# Computations About Tate-Shafarevich Groups Using Iwasawa Theory

William Stein and Christian Wuthrich

25th November 2009

**Abstract**

We explain how to combine deep results from Iwasawa theory with explicit computation to obtain information about $p$-parts of Tate-Shafarevich groups of elliptic curves over $\mathbb{Q}$. This method provides a practical way to compute $\#Ш(E/\mathbb{Q})(p)$ in many cases when traditional $p$-descent methods are completely impractical and also in situations where results of Kolyvagin do not apply, like when the rank of the Mordell-Weil group is greater than 1.

## 1 Introduction

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 that the set of rational points $E(\mathbb{Q})$ is an abelian group of finite rank $r = \mathrm{rank}(E(\mathbb{Q}))$. Birch and Swinnerton-Dyer then conjectured that $r = \mathrm{ord}_{s=1} L(E,s)$, where $L(E,s)$ is the Hasse-Weil $L$-function of $E$ (see Conjecture 2 below). We call $r_{\mathrm{an}} = \mathrm{ord}_{s=1} L(E,s)$ the analytic rank of $E$.

By an *algorithm* we mean a finite sequence of steps that, given any valid input, will terminate in a finite amount of time. There is no known algorithm that *has been proved to be correct* that computes $r$ in all cases. 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. Constructions of complex and $p$-adic Heegner points can also be used in some cases to bound the rank from below. To compute an upper bound on the rank $r$, in the case of analytic ranks 0 and 1 one can use Kolyvagin's work on the Euler systems of Heegner points; in general, the only known method is to do an $n$-descent for some integer $n > 1$. The 2-descents implemented by John Cremona [Cre97], by Denis Simon [Sim02] in Pari [PAR06] (and SAGE [Ste09]) and by Geoffe Bailey in Magma, and the 3 and 4 descents in Magma and described in [CFO+08] and [CFO+06] , are particularly 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

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

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 $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-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:

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

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

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

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 $r_{\mathrm{an}} \geqslant 2$. 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 unconditional 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 possibility of using these results to compute information about the Tate-Shafarevich group is well known to specialists and was for instance mentioned in [Col04b] which gives also a nice overview over the $p$-adic Birch and Swinnerton-Dyer conjecture. For supersingular primes these methods have been used by Perrin-Riou in [PR03].

The first algorithm, which we describe Section 10, finds a 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 $\mathcal{L}_p(E,T)$ at $T=0$ is known to be an upper bound on the rank $r$.

The second algorithm, which we discuss 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 $p$, e.g., those for which $E$ has additive reduction, since much of the theory we rely on has not yet been developed in this case yet (see Section 3.6 and 11).

Our 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 any output, is a proven upper bound on the order of $\text{Ш}(E/\mathbb{Q})(p)$; in particular, it will often 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 $\text{Ш}(E/\mathbb{Q})(p)$ 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, or use visibility [AS02] to relate $\text{Ш}(E/\mathbb{Q})(p)$ to Mordell-Weil groups of other elliptic curves or abelian varieties. The computability of the upper bound on $\#\text{Ш}(E/\mathbb{Q})(p)$ relies on several conjectures, such as the finiteness of $\text{Ш}(E/\mathbb{Q})(p)$ and 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 $\text{Ш}(E/\mathbb{Q})(p)$. 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.

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 $\mathbb{Q}$.

### 1.1 Overview

The article is structured as follows. We start by recalling the Birch and Swinnerton-Dyer conjecture and its algorithmic consequences. In Section 3, we define $p$-adic $L$-functions and explain how to compute them. Next we define the $p$-adic regulator, treating separately the cases of split multiplicative and supersingular reduction. This leads to the formulation of the $p$-adic Birch and Swinnerton-Dyer conjectures. In Section 6, we recall the basic definitions and results for the algebraic $p$-adic $L$-functions defined using Iwasawa theory. This leads us naturally to the statement of the main conjecture and the theorem of Kato. Concrete examples illustrate the theory throughout these sections.

We then explain first the implication of these results in the case the curve has analytic rank 0, followed by the case of analytic rank 1. Finally we present in Section 10 and 11 the algorithms for bounding the rank and the order of the $p$-primary part of $Ш(E/\mathbb{Q})$. We conclude the article with a section of further explicit examples produced by the algorithms. A forthcoming sequence to this paper will apply the theory in this paper to produce numerous tables and analyzes of the resulting data.

### Acknowledgments

The authors would like to thank Henri Darmon, Jerôme Grand'maison, Ralph Greenberg and Dimitar Jetchev for helpful discussions and comments. We are also greatly indebted to Robert Pollack whose code for computing $p$-adic $L$-functions was the starting basis of this article. He also greatly helped us with the error estimates in Section 3.

## 2 The Birch and Swinnerton-Dyer conjecture

Let $E$ be an elliptic curve defined over $\mathbb{Q}$. If the Birch and Swinnerton-Dyer conjecture (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 [BCDT01] (which completes work initiated in [Wil95]), the function $L(E, s)$ is holomorphic on the whole complex plane. Let $\omega_E$ 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 $E$.

**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 $r = \mathrm{rank}(E(\mathbb{Q}))$.*
2. *The leading term $L^*(E,1)$ of the Taylor expansion of $L(E,s)$ at $s=1$ satisfies*
$$\frac{L^*(E,1)}{\Omega_E} = \frac{\prod_v c_v \cdot \#\text{Ш}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{\mathrm{tor}})^2} \cdot \mathrm{Reg}(E/\mathbb{Q}) \tag{2}$$
*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 $E(\mathbb{Q})$.*

Below we write $\#\text{Ш}(E/\mathbb{Q})_{\mathrm{an}}$ for the order of $\text{Ш}(E/\mathbb{Q})$ that is predicted by Conjecture 2.

Cassels proved in [Cas65] that if Conjecture 2 is true for an elliptic curve $E$ over $\mathbb{Q}$, then it is true for all curves that are $\mathbb{Q}$-isogenous to $E$.

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

*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 have no way to know if that has occurred. As explained, e.g., in [Cre97, Coh07, Dok04], we can for any $k$ compute $L^{(k)}(E,1)$ to any desired precision. Such computations yield upper bounds on $r_{\mathrm{an}}$. 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 the correct value of $r_{\mathrm{an}}$, though again without further information we do not know when this will occur. However, if we know Conjecture 2, we know that $r = r_{\mathrm{an}}$, hence at some point the lower bound on $r$ computed using point searches will equal the upper bound on $r_{\mathrm{an}}$ computed using the $L$-series. At this point, by Conjecture 2 we know the true value of both $r$ and $r_{\mathrm{an}}$.

Once $r$ is known, one can compute $E(\mathbb{Q})$ via a point search (as explained in [Cre97, §3.5] or [Ste07, §1.2]), hence we can approximate $\mathrm{Reg}(E/\mathbb{Q})$ to any desired precision. All other quantities in (2) can also be approximated to any desired precision. Solving for $\#\text{Ш}(E/\mathbb{Q})$ in (2) and computing all other quantities to large enough precision to determine the integer $\#\text{Ш}(E/\mathbb{Q})_{\mathrm{an}}$ then determines $\#\text{Ш}(E/\mathbb{Q})$, as claimed. □

We wish to emphasize that this algorithm would only produce the order of $\text{Ш}(E/\mathbb{Q})$ but no information about its structure as an abelian group. One could in theory compute the structure of $\text{Ш}(E/\mathbb{Q})$ by doing an explicit $n$-descent where $n^2 = \#\text{Ш}(E/\mathbb{Q})$. The two algorithms 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, though curves with complex multiplication are an area of active research for these methods (see e.g., [Rub99, PR04]).

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 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 $c_\pi$ 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 (see [Edi91, ARS06]).

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

$$\begin{aligned} \lambda^+(r) &= \frac{c_\pi}{2} \cdot \left( \int_{\pi_*(\{r\})} \omega_E + \int_{\pi_*(\{-r\})} \omega_E \right) \\ &= \pi i \cdot \left( \int_r^{i\infty} f(\tau)\, d\tau + \int_{-r}^{i\infty} f(\tau)\, d\tau \right) . \end{aligned} \tag{3}$$

There is a basis $\{\gamma_+, \gamma_-\}$ of $H_1(E,\mathbb{Z})$ such that $\int_{\gamma_+} \omega_E$ is equal to $\Omega_E$ 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 algebraically using modular symbols and linear algebra (see [Cre97]).

Let $p$ be a prime of semi-stable reduction. We write[1] $a_p$ for the trace of Frobenius. 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 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 $\alpha = a_p$.

