} (1 + T)^{\frac{\log(x)}{\log(\kappa(\gamma))}} \, d\mu_\alpha(x) \,. \tag{3}$$

As in [Pol03], we define the polynomial [19] [20] [[19]]

[[20]]

$$\begin{aligned} P_n &= \sum_{a \in (\mathbb{Z}/p^k\mathbb{Z})^\times} \left[\frac{a}{p^k}\right]^+ \cdot (1 + T)^{\frac{\log(a)}{\log(\kappa(\gamma))}} \\ &= \sum_{j=0}^{p^{k-1}-1} \sum_{b=1}^{p-1} \left[\frac{\omega(b) \cdot \kappa(\gamma)^j}{p^k}\right]^+ \cdot (1 + T)^j, \end{aligned}$$

where we changed the summation by putting $a = \omega(b) \cdot \kappa(\gamma)^j$. Then the approximation as a Riemann sum of the above integral for $\mathcal{L}_\alpha(E, T)$ can be written as

$$\mathcal{L}_\alpha(E, T) = \lim_{k \to \infty} \left(\frac{1}{\alpha^k} \cdot P_k - \frac{1}{\alpha^{k+1}} \cdot P_{k-1} \right) \,.$$

3.1 The p-adic multiplier

For a prime of good reduction, we define the p-adic multiplier by

$$\epsilon_p = \left(1 - \tfrac{1}{\alpha}\right)^2 \,. \tag{4}$$

[19] [[William: The meaning of $\log(a)$ doesn't make sense without further explanation. In fact, I think it means that one makes an arbitrary choice of $a \in \mathbb{Z}/p^k\mathbb{Z}$. Making a different choice can and does change P_n, but the change is only modulo some controlled power of the maximal ideal of Λ. The substitution $a = \omega(b) \cdot \kappa(\gamma)^j$ is one possible choice. Presumably this is made clear in [Pol03], so we can just make a quick remark about it.

By the way, regarding computation of this sum, there are two approaches to computing the modular symbols: (1) use linear algebra and compute a presentation for $H_1(X_0(N), \mathbb{Q})$, as in Cremona, etc.;

(2) Compute the period integrals for the $\#\mathbf{P}^1(N)$ Manin symbols $[\gamma] = \{\gamma(0), \gamma(\infty)\}$ directly numerically, by using Atkin-Lehner involutions to move around cusps, break paths, etc., then use continued fractions to write any $[a/p^k]$ in terms of Manin symbols $[\gamma]$. I'm not 100% certain how general method 2 is.]]

[20] [[Christian: I agree. I should have set a before writing the sum. Of course any choice of a's will make the polynomials expression for $\mathcal{L}$ converge. As to the remark on modular symbols see footnote 17.]]

For a prime of bad multiplicative reduction, we put

$$\epsilon_p = \bigl(1 - \tfrac{1}{\alpha}\bigr) = \begin{cases} 0 & \text{if } p \text{ is split multiplicative and} \\ 2 & \text{ if } p \text{ is non-split.} \end{cases}$$

3.2 Interpolation property

The p-adic L-function constructed above satisfies a desired interpolation property with respect to the complex L-function. For instance, we have that

$$\mathcal{L}_\alpha(E,0) = L_\alpha(E,1) = \int_{\mathbb{Z}_p^\times} d\mu_\alpha = \epsilon_p \cdot \frac{L(E,1)}{\Omega_E}\,.$$

A similar formula holds when integrating nontrivial characters of $\mathbb{Z}_p^\times$ against μ_α. If χ is the character on ${}_\infty G$ sending γ to a root of unity ζ of exact order p^n, then

$$\mathcal{L}_\alpha(E,\zeta) = \frac{1}{\alpha^{n+1}} \cdot \frac{p^{n+1}}{G(\chi^{-1})} \cdot \frac{L(E,\chi^{-1},1)}{\Omega_E}\,.$$

Here $G(\chi^{-1})$ is the Gauss sum and $L(E,\chi^{-1},1)$ is the Hasse-Weil L-function of E twisted by χ^{-1}.

3.3 The good ordinary case

Suppose now that the reduction of the elliptic curve at the prime p is good and ordinary, so a_p is not divisible by p. As mentioned before, in this case there is a unique choice of root α of the characteristic polynomial $x^2 - a_p x + p$ that satisfies $\operatorname{ord}_p(\alpha) < 1$. Since α is an algebraic integer, this implies that $\operatorname{ord}_p(\alpha) = 0$, so α is a unit in $\mathbb{Z}_p$. We get therefore a unique p-adic L-function that we will denote simply by $\mathcal{L}_p(E,T) = \mathcal{L}_\alpha(E,T)$. It is proved in [Wut06] that

Proposition 2. *Let E be an elliptic curve with good ordinary reduction at a prime $p > 2$. Then the series $\mathcal{L}_p(E,T)$ belongs to $\mathbb{Z}_p[\![T]\!]$.*

Note that $\operatorname{ord}_p(\epsilon_p)$ is equal to $-2\operatorname{ord}_p(N_p)$ where $N_p = p + 1 - a_p$ is the number of points in the reduction $\tilde{E}(\mathbb{F}_p)$ at p.

3.4 Multiplicative case

We have to separate the case of split from the case of non-split multiplicative reduction. In fact if the reduction is non-split, then the description of the good ordinary case applies just the same. But if the reduction is split multiplicative (the "exceptional case" in [MTT86]), then the p-adic L-series must have a trivial zero, i.e., $\mathcal{L}_p(E,0) = 0$ because $\epsilon_p = 0$. By a result of Greenberg and Stevens [GS93] (see also [Kob05] for a simple proof), we know that

$$\left.\frac{d\mathcal{L}_p(E,T)}{dT}\right|_{T=0} = \frac{1}{\log_p \kappa(\gamma)} \cdot \frac{\log_p(q_E)}{\operatorname{ord}_p(q_E)} \cdot \frac{L(E,1)}{\Omega_E}$$

where q_E denotes the Tate period of E over $\mathbb{Q}_p$. This will replace the interpolation formula. Note that it is now known thanks to [BSDGP96] that $\log_p(q_E)$ is nonzero. Hence we define the p-adic $\mathscr{L}$-invariant as

$$\mathscr{L}_p = \frac{\log_p(q_E)}{\operatorname{ord}_p(q_E)} \neq 0\,. \tag{5}$$

We refer to [Col04a] for a detailed discussion of the different $\mathscr{L}$-invariants and their connections.

3.5 The supersingular case

In the supersingular case, that is when $a_p \equiv 0 \pmod{p}$, we have two roots α and β both of valuation $\frac{1}{2}$. A careful analysis of the functions $\mathcal{L}_\alpha$ and $\mathcal{L}_\beta$ can be found in [Pol03]. The series $\mathcal{L}_\alpha(E,T)$ will not have integral coefficients in $\mathbb{Q}_p(\alpha)$. Nevertheless one can still extract two integral series $\mathcal{L}_p^{\pm}(E,T)$. We will not need this description.

There is a way of rewriting the p-adic L-series which relates more easily to the p-adic height defined in the next section. We follow Perrin-Riou's description in [PR03].

As before ω_E denotes the chosen invariant differential on E. Let $\eta_E = x \cdot \omega_E$. The pair $\{\omega_E, \eta_E\}$ forms a basis of the Dieudonné module $D_p(E) = \mathbb{Q}_p \otimes \mathrm{H}^1_{\mathrm{dR}}(E/\mathbb{Q})$. This $\mathbb{Q}_p$-vector space comes equipped with a (geometric) Frobenius φ acting on it linearly. Its characteristic polynomial is equal to $X^2 - p^{-1}\, a_p\, X + p^{-1}$.

