MATHEMATICS OF COMPUTATION
Volume 82, Number 283, July 2013, Pages 1757–1792
S 0025-5718(2012)02649-4
Article electronically published on September 14, 2012

ALGORITHMS FOR THE ARITHMETIC OF ELLIPTIC CURVES USING IWASAWA THEORY

WILLIAM STEIN AND CHRISTIAN WUTHRICH

Abstract. We explain how to use results from Iwasawa theory to obtain information about p-parts of Tate-Shafarevich groups of specific elliptic curves over $\mathbb{Q}$. Our 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, e.g., when the rank of the Mordell-Weil group is greater than 1. We apply our results along with a computer calculation to show that $Ш(E/\mathbb{Q})[p] = 0$ for the 1,534,422 pairs (E, p) consisting of a non-CM elliptic curve E over $\mathbb{Q}$ with conductor $\leq$ 30,000, rank ≥ 2, and good ordinary primes p with $5 \leq p < 1000$ and surjective mod-p representation.

1. Introduction

The papers [GJP09, Mil10] describe verification of the Birch and Swinnerton-Dyer conjecture for elliptic curves of conductor ≤ 5000 with rank ≤ 1 by a computational application of Euler system results of Kato and Kolyvagin combined with explicit descent. The main motivation for the present paper is to develop algorithms using Iwasawa theory, in order to enable verification of the conjecture in new directions, e.g., large-scale verification of assertions about $Ш(E/\mathbb{Q})$, when E has rank at least 2. The present paper naturally complements related projects by Perrin-Riou [PR03] and Coates [CLS09, Coa11]. Moreover, we fill small gaps in the literature (e.g., precision bounds in Section 3) and take the opportunity to correct errors in the literature (e.g., Lemma 4.2) that we found in the course of implementing algorithms.

In Sections 2–7 we recall the main objects and theorems involved in the classical and p-adic Birch and Swinnerton-Dyer conjectures (BSD conjectures), correct some minor errors in the literature, and state a tight error bound that is essential for rigorous computation with p-adic L-series. These sections gather together disparate results and provide unified notation and fill minor gaps. 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, and recall p-adic analogues of the BSD conjecture. In Section 6, we recall the basic definitions and results for the algebraic p-adic L-functions defined using Iwasawa theory. This leads to the statement of the main conjecture and Kato's theorem.

Received by the editor July 4, 2011 and, in revised form, November 11, 2011.

2010 *Mathematics Subject Classification.* Primary 11D88, 11G05, 11G40, 11G50, 14G05; Secondary 11Y50, 11Y40, 14G10.

The first author was supported by NSF grants DMS-0555776 and DMS-0821725.

In Section 8 we discuss using p-adic results to bound $Ш(E)(p)$ when E has analytic rank 0, and Section 9 covers the case when the analytic rank is 1. In Section 10 we describe a conditional algorithm for computing the rank of an elliptic curve that uses p-adic methods and hence differs in key ways from the standard n-descent approach. Similarly, Section 11 contains an algorithm that applies to curves of any rank, and either computes $Ш(E/\mathbb{Q})(p)$ or explicitly disproves some standard conjecture. In Section 12 we give examples that illustrate the algorithms described above in numerous cases, including verifying for a rank 2 curve E that $Ш(E/\mathbb{Q})(p) = 0$ for a large number of p, as predicted by the BSD conjecture. In particular, we prove the following theorem via a computation of p-adic regulators and p-adic L-functions, which provides evidence for the BSD conjecture for curves of rank at least 2:

Theorem 1.1. *Let X be the set of* 1,534,422 *pairs (E, p), where E is a non-CM elliptic curve over $\mathbb{Q}$ with rank at least* 2 *and conductor $\leq 30,000$, and $p \geq 5$ is a good ordinary prime for E with $p < 1000$ such that the mod p representation is surjective. Then $Ш(E/\mathbb{Q})[p] = 0$ for each of the pairs in X.*

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

$$y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \tag{1.1}$$

be the unique global minimal Weierstrass equation for E with $a_1, a_3 \in \{0, 1\}$ and $a_2 \in \{-1, 0, 1\}$. Mordell proved that the set of rational points $E(\mathbb{Q})$ is an abelian group of finite rank $r = \operatorname{rank}(E(\mathbb{Q}))$. Birch and Swinnerton-Dyer conjectured that $r = \operatorname{ord}_{s=1} L(E, s)$, where $L(E, s)$ is the Hasse-Weil L-function of E (see Conjecture 2.1 below). We call $r_{\mathrm{an}} = \operatorname{ord}_{s=1} L(E, s)$ the analytic rank of E, which is defined since $L(E, s)$ can be analytically continued to all $\mathbb{C}$ (see [BCDT01]).

There is no known algorithm (procedure that has been proved to terminate) that computes r in all cases. We 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. We can also use constructions of complex and p-adic Heegner points 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, we can use Kolyvagin's work on Euler systems of Heegner points; for general rank, the only known method is to do an n-descent for some integer $n > 1$. The 2-descents implemented by Cremona [Cre97], by Simon [Sim02] in Pari [PAR11] (and SAGE [S11b]), and the $2, 3, 4$, etc., descents in Magma [BCP97] (see also [CFO08, CFO09, CFO11]), 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 $Ш(E/\mathbb{Q})$ is a torsion abelian group associated to $E/\mathbb{Q}$. It is the kernel of the localization map loc in the exact sequence

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

where the sum runs over all places v of $\mathbb{Q}$. The arithmetic importance of this group lies in its geometric interpretation. There is a bijection from $Ш(E/\mathbb{Q})$ 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 $Ш(E/\mathbb{Q})$ correspond to

curves C that defy the Hasse principle, i.e., have a point over every completion of $\mathbb{Q}$, but have no points over $\mathbb{Q}$.

Conjecture 1.2 (Shafarevich and Tate)**.** *The group* $Ш(E/\mathbb{Q})$ *is finite.*

The rank r and the Tate-Shafarevich group $Ш(E/\mathbb{Q})$ 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

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

and

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

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 $Ш(E/\mathbb{Q})$ 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 [GJP09]. The group $Ш(E/\mathbb{Q})$ is not known to be finite for even a single elliptic curve with $r_{\mathrm{an}} \geq 2$. In such cases, the best we can do using current techniques is hope to bound the p-part $Ш(E/\mathbb{Q})(p)$ of $Ш(E/\mathbb{Q})$, for specific primes p. Even this might not be a priori possible, since it is not known that $Ш(E/\mathbb{Q})(p)$ is finite. However, if it were the case that $Ш(E/\mathbb{Q})(p)$ is finite (as Conjecture 1.2 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 $\mathcal{S}^{(p^n)}(E/\mathbb{Q})$ via the method of descent is prohibitively difficult for all but a few very small p^n.

We present in this paper two algorithms using p-adic L-functions $\mathcal{L}_p(E,T)$, which 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 a major breakthrough in the direction of a proof of the p-adic version of the BSD 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 [Col04] which gives a nice overview of the p-adic BSD conjecture. For supersingular primes such methods were used by Perrin-Riou in [PR03] to calculate $Ш(E/\mathbb{Q})(p)$ in many interesting cases when p is a prime of supersingular reduction.

Our first algorithm, which we describe in Section 10, finds a provable upper bound for the rank r of $E(\mathbb{Q})$ by 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 also 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 $Ш(E/\mathbb{Q})(p)$, 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.

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 information, is a proven upper bound on the order of $Ш(E/\mathbb{Q})(p)$; in particular, we expect it to often prove the finiteness of the p-primary part of the Tate-Shafarevich group. But it will not, in general, be able to give any information about the structure of $Ш(E/\mathbb{Q})(p)$ as an abelian group or any information on its elements. For such finer results on the Tate-Shafarevich group, one general method is to use p^n-descents as described above. In some cases, we can also use visibility [AS02] to relate $Ш(E/\mathbb{Q})(p)$ to Mordell-Weil groups of other elliptic curves or abelian varieties. Assuming Kolyvagin's conjecture, it may also be possible to compute the structure of $Ш(E/\mathbb{Q})(p)$, for E of any rank, by making Kolyvagin's Euler system explicit in some cases (see forthcoming work of the first author and Jared Weinstein that builds on [Kol91b], and the remarks at the end of [Kol91a]). The computability of our upper bound on $\#Ш(E/\mathbb{Q})(p)$ relies on several conjectures, such as the finiteness of $Ш(E/\mathbb{Q})(p)$ and Conjectures 4.1 and 4.4 on the nondegeneracy of the p-adic height on E.

Under the assumption of the main conjecture (see Section 7), the number output by our algorithm equals the order of $Ш(E/\mathbb{Q})(p)$. There are several cases when this conjecture is known to hold by Greenberg and Vatsal in [GV00], by Grigorov in [Gri05], and in a forthcoming paper by Skinner and Urban [SU10]. In particular, under appropriate hypotheses, [SU10] prove the main conjecture for elliptic curves with good ordinary reduction (see Theorem 7.5 below). Thus, in some cases, the upper bound on $Ш(E/\mathbb{Q})(p)$ that we obtain is actually a lower bound too, if all the computations go through, e.g., the p-adic height is nondegenerate and we find enough points to verify that the rank is equal to the order of vanishing.