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

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

$$\mu_\alpha(a+p^k\mathbb{Z}_p) = \begin{cases} \frac{1}{\alpha^k}\cdot\left[\frac{a}{p^k}\right]^+ - \frac{1}{\alpha^{k+1}}\cdot\left[\frac{a}{p^{k-1}}\right]^+ & \text{if } E \text{ has good reduction and} \\ \frac{1}{\alpha^k}\cdot\left[\frac{a}{p^k}\right]^+ & \text{otherwise.} \end{cases}$$

for any $k \geqslant 1$ and $a \in \mathbb{Z}_p^\times$. Given a continuous character $\chi$ on $\mathbb{Z}_p^\times$ with values in the completion $\mathbb{C}_p$ of the algebraic closure of $\mathbb{Q}_p$, we may integrate $\chi$ against $\mu_\alpha$. 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 (or a 4-th root of unity when $p=2$) and $\langle x\rangle$ belongs to $1+2p\mathbb{Z}_p$. We define the analytic $p$-adic $L$-function by

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

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 $\kappa$ we denote the cyclotomic character ${}_\infty G \longrightarrow \mathbb{Z}_p^\times$. Because the cyclotomic character is an isomorphism, choosing a topological generator $\gamma$ 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

$$\mathcal{L}_\alpha(E,T) = \int_{\mathbb{Z}_p^\times} (1+T)^{\frac{\log(x)}{\log(\kappa(\gamma))}}\, d\mu_\alpha(x)\,. \tag{4}$$

Recall that $\omega(a)\in\mathbb{Z}_p^*$ is the Teichmüller lift of $a$. For each integer $n\geqslant 1$, define a polynomial

$$P_n(T) = \sum_{a=1}^{p-1}\left(\sum_{j=0}^{p^{n-1}-1} \mu_E\left(\omega(a)(1+p)^j + p^n\mathbb{Z}_p\right)\cdot(1+T)^j\right).$$

**Proposition 2.** *We have that the p-adic limit of these polynomials is the p-adic L-series:*

$$\lim_{n\to\infty} P_n(T) = \mathcal{L}_\alpha(E,T).$$

This convergence is coefficient-by-coefficient, in the sense that if $P_n(T) = \sum_j a_{n,j}T^j$ and $\mathcal{L}_\alpha(E,T) = \sum_j a_j T^j$, then

$$\lim_{n\to\infty} a_{n,j} = a_j.$$

We now give a proof of this convergence and in doing so obtain an upper bound for $|a_j - a_{n,j}|$.

For any choice $\zeta_r$ of $p^r$-th root of unity in $\mathbb{C}_p$, let $\chi_r$ be the $\mathbb{C}_p$-valued character of $\mathbb{Z}_p^\times$ of order $p^r$ which factors through $1 + p\mathbb{Z}_p$ and sends $1 + p$ to $\zeta_r$. Note that the conductor of $\chi_r$ is $p^{r+1}$.

**Lemma 3.** *Let $\zeta_r$ be a $p^r$-th root of unity with $1 \leqslant r \leqslant n-1$, and let $\chi_r$ be the corresponding character of order $p^{r+1}$, as above. Then*

$$P_n(\zeta_r - 1) = \int_{\mathbb{Z}_p^\times} \chi_r \; d\mu_E.$$

*In particular, note that the right hand side does not depend on $n$.*

*Proof.* Writing $\chi = \chi_r$, we have

$$\begin{aligned}
P_n(\zeta_r - 1) &= \sum_{a=1}^{p-1} \sum_{j=0}^{p^{n-1}-1} \mu_E \left(\omega(a)(1+p)^j + p^n\mathbb{Z}_p\right) \cdot \zeta_r^j \\
&= \sum_{a=1}^{p-1} \sum_{j=0}^{p^{n-1}-1} \mu_E \left(\omega(a)(1+p)^j + p^n\mathbb{Z}_p\right) \cdot \chi\left((1+p)^j\right) \\
&= \sum_{b \in (\mathbb{Z}/p^n\mathbb{Z})^*} \mu_E \left(b + p^n\mathbb{Z}_p\right) \cdot \chi(b) \\
&= \int_{\mathbb{Z}_p^\times} \chi \; d\mu_E.
\end{aligned}$$

In the second to the last equality, we use that

$$(\mathbb{Z}/p^n\mathbb{Z})^* \cong (\mathbb{Z}/p\mathbb{Z})^* \times (1 + p(\mathbb{Z}/p^n\mathbb{Z}))^*$$

to sum over lifts of $b \in (\mathbb{Z}/p^n\mathbb{Z})^*$ of the form $\omega(a)(1+p)^j$, i.e., a Teichmüller lift times a power of $(1+p)^j$. In the last equality, we use that $\chi$ has conductor $p^n$, so is constant on the residue classes modulo $p^n$, i.e., the last equality is just the Riemann sums definition of the given integral. $\square$

For each positive integer $n$, let $w_n(T) = (1+T)^{p^n} - 1$.

**Corollary 4.** *We have that*

$$w_{n-1}(T) \textit{ divides } P_{n+1}(T) - P_n(T).$$

*Proof.* By Lemma 3, $P_{n+1}(T)$ and $P_n(T)$ agree on $\zeta_j - 1$ for $0 \leqslant j \leqslant n-1$ and any choice $\zeta_j$ of $p^j$-th root of unity, so their difference vanishes on every root of the polynomial $w_{n-1}(T) = (1+T)^{p^{n-1}} - 1$. The claimed divisibility follows, since $w_{n-1}(T)$ has distinct roots. $\square$

**Lemma 5.** *Let $f(T) = \sum_j b_j T^j$ and $g(T) = \sum_j c_j T^j$ be in $\mathcal{O}[T]$ with $\mathcal{O}$ a finite extension of $\mathbb{Z}_p$. If $f(T)$ divides $g(T)$, then*

$$\operatorname{ord}_p(c_j) \geqslant \min_{0 \leqslant i \leqslant j} \operatorname{ord}_p(b_i).$$

*Proof.* We have $f(T)k(T) = g(T)$. The lemma follows by using the definition of polynomial multiplication and the non-archimedean property of $\operatorname{ord}_p$ on each coefficient of $g(T)$. □

As above, let $a_{n,j}$ be the $j$-th coefficient of the polynomial $P_n(T)$. Let

$$c_n = \max(0, -\min_j \operatorname{ord}_p(a_{n,j}))$$

so that $p^{c_n} P_n(T) \in \mathbb{Z}_p[T]$, i.e., $c_n$ is the smallest power of $p$ that clears the denominator. For any $j > 0$, let

$$e_{n,j} = \min_{1 \leqslant i \leqslant j} \operatorname{ord}_p \binom{p^n}{i}.$$

be the min of the valuations of the coefficients of $w_n(T)$, as in Lemma 5.

**Proposition 6.** *For all $n \geqslant 0$, we have $a_{n+1,0} = a_{n,0}$, and for $j > 0$,*

$$\operatorname{ord}_p(a_{n+1,j} - a_{n,j}) \geqslant e_{n-1,j} - \max(c_n, c_{n+1}).$$

*Proof.* Let $c = \max(c_n, c_{n+1})$. The divisibility of Corollary 4 implies that there is a polynomial $h(T) \in \mathbb{Q}_p[T]$ with

$$w_{n-1}(T) \cdot p^c h(T) = p^c P_{n+1}(T) - p^c P_n(T)$$

and thus (by Gauss' lemma) $p^c h(T) \in \mathbb{Z}_p[T]$ since the right hand side of the equation is integral and $w_{n-1}(T)$ is a primitive polynomial. Applying Lemma 5 and renormalizing by $p^c$ gives the result. □

For $j$ fixed, $e_{n-1,j} - \max(c_{n+1}, c_n)$ goes to infinity as $n$ grows since the $c_k$ are uniformly bounded (they are bounded by the power of $p$ that divides the order of the cuspidal subgroup of $E$). Thus, $\{a_{n,j}\}$ is a Cauchy sequence and Proposition 6 implies that that

$$\operatorname{ord}_p(a_j - a_{n,j}) \geqslant e_{n-1,j} - \max(c_{n+1}, c_n).$$

### 3.1 The $p$-adic multiplier

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

$$\epsilon_p = \left(1 - \tfrac{1}{\alpha}\right)^2 . \tag{5}$$

For a prime of bad multiplicative reduction, we put

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

### 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 $\mu_\alpha$. If $\chi$ is the character on ${}_\infty G$ sending $\gamma$ to a root of unity $\zeta$ of exact order $p^n$, then

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

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

### 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 $\alpha$ of the characteristic polynomial $x^2 - a_p x + p$ that satisfies $\mathrm{ord}_p(\alpha) < 1$. Since $\alpha$ is an algebraic integer, this implies that $\mathrm{ord}_p(\alpha) = 0$, so $\alpha$ is a unit in $\mathbb{Z}_p$. We get therefore a unique $p$-adic $L$-function that we will denote simply by $\mathcal{L}_p(E,T) = \mathcal{L}_\alpha(E,T)$. The following is proved in [Wut06]:

**Proposition 7.** *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 $\mathrm{ord}_p(\epsilon_p)$ is equal to $2\,\mathrm{ord}_p(N_p)$ where $N_p = p + 1 - a_p$ is the number of points in the reduction $\tilde{E}(\mathbb{F}_p)$ at $p$.