Write $\mathcal{L}_\alpha(E,T)$ as $G(T) + \alpha \cdot H(T)$ with $G(T)$ and $H(T)$ in $\mathbb{Q}_p[\![T]\!]$. Then we define

$$\mathcal{L}_p(T) = G(T) \cdot \omega_E + a_p \cdot H(T) \cdot \omega_E - p \cdot H(T) \cdot \varphi(\omega_E)\,.$$

This is a formal power series with coefficients in $D_p(E) \otimes \mathbb{Q}_p[\![T]\!]$ which contains exactly the same information as $\mathcal{L}_\alpha(E,T)$. See [PR03] for a direct definition. The D_p-valued L-series satisfies again certain interpolation properties,[21] e.g.

$$(1-\varphi)^{-2}\,\mathcal{L}_p(0) = \frac{L(E,1)}{\Omega_E} \cdot \omega_E \quad \in D_p(E)\,.$$

3.6 Additive case

The case of additive reduction is much harder to treat, though we are optimistic that such a treatment is possible. We have not tried to include the possibility of additive reduction in our algorithm. Note that there are two interesting paper of Delbourgo [Del98] and [Del02] on this subject. We will not refer to this case anymore throughout the paper.

4 p-adic heights

The second term to be generalized in the Birch-Swinnerton-Dyer formula is the real valued regulator. In p-adic analogues of the conjecture it is replaced by a p-adic regulator, which is defined using a p-adic analogue of the height pairing. We follow here the generalized version [BPR93], [PR03], and [MSJ05].

Let ν be an element of the Dieudonné module $D_p(E)$. We will define a p-adic height function $h_\nu \colon E(\mathbb{Q}) \longrightarrow \mathbb{Q}_p$ which depends linearly on the vector ν. Hence it is sufficient to define it on the basis $\omega = \omega_E$ and $\eta = \eta_E$.

If $\nu = \omega$, then we define

$$h_\omega(P) = -\log(P)^2$$

where log is the linear extension of the p-adic elliptic logarithm $\log_{\hat{E}} \colon \hat{E}(p\mathbb{Z}_p) \longrightarrow p\mathbb{Z}_p$ defined on the formal group $\hat{E}$.

For $\nu = \eta$, we define first the p-adic sigma function of Bernardi $\sigma(z)$ as in [Ber81]. Denote by $t = -\frac{x}{y}$ the uniformizer at O_E and write $z(t) = \log_{\hat{E}}(t)$. Define the Weierstrass $\wp$-function as usual by

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

Here a_1 and a_2 are the coefficients of the minimal Weierstrass equation (1) of E. The function $\wp(t)$ is a solution to the usual differential equation. We define the sigma-function of Bernardi to be a solution of the equation

$$-\wp(t) = \frac{d}{\omega_E}\left(\frac{1}{\sigma} \cdot \frac{d\sigma}{\omega_E}\right)$$

[21] Perrin-Riou writes in [PR03] the multiplier as $(1-\varphi)^{-1} \cdot (1-p^{-1}\varphi^{-1})$ and she multiplies the right hand side with $L(E/\mathbb{Q}_p, 1)^{-1} = N_p \cdot p^{-1}$. It is easy to see that $(1-\varphi)\cdot(1-p^{-1}\varphi^{-1}) = 1 - \varphi - (\varphi - a_p \cdot p^{-1}) + p^{-1} = N_p \cdot p^{-1}$.

such that $\sigma(0)=0$ and $\sigma(t(-P)) = -\sigma(t(P))$. This provides us with a series

$$\sigma(t) = t + \frac{a_1}{2}\,t^2 + \frac{a_1^2+a_2}{3}\,t^3 + \frac{a_1^3+2a_1a_2+3a_3}{4}\,t^4 + \cdots \in \mathbb{Q}(\!(t)\!)\,.$$

As a function on the formal group $\hat{E}(p\mathbb{Z}_p)$ it converges for $\mathrm{ord}_p(t) > \frac{1}{p-1}$.

Given a point P in $E(\mathbb{Q})$ there exists a multiple $m\cdot P$ such that $\sigma(t(P))$ converges and such that $m\cdot P$ has good reduction at all primes. Denote by $e(m\cdot P)\in\mathbb{Z}$ the square root of the denominator of the x-coordinate of $m\cdot P$. Now define

$$h_\eta(P) = \frac{2}{m^2}\cdot\log_p\left(\frac{\sigma(t(m\cdot P))}{e(m\cdot P)}\right)\,.$$

It is proved in [Ber81] that this function is quadratic and satisfies the parallelogram law.

Finally, if $\nu = a\,\omega + b\,\eta$ then put

$$h_\nu(P) = a\,h_\omega(P) + b\,h_\eta(P)\,.$$

This quadratic function induces a bilinear symmetric pairing $\langle\cdot,\cdot\rangle_\nu$ with values in $\mathbb{Q}_p$.

4.1 The good ordinary case

Since we have only a single p-adic L-function in the case that the reduction is good ordinary, we have also to pin down a canonical choice of a p-adic height function. This was first done by Schneider [Sch82] and Perrin-Riou [PR82]. We refer to [MT91] and [MSJ05] for more details.

Let $\nu_\alpha = a\,\omega + b\,\eta$ be an eigenvector of φ on $D_p(E)$ associated to the eigenvalue $\frac{1}{\alpha}$. The value $e_2 = \mathbf{E}_2(E,\omega_E) = -12\cdot\frac{a}{b}$ is the value of the Katz p-adic Eisenstein series of weight 2 at (E,ω_E). Then, if P has good reduction at all primes and lies in the range of convergence of $\sigma(t)$, we define the canonical p-adic height of P to be

$$\begin{aligned}\hat{h}_p(P) &= \frac{1}{b}\cdot h_{\nu_\alpha}(P)\\ &= -\frac{a}{b}\cdot z(P)^2 + 2\,\log\left(\frac{\sigma(t(P))}{e(P)}\right)\\ &= 2\,\log_p\left(\frac{\exp(\frac{e_2}{24}\log(P)^2)\cdot\sigma(t(P))}{e(P)}\right) = 2\,\log_p\left(\frac{\sigma_p(t(P))}{e(P)}\right)\,. \qquad (6)\end{aligned}$$

The function $\sigma_p(t)$, defined by the last line, is called the canonical sigma-function, see [MT91], it is known to lie in $\mathbb{Z}_p[\![t]\!]$. The p-adic height defined here is up to the factor 2 the same as in [MSJ05].[22]

We write $\langle\cdot,\cdot\rangle_p$ for the canonical p-adic height pairing on $E(\mathbb{Q})$ associated to $\hat{h}_p$ and $\mathrm{Reg}_p(E/\mathbb{Q})$ for its determinant.

Conjecture 3. (Schneider [Sch82]) *The canonical p-adic height is non-degenerate on the free part of $E(\mathbb{Q})$. In other words, the canonical p-adic regulator* $\mathrm{Reg}_p(E/\mathbb{Q})$ *is nonzero.*

Apart from the special case treated in [Ber82] of curves with complex multiplication of rank 1, there are hardly any results on this conjecture. See also [Wut04].

4.2 The multiplicative case

In the case of multiplicative reduction, one may use Tate's p-adic uniformization (see [Sil94]). We have an explicit description of the height pairing in [Sch82]. If one wants to have the same closed formula in the p-adic version of the Birch and Swinnerton-Dyer conjecture for multiplicative primes as for other ordinary primes, the p-adic height has to be

[22] This factor is needed if one does not want to modify the p-adic version of the Birch and Swinnerton-Dyer conjecture 5.

changed slightly. We use here the description of the p-adic regulator given in section II.6 of [MTT86]. Alas, their formula is not correct as explained by Werner in [Wer98].