Note that our algorithms can in principle be extended to give bounds in some cases on the rank of $E(K)$ and $\#Ш(E/K)(p)$ for number fields K which are abelian extensions of $\mathbb{Q}$ (here we still assume E is defined over $\mathbb{Q}$).

2. The Birch and Swinnerton-Dyer conjecture

Let E be an elliptic curve defined over $\mathbb{Q}$. If the BSD conjecture (Conjecture 2.1 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 ω_E be the invariant differential $dx/(2y + a_1x + a_3)$ of the minimal Weierstrass equation (1.1) of E. We write $\Omega_E = \int_{E(\mathbb{R})} \omega_E \in \mathbb{R}_{>0}$ for the Néron period of E.

Conjecture 2.1 (Birch and Swinnerton-Dyer)**.**

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

(2) *The leading coefficient* $L^*(E,1)$ *of the Taylor expansion of* $L(E,s)$ *at* $s=1$ *satisfies*

$$\frac{L^*(E,1)}{\Omega_E} = \frac{\prod_v c_v \cdot \#Ш(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{\mathrm{tor}})^2} \cdot \mathrm{Reg}(E/\mathbb{Q}), \tag{2.1}$$

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 $\#Ш(E/\mathbb{Q})_{\mathrm{an}}$ for the order of $Ш(E/\mathbb{Q})$ that is predicted by Conjecture 2.1.

Cassels proved in [Cas65] that if Conjecture 2.1 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 2.2 (Manin)**.** *If Conjecture* 2.1 *is true, then there is an algorithm to compute* r *and* $\#Ш(E/\mathbb{Q})$*.*

Proof. Manin proved this result in [Man71, §11], but we recall the essential ideas here. By searching for points in $E(\mathbb{Q})$ we obtain a lower bound on r, which gets 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 precision. Such computations yield upper bounds on r_{an}. In particular, if we compute $L^{(k)}(E,1)$ and it is nonzero (to the precision of our computation), then $r_{\mathrm{an}} \le k$. Eventually this method will also converge to give the correct value of r_{an}, though again without further information we do not know when this will occur. However, if we know Conjecture 2.1, 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_{an} computed using the L-series. At this point, by Conjecture 2.1 we know the true value of both r and r_{an}.

Once r is known, we can compute $E(\mathbb{Q})$ via a point search (as explained in [Cre97, §3.5] or [Ste07a, §1.2]), hence we can approximate $\mathrm{Reg}(E/\mathbb{Q})$ to any desired precision. All quantities in (2.1) except $\#Ш(E/\mathbb{Q})$ can then be approximated to any desired precision. Solving for $\#Ш(E/\mathbb{Q})$ in (2.1) and computing all other quantities to large enough precision to determine the integer $\#Ш(E/\mathbb{Q})_{\mathrm{an}}$ then determines $\#Ш(E/\mathbb{Q})$, as claimed. □

The above algorithm would only produce the order of $Ш(E/\mathbb{Q})$ but no information about its structure as an abelian group. We could compute the structure of $Ш(E/\mathbb{Q})$ by computing the group $\mathcal{S}^{(n)}(E/\mathbb{Q})$ where $n^2 = \#Ш(E/\mathbb{Q})$, which is possible since $\mathcal{S}^{(m)}(E/\mathbb{Q})$ is computable for all m. The algorithms in Sections 10 and 11 mimic the ideas of the proof of Proposition 2.2, but they replace the complex L-function by a p-adic L-series and use the fact that much is known unconditionally about p-adic analogues of the BSD conjecture.

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, CLS09, CLS10]).

Formulating a p-adic analogue of the BSD conjecture requires a p-adic analogue of the analytic function $L(E,s)$, as introduced by Mazur and Swinnerton-Dyer [MSD74, MTT86]. In this section, we recall the definition of this p-adic L-function, and fill a gap in the literature by giving a *complete recipe* for how to compute it in all cases, including proven error bounds on each coefficient.

Let $\pi\colon X_0(N) \longrightarrow E$ be the modular parametrization and let c_π be the Manin constant, i.e., the positive integer satisfying $c_\pi \cdot \pi^*\omega_E = 2\pi i f(\tau)d\tau$ with f the newform associated to E. When E is an optimal quotient (so the dual map $E \to \mathrm{Jac}(X_0(N))$ is injective), Manin conjectured that $c_\pi = 1$, and much work has been done toward this conjecture (see [Edi91, ARS06]).

Given a rational number r, define

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

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

$$[r]^+ = \frac{\lambda^+(r)}{\Omega_E}.$$

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] and [Ste07b]).

Let p be a prime of semistable reduction. We write[1] a_p for the trace of Frobenius. Suppose first that E has good reduction at p, and let $\tilde{E}$ denote the reduction of a minimal model of E modulo 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 choices of α if E has supersingular reduction at p and there is a single possibility for α when E has good ordinary reduction at p. Next suppose E has bad multiplicative reduction at p. Then a_p is 1 if the reduction is split multiplicative and a_p is -1 if the reduction is nonsplit multiplicative. In either multiplicative case, we define $\alpha = a_p$.

As in [MTT86, §I.10], define a measure on $\mathbb{Z}_p^\times$ with values in $\mathbb{Q}(\alpha)$ by

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

for any $k \geq 1$ and $a \in \mathbb{Z}_p^\times$ (by $\left[\frac{a}{p^k}\right]^+$ we mean $\left[\frac{a'}{p^k}\right]^+$ where $a' \in \mathbb{Z}$ is equivalent to a modulo p^k, which is well defined because of the modular symbols relations). Given a continuous character χ on $\mathbb{Z}_p^\times$ with values in the completion $\mathbb{C}_p$ of the algebraic closure of $\mathbb{Q}_p$, we may integrate χ against μ_α.

We assume henceforth that p is odd.[2] As in [MTT86, §I.13], 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

[1] The context should make it clear if we mean traces a_p of Frobenius, coefficients a_i as in (1.1), or series coefficients as in Proposition 3.1.

[2] Everything in this section can be done for $p = 2$ with $1 + p$ replaced by an integer that is congruent to 5 modulo 8, and various other slight modifications.

and $\langle x\rangle$ belongs to $1+p\mathbb{Z}_p$. We call ω the Teichmüller character. 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 $\exp_p((s-1)\cdot\log_p(\langle x\rangle))$, and $\exp_p$ and $\log_p$ are the p-adic exponential and logarithm. The function $L_\alpha(E,s)$ extends to a locally analytic function in s on the disc defined by $|s-1|<1$ (see the first proposition of [MTT86, §I.13]).

Let ${}_\infty G$ be the Galois group of the cyclotomic extension $\mathbb{Q}(\mu_{p^\infty})$ obtained by adjoining to $\mathbb{Q}$ all p-power roots of unity. By κ we denote the cyclotomic character ${}_\infty G\longrightarrow\mathbb{Z}_p^\times$. Because the cyclotomic character is an isomorphism, choosing a topological generator γ in $\Gamma={}_\infty G^{(p-1)}$ amounts to picking a generator $\kappa(\gamma)$ of $1+p\mathbb{Z}_p^\times$. 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

$$\mathcal{L}_\alpha(E,T)=\int_{\mathbb{Z}_p^\times}(1+T)^{\frac{\log_p(\langle x\rangle)}{\log_p(\kappa(\gamma))}}\,d\mu_\alpha(x)\,. \tag{3.1}$$

For each integer $n\geq 1$, define a polynomial

$$P_n(T)=\sum_{a=1}^{p-1}\left(\sum_{j=0}^{p^{n-1}-1}\mu_\alpha\left(\omega(a)(1+p)^j+p^n\mathbb{Z}_p\right)\cdot(1+T)^j\right)\in\mathbb{Q}_p(\alpha)[T].$$

Note that $P_n(T)$ depends on the choice of α, but for simplicity we do not include α in the notation.

Proposition 3.1. *We have*

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

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

We now give a proof of this convergence and in doing so obtain an explicit upper bound for $|a_j-a_{n,j}|$, which is critical to making the computation of $\mathcal{L}_\alpha(E,T)$ algorithmic, and which appears not to be explicitly stated in the literature.

For any choice ζ_r of p^r-th root of unity in $\mathbb{C}_p$, let χ_r be the $\mathbb{C}_p$-valued character of $\mathbb{Z}_p^\times$ of order p^r obtained by composing the map $\langle\ \rangle:\mathbb{Z}_p^\times\to 1+p\mathbb{Z}_p$ defined above with the map $1+p\mathbb{Z}_p\to\mathbb{C}_p^*$ that sends $1+p$ to ζ_r. Note that the conductor of χ_r is p^{r+1}.