We wish to illustrate the above material with a few numerical examples, one for each type of reduction. See Section 12 for more examples. Let $E_0/\mathbb{Q}$ be the curve

$$E_0\colon \quad y^2 + x\,y = x^3 - x^2 - 4\,x + 4 \tag{6}$$

which is labeled 446d1 in Cremona's tables [Cre]. The Mordell-Weil group $E_0(\mathbb{Q})$ is isomorphic to $\mathbb{Z}^2$ generated by the points $(2,0)$ and $(1,-1)$. We consider the prime $p=5$ where $E_0$ has good and ordinary reduction. As the number of points $N_p = 10$ is divisible by $p$, this is an anomalous prime in the terminology of [Maz72]. Using [Ste09], we compute an approximation to the $p$-adic $L$-series as explained above with $n=5$ to find

$$\begin{aligned}\mathcal{L}_5(E_0,T) = {}& \mathbf{O}(5^4)\cdot T + (5+5^2+3\cdot 5^3+\mathbf{O}(5^4))\cdot T^2\\ &+ (2\cdot 5+3\cdot 5^2+3\cdot 5^3+\mathbf{O}(5^4))\cdot T^3 + (4\cdot 5^2+4\cdot 5^3+\mathbf{O}(5^4))\cdot T^4\\ &+ (4\cdot 5+4\cdot 5^2+\mathbf{O}(5^3))\cdot T^5\\ &+ (1+2\cdot 5+5^2+4\cdot 5^3+\mathbf{O}(5^4))\cdot T^6 + \mathbf{O}(T^7)\,.\end{aligned}$$

Note that we claim here directly that the order of vanishing is at least to 1. This follows from the interpolation formula that $\mathcal{L}_5(E_0,0)=0$ as $[0]^+=0$. We will give an explanation for the vanishing of the term in $T^1$ later. We remark that the term in $T^2$ has valuation 1, but the coefficient of $T^6$ is a unit.

### 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 [Kob06] for a simple proof using Kato's Euler system), we know that

$$\left.\frac{d\,\mathcal{L}_p(E,T)}{d\,T}\right|_{T=0} = \frac{1}{\log_p \kappa(\gamma)}\cdot\frac{\log_p(q_{E})}{\mathrm{ord}_p(q_{E})}\cdot\frac{L(E,1)}{\Omega_{E}}$$

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

$$\mathscr{L}_p = \frac{\log_p(q_{E})}{\mathrm{ord}_p(q_{E})} \neq 0\,. \tag{7}$$

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 $\alpha$ and $\beta$ 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 $\omega_{\scriptscriptstyle E}$ denotes the chosen invariant differential on $E$. Let $\eta_{\scriptscriptstyle E} = x\cdot\omega_{\scriptscriptstyle E}$. The pair $\{\omega_{\scriptscriptstyle E},\eta_{\scriptscriptstyle E}\}$ 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 canonical Frobenius $\varphi$ acting on it linearly. We normalize it in the following way which makes it equal to $\frac{1}{p}\cdot F$ with $F$ being the Frobenius as used in [MST06] or in [Ked01, Ked03, Ked04]. Let $t$ be any uniformizer at $O_{\scriptscriptstyle E}$, like $t = -\frac{x}{y}$. Let $\nu$ be a class in $D_p(E)$ represented by the differential $\sum c_n \cdot t^{n-1}\,dt$ with $c_n \in \mathbb{Q}_p$. Then $\varphi(\nu)$ can be represented by the differential $\sum c_n \cdot t^{pn-1}\,dt$. In particular $\varphi(dt) \equiv t^{p-1}\,dt$. The characteristic polynomial of $\varphi$ 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

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

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. Since the invariant differential $\omega_{\scriptscriptstyle E}$ depends on the choice of the Weierstrass equation (1), the expression $\mathcal{L}_p(E,T)$ is also dependent on this choice. However, if we write the series in the basis $\{\omega_{\scriptscriptstyle E},\phi(\omega_{\scriptscriptstyle E})\}$ rather than in $\{\omega_{\scriptscriptstyle E},\eta_{\scriptscriptstyle E}\}$, then the coordinates as above are independent. The $D_p$-valued $L$-series satisfies again certain interpolation properties,[2] e.g.,

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

We will present a numerical example in Section 12.2.

### 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 especially because the existence of the $p$-adic $L$-function is not yet guaranteed in general. Note that there are two interesting papers [Del98] and [Del02] of Delbourgo on this subject. Also Colmez has recently announced a new construction of the $p$-adic $L$-function which would include the additive case. We will not refer to this case anymore throughout the paper.

[2] 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 $(1-\varphi)\cdot(1-p^{-1}\varphi^{-1}) = 1-\varphi+(\varphi-a_p\cdot p^{-1})+p^{-1} = N_p\cdot p^{-1}$.

### 3.7 Quadratic twists

When the curve $E$ is not semistable, we can try to use the modular symbols of a quadratic twist $E^\dagger$ of $E$ in the computation of the $p$-adic $L$-function for $E$. This is useful when the quadratic twist has lower conductor than $E$.

Suppose that there exists a fundamental discriminant $D$ of a quadratic field satisfying the following conditions:

- $p$ does not divide $D$,
- $D^2$ divides $N$,
- $M = N/D^2$ is coprime to $D$, and
- the conductor $N^\dagger$ of the quadratic twist $E^\dagger$ of $E$ by $D$ is of the form $M \cdot Q$ with $Q$ dividing $D$.

Then $\psi = (\frac{D}{\cdot})$ is the Dirichlet character associated to the quadratic field $\mathbb{Q}(\sqrt{D})$ over which $E$ and $E^\dagger$ become isomorphic. Let $f_E^\dagger$ be the newform of level $N^\dagger$ associated to the isogeny class of $E^\dagger$. As explained in section II.11 of [MTT86], the twist of $f_E^\dagger$ by $\psi$ is equal to $f_E$ and we can use their formula (I.8.3)

$$f_E(\tau) = \frac{1}{G(\psi)} \sum_{u \bmod |D|} \psi(u) \cdot f_E^\dagger\Big(\tau + \frac{u}{|D|}\Big). \tag{8}$$

Here $G(\psi)$ is as before the Gauss sum of $\psi$, whose value we know to be the square root $\sqrt{D}$ of $D$ in $\mathbb{R}_{>0}$ or in $i \cdot \mathbb{R}_{>0}$. Let $c_\mathbb{R}$ be the number of connected components of $E(\mathbb{R})$, which is also the number of connected components of $E^\dagger(\mathbb{R})$. We write $\Omega_{E^\dagger}^-$ for $c_\mathbb{R} \cdot \int_{\gamma^-} \omega_E$, similar to $\Omega_{E^\dagger} = \Omega_{E^\dagger}^+ = c_\mathbb{R} \cdot \int_{\gamma^+} \omega_E$ with the notations from (3). We also put

$$\lambda^-(r) = \pi i \cdot \left( \int_r^{i\infty} - \int_{-r}^{i\infty} \right) f(\tau)\, d\tau$$

and $[r]^- = \lambda^-(r)/\Omega_E^-$. As for the modular symbol $[r]^+$, we have $[r]^- \in \mathbb{Q}$. Following [MTT86], we define the quantity $\eta$ such that

$$\sqrt{D} \cdot \Omega_E^+ = \eta \cdot \Omega_{E^\dagger}^{\mathrm{sign}(D)}\,.$$

It is known that $\eta$ is either 1 or 2.

Now we can compute the modular symbol $[r]^+$ for the curve $E$ in terms of modular symbols for $E^\dagger$. Suppose first that $D > 0$.

$$\begin{aligned}
\lambda^+_E(r) &= \pi i \cdot \left(\int_r^{i\infty} + \int_{-r}^{i\infty}\right) \frac{1}{\sqrt{D}} \sum_{u=1}^{D-1} \psi(u) f^\dagger_{\scriptscriptstyle E}\Bigl(\tau + \frac{u}{D}\Bigr) d\tau \\
&= \frac{\pi i}{\sqrt{D}} \sum_{u=1}^{D-1} \psi(u) \int_{r+u/D}^{i\infty} f^\dagger_{\scriptscriptstyle E}(\tau) d\tau \, + \\
&\qquad + \frac{\pi i}{\sqrt{D}} \sum_{v=1}^{D-1} \psi(D-v) \int_{-r}^{i\infty} f^\dagger_{\scriptscriptstyle E}\Bigl(\tau + 1 - \frac{v}{D}\Bigr) d\tau \\
&= \frac{\pi i}{\sqrt{D}} \sum_{u=1}^{D-1} \psi(u) \left(\int_{r+u/D}^{i\infty} + \int_{-r-u/D}^{i\infty}\right) f^\dagger_{\scriptscriptstyle E}(\tau) d\tau \\
&= \frac{1}{\sqrt{D}} \sum_{u=1}^{D-1} \psi(u)\, \lambda^+_{E^\dagger}\Bigl(r + \frac{u}{D}\Bigr)
\end{aligned}$$

We used that $\psi(u) = \operatorname{sign}(D)\, \psi(D-u)$, that $f^\dagger_{\scriptscriptstyle E}(\tau+1) = f^\dagger_{\scriptscriptstyle E}(\tau)$ and equation (8). Similarly for $D < 0$, we find

$$\lambda^+_E(r) = \frac{-1}{\sqrt{D}} \sum_{u=1}^{|D|-1} \psi(u)\, \lambda^-_{E^\dagger}\Bigl(r + \frac{u}{D}\Bigr).$$

Therefore, we have for any fundamental discriminant $D$

$$[r]^+_E = \frac{\operatorname{sign}(D)}{\eta} \sum_{u=1}^{|D|-1} \Bigl(\frac{D}{u}\Bigr) \cdot \Bigl[r + \frac{u}{D}\Bigr]^{\operatorname{sign}(D)}_{E^\dagger}.$$

We can also express the unit eigenvalue $\alpha$ of Frobenius in terms of the corresponding $\alpha^\dagger$ unit eigenvalue for $E^\dagger$ as

$$\alpha = \psi(p) \cdot \alpha^\dagger.$$

In summary, we can evaluate the approximations to the $p$-adic $L$-function of $E$ using only modular symbols of the curve $E^\dagger$ with smaller conductor. The estimations for the error of these approximations remain exactly the same.