Let q_E be the Tate parameter of the elliptic curve over $\mathbb{Q}_p$, i.e., we have a homomorphism $\psi\colon \bar{\mathbb{Q}}_p^\times \longrightarrow E(\bar{\mathbb{Q}}_p)$ whose kernel is precisely $q_E^{\mathbb{Z}}$. The image of $\mathbb{Z}_p^\times$ under ψ is equal to the subgroup of points of $E(\mathbb{Q}_p)$ lying on the connected component of the Néron model of E. Now let C be the constant such that $\psi^*(\omega_E) = C \cdot \frac{du}{u}$ where u is a uniformizer of $\mathbb{Q}_p^\times$ at 1. The value of the weight 2 p-adic Eisenstein series can then be computed as

$$e_2 = \mathbf{E}_2(E, \omega_E) = C^2 \cdot \left(1 - 24 \cdot \sum_{n \geqslant 1} \sum_{d \mid n} d. \cdot q^n \right)$$

Then we use the formula of the good ordinary case to define the canonical σ function $\sigma_p(t(P)) = \exp(\frac{e_2}{24} z(P)^2) \cdot \sigma(t(P))$. If the reduction is non-split multiplicative, then we use the formula (6) for the good ordinary case.

Suppose now that the reduction is split multiplicative. Let P be a point in $E(\mathbb{Q})$ having good reduction at all finite places and with trivial reduction at p. Then

$$\hat{h}_p(P) = 2 \log_p \left(\frac{\sigma_p(t(P))}{e(P)} \right) + \frac{\log_p(u(P))^2}{\log(q_E)}$$

where $u(P)$ is the unique element of $\mathbb{Z}_p^\times$ mapping to P under the Tate parametrization ψ. The p-adic regulator is formed as before but with this modified p-adic height $\hat{h}_p$.

4.3 The supersingular case

In the supersingular case, we cannot find a canonical p-adic height with values in $\mathbb{Q}_p$. Instead, the height will have values in the Dieudonné module $D_p(E)$. The main references for this height are [BPR93] and [PR03].

Suppose that $\nu = a\,\omega + b\,\eta$ is any element of $D_p(E)$ not lying in $\mathbb{Q}_p\,\omega_E$ (so $b \neq 0$). It can be easily checked that the value of

$$H_p(P) = \frac{1}{b} \cdot \left(h_\nu(P) \cdot \omega - h_\omega(P) \cdot \nu \right) \quad \in D_p$$

is independent of the choice of ν. We will call this the D_p-valued height on $E(\mathbb{Q})$.

On $D_p(E)$ there is a alternating bilinear form $[\cdot, \cdot]$ characterized by the property that $[\omega_E, \eta_E] = 1$. Write $\mathrm{Reg}_\nu \in \mathbb{Q}_p$ for the regulator of h_ν on a $\mathbb{Z}$-basis of the free part of $E(\mathbb{Q})$ with respect to some decomposition $E(\mathbb{Q}) = F \oplus E(\mathbb{Q})_{\mathrm{tor}}$ (since the height is 0 on torsion, the choice of decomposition does not matter). Then

$$\mathrm{Reg}_p(E/\mathbb{Q}) = \frac{\mathrm{Reg}_\nu \cdot \nu' - \mathrm{Reg}_{\nu'} \cdot \nu}{[\nu', \nu]} \quad \in D_p(E)$$

is independent of the choice of ν and ν' in $D_p(E)$, as long as they do not belong to $\mathbb{Q}_p\,\omega_E$. We call this the D_p-valued regulator of $E/\mathbb{Q}$.

It is not difficult to see that $\mathrm{Reg}_p(E/\mathbb{Q}) = H_p(P)$ if the curve is of rank 1 with generator P. If $E(\mathbb{Q})$ is finite, then $\mathrm{Reg}_p(E/\mathbb{Q})$ is simply ω_E. In both these cases the D_p-valued regulator can not vanish.

If one restricts any p-adic height h_ν to the fine Mordell-Weil group defined in [Wut07] to be the kernel

$$\mathfrak{M}(E/\mathbb{Q}) = \ker \left(E(\mathbb{Q}) \otimes \mathbb{Z}_p \longrightarrow \widehat{E(\mathbb{Q}_p)} \right),$$

where $\widehat{E(\mathbb{Q}_p)}$ is the p-adic completion of $E(\mathbb{Q}_p)$. The restricted height is then independent of the chosen element ν in $D_p(E)$. We call its regulator the fine regulator, which is an element of $\mathbb{Q}_p$ defined up to multiplication by a unit in $\mathbb{Z}_p$.

In general, the D_p-valued regulator is 0 if and only if the fine regulator vanishes.

Conjecture 4. (Perrin-Riou [PR93, Conjecture 3.3.7.i]) *The fine regulator of $E/\mathbb{Q}$ is nonzero for all primes p. In particular, $\mathrm{Reg}_p(E/\mathbb{Q}) \neq 0$ for all primes where E has supersingular reduction.*

4.4 Normalization

In view of Iwasawa theory, it is actually natural to normalize the heights and the regulators depending on the choice of the generator γ. In this way the heights depend on the choice of an isomorphism $\Gamma \longrightarrow \mathbb{Z}_p$ rather than on the $\mathbb{Z}_p$-extension only. This normalization can be achieved by simply dividing $\hat{h}_p(P)$ and $h_\nu(P)$ by $\kappa(\gamma)$. The regulators will be divided by $\kappa(\gamma)^r$ where r is the rank of $E(\mathbb{Q})$. Hence we write

$$\operatorname{Reg}_\gamma(E/\mathbb{Q}) = \frac{\operatorname{Reg}_p(E/\mathbb{Q})}{\kappa(\gamma)^r}$$

5 The p-adic Birch and Swinnerton-Dyer conjecture

5.1 The ordinary case

The following conjecture is due to Mazur, Tate and Teitelbaum [MTT86]. Rather than formulating it for the function $L_\alpha(E,s)$, we state it directly for the series $\mathcal{L}_p(E,T)$. It is then a statement about the development of this function at $T=0$ rather than at $s=1$.

Conjecture 5. (Mazur, Tate and Teitelbaum [MTT86]) *Let E be an elliptic curve with good ordinary reduction or with multiplicative reduction at a prime p.*

- *The order of vanishing of the p-adic L-function $\mathcal{L}_p(E,T)$ at $T=0$ is equal to the rank r, unless E has split multiplicative reduction at p in which case the order of vanishing is equal to $r+1$.*
- *The leading term $\mathcal{L}_p^*(E,0)$ satisfies*

$$\mathcal{L}_p^*(E,0) = \epsilon_p \cdot \frac{\prod_v c_v \cdot \#\text{Ш}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{tors})^2} \cdot \operatorname{Reg}_\gamma(E/\mathbb{Q}) \tag{7}$$

unless the reduction is split multiplicative in which case the leading term is

$$\mathcal{L}_p^*(E,0) = \mathscr{L}_p \cdot \frac{\prod_v c_v \cdot \#\text{Ш}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{tors})^2} \cdot \operatorname{Reg}_\gamma(E/\mathbb{Q}). \tag{8}$$

The conjecture assert exact equality, not just equality up to a p-adic unit. However, the current approaches to the conjecture, which go via the main conjecture of Iwasawa theory, all prove results up to a p-adic unit, since the characteristic power series is only defined up to a unit.

5.2 The supersingular case

The conjecture in the case of supersingular reduction is given in [BPR93] and [PR03]. The conjecture relates here an algebraic and an analytic value in the $\mathbb{Q}_p$-vector space $D_p(E)$ of dimension 2. The fact of having two coordinates was used cleverly by Kurihara and Pollack in [KP05] to construct global points via a p-adic analytic computation.