Lemma 3.2. *Let* ζ_r *be a* p^r*-th root of unity with* $1\leq r\leq n-1$, *and let* χ_r *be the corresponding character of order* p^r, *as above. Then*

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

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

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

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

In the second to the last equality, we use that

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

to sum over lifts of $b \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ 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 χ has conductor dividing p^n, so is constant on the residue classes modulo p^n, and use the Riemann sums definition of the given integral. □

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

Corollary 3.3. *We have in $\mathbb{Q}_p(\alpha)[T]$ that*

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

Proof. By Lemma 3.2, $P_{n+1}(T)$ and $P_n(T)$ agree on $\zeta_j - 1$ for $0 \le j \le n-1$ and any choice ζ_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. □

Lemma 3.4. *Let $f(T) = \sum_j b_j T^j$ and $g(T) = \sum_j c_j T^j$ be in $\mathcal{O}[T]$ with $\mathcal{O}$ the ring of integers of a finite field extension of $\mathbb{Q}_p$. If $f(T)$ divides $g(T)$, then*

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

Proof. We have $f(T)k(T) = g(T)$ with $k(T) \in \mathcal{O}[T]$. The lemma follows by using the definition of polynomial multiplication and the nonarchimedean property of ord_p. □

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 $p^{c_n} P_n(T) \in (\mathbb{Z}_p[\alpha])[T]$. For any $j > 0$, let

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

Proposition 3.5. *For all $n \ge 0$, we have $a_{n+1,0} = a_{n,0}$, and for $j > 0$,*

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

Proof. Corollary 3.3 implies that there is a polynomial $h(T) \in \mathbb{Q}_p(\alpha)[T]$ with $w_{n-1}(T) \cdot h(T) = P_{n+1}(T) - P_n(T)$. Let $c \leq \max(c_n, c_{n+1})$ be the integer such that $p^c \cdot (P_{n+1}(T) - P_n(T)) \in \mathbb{Z}_p[\alpha][T]$ is primitive. Multiply both sides of the above equation by p^c, to get

$$w_{n-1}(T) \cdot p^c h(T) = p^c P_{n+1}(T) - p^c P_n(T) \in \mathbb{Z}_p[\alpha][T].$$

The right-hand side is primitive and integral, so it is reducible in $\mathbb{Z}_p[\alpha][T]$. Since $w_{n-1}(T)$ is integral, we must have $p^c h(T) \in \mathbb{Z}_p[\alpha][T]$. Applying Lemma 3.4 and renormalizing by p^c gives $c + \operatorname{ord}_p(a_{n+1,j} - a_{n,j}) \geq e_{n-1,j}$, so

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

Lemma 3.6. *The c_k are uniformly bounded above.*

Proof. Tracing through the definitions and using that $\operatorname{ord}_p(1/\alpha) > 1$, we see that the lemma is equivalent to showing that the modular symbol $[x]^+$ appearing in the definition of μ_α has bounded denominator. By the Abel-Jacobi theorem, the quotient of the image of the modular symbol map $[x]$ modulo $\mathbb{Z}^2 \approx H_1(E, \mathbb{Z})$ is equal to the image of the cuspidal subgroup C of $J_0(N)$. In particular, a bound on the denominator of $[x]^+$ is the largest power of p that divides the exponent of the image of C in $E(\bar{\mathbb{Q}})$. The claim follows since C is finite, since it is generated by finitely many "Manin symbols" as explained in [Man72, Thm. 2.7] or [Cre97, Ch. 2], and C is torsion as noted on the footnote of [Man72, p. 35]. $\square$

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 above, by Lemma 3.6. Thus, $\{a_{n,j}\}$ is a Cauchy sequence and Proposition 3.5 implies that

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

3.1. **The p-adic multiplier.** In this section we specialize the definition of p-adic multiplier from [MTT86, §I.14] to the case of an elliptic curve. For a prime p of good reduction, we define the p-adic multiplier by

$$\epsilon_p = \left(1 - \tfrac{1}{\alpha}\right)^2 . \tag{3.2}$$

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

For a prime of bad multiplicative reduction, we put

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

3.2. **Interpolation property.** The p-adic L-function constructed above satisfies an interpolation property with respect to the complex L-function (see [MTT86, §I.14]). 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 $d\mu_\alpha$. If χ is the character on ${}_\infty G$ sending γ to a root of unity ζ of exact order p^n, then

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

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

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

Proposition 3.7. *Let E be an elliptic curve with good ordinary reduction at a prime $p > 2$ such that $E[p]$ is irreducible. Then the series $\mathcal{L}_p(E,T)$ belongs to $\mathbb{Z}_p[\![T]\!]$.*

Proof. See [GV00, Prop. 3.7] with $\chi = 1$. □

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

$$E_0: \quad y^2 + x\,y = x^3 - x^2 - 4\,x + 4 \tag{3.3}$$

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 [S11b], we compute an approximation to the p-adic L-series as explained above with $n = 5$ to find

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

We see that the order of vanishing is at least 1 as follows. The interpolation formula implies that $\mathcal{L}_5(E_0,0) = 0$ since $[0]^+ = 0$. We will give an explanation for the vanishing of the coefficient of T^1 later in the comments right after Theorem 6.1. We remark that the coefficient of T^2 has valuation 1, but the coefficient of T^6 is a unit.

3.4. **Multiplicative case.** We separate the cases of split and nonsplit multiplicative reduction. In fact, if the reduction is nonsplit, 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 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 $\mathbb{Q}_p$. It is now known, thanks to [BDGP96], that $\log_p(q_E)$ is nonzero. Hence we define the p-adic $\mathscr{L}$-invariant as

$$\mathscr{L}_p = \frac{\log_p(q_E)}{\mathrm{ord}_p(q_E)} \neq 0\,. \tag{3.4}$$

We refer to [Col10] for a detailed discussion of the different $\mathscr{L}$-invariants and their connections.

3.5. **The supersingular case.** Assume $p \geq 5$. In the supersingular case, that is, when $a_p \equiv 0 \pmod{p}$, we have two roots α and β both of valuation $\frac{1}{2}$. An analysis of the functions $\mathcal{L}_\alpha$ and $\mathcal{L}_\beta$ is in [Pol03]. The series $\mathcal{L}_\alpha(E,T)$ might not have integral coefficients in $\mathbb{Q}_p(\alpha)$. Nevertheless, we can still extract two integral series $\mathcal{L}_p^{\pm}(E,T)$. We will not need this description.

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

As before, ω_E denotes the chosen invariant differential on E. Let $\eta_E = x \cdot \omega_E$. The pair $\{\omega_E, \eta_E\}$ forms a basis of the Dieudonné module

$$D_p(E) = \mathbb{Q}_p \otimes \mathrm{H}^1_{\mathrm{dR}}(E/\mathbb{Q}).$$

This $\mathbb{Q}_p$-vector space comes equipped with a canonical Frobenius endomorphism φ that acts 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] and [Ked01, Ked03, Ked04]. Let t be any uniformizer at the point O_E at infinity on E, e.g., take $t = -\frac{x}{y}$. Let ν 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, $\varphi(dt) = t^{p-1}\,dt$. The characteristic polynomial of φ 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

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

which we view as 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, §1] for a direct definition. Since the invariant differential ω_E depends on the choice of the Weierstrass equation (1.1), the expression $\mathcal{L}_p(E,T)$ is also dependent on this choice. However, if we write the series in the basis $\{\omega_E, \varphi(\omega_E)\}$ rather than in $\{\omega_E, \eta_E\}$, then the coordinates as above are independent. The D_p-valued L-series satisfies again certain interpolation properties,[3] e.g.,

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

See Section 12.2 for an example.

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.

[3] 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 leads to dramatic speedups 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 [MTT86, §II.11], the twist of $f_E^\dagger$ by ψ is equal to f_E and we can use their formula (I.8.3)

$$f_E(\tau) = \frac{1}{G(\psi)} \sum_{u \bmod |D|} \psi(u) \cdot f_E^\dagger\Big(\tau + \frac{u}{|D|}\Big). \tag{3.5}$$

Here $G(\psi)$ is as before the Gauss sum of ψ, 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 $c_\mathbb{R} \cdot \int_{\gamma^-} \omega_{E^\dagger}$, similar to $\Omega_{E^\dagger} = \Omega_{E^\dagger}^+ = c_\mathbb{R} \cdot \int_{\gamma^+} \omega_{E^\dagger}$ with the notations from (3.1). 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 η such that

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

It is known that η 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 $D > 0$.

$$\begin{aligned}
\lambda_E^+(r) &= \pi i \cdot \left(\int_r^{i\infty} + \int_{-r}^{i\infty} \right) \frac{1}{\sqrt{D}} \sum_{u=1}^{D-1} \psi(u) f_E^\dagger\Big(\tau + \frac{u}{D}\Big) d\tau \\
&= \frac{\pi i}{\sqrt{D}} \sum_{u=1}^{D-1} \psi(u) \int_{r+u/D}^{i\infty} f_E^\dagger(\tau) d\tau \\
&\qquad + \frac{\pi i}{\sqrt{D}} \sum_{v=1}^{D-1} \psi(D-v) \int_{-r}^{i\infty} f_E^\dagger\Big(\tau + 1 - \frac{v}{D}\Big) d\tau \\
&= \frac{\pi i}{\sqrt{D}} \sum_{u=1}^{D-1} \psi(u) \left(\int_{r+u/D}^{i\infty} + \int_{-r-u/D}^{i\infty} \right) f_E^\dagger(\tau) d\tau \\
&= \frac{1}{\sqrt{D}} \sum_{u=1}^{D-1} \psi(u)\, \lambda_{E^\dagger}^+\Big(r + \frac{u}{D}\Big).
\end{aligned}$$

We used that $\psi(u) = \operatorname{sign}(D)\,\psi(D-u)$, that $f_E^\dagger(\tau+1) = f_E^\dagger(\tau)$ and equation (3.5). Similarly, for $D<0$, we find

$$\lambda_E^+(r) = \frac{-1}{\sqrt{D}} \sum_{u=1}^{|D|-1} \psi(u)\,\lambda_{E^\dagger}^-\Big(r+\frac{u}{D}\Big).$$

Therefore, we have for any fundamental discriminant D,

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

We can also express the unit eigenvalue α 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 one single fixed choice of sign. If $[0]^+$ is nonzero, we can simply compare the value of the modular symbol at 0 with $L(E,1)/\Omega_E$ 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 nonvanishing 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 cannot 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 that we will generalize in the BSD formula is the real-valued regulator. In p-adic analogues of the conjecture we replace it by a p-adic regulator, which we define using a p-adic analogue of the height pairing. We follow here the generalized version [BPR93] and [PR03].