We recalled that the computation of the modular symbols $[r]^\pm$ can be done purely algebraically. Unfortunately the algebraic computation determines them only up to sign. If $[0]^+$ is non-zero, we can simply compare the value of the modular symbol at 0 with $L(E,1)/\Omega_{\scriptscriptstyle E} > 0$ and adjust the sign when needed. If $L(E,1) = 0$, we can use the above formula to compute $[0]^+_{E^\dagger}$ for some quadratic twist $E^\dagger$ with non-vanishing $L$-value. So we can easily adjust the unknown sign. Also, if we only know the modular symbols up to a rational multiple, we can use these formulae to scale them.

We should also add here that we can not possibly do a similar thing with quartic or sextic twists when they exist. This is due to the fact that the extension over which the twists become isomorphic is no longer an abelian extension. So we would have to twist the modular symbols with a Galois representation of dimension at least 2. Nevertheless there is a way of using these twists for computing the $p$-adic $L$-function as explained in [CLS09], using the fact that these curves have complex multiplication.

# 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] and [PR03].

Let $\nu$ 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 $\nu$. Hence it is sufficient to define it on the basis $\omega = \omega_E$ and $\eta = \eta_E$.

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

$$h_\omega(P) = \log_E(P)^2$$

where $\log_E$ 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 $\hat{E}$, by integrating our fixed differential $\omega_E$.

For $\nu = \eta$, we define the $p$-adic sigma function of Bernardi as in [Ber81] to be the solution $\sigma$ of the differential equation

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

such that $\sigma(O_E) = 0$, $\frac{d\sigma}{\omega}(O_E) = 1$, and $\sigma(-P) = -\sigma(P)$. If we denote by $t = -\frac{x}{y}$ the uniformizer at $O_E$, we may develop the sigma-function as a series in $t$:

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

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

We say that a point $P$ in $E(\mathbb{Q})$ has good reduction at a prime $p$ if $P$ reduces to the identity component of the special fiber of the Néron model of $E$ at $p$. Given a point $P$ in $E(\mathbb{Q})$ there exists a multiple $m\cdot P$ such that $\sigma(P)$ 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

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

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

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

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

Since this function is quadratic and satisfies the parallelogram law, it induces a bilinear symmetric pairing $\langle \cdot, \cdot \rangle_\nu$ with values in $\mathbb{Q}_p$ defined by

$$\langle P, Q\rangle_\nu = \frac{1}{2} \cdot \bigl( h_\nu(P+Q) - h_\nu(P) - h_\nu(Q) \bigr)\,.$$

Note that all these definitions are dependent on the choice of the Weierstrass equation. It is easy to verify that the pairing is zero if one of the points is a torsion point.

## 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 [MST06] for more details.

Let $\nu_\alpha = a\,\omega + b\,\eta$ be an eigenvector of $\varphi$ 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 $(E, \omega_E)$. Then, if a point $P$ 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

$$\begin{aligned} \hat{h}_p(P) &= \frac{1}{b} \cdot h_{\nu_\alpha}(P) \\ &= -\frac{a}{b} \cdot \log_E(P)^2 + 2 \log\left( \frac{e(P)}{\sigma(P)} \right) \\ &= 2 \log_p \left( \frac{e(P)}{\exp(\frac{e_2}{24} \log_E(P)^2) \cdot \sigma(P)} \right) = 2 \log_p \left( \frac{e(P)}{\sigma_p(P)} \right)\,. \end{aligned} \tag{9}$$

The function $\sigma_p$, 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 a factor of 2 the same as in [MST06].[3] It is also important to note that the function $\hat{h}_p$ is now independent of the Weierstrass equation.

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

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

**Conjecture 3. (Schneider [Sch82])** *The canonical $p$-adic height is non-degenerate on $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tor}}$. 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].

We return to our example $E_0$ from Section 3.3. The methods of [MST06, Har08] permit us to compute the $p$-adic regulator of $E_0$ quite quickly. We have

$$\mathbf{E}_2(E_0, \omega_E) = 3 \cdot 5 + 4 \cdot 5^2 + 5^3 + 5^4 + 5^5 + 2 \cdot 5^6 + 4 \cdot 5^7 + 3 \cdot 5^9 + \mathbf{O}(5^{10}),$$

and the regulator associated to the canonical $p$-adic height is

$$\mathrm{Reg}_p(E_0/\mathbb{Q}) = 2 \cdot 5 + 2 \cdot 5^2 + 5^4 + 4 \cdot 5^5 + 2 \cdot 5^7 + 4 \cdot 5^8 + 2 \cdot 5^9 + \mathbf{O}(5^{10}).$$

## 4.2 The multiplicative case

When $E$ has multiplicative reduction at $p$, we may use Tate's $p$-adic uniformization (see for instance in [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 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 $\psi$ is equal to the subgroup of points of $E(\mathbb{Q}_p)$ lying on the connected component of the reduction modulo $p$ 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 $p$-adic Eisenstein series of weight 2 can then be computed as

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

Then we use the formula as in the good ordinary case to define the canonical sigma function $\sigma_p(t(P)) = \exp(\frac{e_2}{24} \log_E(P)^2) \cdot \sigma(t(P))$. We could also have used directly the formula

$$\sigma_p(u) = \frac{u-1}{u^{1/2}} \cdot \prod_{n \geqslant 1} \frac{(1 - q_E^n \cdot u)(1 - q_E^n/u)}{(1-q^n)^2}$$

where $u \in 1 + p\mathbb{Z}_p$ is the unique preimage of $P \in \widehat{E}(p\mathbb{Z}_p)$ under the Tate parametrization $\psi$, where $\widehat{E}$ is the formal group of $E$ at $p$.

If the reduction is non-split multiplicative, then we use the same formula (9) to define the $p$-adic height as 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 we define

$$\hat{h}_p(P) = 2\log_p\left(\frac{e(P)}{\sigma_p(t(P))}\right) - \frac{\log_p(u)^2}{\log_p(q_{\scriptscriptstyle E})}$$

with $u$ as above. 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].

First, if the rank of the curve is 0, we define the $p$-adic regulator of $E/\mathbb{Q}$ to be $\omega = \omega_{\scriptscriptstyle E} \in D_p(E)$. Assume for the rest of this section that the rank $r$ of $E(\mathbb{Q})$ is positive. Let $\nu = a\,\omega + b\,\eta$ be any element of $D_p(E)$ not lying in $\mathbb{Q}_p\,\omega$, (so $b \neq 0$). It can be easily checked that the value of

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

is independent of the choice of $\nu$. We will call this the $D_p$-valued height on $E(\mathbb{Q})$. But note that it depends on the choice of the Weierstrass equation of $E$: If we change coordinates by putting $x' = u^2\cdot x + r$ and $y' = u^3\cdot y + s\cdot x + t$, then the $D_p$-valued height $H'_p(P)$ computed in the new coordinates $x'$, $y'$ will satisfy $H'_p(P) = \frac{1}{u}\cdot H_p(P)$ for all points $P \in E(\mathbb{Q})$.

On $D_p(E)$ there is a canonical alternating bilinear form $[\cdot,\cdot]$ characterized by the property that $[\omega_{\scriptscriptstyle E}, \eta_{\scriptscriptstyle E}] = 1$. Write $\mathrm{Reg}_\nu \in \mathbb{Q}_p$ for the regulator of $h_\nu$ on $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tor}}$. Then we have the following lemma which is the correction[4] of Lemme 2.6 in [PR03].

**Lemma 8.** *Suppose that the rank $r$ of $E(\mathbb{Q})$ is positive. There exists a unique element $\mathrm{Reg}_p(E/\mathbb{Q})$ in $D_p(E)$ such that for all $\nu \in D_p(E)$, we have*

$$[\mathrm{Reg}_p(E/\mathbb{Q}), \nu] = \frac{\mathrm{Reg}_\nu}{[\omega,\nu]^{r-1}}. \tag{10}$$

*Furthermore, if the rank $r$ is 1, then $\mathrm{Reg}_p(E/\mathbb{Q}) = H_p(P)$ for a generator $P$. If the Weierstrass equation is changed as above, the regulator $\mathrm{Reg}'_p(E/\mathbb{Q})$ computed in the new equation satisfies $\mathrm{Reg}'_p(E/\mathbb{Q}) = \frac{1}{u}\cdot\mathrm{Reg}_p(E/\mathbb{Q})$.*

[4]The wrong normalization in [PR03] only influences the computations with curves of rank greater than 1. It seems that, by chance, the computations in [PR03] were done with a $\nu$ in $D_p(E)$ such that $[\omega,\nu] = 1$, so that the normalization did not enter the end results.

We call $\mathrm{Reg}_p(E/\mathbb{Q}) \in D_p(E)$ the $D_p$-valued regulator of $E/\mathbb{Q}$, or better, of the chosen Weierstrass equation.