We say that an element $a(T)\cdot\omega_E + b(T)\cdot\eta_E$ in $D_p(E)\otimes\mathbb{Q}_p[\![T]\!]$ has order d at $T=0$ if d is equal to the minimum of the orders of $a(T)$ and $b(T)$.

Conjecture 6. (Bernardi and Perrin-Riou [BPR93]) *Let E be an elliptic curve with good supersingular reduction at a prime p.*

- *The order of vanishing of the D_p-valued L-function $\mathcal{L}_p(E,T)$ at $T=0$ is equal to the rank r.*
- *The leading term $\mathcal{L}_p^*(E,0)$ satisfies*

$$(1-\varphi)^{-2}\cdot\mathcal{L}_p^*(E,0) = \frac{\prod_v c_v \cdot \#\text{Ш}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{tors})^2} \cdot \operatorname{Reg}_\gamma(E/\mathbb{Q}) \quad \in D_p(E) \tag{9}$$

6 Iwasawa theory of elliptic curves

We suppose from now on that $p > 2$. Let ${}_{\infty}\mathbb{Q}$ be the Galois extension of $\mathbb{Q}$ whose Galois group is Γ. It is the unique $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$. Let Λ be the completed group algebra $\mathbb{Z}_p[\![\Gamma]\!]$. We use the fixed topological generator γ of Γ to identify Λ with $\mathbb{Z}_p[\![T]\!]$ by sending γ to $1+T$. It is well-known that any finitely generated Λ-module admits a decomposition as a direct sum of elementary Λ-modules. Denote by ${}_{n}\mathbb{Q}$ the n^{th} layer of the $\mathbb{Z}_p$-extension. As before, we may define the p-Selmer group over ${}_{n}\mathbb{Q}$ by the exact sequence

$$0 \longrightarrow \mathcal{S}_p(E/{}_{n}\mathbb{Q}) \longrightarrow \mathrm{H}^1({}_{n}\mathbb{Q}, E(p)) \longrightarrow \prod_{\upsilon} \mathrm{H}^1({}_{n}\mathbb{Q}_{\upsilon}, E)$$

[23] [24] with the product running over all places υ of ${}_{n}\mathbb{Q}$. Moreover, we define $\mathcal{S}_p(E/{}_{\infty}\mathbb{Q})$ to be the limit $\varinjlim \mathcal{S}_p(E/{}_{n}\mathbb{Q})$ following the maps induced by the restriction maps $\mathrm{H}^1({}_{n}\mathbb{Q}, E(p)) \longrightarrow \mathrm{H}^1({}_{n+1}\mathbb{Q}, E(p))$. The group $\mathcal{S}_p(E/{}_{\infty}\mathbb{Q})$ contains essentially the information about the growth of the rank of $E({}_{n}\mathbb{Q})$ and of the size of $\text{Ш}(E/{}_{n}\mathbb{Q})(p)$ as n tends to infinity. We will consider the Pontryagin dual [[23]] [[24]]

$$X(E/{}_{\infty}\mathbb{Q}) = \mathrm{Hom}\,(\mathcal{S}_p(E/{}_{\infty}\mathbb{Q}), \mathbb{Q}_p/\mathbb{Z}_p)$$

which is a finitely generated Λ-module (see [CS00]).

6.1 The ordinary case

Assume now that the reduction at p is good and ordinary or of multiplicative type. Kato's[25][26] theorem 17.4 in [Kat04], which uses the work of Rohrlich [**?**], states that $X(E/{}_{\infty}\mathbb{Q})$ is a torsion Λ-module. Hence by the decomposition theorem, we may associated to it a characteristic series $f_E(T)$ in Λ. The series [[25]] [[26]]

$$f_E(T) \in \mathbb{Z}_p[\![T]\!] \tag{10}$$

is well-defined up to multiplication by a unit in $\Lambda^{\times}$.

In analogy to the zeta-function of a variety over a finite field, one should think of $f_E(T)$ as a generating function encoding the growth of the rank and the Tate-Shafarevich group. For instance, the zeros of $f_E(T)$ at roots of unity whose orders are powers of p describe the growth of the rank. Since a nonzero power series with coefficients in $\mathbb{Z}_p$ can only have finitely many zeros, one can show that the rank of $E({}_{n}\mathbb{Q})$ has to stabilize in the tower ${}_{n}\mathbb{Q}$. In other words, the Mordell-Weil group $E({}_{\infty}\mathbb{Q})$ is still of finite rank.

The following relatively old result is due to Schneider [Sch85] and Perrin-Riou [PR82]. The multiplicative case is due to Jones [Jon89].

Theorem 3 (Schneider, Perrin-Riou, Jones)**.**
The order of vanishing of $f_E(T)$ at $T = 0$ is at least equal to the rank r. It is equal to r if and only if the p-adic height pairing is non-degenerate (conjecture 3) and the p-primary part of the Tate-Shafarevich group $\text{Ш}(E/\mathbb{Q})(p)$ is finite (conjecture 1). In this case the leading term of the series $f_E(T)$ has the same valuation as

$$\epsilon_p \cdot \frac{\prod_{\upsilon} c_{\upsilon} \cdot \#\text{Ш}(E/\mathbb{Q})(p)}{(\#E(\mathbb{Q})(p))^2} \cdot \mathrm{Reg}_{\gamma}(E/\mathbb{Q})$$

unless the reduction is split multiplicative in which case the same formula holds with ϵ_p replaced by $\mathscr{L}_p$.

[23] [[William: Would you be opposed to using the notation $\mathcal{S}_p(E/{}_{n}\mathbb{Q})$? It's clearer and easier to read in this case.]]

[24] [[Christian: I agree. But do we want to change to $X({}_{\infty}\mathbb{Q}, E)$ which is certainly not very standard ? Or $\text{Ш}({}_{n}\mathbb{Q}, E)$?]]

[25] [[William: that $f_E(T) \mid \mathcal{L}$]]

[26] [[Christian: no. it is actually a step in proving the divisibility.]]

6.2 The supersingular case

The supersingular case is much more complicated, since the Λ-module $X(E/_\infty\mathbb{Q})$ is not torsion. A very beautiful approach to the supersingular case has been found by Pollack [Pol03] and Kobayashi [Kob03]. As mentioned above there exists two p-adic series $\mathcal{L}_p^{\pm}(E,T)$ to which will correspond two new Selmer groups $X^{\pm}(E/_\infty\mathbb{Q})$ which now are Λ-torsion. Despite the advantages of this $\pm$-theory, we are using the approach of Perrin-Riou here. See section 3 in [PR03].

Let T_pE be the Tate module and define ${}_\infty\mathrm{H}^1_{\mathrm{loc}}$ to be the projective limit of the cohomology groups $\mathrm{H}^1({}_n\mathbb{Q}_\mathfrak{p}, T_pE)$ following the corestriction maps. Here ${}_n\mathbb{Q}_\mathfrak{p}$ is the localization of ${}_n\mathbb{Q}$ at the unique prime $\mathfrak{p}$ above p. Perrin-Riou [PR94] has constructed a Λ-linear Coleman map Col from ${}_\infty\mathrm{H}^1_{\mathrm{loc}}$ to a sub-module of $\mathbb{Q}_p[\![T]\!]\otimes D_p(E)$.

Define the fine Selmer group to be the kernel

$$\mathcal{R}(E/_n\mathbb{Q}) = \ker\left(\mathcal{S}(E/_n\mathbb{Q}) \longrightarrow E({}_n\mathbb{Q}_\mathfrak{p})\otimes \mathbb{Q}_p/\mathbb{Z}_p\right) .$$

It is again a consequence of the work of Kato, namely theorem 12.4 in [Kat04], that the Pontryagin dual $Y(E/_\infty\mathbb{Q})$ of $\mathcal{R}(E/_\infty\mathbb{Q})$ is a Λ-torsion module. Denote by $g_E(T)$ its characteristic series.