Let ν be an element of the Dieudonné module $D_p(E)$ (see Section 3.5). We will define a p-adic height function $h_\nu\colon E(\mathbb{Q}) \longrightarrow \mathbb{Q}_p$ which depends linearly on the vector ν. Hence it is sufficient to define it on the basis $\omega=\omega_E$ and $\eta=\eta_E$.

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

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

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 ω_E.

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

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

such that $\sigma(O_E) = 0$, $\frac{d\sigma}{\omega_E}(O_E) = 1$, 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:

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

where the a_i are the coefficients of the Weierstrass equation (1.1). 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 $\sigma(m\cdot P)$ 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 $m\cdot P$. Define

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

Bernardi [Ber81] proves 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

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

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 φ on $D_p(E)$ associated to the eigenvalue $\frac{1}{\alpha}$. The value $e_2 = \mathbf{E}_2(E,\omega_E) = -12\cdot\frac{a}{b}$ is the value of the Katz p-adic Eisenstein series of weight 2 at (E,ω_E). 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

$$\begin{aligned}\hat{h}_p(P) &= \frac{1}{b}\cdot h_{\nu_\alpha}(P)\\ &= -\frac{a}{b}\cdot\log_E(P)^2 + 2\,\log\left(\frac{e(P)}{\sigma(P)}\right)\\ &= 2\,\log_p\left(\frac{e(P)}{\exp(\frac{e_2}{24}\log_E(P)^2)\cdot\sigma(P)}\right) = 2\,\log_p\left(\frac{e(P)}{\sigma_p(P)}\right).\end{aligned}\tag{4.1}$$

The function σ_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].[4] It is also important to note that the function $\hat{h}_p$ is 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 $\mathrm{Reg}_p(E/\mathbb{Q})$ for the discriminant of the height pairing on $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tor}}$.

Conjecture 4.1 (Schneider [Sch82])**.** *The canonical p-adic height is nondegenerate 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 running example curve E_0 from Section 3.3. The methods of [MST06, Har08] permit us to quickly compute to relatively high precision the p-adic regulator of E_0. 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

$$\mathrm{Reg}_p(E_0/\mathbb{Q}) = 2 \cdot 5 + 2 \cdot 5^2 + 5^4 + 4 \cdot 5^5 + 2 \cdot 5^7 + 4 \cdot 5^8 + 2 \cdot 5^9 + \mathbf{O}(5^{10}). \tag{4.2}$$

4.2. **The multiplicative case.** When E has multiplicative reduction at p, if we want to have the same closed formula in the p-adic version of the BSD conjecture for multiplicative primes as for other ordinary primes, the p-adic height has to be changed slightly. We use the description of the p-adic regulator given in [MTT86, §II.6]. Alas, their formula is not correct, as explained in [Wer98], so we use the corrected version.

If the reduction is nonsplit multiplicative, we use the same formula (4.1) to define the p-adic height as for the good ordinary case.

We assume for the rest of this section that the reduction is split multiplicative. We use Tate's p-adic uniformization (see for instance in [Sil94, Ch. V]). We have an explicit description of the height pairing in [Sch82]. Let q_E be the Tate parameter of the elliptic curve E over $\mathbb{Q}_p$, so we have an analytic homomorphism $\psi\colon \bar{\mathbb{Q}}_p^\times \longrightarrow E(\bar{\mathbb{Q}}_p)$ whose kernel is precisely $q_E^{\mathbb{Z}}$. The image of $\mathbb{Z}_p^\times$ under ψ is equal to the subgroup of points of $E(\mathbb{Q}_p)$ lying on the connected component of the reduction modulo p of the Néron model of E. 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 is

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

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

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

[4] This factor is needed if we do not want to modify the p-adic version of the BSD conjecture (Conjecture 5.1).

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 ψ, where $\widehat{E}$ is the formal group of E at p.

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

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

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 do not find a canonical p-adic height with values in $\mathbb{Q}_p$. Instead, the height has values in the Dieudonné module $D_p(E)$, as explained in [BPR93] and [PR03].

First, if the rank of the curve is 0, we define the p-adic regulator of $E/\mathbb{Q}$ to be $\omega = \omega_E \in D_p(E)$. Thus 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

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

is independent of the choice of ν. 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

$$x' = u^2\cdot x + r \qquad \text{and} \qquad y' = u^3\cdot y + s\cdot x + t, \tag{4.3}$$

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 $[\omega_E, \eta_E] = 1$. Write $\mathrm{Reg}_\nu \in \mathbb{Q}_p$ for the regulator of h_ν on $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tor}}$. Then we have the following lemma which is a corrected version[5] of [PR03, Lem. 2.6].

Lemma 4.2. *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 $\nu \in D_p(E)$ not in $\mathbb{Q}_p\omega$, we have*

$$[\mathrm{Reg}_p(E/\mathbb{Q}), \nu] = \frac{\mathrm{Reg}_\nu}{[\omega,\nu]^{r-1}}. \tag{4.4}$$

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 in (4.3), the regulator $\mathrm{Reg}'_p(E/\mathbb{Q})$ computed in the new equation satisfies $\mathrm{Reg}'_p(E/\mathbb{Q}) = \frac{1}{u}\cdot\mathrm{Reg}_p(E/\mathbb{Q})$.

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_ω is made out of the square of the linear function $\log_E$, the matrix of the associated pairing on a basis $\{P_i\}$ of $E(\mathbb{Q})$ modulo torsion has entries of

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

the form $\log_E(P_i) \cdot \log_E(P_j)$ 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 (4.4) is linear in ν. 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. □

We continue to assume that the rank r of $E/\mathbb{Q}$ is positive, as in Lemma 4.2. Define the *fine Mordell-Weil group* as in [Wut07] to be the kernel

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

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 obtain a pairing

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

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 4.3. *Suppose there exists a point Q in $E(\mathbb{Q}) \otimes \mathbb{Z}_p$ such that $\mathfrak{M}(E/\mathbb{Q}) + \mathbb{Z}_p Q = E(\mathbb{Q}) \otimes \mathbb{Z}_p$. Then*

$$[\mathrm{Reg}_p(E/\mathbb{Q}_p), \omega] \equiv \log_E(Q)^2 \cdot \mathrm{Reg}_0(E/\mathbb{Q}) \pmod{\mathbb{Z}_p^\times}.$$

Proof. From the proof of the Lemma 4.2, we only have to show that

$$X = \mathrm{Reg}_{\omega+\eta} - \mathrm{Reg}_\eta \equiv h_\omega(Q)\,\mathrm{Reg}_0(E/\mathbb{Q}).$$

By hypothesis, there is a basis of $\mathfrak{M}(E/\mathbb{Q})$ that we can complete to a basis of $E(\mathbb{Q}) \otimes \mathbb{Z}_p$ by adding Q to it. If M is the matrix of the pairing for η in this basis, then the matrix for $\omega + \eta$ is obtained by changing the entry for $\langle Q, Q \rangle$ by adding $h_\omega(Q)$ to it. Since X is the difference of the two determinants, it is $h_\omega(Q)$ times the determinant of $\langle \cdot, \cdot \rangle_\eta$ on the basis of $\mathfrak{M}(E/\mathbb{Q})$, which equals $\mathrm{Reg}_0(E/\mathbb{Q})$ by definition. □

This lemma proves the last equality in [PR03, §2]. We should mention that the formula just above it, linking $\mathrm{Reg}_p(E/\mathbb{Q})$ to $H_p(Q) \cdot \mathrm{Reg}_0(E/\mathbb{Q})$, is not known to hold as it cannot be assumed in general that we can find a point Q as in the lemma above which is orthogonal to $\mathfrak{M}(E/\mathbb{Q})$. In particular, the D_p-valued regulator $\mathrm{Reg}_p(E/\mathbb{Q})$ is nonzero provided the fine regulator does not vanish, because $\log_E(Q) \neq 0$.

Conjecture 4.4 (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.*

Conjecture 3.3.7.ii' in [PR93], which asserts that Reg_ν is nonzero for at least one ν, is implied by the above conjecture. This is explained in remark iii) following the conjecture there, if we use the fact that the weak Leopoldt conjecture is now known for E and p.

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.

In [BPR93, p. 232], there is an algorithm for computing the action of φ by successive approximation using the expansion of ω in terms of a uniformizer t. It is dramatically more efficient to replace this by the computation of φ using Monsky-Washnitzer cohomology as explained in [Ked01, Ked03, Ked04, Har08].