*Proof.* Since $h_\omega$ is made out of the square of the linear function $\log_{\scriptscriptstyle E}$, the matrix of the associated pairing on a basis $\{P_i\}$ of $E(\mathbb{Q})$ modulo torsion has entries of the form $\log_{\scriptscriptstyle E}(P_i) \cdot \log_{\scriptscriptstyle E}(P_j)$ and hence has rank 1. Therefore the regulator of the pairing associated to $\nu = a \cdot \omega + b \cdot \eta$ is equal to

$$\mathrm{Reg}_{a\omega + b\eta} = a \cdot b^{r-1} \cdot X + b^r \cdot Y$$

for some constants $X$ and $Y$. In fact, we must have $X = \mathrm{Reg}_{\omega+\eta} - \mathrm{Reg}_\eta$ and $Y = \mathrm{Reg}_\eta$. Therefore the expression on the right hand side of (10) is linear in $\nu$. More explicitly, we may define

$$\mathrm{Reg}_p(E/\mathbb{Q}) = Y \cdot \omega - X \cdot \eta.$$

The formula for the case of rank 1 is then also immediate. The variance of the regulator with the change of the equation can be checked just as for $H_p$. $\square$

Define the fine Mordell-Weil group as in [Wut07] to be the kernel

$$\mathfrak{M}(E/\mathbb{Q}) = \ker\bigl(E(\mathbb{Q}) \otimes \mathbb{Z}_p \longrightarrow E(\mathbb{Q}_p)^{p\text{-adic completion}}\bigr)$$

which is a free $\mathbb{Z}_p$-module of rank $r-1$. The bilinear form associated to the normalized $p$-adic height

$$\frac{h_\nu(P)}{[\omega,\nu]},$$

can be restricted to

$$\langle\cdot,\cdot\rangle_0 \colon \mathfrak{M}(E/\mathbb{Q}) \times (E(\mathbb{Q}) \otimes \mathbb{Z}_p) \longrightarrow \mathbb{Q}_p\,.$$

It is then independent of the choice of $\nu \notin \mathbb{Q}_p\omega$. We call the regulator of this bilinear form $\langle\cdot,\cdot\rangle_0$ on a basis of $\mathfrak{M}(E/\mathbb{Q})$ the fine regulator $\mathrm{Reg}_0(E/\mathbb{Q}) \in \mathbb{Q}_p$, which is an element of $\mathbb{Q}_p$ defined up to multiplication by a unit in $\mathbb{Z}_p$.

**Lemma 9.** *Let $Q$ be a generator of the orthogonal complement of $\mathfrak{M}(E/\mathbb{Q})$ in $E(\mathbb{Q}) \otimes \mathbb{Z}_p$. Then*

$$\mathrm{Reg}_p(E/\mathbb{Q}) \equiv \mathrm{Reg}_0(E/\mathbb{Q}) \cdot H_p(Q) \pmod{\mathbb{Z}_p^\times}.$$

*Proof.* Choose a $\mathbb{Z}_p$-basis of $E(\mathbb{Q}) \otimes \mathbb{Z}_p$ containing $Q$ and a basis of $\mathfrak{M}(E/\mathbb{Q})$. Then $\mathrm{Reg}_\nu$ is, up to multiplication by a unit in $\mathbb{Z}_p$, equal to $\mathrm{Reg}_\nu(\mathfrak{M}) \cdot h_\nu(Q)$, where $\mathrm{Reg}_\nu(\mathfrak{M})$ is the regulator of $\langle\cdot,\cdot\rangle_\nu = \langle\cdot,\cdot\rangle_0 \cdot [\omega,\nu]$ on $\mathfrak{M}(E/\mathbb{Q})$. Hence

$$\frac{\mathrm{Reg}_\nu}{[\omega,\nu]^{r-1}} \equiv \mathrm{Reg}_0(E/\mathbb{Q}) \cdot h_\nu(Q) \pmod{\mathbb{Z}_p^\times}$$

and the statement follows from the previous lemma. $\square$

In particular, 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.*

We have presented here how to compute the $p$-adic regulator in the basis $\{\omega, \eta\}$, but in order to compare it later to the leading term of the $p$-adic $L$-function, it is better to write it in terms of the basis $\{\omega, \varphi(\omega)\}$. In particular, we would then have a vector whose coordinates are independent of the chosen Weierstrass equation.

On page 232 of [BPR93], there is an algorithm for computing $\varphi$ by successive approximation using the development of $\omega$ in terms of a uniformizer $t$. We can now replace this by the computation of $\varphi$ using the cohomology of Monsky and Washnitzer as explained in [Ked01, Ked03, Ked04].

### 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 $\gamma$. 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 $\log_p \kappa(\gamma)^r$ where $r$ is the rank of $E(\mathbb{Q})$. Hence we write

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

## 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*

$$\mathcal{L}_p^*(E,0) = \epsilon_p \cdot \frac{\prod_v c_v \cdot \#\text{Ш}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{\text{tor}})^2} \cdot \operatorname{Reg}_\gamma(E/\mathbb{Q}) \tag{11}$$

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

$$\mathcal{L}_p^*(E,0) = \frac{\mathscr{L}_p}{\log(\kappa(\gamma))} \cdot \frac{\prod_v c_v \cdot \#\text{Ш}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{\text{tor}})^2} \cdot \operatorname{Reg}_\gamma(E/\mathbb{Q}), \tag{12}$$

*where $\mathscr{L}_p$ is as in Equation* (7)*.*

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, as we will see in Section 7.

Again, we consider the curve $E_0$ (see Equation (6)) for an example in the good ordinary case. For this curve, we have $\prod c_v = 2$ and $E_0(\mathbb{Q})_{\text{tor}} = 0$. So all the terms in the expression above can now be computed except for the unknown size of $\text{Ш}(E_0/\mathbb{Q})$. The $p$-adic Birch and Swinnerton-Dyer conjecture predicts now that

$$\#\text{Ш}(E_0/\mathbb{Q}) = 1 + \mathbf{O}(5^3)$$

just as the complex Birch and Swinnerton-Dyer conjecture claims that the Tate-Shafarevich group $\#\text{Ш}(E_0/\mathbb{Q})$ is trivial.

## 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 that we have two coordinates was used cleverly by Kurihara and Pollack in [KP07] 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 supersingular reduction at a prime $p$.*

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

$$(1-\varphi)^{-2} \cdot \mathcal{L}_p^*(E,0) = \frac{\prod_v c_v \cdot \#\text{Ш}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{\text{tor}})^2} \cdot \operatorname{Reg}_\gamma(E/\mathbb{Q}) \quad \in D_p(E)\,. \tag{13}$$

It should be emphasized that both sides of the formula (13) are dependent of the Weierstrass equation. But under a change of the form $x' = u^2 \cdot x + r$, they both get multiplied by $\frac{1}{u}$ and hence the conjecture is independent of this choice.

# 6 Iwasawa theory of elliptic curves

We suppose from now on that $p > 2$. Let ${}_\infty\mathbb{Q}$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, which is a Galois extension of $\mathbb{Q}$ whose Galois group is $\Gamma$. It is the unique $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Let $\Lambda$ be the completed group algebra $\mathbb{Z}_p[\![\Gamma]\!]$. We use a fixed topological generator $\gamma$ of $\Gamma$ to identify $\Lambda$ with $\mathbb{Z}_p[\![T]\!]$ by sending $\gamma$ to $1+T$. It is well known that any finitely generated $\Lambda$-module admits a decomposition up to quasi-isomorphism as a direct sum of elementary $\Lambda$-modules. Denote by ${}_n\mathbb{Q}$ the $n$-th layer of the $\mathbb{Z}_p$-extension, so ${}_n\mathbb{Q}$ is a subfield of ${}_\infty\mathbb{Q}$ and $\mathrm{Gal}({}_n\mathbb{Q}/\mathbb{Q}) \cong \mathbb{Z}/p^n\mathbb{Z}$. As before, we may define the $p$-Selmer group over ${}_n\mathbb{Q}$ by the exact sequence

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

with the product running over all places $\upsilon$ of ${}_n\mathbb{Q}$. Moreover, over the full $\mathbb{Z}_p$-extension, we define $\mathcal{S}_p(E/{}_\infty\mathbb{Q})$ to be the direct 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 $Ш(E/{}_n\mathbb{Q})(p)$ as $n$ tends to infinity. We will consider the Pontryagin dual

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

which is a finitely generated $\Lambda$-module (see [CS00]).

## 6.1 The ordinary case

Assume now that the reduction at $p$ is either good ordinary or of multiplicative type. Kato's Theorem 17.4 in [Kat04], which uses the work of Rohrlich [Roh84], states that $X(E/{}_\infty\mathbb{Q})$ is a torsion $\Lambda$-module. Hence by the decomposition theorem, we may associate to it a characteristic series

$$f_{E}(T) \in \mathbb{Z}_p[\![T]\!] \tag{14}$$

that is well-defined up to multiplication by a unit in $\mathbb{Z}_p[\![T]\!]^\times$.

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 $T = \zeta - 1$ with $\zeta$ a root of unity whose order is a power of $p$ describe the growth of the rank. Since a non-zero power series with coefficients in $\mathbb{Z}_p$ can only have finitely many zeros, one can deduce 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 result is due to Schneider [Sch85] and Perrin-Riou [PR82]. The multiplicative case is due to Jones [Jon89]. Note that he uses the analytic and algebraic $p$-adic height defined by Schneider in [Sch82]; with the mentioned correction by Werner they agree with our definition in Section 4.2.