Let Σ be any finite set of places in $\mathbb{Q}$ containing the places of bad reduction for E and the places ∞ and p. By $G_\Sigma({}_n\mathbb{Q})$, we denote the Galois group of the maximal extension of ${}_n\mathbb{Q}$ unramified at all places which do not lie above Σ. Next we define ${}_\infty\mathrm{H}^1_{\mathrm{glob}}$ as the projective limit of $\mathrm{H}^1(G_\Sigma({}_n\mathbb{Q}), T_pE)$. It is a Λ-module of rank 1 and it is actually independent of the choice of Σ.

Choose now any element ${}_\infty c$ in ${}_\infty\mathrm{H}^1_{\mathrm{glob}}$ such that $Z_c = {}_\infty\mathrm{H}^1_{\mathrm{glob}}/(\Lambda\cdot {}_\infty c)$ is Λ-torsion. Typically the "zeta element" of Kato could be such a choice.[27][28] Write $h_c(T)$ for the characteristic series of Z_c. Then we define an algebraic equivalent of the $D_p(E)$-valued L-series by [[27]] [[28]]

$$f_E(T) = g_E(T)\cdot \mathrm{Col}({}_\infty c)\cdot h_c(T)^{-1} \in \mathbb{Q}_p[\![T]\!]\otimes D_p(E)$$

where by $\mathrm{Col}({}_\infty c)$ we mean the image of the localization of ${}_\infty c$ to ${}_\infty\mathrm{H}^1_{\mathrm{loc}}$ under the Coleman map Col. The resulting series $f_E(T)$ is independent of the choice of ${}_\infty c$. Of course, $f_E(T)$ is again only defined up to multiplication by a unit in $\Lambda^\times$.

Again we have an Euler-characteristic result due to Perrin-Riou [PR93]:

Theorem 4 (Perrin-Riou). *The order of vanishing of $f_E(T)$ at $T=0$ is at least equal to the rank r. It is equal to r if and only if the $D_p(E)$-valued regulator $\mathrm{Reg}_p(E/\mathbb{Q})$ is nonzero (conjecture 4) and the p-primary part of the Tate-Shafarevich group $Ш(E/\mathbb{Q})(p)$ is finite (conjecture 1). In this case the leading term of the series $(1-\varphi)^{-2}\,f_E(T)$ has the same valuation as*

$$\prod_v c_v \cdot \#Ш(E/\mathbb{Q})(p)\cdot \mathrm{Reg}_\gamma(E/\mathbb{Q})$$

Note that we simplified the right hand term in comparison to (9), because $N_p \equiv 1 \pmod{p}$ and hence $\#E(\mathbb{Q})_{\mathrm{tors}}$ must be p-adic unit if the reduction at p is supersingular.

7 The Main Conjecture

The main conjecture links the two p-adic power series (3) and (10) of the previous sections. We formulate everything now simultaneously for the ordinary and the supersingular case, even if they are of quite different nature. We still assume that $p\neq 2$.

Conjecture 7. (Main conjecture of Iwasawa theory for elliptic curves) *If E has good or non-split multiplicative reduction at p, then there exists an element $u(T)$ in $\Lambda^\times$ such that $\mathcal{L}_p(E,T) = f_E(T)\cdot u(T)$. If the reduction of E at p is split multiplicative, then there exists such a $u(T)$ in $T\cdot\Lambda^\times$.*

[27] [[William: Huh?]]

[28] [[Christian: The Euler system elements in the H^1 are called zeta elements in Kato. Do you want me to omit the sentence or write more about it ?]]

Much is now known about this conjecture. To the elliptic curve E we attach the mod-p representation

$$\bar{\rho}_p \colon \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \operatorname{Aut}(E[p]) \cong \operatorname{GL}_2(\mathbb{F}_p)$$

of the absolute Galois group of $\mathbb{Q}$. Serre proved that $\bar{\rho}_p$ is almost always surjective (note that by hypothesis E does not have complex multiplication) and that for semistable curves surjectivity can only fail when there is an isogeny of degree p defined over $\mathbb{Q}$. See [Ser72] and [Ser96].

Kato's Theorem 5.
Suppose that E has semistable reduction at p and that $\bar{\rho}_p$ is either surjective or that its image is contained in a Borel subgroup. Then there exists a series $d(T)$ in Λ such that $\mathcal{L}_p(E,T) = f_E(T) \cdot d(T)$. If the reduction is split multiplicative then T divides $d(T)$.

The main ingredient for this theorem is in theorem 17.4 in [Kat04] for the good ordinary case when $\bar{\rho}_p$ is surjective, or in [Wut06] when there is a p-isogeny. For the exceptional case we refer to [Kob05][29]. [[29]] The statement of the main conjecture for supersingular primes is known to be equivalent to Kato's formulation in Conjecture 12.10 in [Kat04] and to Kobayashi's version in [Kob03].

In particular the theorem applies to all odd primes p if E is a semistable curve. For the remaining cases, e.g., if the image of $\bar{\rho}_p$ is contained in the normalizer of a Cartan subgroup, one obtains only a weaker statement:

Kato's Theorem 6.
Suppose the image of $\bar{\rho}_p$ is not contained in a Borel subgroup of $\operatorname{GL}_2(\mathbb{F}_p)$ and that $\bar{\rho}_p$ is not surjective, then there is an integer $m \geqslant 0$ such that $f_E(T)$ divides $p^m \cdot \mathcal{L}_p(E,T)$.

Greenberg and Vatsal [GV00] have shown that in certain cases the main conjecture holds. There is hope that the main conjecture will be proved soon for primes p subject to certain conditions. We are awaiting the forthcoming paper of Skinner and Urban.

8 If the L-series does not vanish

Suppose the Hasse-Weil L-function $L(E,s)$ does not vanish at $s = 1$. In this case Kolyvagin proved that $E(\mathbb{Q})$ and $\text{Ш}(E/\mathbb{Q})$ are finite. In particular Conjecture 1 is valid; also, Conjectures 3 and 4 are trivially true in this case.

Let $p > 2$ be a prime of semistable reduction such that the representations $\bar{\rho}_p$ is either surjective or has its image contained in a Borel subgroup of $\operatorname{GL}_2(\mathbb{F}_p)$. By the interpolation property, we know that $\mathcal{L}_p(E,0)$ is nonzero, unless E has split multiplicative reduction.

8.1 The good ordinary case

In the ordinary case we have

$$\epsilon_p^{-1} \cdot \mathcal{L}_p(E,0) = \frac{L(E,1)}{\Omega_E} = [0]^+,$$

which is a nonzero rational number by [Man72]. In the following inequality, we use the theorem[30] 3 of Perrin-Riou and Schneider for the first equality and Kato's theorem 5 on the main conjecture for the inequality in the second line.[31][32] [[31]]

[29] [[Christian: I have to omit the reference to [KKT96] as I still haven't seen this eternal well-hidden preprint]] [[32]]

[30] In the case of analytic rank 0, the theorem is actually relatively easy and well explained in [CS00].

[31] [[William: What does it mean "in the first line"? "In the second line" ??]]