4.4. **Normalization.** In view of Iwasawa theory, it is natural to normalize the heights and the regulators depending on the choice of the generator γ. In this way the heights depend on the choice of an isomorphism $\Gamma \longrightarrow \mathbb{Z}_p$ rather than on the $\mathbb{Z}_p$-extension only. This normalization can be achieved by simply dividing $\hat{h}_p(P)$ and $h_\nu(P)$ by $\kappa(\gamma)$. The regulators will be divided by $\log_p \kappa(\gamma)^r$ 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 expansion of this function at $T = 0$ rather than at $s = 1$.

Conjecture 5.1 (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 $r = \mathrm{rank}(E(\mathbb{Q}))$, 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*

$$\mathcal{L}_p^*(E,0) = \epsilon_p \cdot \frac{\prod_v c_v \cdot \#Ш(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{\mathrm{tor}})^2} \cdot \mathrm{Reg}_\gamma(E/\mathbb{Q}) \tag{5.1}$$

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

$$\mathcal{L}_p^*(E,0) = \frac{\mathscr{L}_p}{\log(\kappa(\gamma))} \cdot \frac{\prod_v c_v \cdot \#Ш(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{\mathrm{tor}})^2} \cdot \mathrm{Reg}_\gamma(E/\mathbb{Q}), \tag{5.2}$$

where $\mathscr{L}_p$ is as in equation (3.4)*.*

The conjecture asserts exact equality, not just equality up to a p-adic unit. However, the current approaches to the conjecture, which involve the main conjecture of Iwasawa theory, 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 (3.3)) for an example in the good ordinary case. For this curve, we have $\prod c_v = 2$ and $E_0(\mathbb{Q})_{\mathrm{tor}} = 0$, so all the terms

in the expression above can be computed except for the unknown size of $Ш(E_0/\mathbb{Q})$. The p-adic BSD conjecture predicts that

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

which is consistent with the complex BSD conjecture, which predicts that $Ш(E_0/\mathbb{Q})$ is trivial.

5.2. **The supersingular case.** The conjecture in the case of supersingular reduction is given in [BPR93] and [PR03]. The conjecture relates 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 by Kurihara and Pollack in [KP07] to construct global points via a p-adic analytic computation.)

Conjecture 5.2 (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*

$$(1-\varphi)^{-2}\cdot\mathcal{L}_p^*(E,0) = \frac{\prod_v c_v \cdot \#Ш(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{\mathrm{tor}})^2}\cdot \mathrm{Reg}_\gamma(E/\mathbb{Q}) \quad \in D_p(E)\,. \tag{5.3}$$

We emphasize that both sides of (5.3) are dependent on 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 Γ. Let Λ be the completed group algebra $\mathbb{Z}_p[\![\Gamma]\!]$. We use a fixed topological generator γ of Γ to identify Λ with $\mathbb{Z}_p[\![T]\!]$ by sending γ to $1+T$. Any finitely generated Λ-module admits a decomposition up to quasi-isomorphism as a direct sum of elementary Λ-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 $\mathrm{Gal}({}_n\mathbb{Q}/\mathbb{Q}) \approx \mathbb{Z}/p^n\mathbb{Z}$. As in Section 1.1, we define the p-Selmer group of E over ${}_n\mathbb{Q}$ by the exact sequence

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

with the product running over all places v of ${}_n\mathbb{Q}$. Over the full $\mathbb{Z}_p$-extension, we define $\mathcal{S}_p(E/{}_\infty\mathbb{Q})$ to be the direct limit $\varinjlim \mathcal{S}_p(E/{}_n\mathbb{Q})$ with respect to 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 $\mathcal{S}_p(E/{}_\infty\mathbb{Q})$ encodes 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 Λ-module (see [CS00]). For further introduction to these objects, see [Gre01].

6.1. **The ordinary case.** Assume that the reduction at p is either good ordinary or of multiplicative type. Kato's theorem (see [Kat04, Thm. 17.4]), which uses the work of Rohrlich [Roh84], states that $X(E/_\infty\mathbb{Q})$ is a torsion Λ-module, so we may associate to it a characteristic series

$$f_E(T) \in \mathbb{Z}_p[\![T]\!] \tag{6.1}$$

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

The following result is due to Schneider [Sch85] and Perrin-Riou [PR82], and the multiplicative case is due to Jones [Jon89]. Note that it uses the analytic and algebraic p-adic height defined by Schneider in [Sch82]; taking into account the mentioned correction by Werner, these heights agree with the height in Section 4.2.

Theorem 6.1 (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 nondegenerate* (*Conjecture* 4.1) *and the p-primary part of the Tate-Shafarevich group $Ш(E/\mathbb{Q})(p)$ is finite* (*Conjecture* 1.2)*. In this case the leading term of the series $f_E(T)$ has the same valuation as*

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

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

Let us consider again our running example curve E_0. We have computed the 5-adic regulator and found that it is nonzero. The above theorem shows that the order of vanishing of $f_{E_0}(T)$ is at least equal to the rank. The finiteness of $Ш(E_0/\mathbb{Q})(5)$ is now equivalent to the statement that the order of vanishing of $f_{E_0}(T)$ is equal to the rank 2 of E_0. If this is the case, then the leading coefficient has valuation equal to

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

since $\mathrm{ord}_5(\mathrm{Reg}_5(E_0/\mathbb{Q})) = 1$ by equation (4.2) and c_v, ϵ_5 and torsion are coprime to 5.

For general E, if the valuation of the leading term of $f_E(T)$ is positive we call p an *irregular*[6] 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 $Ш(E/_\infty\mathbb{Q})$ is no longer finite or both. We will determine exactly what happens for E_0 with $p = 5$ in Section 7.1 below.

6.2. **The supersingular case.** Assume $p \geq 5$. The supersingular case is more complicated, since the Λ-module $X(E/_\infty\mathbb{Q})$ is not torsion. A beautiful approach to the supersingular case has been found by Pollack [Pol03] and Kobayashi [Kob03]. As mentioned above (in Section 3.5), there are 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 are Λ-torsion. Despite the advantages of this $\pm$-theory, we use the approach of Perrin-Riou here (see [PR03, §3]).

Let T_pE be the Tate module and define $\mathbb{H}^1_{\mathrm{loc}}$ 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]

[6]For a good introduction to such terminology and the basics of Iwasawa theory of elliptic curves, we refer the reader to [Gre99].

constructed a Λ-linear Coleman map Col from $\mathbb{H}^1_{\mathrm{loc}}$ to a submodule 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 [Kat04, Thm. 12.4], that the Pontryagin dual $Y(E/_\infty\mathbb{Q})$ of $\mathcal{R}(E/_\infty\mathbb{Q})$ is a Λ-torsion module. Denote by $g_{E}(T)$ its characteristic series.

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

By Kato again, the Λ-module $\mathbb{H}^1_{\mathrm{glob}}$ is torsion-free and $\mathbb{H}^1_{\mathrm{glob}} \otimes \mathbb{Q}_p$ has $\Lambda \otimes \mathbb{Q}_p$-rank 1. Now, choose any element $_\infty c$ in $\mathbb{H}^1_{\mathrm{glob}}$ such that $Z_c = \mathbb{H}^1_{\mathrm{glob}}/(\Lambda \cdot {}_\infty c)$ is Λ-torsion. Typically such a choice could be the "zeta element" of Kato, i.e., the image of his Euler system in $\mathbb{H}^1_{\mathrm{glob}}$. 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 $\mathbb{H}^1_{\mathrm{loc}}$. 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 a result due to Perrin-Riou [PR93]:

Theorem 6.2 (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* 4.4*) and the p-primary part of the Tate-Shafarevich group $Ш(E/\mathbb{Q})(p)$ is finite (Conjecture* 1.2*). In this case the leading term of the series $(1-\varphi)^{-2} f_{E}(T)$ has the same valuation as*

$$\prod_{\upsilon} c_\upsilon \cdot \#Ш(E/\mathbb{Q})(p) \cdot \mathrm{Reg}_p(E/\mathbb{Q}) .$$

Note that the proof of this theorem in the appendix of [PR03] for the supersingular case uses the formula in Lemma 4.3 rather than the wrong definition of the regulator. Also, we simplified the right-hand term in comparison to (5.3), because the reduction at p is supersingular, so $N_p \equiv 1 \pmod p$, hence $\#E(\mathbb{Q})_{\mathrm{tor}}$ must be a p-adic unit.

7. The Main Conjecture

The main conjecture links the two p-adic power series (3.1) and (6.1) of the previous sections. We formulate everything simultaneously for the ordinary and the supersingular case, even though they are of a quite different nature. We still assume that $p \neq 2$.

Conjecture 7.1 (Main conjecture of Iwasawa theory for elliptic curves)**.** *If E has good or nonsplit 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 $T \cdot \Lambda^\times$.*

Our statement above of the main conjecture for supersingular primes is equivalent to Kato's formulation in [Kat04, Conj. 12.10] and to Kobayashi's version in [Kob03]. In the notation of Section 6.2, it asserts that $g_E(T) = h_c(T)$, where c is Kato's zeta element.

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

$$\rho_p : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_p(E)) \approx \mathrm{GL}_2(\mathbb{Z}_p)$$

and its reduction

$$\bar{\rho}_p : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[p]) \approx \mathrm{GL}_2(\mathbb{F}_p).$$

Serre [Ser72] proved that $\bar{\rho}_p$ is almost always surjective (note our running hypothesis that E does not have complex multiplication) and that for curves with multiplicative reduction at p, surjectivity can only fail when there is an isogeny of degree p defined over $\mathbb{Q}$ (see [Ser96] and [RS01, Prop. 1.1] for the case $p = 2$ of this statement, though the theorem below has the hypothesis that p is odd).