**Theorem 10** (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*

$$\epsilon_p \cdot \frac{\prod_v c_v \cdot \#\text{Ш}(E/\mathbb{Q})(p)}{(\#E(\mathbb{Q})(p))^2} \cdot \operatorname{Reg}_\gamma(E/\mathbb{Q})$$

*unless the reduction is split multiplicative in which case the same formula holds with $\epsilon_p$ replaced by $\mathscr{L}_p/\log(\kappa(\gamma))$.*

Let us consider again the curve $E_0$. We have computed the 5-adic regulator and found that it is non-zero. The above theorem shows now that the order of vanishing of $f_{E_0}(T)$ is at least equal to the rank. The finiteness of $\text{Ш}(E_0/\mathbb{Q})(5)$ is now equivalent to the statement that the order of vanishing is equal to the rank. If it is the case then the leading coefficient has valuation equal to

$$\operatorname{ord}_5(f^*_{E_0}(0)) = 1 + \operatorname{ord}_5(\#\text{Ш}(E_0/\mathbb{Q})(5))\,.$$

If the valuation of the leading term of $f_{E_0}(T)$ is positive we call $p$ an irregular prime for $E$. For irregular primes either the Mordell-Weil rank of $E$ over ${}_\infty\mathbb{Q}$ is larger than the rank of $E(\mathbb{Q})$ or the Tate-Shafarevich group $\text{Ш}(E/{}_\infty\mathbb{Q})$ is no longer finite. We will later determine exactly what happens for $E_0$.

### 6.2 The supersingular case

The supersingular case is more complicated, since the $\Lambda$-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 $\Lambda$-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 $\mathbb{H}^1_{\text{loc}}$ to be the projective limit of the cohomology groups $\mathrm{H}^1({}_n\mathbb{Q}_\mathfrak{p}, T_pE)$ with respect to 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 $\Lambda$-linear Coleman map Col from $\mathbb{H}^1_{\text{loc}}$ 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 $\Lambda$-torsion module. Denote by $g_E(T)$ its characteristic series.

Let $\Sigma$ be any finite set of places in $\mathbb{Q}$ containing the places of bad reduction for $E$ and the places $\infty$ 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 $\Sigma$. Next we define $\mathbb{H}^1_{\text{glob}}$ as the projective limit of $\mathrm{H}^1(G_\Sigma(_n\mathbb{Q}), T_pE)$. It is a $\Lambda$-module of rank 1 and it is actually independent of the choice of $\Sigma$.

By Kato again, the $\Lambda$-module $\mathbb{H}^1_{\text{glob}}$ is torsion-free and $\mathbb{H}^1_{\text{glob}}\otimes\mathbb{Q}_p$ has $\Lambda\otimes\mathbb{Q}_p$-rank 1. Choose now any element $_\infty c$ in $\mathbb{H}^1_{\text{glob}}$ such that $Z_c = \mathbb{H}^1_{\text{glob}}/(\Lambda \cdot {}_\infty c)$ is $\Lambda$-torsion. Typically such a choice could be the "zeta element" of Kato, i.e. the image of his Euler system in $\mathbb{H}^1_{\text{glob}}$. 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

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

where by $\mathrm{Col}(_\infty c)$ we mean the image under the Coleman map Col of the localization of $_\infty c$ to $\mathbb{H}^1_{\text{loc}}$. 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 11** (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 $\text{Ш}(E/\mathbb{Q})(p)$ is finite (Conjecture 1). In this case the leading term of the series $(1-\varphi)^{-2} f_E(T)$ has the same valuation as*

$$\prod_v c_v \cdot \#\text{Ш}(E/\mathbb{Q})(p) \cdot \mathrm{Reg}_p(E/\mathbb{Q})\,.$$

Note that the proof of this theorem in the appendix of [PR03] for the supersingular case uses the formula in lemma 9 rather than the wrong definition of the regulator. Also we simplified the right hand term in comparison to (13), because $N_p \equiv 1 \pmod p$ and hence $\#E(\mathbb{Q})_{\text{tor}}$ must be a $p$-adic unit, since the reduction at $p$ is supersingular.

# 7 The Main Conjecture

The main conjecture links the two $p$-adic power series (4) and (14) 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 $T \cdot \Lambda^\times$.*

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 the notations of the previous section, it can be reformulated by saying that $g_E(T) = h_c(T)$ when $c$ is Kato's zeta element.

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

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

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 semi-stable curves surjectivity can only fail when there is an isogeny of degree $p$ defined over $\mathbb{Q}$. See [Ser72] and [Ser96].

**Kato's Theorem 12.**
*Suppose that $E$ has semi-stable 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 $\Lambda$ 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 [Kob06].

In particular, the theorem applies to all odd primes $p$ if $E$ is a semi-stable 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 13.**
*Suppose the image of $\bar{\rho}_p$ is not contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ 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.

## 7.1 The examples

Consider again the curve $E_0$ (see Equation (6)) and the good ordinary prime $p = 5$. The theorem of Kato shows that $f_{E_0}(T)$ divides $\mathcal{L}_p(E_0, T)$. Since we have found two linearly independent points of infinite order on $E_0(\mathbb{Q})$, we know that the rank of $E_0(\mathbb{Q})$ is at least 2. Hence the order of vanishing of $f_{E_0}(T)$ at $T = 0$ is at least 2 and, by the above theorem, so is the order of vanishing for $\mathcal{L}_p(E_0, T)$. But we have computed an approximation to $\mathcal{L}_p(E_0, T)$ showing that the order of vanishing cannot be larger than 2. Therefore the rank of $E_0(\mathbb{Q})$ is equal to the order of vanishing of the $p$-adic $L$-series.

But we know more now. The fact that the order of vanishing of $f_{E_0}(T)$ is equal to 2 shows that the 5-primary part of $Ш(E_0/\mathbb{Q})$ cannot be infinite. Comparing the leading term of $\mathcal{L}_p(E_0, T)$, which has valuation 1, and the leading term of $f_{E_0}(T)$, which has valuation $1 + \mathrm{ord}_5(\#Ш(E_0/\mathbb{Q})(5))$, shows that *the* 5*-primary part of* $Ш(E_0/\mathbb{Q})$ *is trivial*.

Moreover, the series $f_{E_0}(T)$ and $\mathcal{L}_p(E_0, T)$ have now the same leading term. This implies that the main conjecture holds, i.e. $f_{E_0}(T) \in \mathcal{L}_p(E_0, T) \cdot \Lambda^\times$. By analyzing the series $\mathcal{L}_p(E_0, T)$, it can be shown that

$$f_E(T) = T \cdot ((T + 1)^5 - 1) \cdot u(T)$$

for a unit $u(T) \in \Lambda^\times$. Let ${}_1\mathbb{Q}$ be the first layer of the $\mathbb{Z}_5$-extension of $\mathbb{Q}$. Unless the Tate-Shafarevich group $Ш(E/{}_1\mathbb{Q})(5)$ is infinite, Iwasawa theory predicts now that the rank of the Mordell-Weil group $E_0({}_1\mathbb{Q})$ is 6. Doing a quick search it is easy to find points of infinite order in $E({}_1\mathbb{Q})$ which are not defined over $\mathbb{Q}$. Therefore, we know that the rank of $E({}_1\mathbb{Q})$ and of $E({}_\infty\mathbb{Q})$ is 6 and that $Ш(E_0/{}_1\mathbb{Q})(5)$ and $Ш(E_0/{}_\infty\mathbb{Q})(5)$ are finite. For more examples of such factorizations of $p$-adic $L$-series we refer to [Pol].

# 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 $Ш(E/\mathbb{Q})$ 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 semi-stable reduction such that the representation $\bar{\rho}_p$ is either surjective or has image contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. 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 Theorem[5] 10 of Perrin-Riou and Schneider for the first equality and Kato's Theorem 12 on the main conjecture for the inequality in the second line.

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

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:

$$\begin{aligned}\operatorname{ord}_p\left(\#\text{Ш}(E/\mathbb{Q})(p)\right) &\leqslant \operatorname{ord}_p\left(\frac{L(E,1)}{\Omega_E}\right)-\operatorname{ord}_p\left(\frac{\prod c_v}{(\#E(\mathbb{Q})_{\text{tor}})^2}\right)\\ &= \operatorname{ord}_p(\#\text{Ш}(E/\mathbb{Q})_{\text{an}}).\end{aligned}\tag{15}$$

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

### 8.2 The multiplicative case

If the reduction is not split, then the above holds just the same, because in all the theorems involved the non-split case never differs form the good ordinary case (only the split multiplicative case is exceptional). If instead the reduction is split multiplicative, we have that $\mathcal{L}_p(E,0)=0$ and

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

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 (15) 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 $\omega_E$. We may therefore concentrate solely on the coordinate in $\omega_E$.