[32] [[Christian: better ?]]

$$\begin{aligned}\operatorname{ord}_p\left(\epsilon_p\cdot\frac{\prod_v c_v\cdot\#\text{Ш}(E/\mathbb{Q})(p)}{(\#E(\mathbb{Q})(p))^2}\right) &= \operatorname{ord}_p(f_E(0))\\ &\leqslant \operatorname{ord}_p(\mathcal{L}_p(E,0))\\ &= \operatorname{ord}_p\left(\frac{L(E,1)}{\Omega_E}\right)+\operatorname{ord}_p(\epsilon_p)\end{aligned}$$

Hence, we have the following upper bound on the p-primary part of the Tate-Shafarevich group, which is sharp under the assumption of the main conjecture:

$$\operatorname{ord}_p\left(\text{Ш}(E/\mathbb{Q})(p)\right)\leqslant\operatorname{ord}_p\left(\frac{L(E,1)}{\Omega_E}\right)-\operatorname{ord}_p\left(\frac{\prod c_v}{(\#E(\mathbb{Q})_{\text{tors}})^2}\right). \tag{11}$$

This bound agrees with the Birch and Swinnerton-Dyer conjecture. [33] [[33]]

8.2 The multiplicative case

If the reduction is not split, then the above holds just the same.[34][35] If instead the reduction is split multiplicative, we have that $\mathcal{L}_p(E,0)=0$ and [[34]] [[35]]

$$\mathcal{L}_p'(E,0)=\mathscr{L}_p\cdot\frac{L(E,1)}{\Omega_E}=\mathscr{L}_p\cdot[0]^+\neq 0\,.$$

Since the p-adic multiplier is the same on the algebraic as on the analytic side, we can once again compute it as above to obtain the same bound (11) again.

8.3 The supersingular case

For the supersingular $D_p(E)$-valued series, we have

$$(1-\varphi)^{-2}\cdot\mathcal{L}_p(E,0)=\frac{L(E,1)}{\Omega_E}\cdot\omega_E=[0]^+\cdot\omega_E$$

which is a nonzero element of $D_p(E)$. The $D_p(E)$-valued regulator $\operatorname{Reg}_p(E/\mathbb{Q})$ is equal to ω_E. We may therefore concentrate solely on the coordinate in ω_E. Write $\operatorname{ord}_p(f_E(0))$ for the p-adic valuation of the leading coefficient of the ω_E-coordinate of $f_E(T)$. Again we obtain an inequality by using theorem 4

$$\begin{aligned}\operatorname{ord}_p\left(\prod_v c_v\cdot\#\text{Ш}(E/\mathbb{Q})(p)\right) &= \operatorname{ord}_p((1-\varphi)^{-2}\,f_E(0))\\ &\leqslant \operatorname{ord}_p((1-\varphi)^{-2}\,\mathcal{L}_p(E,0))\\ &= \operatorname{ord}_p\left(\frac{L(E,1)}{\Omega_E}\right).\end{aligned}$$

8.4 Conclusion

Summarizing the above computations, we have

Theorem 7.
Let E be an elliptic curve such that $L(E,1)\neq 0$. Then $\text{Ш}(E/\mathbb{Q})$ is finite and

$$\#\text{Ш}(E/\mathbb{Q})\leqslant C\cdot\frac{L(E,1)}{\Omega_E}\cdot\frac{(\#E(\mathbb{Q})_{\text{tors}})^2}{\prod c_v}$$

where C is a product of a power of 2 and of power of primes of additive reduction and of powers of primes for which the representation $\bar\rho_p$ is not surjective and there is no isogeny of degree p on E defined over $\mathbb{Q}$.

In particular if E is semistable, then C is a power of 2.

This improves Corollary 3.5.19 in [Rub00].

[33] [[William: This is stronger than what I stated in my previous bsd computation paper.]]

[34] [[William: Why?]]

[35] [[Christian: because in all the theorems involved the non-split case never differs form the good ordinary case. Only the split multiplicative case is exceptional]]

9 If the L-series vanishes to the first order

We suppose for this section that E has good and ordinary reduction at p and that the complex L-series $L(E,s)$ has a zero of order 1 at $s=1$. The method of Heegner points and the theorem of Kolyvagin show again that $\text{Ш}(E/\mathbb{Q})$ is finite and that the rank of $E(\mathbb{Q})$ is equal to 1. Let P be a choice of generator of the free part of the Mordell-Weil group (modulo torsion). Suppose that the p-adic height $\hat{h}_p(P)$ is nonzero. Thanks to a theorem of Perrin-Riou in [PR87], we must have the following equality of rational numbers

$$\frac{1}{\mathrm{Reg}(E/\mathbb{Q})}\cdot\frac{L'(E,1)}{\Omega_E}=\frac{1}{\mathrm{Reg}_p(E/\mathbb{Q})}\cdot\frac{\mathcal{L}_p'(E,0)}{(1-\frac{1}{\alpha})^2\cdot\log(\kappa(\gamma))}$$

where, on the left hand side, we have the canonical real-valued regulator $\mathrm{Reg}(E/\mathbb{Q})=\hat{h}(P)$ and the leading coefficient of $L(E,s)$, while, on the right hand side, we have the p-adic regulator $\mathrm{Reg}_p(E/\mathbb{Q})=\hat{h}_p(P)$ and the leading term of the p-adic L-series. By the conjecture of Birch and Swinnerton-Dyer (or its p-adic analogue), this rational number should be equal to $\prod c_v\cdot\#\text{Ш}(E/\mathbb{Q})\cdot(\#E(\mathbb{Q})_{\mathrm{tors}})^{-2}$. By Kato's theorem, one knows that the characteristic series $f_E(T)$ of the Selmer group divides $\mathcal{L}_p(E,T)$; at least up to a power of p. Hence the series $f_E(T)$ has a zero of order 1 at $T=0$ and its leading term divides the above rational number in $\mathbb{Q}_p$ (here we use that $E(\mathbb{Q})$ has rank 1 so $T\mid f_E(T)$). Hence we have

Theorem 8.
Let $E/\mathbb{Q}$ be an elliptic curve with good ordinary reduction at the odd prime p. Suppose that the representation $\bar{\rho}_p$ is surjective onto $\mathrm{GL}_2(\mathbb{F}_p)$ or that the curve admits an isogeny of degree p defined over $\mathbb{Q}$. If $L(E,s)$ has a simple zero at $s=1$, then the p-primary part of $\text{Ш}(E/\mathbb{Q})$ is finite and its valuation is bounded by

$$\mathrm{ord}_p(\#\text{Ш}(E/\mathbb{Q})(p))\leqslant\mathrm{ord}_p\left(\frac{(\#E(\mathbb{Q})_{\mathrm{tors}})^2}{\prod c_v}\cdot\frac{1}{\mathrm{Reg}(E/\mathbb{Q})}\cdot\frac{L'(E,1)}{\Omega_E}\right)$$

In other words the Birch and Swinnerton-Dyer conjecture if true up to a factor involving only bad and supersingular primes, and primes for which the representation is neither surjective nor has its image contained in a Borel subgroup.

10 The algorithm for the rank

[36] [[36]]

[37] [[37]]

Let $E/\mathbb{Q}$ be an elliptic curve. We have now a possibility of computing upper bounds on the rank r of the Mordell-Weil group $E(\mathbb{Q})$. For this purpose, we choose a prime p satisfying the following conditions

- $p>2$,
- E has good reduction at p.

By computing the analytic p-adic L-function $\mathcal{L}_p(E,T)$ to a certain precision, we find an upper bound, say b, on the order of vanishing of $\mathcal{L}_p(E,T)$ at $T=0$. Then

$$b\ \geqslant\ \mathrm{ord}_{T=0}\,\mathcal{L}_p(E,1)\ \geqslant\ \mathrm{ord}_{T=0}\,f_E(T)\ \geqslant\ r$$

by Kato's theorems 5 and 6 and by the theorems 3 and 4. Hence we have an upper bound on the rank r.

[36] [[William: The procedure described in this section is *NOT* an algorithm. It depends on "the p-adic Birch and Swinnerton-Dyer conjecture tells us exactly what the needed precision should be", but my understanding is that we do not know enough of that conjecture to read off this precision. Thus given current theorems, we would never know when we're done. So this section is not about an algorithm – or it is about an algorithm that is conditional on knowing the p-adic BSD conjecture. Please clarify.]]