Proposition 7.2. *If $p \geq 5$, then $\bar{\rho}_p$ is surjective if and only if ρ_p is surjective.*

Proof. See [GJP09, §2.1] for references for this and related results. □

Kato's Theorem 7.3. *Suppose that E has semistable reduction at p and that ρ_p is surjective. Then there exists a series $d(T)$ in Λ such that $\mathcal{L}_p(E,T) = f_E(T) \cdot d(T)$. If the reduction is split multiplicative, then T divides $d(T)$.*

The main ingredient for this theorem is in [Kat04, Thm. 17.4], which addresses the good ordinary case when $\bar{\rho}_p$ is surjective. For the exceptional case we refer to [Kob06], which treats the case of split multiplicative reduction (i.e., where exceptional zeroes appear).

For the remaining cases, we obtain only a weaker statement:

Kato's Theorem 7.4. *Suppose that $\bar{\rho}_p$ is not surjective. Then there is an integer $m \geq 0$ 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 when $E[p]$ is reducible. Recently, Skinner-Urban have proved the main conjecture in many more cases. The following is a slightly weaker form of [SU10, Thm. 1]:

Theorem 7.5 (Skinner-Urban)**.** *Suppose that E has good ordinary reduction at p, that ρ_p is surjective and that there exists a prime q of multiplicative reduction such that $\bar{\rho}_p$ is ramified at q. Then the main conjecture holds, i.e., $\mathcal{L}_p(E,T)$ is equal to $f_E(T)$, up to a unit in Λ.*

The condition on the extra prime q is satisfied if E has split multiplicative reduction at q and p does not divide the Tamagawa number c_q. If E has nonsplit multiplicative reduction, one has to check that p does not divide the Tamagawa number over the unramified quadratic extension of $\mathbb{Q}_q$. Equivalently, in both cases of multiplicative reduction, the representation $\bar{\rho}_p$ is ramified at q if $p \nmid \mathrm{ord}_q(\Delta_E)$, as explained in [RS01, §2.4].

7.1. **The Example.** Consider again the curve E_0 (see equation (3.3)) and the good ordinary prime $p = 5$. Kato's theorem implies that $f_{E_0}(T)$ divides $\mathcal{L}_p(E_0, T)$. Since we have found two linearly independent points of infinite order in $E_0(\mathbb{Q})$, 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 Theorem 7.3, so is the order of vanishing of $\mathcal{L}_p(E_0, T)$. By explicitly computing an approximation to $\mathcal{L}_p(E_0, T)$ we see 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. We compute the p-adic valuation of the leading term of $f_{E_0}(T)$ by approximating $\mathrm{Reg}_p(E)$ and using Theorem 6.1. 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 the same leading term, which 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 $\mathcal{L}_p(E_0, T)$, one can show that

$$f_{E_0}(T) = T \cdot ((T+1)^5 - 1) \cdot u(T)$$

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 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 $E_0({}_1\mathbb{Q})$ which are not defined over $\mathbb{Q}$. Therefore, we know that the rank of $E_0({}_1\mathbb{Q})$ and of $E_0({}_\infty\mathbb{Q})$ 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 1.2 is valid; also, Conjectures 4.1 and 4.4 are trivially true in this case.

Let $p > 2$ be a prime of semistable reduction such that the representation $\bar{\rho}_p$ is surjective. 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 6.1[7] of Perrin-Riou and Schneider for the first equality and Kato's

[7]In the case of analytic rank 0, the theorem is actually relatively easy and well explained in [CS00, Ch. 3].

Theorem 7.3 on the main conjecture for the inequality in the second line:

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

Hence, we have the following upper bound on the p-primary part of the Tate-Shafarevich group

$$\begin{aligned}\operatorname{ord}_p\left(\#Ш(E/\mathbb{Q})(p)\right) &\leq \operatorname{ord}_p\left(\frac{L(E,1)}{\Omega_E}\right) - \operatorname{ord}_p\left(\frac{\prod c_v}{(\#E(\mathbb{Q})_{\mathrm{tor}})^2}\right) \\ &= \operatorname{ord}_p(\#Ш(E/\mathbb{Q})_{\mathrm{an}}). \qquad (8.1)\end{aligned}$$

Under the assumption of the main conjecture, this is sharp. In particular, if the conditions of Theorem 7.5 are satified for p, then we have the equality

$$\operatorname{ord}_p(\#Ш(E/\mathbb{Q})(p)) = \operatorname{ord}_p(\#Ш(E/\mathbb{Q})_{\mathrm{an}}).$$

This is Theorem 2.a in [SU10].

8.2. **The multiplicative case.** If the reduction is nonsplit, then the above holds just the same, because in all of the theorems involved the nonsplit case never differs from 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 as above to obtain the same bound (8.1).

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 $\mathrm{Reg}_p(E/\mathbb{Q})$ is equal to ω_E. We may therefore concentrate solely on the coordinate in ω_E. Write $\operatorname{ord}_p(f_E(0))$ for the p-adic valuation of the leading coefficient of the ω_E-coordinate of $f_E(T)$. Again we obtain an inequality by using Theorem 6.2:

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

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

8.4. **Conclusion.** Summarizing the above computations, we have

Theorem 8.1 (Kato, Perrin-Riou, Schneider)**.** *Let E be an elliptic curve such that $L(E,1) \neq 0$. Then $Ш(E/\mathbb{Q})$ is finite and*

$$\#Ш(E/\mathbb{Q}) \;\Big|\; C \cdot \frac{L(E,1)}{\Omega_E} \cdot \frac{(\#E(\mathbb{Q})_{\mathrm{tor}})^2}{\prod c_v}$$

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.

This improves [Rub00, Cor. 3.5.19].

9. If the L-series vanishes to the first order

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

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

where, on the left-hand side, the canonical real-valued regulator $\mathrm{Reg}(E/\mathbb{Q}) = \hat{h}(P)$ appears along with 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 BSD conjecture (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, we know 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 $T \mid f_E(T)$). Imposing the additional hypothesis that ρ_p is surjective, Theorem 7.3 implies the above divisibility over $\mathbb{Z}_p$ (rather than just up to a power of p), and we thus arrive at the following theorem.

Theorem 9.1 (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 ρ_p is surjective. If $L(E,s)$ has a simple zero at $s=1$, then*

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

In other words, the upper bound asserted by the BSD conjecture is true up to a factor involving only bad and supersingular primes, and primes p for which $\bar{\rho}_p$ is not surjective or the p-adic regulator is 0.

The above theorem has as a hypothesis that the reduction is good ordinary, because this is the only case when we know a proof of the p-adic Gross-Zagier formula. It would be interesting to obtain a generalization of the p-adic Gross-Zagier formula to the supersingular case.

10. Algorithm for an upper bound on the rank

Let $E/\mathbb{Q}$ be an elliptic curve. In this section we explain how to compute 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

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

by Kato's Theorems 7.3 and 7.4 and by Theorems 6.1 and 6.2. Hence we have an upper bound on the rank r.

Proposition 10.1. *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, we also obtain a lower bound on the rank r. Simultaneously, we 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 BSD Conjecture 5.1 or 5.2 is false. This is similar to the conditional algorithm described in Proposition 2.2, except that we do know here that our upper bounds are unconditional. We do not know unconditionally that this procedure terminates after finitely many steps. Summarizing, we can claim the following.

Proposition 10.2. *Let E be an elliptic curve, and assume that there is a prime p of good reduction such that the p-adic BSD conjecture is true. Then there is an algorithm that computes the rank r of E using p-adic L-functions.*

Of course, the procedure 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 procedure 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 small m, but it would be prohibitively time-consuming for larger m (e.g., $m \geq 13$). In contrast, computing the p-adic L-series even for p around 1000 is reasonably efficient, assuming one can compute the relevant modular symbols spaces.

10.1. **Technical remarks.** The second condition above (good reduction) 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 $b \geq r+1$.

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

For practical purposes, we take p as small as possible. The computation of the leading term of $\mathcal{L}_p(E,T)$ using the algorithm of Section 3 for curves of higher rank r is time-consuming for large p. Also, we 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 computed using modular symbols following the linear algebra algorithm of [Cre97]. However, using p-adic L-series may provide an advantage when considering families of quadratic twists.

An 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 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 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 apply the results above, we impose the following conditions on (E,p):

- $p > 2$,
- E does not have additive reduction at p,
- the image of $\bar{\rho}_p$ is the full group $\mathrm{GL}_2(\mathbb{F}_p)$.

As mentioned above, these conditions apply to all but finitely many primes p.

Algorithm 11.1. 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) Attempt to 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 higher and higher approximations to the p-adic regulator of E over $\mathbb{Q}$ using the algorithm in [MST06, Har08]. Exit with an error if after a predetermined number of steps, the p-adic height pairing is not shown to be nondegenerate.