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

Write $\mathrm{ord}_p(f_{\scriptscriptstyle E}(0))$ for the $p$-adic valuation of the leading coefficient of the $\omega_{\scriptscriptstyle E}$-coordinate of $f_{\scriptscriptstyle E}(T)$. Again we obtain an inequality by using Theorem 11

$$\begin{aligned}\mathrm{ord}_p\left(\prod_{\upsilon} c_\upsilon \cdot \#\text{Ш}(E/\mathbb{Q})(p)\right) &= \mathrm{ord}_p((1-\varphi)^{-2}\, f_{\scriptscriptstyle E}(0)) \\ &\leqslant \mathrm{ord}_p((1-\varphi)^{-2}\, \mathcal{L}_p(E,0)) \\ &= \mathrm{ord}_p\left(\frac{L(E,1)}{\Omega_{\scriptscriptstyle E}}\right).\end{aligned}$$

So we have once again that $\#\text{Ш}(E/\mathbb{Q})(p)$ is bounded from above by the highest power of $p$ dividing $\#\text{Ш}(E/\mathbb{Q})_{\mathrm{an}}$.

### 8.4 Conclusion

Summarizing the above computations, we have

**Theorem 14** (Kato, Perrin-Riou, Schneider)**.**
*Let $E$ be an elliptic curve such that $L(E,1)\neq 0$. Then $\text{Ш}(E/\mathbb{Q})$ is finite and*

$$\#\text{Ш}(E/\mathbb{Q}) \;\Big|\; C\cdot \frac{L(E,1)}{\Omega_{\scriptscriptstyle E}}\cdot\frac{(\#E(\mathbb{Q})_{\mathrm{tor}})^2}{\prod c_\upsilon}$$

*where $C$ is a product of a power of 2 and of powers 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 semi-stable, then $C$ is a power of 2.*

This improves Corollary 3.5.19 in [Rub00].

## 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

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

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 $\prod c_v \cdot \#Ш(E/\mathbb{Q}) \cdot (\#E(\mathbb{Q})_{\mathrm{tor}})^{-2}$. 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 $T \mid f_E(T)$). We thus arrive at the following theorem.

**Theorem 15** (Kato, Perrin-Riou).
*Let $E/\mathbb{Q}$ be an elliptic curve with good ordinary reduction at the odd prime $p$. Assume that the $p$-adic regulator of $E$ is nonzero. 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 $Ш(E/\mathbb{Q})$ is finite and its valuation is bounded by*

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

In other words the upper bound asserted by the Birch and Swinnerton-Dyer conjecture is 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.

The above theorem is valid only under the assumption that the reduction is good ordinary. This is only this case when we know a proof of the $p$-adic Gross-Zagier formula. It would be very interesting to obtain a generalization of this formula to the supersingular case.

# 10 The algorithm for an upper bound of the rank

Let $E/\mathbb{Q}$ be an elliptic curve. We now have 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 $T=0$. Note that a theorem of Rohrlich [Roh84] guarantees that $\mathcal{L}_p(E,T)$ is not zero. Then

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

by Kato's Theorems 12 and 13 and by the theorems 10 and 11. Hence we have an upper bound on the rank $r$.

**Proposition 16.** *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 also obtains 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 17.** *Let $E$ be an elliptic curve, and assume that there is a prime $p$ of good reduction such that the $p$-adic Birch and Swinnerton-Dyer conjecture is true. Then there is an algorithm that computes the rank $r$ of $E$ using $p$-adic $L$-functions.*

Of course, the algorithm for computing bounds on the rank $r$ using $m$-descents has the same properties: it tries to determine the rank by searching for points and by bounding $r$ from above by the rank of the various $m$-Selmer groups. Unless all the $p$-primary parts of the Tate-Shafarevich group are infinite this algorithm returns the rank $r$ after a finite number of steps.

But the two algorithms are fundamentally different, since the $m$-descent algorithm is fast and there are optimized implementations for $m = 2, 3, 4$, but it would be extremely time-consuming for larger $m$, e.g., $m \geqslant 7$. (In fact, nobody has yet implemented and run a program that computes general 7-descents.)

## 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 for 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.

Also the speed of the computation of $\mathcal{L}_p(E,T)$ using modular symbols depends on the size of the conductor. As the conductor grows, the determination of the rank, when it is larger than 1, using the descent method becomes much more efficient than the use of $p$-adic $L$-series. However, using $p$-adic $L$-series may provide an advantage when considering families of quadratic twists.

Another advantage to the descent method is that the determination of the $m$-Selmer group for some $m > 1$ can be used for the search of points of infinite order. If the elements of the Selmer group can be expressed as coverings, it is much more efficient to search for rational points on the coverings rather than on the elliptic curve itself.

## 11 The algorithm for the Tate-Shafarevich group

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 $Ш(E/\mathbb{Q})$. 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 $p$,
- and 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 of $\mathrm{GL}_2(\mathbb{F}_p)$.

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

**Algorithm 18.** Given an elliptic curve $E/\mathbb{Q}$ and a prime $p$ satisfying the above conditions, this procedure either gives an upper bound for $\#Ш(E/\mathbb{Q})(p)$ or terminates with an error.

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 [MST06]. Exit with an error if the $p$-adic height pairing cannot be 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
$$\mathrm{ord}_{T=0}\, \mathcal{L}_p(E, T)$$
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 $\mathrm{ord}_{T=0}\, \mathcal{L}_p(E, T) = r$ (or $r + 1$), then exit with an error.
4. Now compute the remaining information, including the Tamagawa numbers $c_v$ and the $p$-adic multiplier $\epsilon_p$. 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, 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 $p$, 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. Output 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 regulator holds and that $Ш(E/\mathbb{Q})(p)$ is indeed finite by Theorem 10 (or Theorem 11 in the supersingular case). Moreover this theorem shows 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 $\epsilon_p$ replaces by $\mathscr{L}_p$ in the split multiplicative case) and

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

in the supersingular case. Finally use Kato's Theorem 12 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 $\operatorname{ord}_p(\#Ш(E/\mathbb{Q})(p))$. □

In the next proposition we summarize the discussion of this section.

**Proposition 19.** *Let $E$ be an elliptic curve and $p > 2$ a prime for which $E$ has semi-stable reduction. If Conjectures 3 and 4 hold and if we are able to determine the Mordell-Weil group of $E$, then there is a algorithm to verify that the $p$-primary part of $Ш(E/\mathbb{Q})$ is finite. If moreover the representation $\bar{\rho}_p$ is either surjective or has its image contained in a Borel subgroup, then the algorithm produces an upper bound on $\#Ш(E/\mathbb{Q})(p)$. If the main Conjecture 7 holds then the result of the algorithm is equal to the 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. E.g., 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 for points 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.

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 only weaker variants of the $p$-adic Birch and Swinnerton-Dyer conjecture are needed.

Another application of the algorithm is the following remark. If, for a given elliptic curve $E$ and a prime $p$, the algorithm yields the answer that the $p$-primary part of $\text{Ш}(E/\mathbb{Q})$ is trivial, then the algorithm has actually also proved the main conjecture for $E$ and $p$. Because we know by then that $\mathcal{L}_p(E,T)$ and the characteristic series $f_E(T)$ of the Selmer group have the same order of vanishing at $T=0$ and the leading terms have the same valuation. Since, by Kato's theorem $f_E(T)$ divides $\mathcal{L}_p(E,T)$, we know then that the quotient is a unit in $\mathbb{Z}_p[\![T]\!]$. Such calculations and especially this remark on how to verify the main conjecture in special cases are already contained in [PR03] for supersingular primes $p$.

## 12 Numerical results

The algorithms described above are implemented in Sage (see [Ste09]), which is a free open source mathematics software package. All of the calculations given below can be carried out using Sage.

### 12.1 A split multiplicative example

To give an example of a curve with split multiplicative reduction, we use the same curve as before (see Equation (6))

$$E_0\colon \quad y^2 + x\,y = x^3 - x^2 - 4\,x + 4$$

but with the prime $p = 223$. Of course, there is no hope in practice that a 223-descent could be used to compute the order of $Ш(E_0/\mathbb{Q})(223)$. We can compute the $p$-adic regulator and the $L$-invariant to high precision very quickly using Tate's parametrization of $E$:

$$\mathrm{Reg}_p(E_0/\mathbb{Q}) = 153 \cdot 223^2 + 125 \cdot 223^3 + 124 \cdot 223^4 + \mathbf{O}(223^5),$$
$$\mathscr{L} = 179 \cdot 223 + 85 \cdot 223^2 + 30 \cdot 223^3 + \mathbf{O}(223^4).$$

The computation of the $p$-adic $L$-series is more time consuming. But as we only need the first $p$-adic digit to prove the triviality of $Ш(E_0/\mathbb{Q})(223)$, we only need to sum over 222 modular symbols. This yields

$$\mathcal{L}_p(E_0, T) = \mathbf{O}(223^4) + \mathbf{O}(223^1) \cdot T + \mathbf{O}(223^1) \cdot T^2 + (139 + \mathbf{O}(223)) \cdot T^3 + \mathbf{O}(T^4).$$

In fact, we know that the first three coefficients vanish as we are in the exceptional case, so the leading term has valuation 0. From these computations, we see that the $p$-adic Birch and Swinnerton-Dyer conjecture predicts that

$$\#Ш(E_0/\mathbb{Q}) \equiv 1 \pmod{223};$$

in particular we may conclude that $Ш(E_0/\mathbb{Q})(223) = 0$.