[37] [[Christian: I agree. So I changed it, but I am not very good in writing such things. Maybe a formal algorithm would be better]]

Proposition 9. *The computation of an approximation of the p-adic L-series of E for an odd prime p of good reduction produces an upper bound on the rank r of the Mordell-Weil group $E(\mathbb{Q})$.*

By searching for points of small height on E at the same time, one obtains also a lower bound on the rank r. Simultaneously one can increase the precision of the computation of the p-adic L-function in order to try to lower the bound b. Eventually the lower bound is equal to the upper bound, unless the p-adic Birch and Swinnerton-Dyer conjecture 5 or 6 is false. This is very similar to the algorithm described in Proposition 1, except that we do know here that our upper bounds are unconditional. But we do not know if the algorithm terminates after finitely many steps. Summarizing we can claim the following.

Proposition 10. *There is an algorithm which aims to compute the rank r of an elliptic curve $E/\mathbb{Q}$ using p-adic L-functions. The algorithm succeeds to determine r in a finite amount of time, unless the p-adic Birch and Swinnerton-Dyer conjectures are false for all odd primes p of good reduction.*

Of course, the algorithm for computing the rank r using m-descents has the same properties : It tries to determine the rank by searching points and by bounding r from above by the rank of the various m-Selmer groups. This algorithm terminates after finitely many steps unless all the p-primary parts of the Tate-Shafarevich groups are infinite.

But the two algorithms are fundamentally different. The m-descent algorithm is fast and well-implemented for small m, but it would be extremely time-consuming for larger m, like $m > 8$. [38] [[38]]

10.1 Technical remarks

The second condition on the prime p is too strict. We may actually allow primes of multiplicative reduction, too. Of course in the exceptional case, when E has split multiplicative reduction, the upper bound b on the order of vanishing of the p-adic L-function $\mathcal{L}_p(E,T)$ at $T = 0$ satisfies $b \geqslant r + 1$.

Note that, assuming that the p-adic Birch and Swinnerton-Dyer conjecture holds, it is easy to predict the needed precision in the computation of the p-adic L-series. So one can actually compute immediately with the precision which should be sufficient and concentrate on the search of points of small heights.

For all practical purposes, one has to take p as small as possible. The computation of the leading term of $\mathcal{L}_p(E,T)$ for curves of higher rank r is very time-consuming for large p. Also one should avoid primes p with supersingular or split multiplicative reduction as there the needed precision is much higher and the computation of b is much slower.

11 The algorithm for the Tate-Shafarevich group

[39] [[39]]

The second algorithm that we are presenting here takes as input an elliptic curve E and a prime p and tries to compute an upper bound on the p-primary part of $\text{Ш}(E/\mathbb{Q})$. To be able to apply the results in the previous section, we need the following conditions on (E,p)

- $p > 2$,
- E does not have additive reduction at p.
- The image of $\bar{\rho}_p$ is either the full group $\mathrm{GL}_2(\mathbb{F}_p)$ or it is contained in a Borel subgroup.

[38] [[Christian: I think I should add more here]]

[39] [[Christian: This is rewritten, too.]]

Note that, for any given curve E, these conditions apply to all but finitely many primes p.

Algorithm 11. Given an elliptic curve $E/\mathbb{Q}$ and a prime p satisfying the above conditions, this algorithm tries to give an upper bound for $\#Ш(E/\mathbb{Q})(p)$.

1. Determine the rank r and the full Mordell-Weil group $E(\mathbb{Q})$. Exit with an error if we fail to do this.
2. Compute the p-adic regulator of E over $\mathbb{Q}$ using the efficient algorithm in [MSJ05]. Exit with an error if the p-adic height pairing can not shown to be non-degenerate.
3. Using modular symbols, compute an approximation of the leading term $\mathcal{L}_p^*(E,0)$ of the p-adic L-function $\mathcal{L}_p(E,T)$. If the order of vanishing $\operatorname{ord}_{T=0}\mathcal{L}_p(E,T)$ is equal to r (or $r+1$ if E has split multiplicative reduction at p), then we print that $Ш(E/\mathbb{Q})(p)$ is finite, otherwise we have to increase the precision of the computation of $\mathcal{L}_p(E,T)$. It this fails to prove that $\operatorname{ord}_{T=0}\mathcal{L}_p(E,T) = r$ (or $r+1$), then exit with an error.
4. Now compute the remaining information, like Tamagawa numbers c_v and the p-adic multiplier ϵ_p. If p is an good ordinary prime or a prime at which E has non-split multiplicative reduction then let
$$\begin{aligned} b_p =& \operatorname{ord}_p(\mathcal{L}_p^*(E,0)) + 2\cdot\operatorname{ord}_p(\#(E(\mathbb{Q})(p)) - \operatorname{ord}_p(\epsilon_p) \\ &- \sum_v \operatorname{ord}_p(c_v) - \operatorname{ord}_p(\operatorname{Reg}_\gamma(E/\mathbb{Q}))\,, \end{aligned}$$
if p is supersingular, then let
$$b_p = \operatorname{ord}_p((1-\varphi)^{-2}\,\mathcal{L}_p^*(E,0)) - \operatorname{ord}_p(\operatorname{Reg}_p(E/\mathbb{Q})) - \sum_v \operatorname{ord}_p(c_v)\,,$$
and finally if E has split multiplicative reduction at p then let
$$\begin{aligned} b_p =& \operatorname{ord}_p(\mathcal{L}_p^*(E,0)) + 2\cdot\operatorname{ord}_p(\#(E(\mathbb{Q})(p)) - \operatorname{ord}_p(\mathscr{L}_p) \\ &- \sum_v \operatorname{ord}_p(c_v) - \operatorname{ord}_p(\operatorname{Reg}_\gamma(E/\mathbb{Q}))\,. \end{aligned}$$
5. Return that $\#Ш(E/\mathbb{Q})(p)$ is bounded by p^{b_p}.

Proof. When arriving at step 4, we have shown that conjecture 3 (or conjecture 4 in the supersingular case) on the non-degeneracy of the p-adic holds and that $Ш(E/\mathbb{Q})(p)$ is indeed finite by theorem 3 (or theorem 4 in the supersingular case). Moreover this theorems show that

$$\operatorname{ord}_p(\#Ш(E/\mathbb{Q})(p)) = \operatorname{ord}_p(f_E^*(0)) + \operatorname{ord}_p\left(\frac{(\#E(\mathbb{Q})(p))^2}{\epsilon_p\cdot\prod_v c_v}\cdot\frac{1}{\operatorname{Reg}_\gamma(E/\mathbb{Q})}\right)$$

in the ordinary case (or the same formula where ϵ_p replaces by $\mathscr{L}_p$ in the split multiplicative case) and

$$\operatorname{ord}_p(\#Ш(E/\mathbb{Q})(p)) = \operatorname{ord}_p((1-\varphi)^{-2}\,f_E^*(0)) - \operatorname{ord}_p(\operatorname{Reg}_p(E/\mathbb{Q})) - \operatorname{ord}_p(\prod_v c_v)$$

in the supersingular case. Finally use Kato's theorem 5 stating that $\operatorname{ord}_p(f_E^*(0)) \leqslant \operatorname{ord}_p(\mathcal{L}_p^*(E,0))$ to prove that b_p is indeed an upper bound on $\operatorname{ord}_p(Ш(E/\mathbb{Q})(p))$. □

Note that the only inequality in the proof comes from Kato's theorem. If the main conjecture holds, and in some cases this is known, then the resulting bound is the actual order of $Ш(E/\mathbb{Q})(p)$.