(3) Using modular symbols, compute an approximation of the coefficient $\mathcal{L}_p^*(E,0)$ of the leading term of the p-adic L-series $\mathcal{L}_p(E,T)$. 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 increase the precision of the computation of $\mathcal{L}_p(E,T)$. If, after some prespecified cutoff, this fails to prove that $\mathrm{ord}_{T=0}\,\mathcal{L}_p(E,T) = r$ (or $r+1$), then exit with an error.

(4) Compute the remaining information, including the Tamagawa numbers c_v and the p-adic multiplier ϵ_p. If p is a good ordinary prime or a prime at which E has nonsplit multiplicative reduction, let

$$b_p = \mathrm{ord}_p(\mathcal{L}_p^*(E,0)) - \mathrm{ord}_p(\epsilon_p) - \sum_v \mathrm{ord}_p(c_v) - \mathrm{ord}_p(\mathrm{Reg}_\gamma(E/\mathbb{Q})).$$

If p is supersingular, let

$$b_p = \mathrm{ord}_p((1-\varphi)^{-2}\,\mathcal{L}_p^*(E,0)) - \mathrm{ord}_p(\mathrm{Reg}_p(E/\mathbb{Q})) - \sum_v \mathrm{ord}_p(c_v).$$

Finally, if E has split multiplicative reduction at p, let

$$b_p = \mathrm{ord}_p(\mathcal{L}_p^*(E,0)) - \mathrm{ord}_p(\mathscr{L}_p) - \sum_v \mathrm{ord}_p(c_v) - \mathrm{ord}_p(\mathrm{Reg}_\gamma(E/\mathbb{Q}))\,.$$

(5) Output that $\#Ш(E/\mathbb{Q})(p)$ is bounded by p^{b_p}.

Proof. At Step 4, we have shown that Conjecture 4.1 (or Conjecture 4.4 in the supersingular case) on the nondegeneracy of the p-adic regulator holds and that $Ш(E/\mathbb{Q})(p)$ is indeed finite by Theorem 6.1 (or Theorem 6.2 in the supersingular case). Moreover, this theorem shows that

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

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

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

in the supersingular case. Note that $\#E(\mathbb{Q})(p) = 1$ since we assumed that $\bar{\rho}_p$ is surjective. Finally, we use Kato's Theorem 7.3 that

$$\mathrm{ord}_p(f_E^*(0)) \le \mathrm{ord}_p(\mathcal{L}_p^*(E,0))$$

to prove that b_p is indeed an upper bound on $\mathrm{ord}_p(\#Ш(E/\mathbb{Q})(p))$. □

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

Proposition 11.2. *Let E be an elliptic curve and $p > 2$ a prime for which E has semistable reduction. If Conjectures* 4.1 *and* 4.4 *hold and if we are able to determine the Mordell-Weil group of E, then there is an algorithm to verify that the p-primary part of $Ш(E/\mathbb{Q})$ is finite. If, moreover, the representation $\bar{\rho}_p$ is surjective, then the algorithm produces an upper bound on $\#Ш(E/\mathbb{Q})(p)$. If Conjecture* 7.1 *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 of Algorithm 11.1 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 use descent methods or the algorithm in the previous section to bound the rank from above and search for points to find a lower bound. When enough points are found to generate a group of finite index, we 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 we assume the complex and the p-adic version of the BSD conjecture. 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 4.1 or 4.4 is wrong (in Step 2), if the p-primary part of $Ш(E/\mathbb{Q})$ 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 as output that the p-primary part of $Ш(E/\mathbb{Q})$ 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 were implemented by the authors in Sage (see [S11b]) and all of the calculations given below can be carried out using Sage and PSage [S11a].

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 (3.3))

$$E_0: \quad y^2 + xy = x^3 - x^2 - 4x + 4$$

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

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

The computation of the p-adic L-series is more time consuming[8]. 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 $222\cdot 223$ 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 BSD conjecture predicts that

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

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

[8]The optimized implementation mentioned in Section 12.4 does this entire computation in less than one second total time, including the modular symbols space computation.

12.2. **A supersingular example.** Let E be the elliptic curve

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

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-series is

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

where we have already taken into 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 BSD 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 nontrivial.** Let E be the elliptic curve given by

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

which is labeled 858k2 in [Cre]. The curve has rank 0 and is semistable, and the full BSD 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 $\#Ш(E/\mathbb{Q})(7) \le 7^2$. 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. (Also, this can be deduced from Theorem 7.5 taking $q = 11$.)

Once again we learn even more from the computation of the p-adic L-series. Iwasawa theory tells us that the order of the Tate-Shafarevich group grows 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. **Tate-Shafarevich groups of elliptic curves of rank at least 2.** According to [Cre], for every elliptic curve with rank ≥ 2 and conductor up to 130,000, the BSD conjecture predicts that $Ш(E/\mathbb{Q}) = 0$. In this section, we describe the computation we did to verify Theorem 1.1, which gives evidence for this observation, at least up to conductor 30,000.

Consider a pair (E, p) consisting of

(1) an optimal elliptic curve E defined over $\mathbb{Q}$ with rank $r \geq 2$ and conductor $\leq 30{,}000$, and
(2) a good ordinary prime p with $5 \leq p < 1{,}000$ such that $\bar{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p])$ is surjective.

There are 9,679 such curves E and 1,534,422 such pairs (E, p). For each pair, we do the following:

(1) Show that $r = \mathrm{ord}_T \mathcal{L}_p(E, T)$.
(2) Compute the conjectural order of $Ш(E/\mathbb{Q})$ according to Conjecture 5.1 mod p, and check that it is $1 + O(p)$.

As explained in the proof of Algorithm 11.1, our hypotheses on p then imply that $Ш(E/\mathbb{Q})[p] = 0$. As evidence for Conjecture 5.1 and as a double check on our implementation, we also verify the conjecture to precision $O(p)$ for each pair (E, p).

(1) We compute[9] approximations to $\mathcal{L}_p(E, T)$ that are sufficient to show that $\mathrm{ord}_T(\mathcal{L}_p(E, T)) = r$. For 1,523,413 of our 1,534,422 pairs (E, p), we did this by computing $P_2 \equiv \mathcal{L}_p(E, T) \pmod{(p, T^5)}$; for the remaining 11,009 pairs, we computed to higher precision.
(2) For all of our pairs (E, p), we computed the p-adic regulator $\mathrm{Reg}_p(E) \in \mathbb{Q}_p$ to precision at least $O(p^{12})$. In all cases this computation confirmed that $\mathrm{Reg}_p(E) \neq 0$.
(3) With the above data for our pairs (E, p), it was then straightforward to compute the conjectural order of $Ш(E/\mathbb{Q})$ according to Conjecture 5.1, and in all cases we got $1 + O(p)$, so $Ш(E/\mathbb{Q})[p] = 0$.

Remark 12.1. In fact, we carried out the regulator calculation mentioned above for all pairs (E, p) with $5 \leq p < 1000$ good ordinary for which the conductor of E is $\leq 130{,}000$ and the rank is ≥ 2. A selection of large $\mathrm{ord}_p(\mathrm{Reg}_p(E))$ is given in Table 1. For example, for the first curve 53770a1 with $p = 7$, the conductor factors as $53770 = 2 \cdot 5 \cdot 19 \cdot 283$, the Tamagawa numbers are $12, 2, 6, 1$, which are all coprime to 7, we have $Ш(E/\mathbb{Q})_{\mathrm{an}} = 1$, and $N_7 = 9$, which is coprime to 7, but

$$\mathrm{Reg}_7(E) = 7^7 \cdot 419257219506 + O(7^{21})$$

is divisible by a rather large power of 7. The leading coefficient of the 7-adic L-series vanishes to order $7 - \mathrm{rank}(E)$, as expected, so $Ш(E/\mathbb{Q})(7) = 0$:

$$\mathcal{L}_7(E, T) = O(7^9) + O(7^6)T + \left(6 \cdot 7^5 + O(7^6)\right) T^2 + \left(3 \cdot 7^5 + O(7^6)\right) T^3 + \left(5 + 5 \cdot 7 + 2 \cdot 7^4 + 7^5 + O(7^6)\right) T^4 + O(T^5).$$

Remark 12.2. A very hard case is $(E, p) = (17856j1, 757)$, in which E has rank 2 and

$$\mathrm{Reg}_p(E) = 261 \cdot 757^4 + 531 \cdot 757^5 + 293 \cdot 757^6 + 309 \cdot 757^7 + \cdots.$$

[9]The computation of the approximate p-adic L-series for all of our pairs (E, p) took *several months of CPU time* using an optimized implementation of the algorithm of Section 3.

The leading coefficient of the 757-adic L-series must be divisible by 757^2, so we must compute $\mathcal{L}_7(E,T) \pmod{757^3}$, which is enormously time consuming, even with our highly optimized implementation, since each power of p increases the time by a factor of p (and, in addition, we use slower arbitrary precision arithmetic to avoid overflow). The computation took over two months of CPU time, and yielded

$$\mathcal{L}_{757}(T) = O(757^3) + O(757^3)T + \left(399 \cdot 757^2 + O(757^3)\right) T^2 + \cdots .$$

Thus, the p-adic BSD conjecture predicts that $\#Ш(E/\mathbb{Q})(757) \equiv 1 \pmod{757}$, hence $Ш(E/\mathbb{Q})[757] = 0$.