## 12.2 A supersingular example

Let $E$ be the elliptic curve

$$E\colon \quad y^2 + x = x^3 + x^2 + 2 \cdot x + 2$$

listed as curve 1483a1 in Cremona's tables. The curve has rank 2 generated by $(-1, 0)$ and $(0, 1)$. The reduction of $E$ at $p = 5$ is supersingular. The $p$-adic $L$-function equals

$$\begin{aligned}\mathcal{L}_p(E, T) =& \big((1 + \mathbf{O}(5)) \cdot T^2 + (1 + \mathbf{O}(5)) \cdot T^3 + \mathbf{O}(T^4)\big) \cdot \omega_E \\ &+ \big((4 \cdot 5 + \mathbf{O}(5^2)) \cdot T^2 + (4 \cdot 5 + \mathbf{O}(5^2)) \cdot T^3 + \mathbf{O}(T^4)\big) \cdot \varphi(\omega_E)\end{aligned}$$

where we have already taken in account that the first two terms vanish. We compute the normalized $D_p$-valued regulator

$$\begin{aligned}\mathrm{Reg}_\gamma(E/\mathbb{Q}) =& \big(1 + 2 \cdot 5 + 3 \cdot 5^2 + 5^3 + \mathbf{O}(5^5)\big) \cdot \omega_E \\ &+ \big(4 \cdot 5 + 4 \cdot 5^2 + 4 \cdot 5^3 + 5^4 + 2 \cdot 5^5 + \mathbf{O}(5^6)\big) \cdot \varphi(\omega_E)\,.\end{aligned}$$

Hence the $p$-adic Birch and Swinnerton-Dyer conjecture predicts that

$$\begin{aligned}&\big(1 + \mathbf{O}(5)\big)\, \omega_E + \big(4 \cdot 5 + \mathbf{O}(5^2)\big)\, \varphi(\omega_E) = \\ &\qquad \#Ш(E/\mathbb{Q}) \cdot \Big(\big(1 + \mathbf{O}(5)\big)\, \omega_E + \big(4 \cdot 5 + \mathbf{O}(5^2)\big)\, \varphi(\omega_E)\Big).\end{aligned}$$

In particular, we have shown that $Ш(E/\mathbb{Q})(5)$ is trivial. It follows from Iwasawa-theoretic consideration as in [PR03] that, if $\#Ш(E/_n\mathbb{Q})(5) = 5^{e_n}$ then

$$e_n = \frac{p}{p^2 - 1} \cdot p^n + \mathbf{O}(1)\,.$$

### 12.3 An example whose Tate-Shafarevich group is non-trivial

Let $E$ be the elliptic curve given by

$$E: \quad y^2 + x\,y = x^3 + 16353089\,x - 335543012233$$

which is labeled 858k2 in [Cre]. The curve has rank 0 and is semi-stable, and the full Birch and Swinnerton-Dyer conjecture predicts that the Tate-Shafarevich group $Ш(E/\mathbb{Q})$ consists of two copies of $\mathbb{Z}/7\mathbb{Z}$.

We may compute the 7-adic $L$-series, which yields

$$\begin{aligned}\mathcal{L}_7(E,T) =& 7^2 \cdot (2 \cdot 7^2 + 7^3 + 7^4 + 3 \cdot 7^5 + \mathbf{O}(7^6) + (5 \cdot 7^2 + \mathbf{O}(7^3)) \cdot T \\ & + (3 + 4 \cdot 7 + 5 \cdot 7^2 + \mathbf{O}(7^3)) \cdot T^2 + \mathbf{O}(T^3))\end{aligned}$$

On the algebraic side, we find that the constant term of the characteristic series of $E$ has valuation $2 + \mathrm{ord}_7(\#Ш(E/\mathbb{Q}))$. So our algorithm yields the correct upper bound, that $\#Ш(E/\mathbb{Q})(7) \leqslant 7^2$. We can change to the curve 858k1 with a 7-isogeny and prove there directly that the upper bound on the 7-primary part of the Tate-Shafarevich group is 1, so by isogeny invariance of the Birch and Swinnerton-Dyer conjecture it follows that $\#Ш(E/\mathbb{Q})(7) = 7^2$. (Of course, this can be shown with other methods for this curve of rank 0, e.g. by using Heegner points.) Since we know the exact order of $Ш(E/\mathbb{Q})$, we deduce that the main conjecture holds.

Once again we learn even more from the computation of the $p$-adic $L$-series. Iwasawa theory tells us now that the order of the Tate-Shafarevich group grows very quickly (for an ordinary prime) in the $\mathbb{Z}_7$-extension. Namely if $\#Ш(E/_n\mathbb{Q}) = 7^{e_n}$ then $e_n = 2 \cdot 7^n + 2 \cdot n + \mathbf{O}(1)$.

### 12.4 Future Tables

We intend to write a follow-up paper to the present article that contains extensive tables, analysis of the resulting data, and more detailed discussion of computational complexity and implementation issues. These tables will include $p$-adic regulators, and the $p$-adic analytic order of the Tate-Shafarevich group $Ш(E/\mathbb{Q})$ for various small primes and a large number of curves of various ranks. In particular, we will compute the upper bound on the order of $Ш(E/\mathbb{Q})(p)$ for many pairs $(E, p)$ where we expect to have nontrivial elements $Ш(E/\mathbb{Q})(p)$.

## References

[ARS06] Amod Agashe, Kenneth Ribet, and William A. Stein, *The Manin constant*, Pure Appl. Math. Q. **2** (2006), no. 2, 617–636.

[AS02] Amod Agashe and William Stein, *Visibility of Shafarevich-Tate groups of abelian varieties*, J. Number Theory **97** (2002), no. 1, 171–185.

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic).

[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.

[CFO+06] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll, *Explicit n-descent on elliptic curves, II, III*, preprints, 2006.

[CFO+08] ———, *Explicit n-descent on elliptic curves. I. Algebra*, J. Reine Angew. Math. **615** (2008), 121–155.

[CLS09] John Coates, Zhibin Liang, and Ramdorai Sujatha, *The Tate-Shafarevich group for elliptic curves with complex multiplication*, preprint, 2009.

[Coh07] Henri Cohen, *Number theory. Vol. II. Analytic and modern tools*, Graduate Texts in Mathematics, vol. 240, Springer, New York, 2007. MR MR2312338

[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.

[Cre] J. E. Cremona, *Elliptic Curves Data*, `http://www.warwick.ac.uk/~masgaj/ftp/data/INDEX.html`.

[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.

[Dok04] Tim Dokchitser, *Computing special values of motivic L-functions*, Experiment. Math. **13** (2004), no. 2, 137–149. MR MR2068888 (2005f:11128)

[Edi91] Bas Edixhoven, *On the Manin constants of modular elliptic curves*, Arithmetic algebraic geometry (Texel, 1989), Progr. Math., vol. 89, Birkhäuser Boston, Boston, MA, 1991, pp. 25–39.

[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.

[Har08] David Harvey, *Efficient computation of p-adic heights*, LMS J. Comput. Math. **11** (2008), 40–59.

[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.

[Ked01] Kiran S. Kedlaya, *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, J. Ramanujan Math. Soc. **16** (2001), no. 4, 323–338. MR MR1877805 (2002m:14019)

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

[Ked04] K. Kedlaya, *Computing zeta functions via p-adic cohomology*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 1–17.

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

[Kob06] Shinichi Kobayashi, *An elementary proof of the Mazur-Tate-Teitelbaum conjecture for elliptic curves*, Doc. Math. (2006), no. Extra Vol., 567–575 (electronic).

[KP07] Masato Kurihara and Robert Pollack, *Two $p$-adic $L$-functions and rational points on elliptic curves with supersingular reduction*, $L$-functions and Galois representations, London Math. Soc. Lecture Note Ser., vol. 320, Cambridge Univ. Press, Cambridge, 2007, pp. 300–332.

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

[Maz72] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.

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

[MST06] Barry Mazur, William Stein, and John Tate, *Computation of $p$-adic heights and log convergence*, Doc. Math. (2006), no. Extra Vol., 577–614 (electronic).

[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.

[PAR06] The PARI Group, Bordeaux, *PARI/GP, version* `2.3.1`, 2006, available from `http://pari.math.u-bordeaux.fr/`.

[Pol] Robert Pollack, *Tables of iwasawa invariants of elliptic curves*, `http://math.bu.edu/people/rpollack/Data/data.html`.

[Pol03] ———, *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.

[PR04] Robert Pollack and Karl Rubin, *The main conjecture for CM elliptic curves at supersingular primes*, Ann. of Math. (2) **159** (2004), no. 1, 447–464.

[Roh84] David E. Rohrlich, *On L-functions of elliptic curves and cyclotomic towers*, Invent. Math. **75** (1984), no. 3, 409–423.

[Rub99] Karl Rubin, *Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer*, Arithmetic theory of elliptic curves (Cetraro, 1997), Lecture Notes in Math., vol. 1716, Springer, Berlin, 1999, pp. 167–234.

[Rub00] ———, *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.

[Sim02] Denis Simon, *Computing the rank of elliptic curves over number fields*, LMS J. Comput. Math. **5** (2002), 7–17 (electronic).

[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.

[Ste07] William Stein, *The Birch and Swinnerton-Dyer Conjecture, a Computational Approach*, 2007, http://wstein.org/books/bsd/.

[Ste09] William Stein, *Sage Mathematics Software (Version 3.2.3)*, The Sage Group, 2009, `http://www.sagemath.org`.

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

[Wil95] Andrew Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.

[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.