11.1 Technical remarks

In step 1 we may use several ways to determine the rank and the Mordell-Weil group. First compute the modular symbol $[0]^+$. If it is not zero, we have that $L(E,1) \neq 0$ and the rank has to be 0. If the order of vanishing of $L(E,s)$ at $s = 1$ is 1, we may use Heegner points to find the full Mordell-Weil group, which then is of rank 1. Otherwise we have to use descent methods or the algorithm in the previous section to bound the rank from above and a search of points of small height to find a lower bound. When enough points are found to generate a group of finite index, one has to saturate the group using infinite descent in order to find the full group $E(\mathbb{Q})$. In practice this step does not create any problems as step 3 is usually computationally more difficult.

The implementation of the algorithm in [MSJ05] can also be used to compute the p-adic heights for supersingular primes as in both cases one needs to know the action of φ on $D_p(E)$.

In step 3, it is easy to determine the precision that will be needed to compute the p-adic valuation of the leading term $\mathcal{L}_p^*(E,0)$ if one assumes the complex and the p-adic version of the conjecture of Birch and Swinnerton-Dyer. Hence it is easy to decide when to exit at this step.

The algorithm exits with an error only if the Mordell-Weil group could not be determined (in step 1), if conjecture 3 or 4 is wrong (in step 2), if the p-primary part of $\text{Ш}(E/\mathbb{Q})$ is infinite or if the main conjecture is false (both in step 3). Hence not the full variant of the p-adic Birch and Swinnerton-Dyer conjecture is needed, only weaker statements.

12 Numerical results

References

[Ber81] Dominique Bernardi, *Hauteur p-adique sur les courbes elliptiques*, Seminar on Number Theory, Paris 1979–80, Progr. Math., vol. 12, Birkhäuser Boston, 1981, pp. 1–14.

[Ber82] Daniel Bertrand, *Valuers de fonctions thêta et hauteur p-adiques*, Seminar on Number Theory, Paris 1980-81, Progr. Math., vol. 22, Birkhäuser Boston, 1982, pp. 1–11.

[BPR93] Dominique Bernardi and Bernadette Perrin-Riou, *Variante p-adique de la conjecture de Birch et Swinnerton-Dyer (le cas supersingulier)*, C. R. Acad. Sci. Paris Sér. I Math. **317** (1993), no. 3, 227–232.

[BSDGP96] Katia Barré-Sirieix, Guy Diaz, François Gramain, and Georges Philibert, *Une preuve de la conjecture de Mahler-Manin*, Invent. Math. **124** (1996), no. 1-3, 1–9.

[Cas65] J. W. S. Cassels, *Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer*, J. Reine Angew. Math. **217** (1965), 180–199.

[Col04a] Pierre Colmez, *Invariants $\mathscr{L}$ et dérivées de valeurs propres de Frobenius*, preprint, 2004.

[Col04b] ———, *La conjecture de Birch et Swinnerton-Dyer p-adique*, Astérisque (2004), no. 294, ix, 251–319.

[Cre97] John E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, 1997.

[CS00] John Coates and Ramdorai Sujatha, *Galois cohomology of elliptic curves*, Tata Institute of Fundamental Research Lectures on Mathematics, vol. 88, Narosa Publishing House, 2000.

[Del98] Daniel Delbourgo, *Iwasawa theory for elliptic curves at unstable primes*, Compositio Math. **113** (1998), no. 2, 123–153.

[Del02] ———, *On the p-adic Birch, Swinnerton-Dyer conjecture for non-semistable reduction*, J. Number Theory **95** (2002), no. 1, 38–71.

[Gri05] Grigor Tsankov Grigorov, *Kato's Euler System and the Main Conjecture*, Ph.D. thesis, Harvard University, 2005.

[GS93] Ralph Greenberg and Glenn Stevens, *p-adic L-functions and p-adic periods of modular forms*, Invent. Math. **111** (1993), no. 2, 407–447.

[GV00] Ralph Greenberg and Vinayak Vatsal, *On the Iwasawa invariants of elliptic curves*, Invent. Math. **142** (2000), no. 1, 17–63.

[Jon89] John W. Jones, *Iwasawa L-functions for multiplicative abelian varieties*, Duke Math. J. **59** (1989), no. 2, 399–420.

[Kat04] Kazuya Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Cohomologies p-adiques et application arithmétiques. III, Astérisque, vol. 295, Société Mathématique de France, Paris, 2004.

[KKT96] Kazuya Kato, Masato Kurihara, and Takeshi Tsuji, *Local Iwasawa theory of Perrin-Riou and syntomic complexes*, preprint, 1996.

[Kob03] Shin-ichi Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. **152** (2003), no. 1, 1–36.

[Kob05] ______, *An elementary proof of the Mazur-Tate-Teitelbaum conjecture for elliptic curves*, preprint, 2005.

[KP05] Masato Kurihara and Robert Pollack, *Two p-aidc L-functions and rational ponts on elliptic curves with supersingular reduction*, preprint, 2005.

[Man72] Ju. I. Manin, *Parabolic points and zeta functions of modular curves*, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 19–66.

[MSD74] Barry Mazur and Peter Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), 1–61.

[MSJ05] Barry Mazur, William Stein, and Tate John, *Computation of p-adic Heights and Log Convergence*, preprint, 2005.

[MT91] Barry Mazur and John Tate, *The p-adic sigma function*, Duke Math. J. **62** (1991), no. 3, 663–688.

[MTT86] Barry Mazur, John Tate, and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), no. 1, 1–48.

[Pol03] Robert Pollack, *On the p-adic L-function of a modular form at a supersingular prime*, Duke Math. J. **118** (2003), no. 3, 523–558.

[PR82] Bernadette Perrin-Riou, *Descente infinie et hauteur p-adique sur les courbes elliptiques à multiplication complexe*, Invent. Math. **70** (1982), no. 3, 369–398.

[PR87] ______, *Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner*, Bull. Soc. Math. France **115** (1987), no. 4, 399–456.

[PR93] ______, *Fonctions L p-adiques d'une courbe elliptique et points rationnels*, Ann. Inst. Fourier (Grenoble) **43** (1993), no. 4, 945–995.

[PR94] ______, *Théorie d'Iwasawa des représentations p-adiques sur un corps local*, Invent. Math. **115** (1994), no. 1, 81–161, With an appendix by Jean-Marc Fontaine.

[PR03] ______, *Arithmétique des courbes elliptiques à réduction supersingulière en p*, Experiment. Math. **12** (2003), no. 2, 155–186.

[Rub00] Karl Rubin, *Euler systems*, Annals of Mathematics Studies, vol. 147, Princeton University Press, Princeton, NJ, 2000, Hermann Weyl Lectures. The Institute for Advanced Study.

[Sch82] Peter Schneider, *p-adic height pairings. I*, Invent. Math. **69** (1982), no. 3, 401–409.

[Sch85] ______, *p-adic height pairings. II*, Invent. Math. **79** (1985), no. 2, 329–374.

[Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.

[Ser96] ———, *Travaux de Wiles (et Taylor, ...). I*, Astérisque (1996), no. 237, Exp. No. 803, 5, 319–332, Séminaire Bourbaki, Vol. 1994/95.

[Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.

[SS04] Edward F. Schaefer and Michael Stoll, *How to do a p-descent on an elliptic curve*, Trans. Amer. Math. Soc. **356** (2004), no. 3, 1209–1231.

[Wer98] Annette Werner, *Local heights on abelian varieties and rigid analytic uniformization*, Doc. Math. **3** (1998), 301–319.

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

[Wut06] ———, *Extending Kato's results to elliptic curves with p-isogenies*, Math. Res. Lett. **13** (2006), no. 5, 713 – 718.

[Wut07] ———, *Iwasawa theory of the fine Selmer group*, J. Algebraic Geom. **16** (2007), 83–108.