TABLE 1. Various examples in which $\mathrm{ord}_p(\mathrm{Reg}_p(E))$ is large

Curve	Rank	p	$\mathrm{Reg}_p(E)$
53770a1	2	7	$7^7 \cdot 419257219506 + O(7^{21})$
60237b1	2	7	$7^7 \cdot 195984223121 + O(7^{21})$
65088bm1	2	5	$5^7 \cdot 3628814228 + O(5^{21})$
71236b1	2	5	$5^7 \cdot 2905505203 + O(5^{21})$
74220b1	2	7	$7^7 \cdot 411568240919 + O(7^{21})$
82096e1	2	11	$11^7 \cdot 163096174634581 + O(11^{21})$
91143f1	2	17	$17^7 \cdot 32722747582988964 + O(17^{21})$
101552a1	2	5	$5^7 \cdot 1575344534 + O(5^{21})$
116634k1	2	5	$5^7 \cdot 1877361868 + O(5^{21})$
121212q1	2	5	$5^7 \cdot 5806958402 + O(5^{21})$
123888bm1	2	7	$7^7 \cdot 537125029809 + O(7^{21})$
127368d1	2	13	$13^7 \cdot 485242111874635 + O(13^{21})$
27448d1	3	5	$5^6 \cdot 115188708423 + O(5^{22})$
53122a1	3	5	$5^6 \cdot 31988633 + O(5^{22})$
90953a1	3	7	$7^6 \cdot 28674298268349 + O(7^{22})$

Let E be the elliptic curve 389a of rank 2. We verified for a large number of primes p that $Ш(E/\mathbb{Q})[p] = 0$.

Theorem 12.3. *Let E be the rank 2 elliptic curve of conductor 389. Then for 2 and all 5,005 good ordinary primes $p < 48{,}859$ except $p = 16{,}231$ we have $Ш(E/\mathbb{Q})[p] = 0$. For each such p, the p-adic BSD conjectural order of Ш is congruent to 1 modulo p. This only excludes the following bad or supersingular primes and the good ordinary prime 16,231:*

$$p = 107, 389, 599, 1049, 2957, 6661, 8263, 9397, 9551, 14633, 15101, 28591,$$
$$30671, 30869, 31799, 34781, 36263, 45161.$$

Proof. This is a computation similar to the one described above that takes several weeks of CPU time. □

Remark 12.4. For the prime $p = 16{,}231$, we have $\mathrm{ord}_p(\mathrm{Reg}_p) = 3$ instead of $2 = \mathrm{rank}(E)$. Thus, the computation is roughly 16,231 times as difficult as it is for nearby primes using our algorithm, so we estimate it would take several CPU years to finish. It should be possible to instead deal with this exceptional case efficiently using the overconvergent modular symbols approach of Pollack-Stevens [PS11], when a suitable implementation is available.

Remark 12.5. We have excluded supersingular primes from this section not because our algorithms do not apply (they do apply), but because our implementations are significantly slower in this case. We hope to address this shortcoming in future work.

Acknowledgments

It is a pleasure to thank John Coates, Henri Darmon, Jerôme Grand'maison, Ralph Greenberg and Dimitar Jetchev for helpful discussions and comments. We are also greatly indebted to Robert Pollack who shared his code for computing p-adic L-functions and helped with the error estimates in Section 3. The authors also thank Mark Watkins, who independently implemented in Magma some of the algorithms of this paper, and in so doing found bugs in our implementation and discovered mistakes in an early draft of this manuscript.

References

[ARS06] Amod Agashe, Kenneth Ribet, and William A. Stein, *The Manin constant*, Pure Appl. Math. Q. **2** (2006), no. 2, 617–636. MR2251484 (2007c:11076)

[AS02] Amod Agashe and William Stein, *Visibility of Shafarevich-Tate groups of abelian varieties*, J. Number Theory **97** (2002), no. 1, 171–185. MR1939144 (2003h:11070)

[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). MR1839918 (2002d:11058)

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR1484478

[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. MR633886 (83i:14030)

[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. MR1233417 (94k:11071)

[BDGP96] 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. MR1369409 (96j:11103)

[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. MR0179169 (31:3420)

[CFO08] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll, *Explicit n-descent on elliptic curves. I. Algebra*, J. Reine Angew. Math. **615** (2008), 121–155. MR2384334 (2009g:11067)

[CFO09] ———, *Explicit n-descent on elliptic curves. II. Geometry*, J. Reine Angew. Math. **632** (2009), 63–84. MR2544143 (2011d:11128)

[CFO11] ———, *Explicit n-descent on elliptic curves. III. Algorithms*, Preprint. `http://arxiv.org/abs/1107.3516`, 2011.

[CLS09] J. Coates, Z. Liang, and R. Sujatha, *The Tate-Shafarevich group for elliptic curves with complex multiplication*, J. Algebra **322** (2009), no. 3, 657–674. MR2531216 (2010e:11052)

[CLS10] ———, *The Tate-Shafarevich group for elliptic curves with complex multiplication II*, Milan J. Math. **78** (2010), no. 2, 395–416. MR2781846

[Coa11] John Coates, *The enigmatic Tate-Shafarevich group*, 2010 Proceedings of International Congress of Chinese Mathematicians (2011). MR2908059

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

[Col04] Pierre Colmez, *La conjecture de Birch et Swinnerton-Dyer p-adique*, Astérisque (2004), no. 294, ix, 251–319. MR2111647 (2005i:11080)

[Col10] ———, *Invariants $\mathscr{L}$ et dérivées de valeurs propres de Frobenius*, Astérisque (2010), no. 331, 13–28. MR2667885 (2011i:11171)

[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. MR1628193 (99e:11068)

[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. MR1759312 (2001b:11046)

[Del98] Daniel Delbourgo, *Iwasawa theory for elliptic curves at unstable primes*, Compositio Math. **113** (1998), no. 2, 123–153. MR1639179 (99g:11083)

[Del02] ———, *On the p-adic Birch, Swinnerton-Dyer conjecture for non-semistable reduction*, J. Number Theory **95** (2002), no. 1, 38–71. MR1916079 (2004a:11053)

[Dok04] Tim Dokchitser, *Computing special values of motivic L-functions*, Experiment. Math. **13** (2004), no. 2, 137–149. 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. MR1085254 (92a:11066)

[GJP09] G. Grigorov, A. Jorza, S. Patrikis, C. Tarnita, and W. Stein, *Computational verification of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves*, Math. Comp. **78** (2009), 2397–2425, `http://wstein.org/papers/bsdalg/`. MR2521294 (2010g:11106)

[Gre99] Ralph Greenberg, *Iwasawa theory for elliptic curves*, Arithmetic theory of elliptic curves (Cetraro, 1997), Lecture Notes in Math., vol. 1716, Springer, Berlin, 1999, pp. 51–144. MR1754686 (2002a:11056)

[Gre01] ———, *Introduction to Iwasawa theory for elliptic curves*, Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Math. Ser., vol. 9, Amer. Math. Soc., Providence, RI, 2001, pp. 407–464. MR1860044 (2003a:11067)

[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. MR1198816 (93m:11054)

[GV00] Ralph Greenberg and Vinayak Vatsal, *On the Iwasawa invariants of elliptic curves*, Invent. Math. **142** (2000), no. 1, 17–63. MR1784796 (2001g:11169)

[Har08] David Harvey, *Efficient computation of p-adic heights*, LMS J. Comput. Math. **11** (2008), 40–59. MR2395362 (2009j:11201)

[Jon89] John W. Jones, *Iwasawa L-functions for multiplicative abelian varieties*, Duke Math. J. **59** (1989), no. 2, 399–420. MR1016896 (90m:11094)

[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. MR2104361 (2006b:11051)

[Ked01] Kiran S. Kedlaya, *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, J. Ramanujan Math. Soc. **16** (2001), no. 4, 323–338. 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. MR2043934 (2005c:14027); MR1877805

[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. MR2137340 (2006a:14033)

[Kob03] Shin-ichi Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. **152** (2003), no. 1, 1–36. MR1965358 (2004b:11153)

[Kob06] Shinichi Kobayashi, *An elementary proof of the Mazur-Tate-Teitelbaum conjecture for elliptic curves*, Doc. Math. (2006), no. Extra Vol., 567–575 (electronic). MR2290598 (2007k:11099)

[Kol91a] V. A. Kolyvagin, *On the structure of Shafarevich-Tate groups*, Algebraic geometry (Chicago, IL, 1989), Lecture Notes in Math., vol. 1479, Springer, Berlin, 1991, pp. 94–121. MR1181210 (94b:11055)

[Kol91b] V. A. Kolyvagin, *On the structure of Selmer groups*, Math. Ann. **291** (1991), no. 2, 253–259. MR1129365 (93e:11073)

[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. MR2392358 (2009g:11069)

[Man71] J. I. Manin, *Cyclotomic fields and modular curves*, Russian Math. Surveys **26** (1971), no. 6, 7–78. MR0401653 (53:5480)

[Man72] Ju. I. Manin, *Parabolic points and zeta functions of modular curves*, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 19–66. MR0314846 (47:3396)

[Maz72] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266. MR0444670 (56:3020)

[Mil10] Robert L. Miller, *Proving the Birch and Swinnerton-Dyer conjecture for specific elliptic curves of analytic rank zero and one*, `http://arxiv.org/abs/1010.2431`, 2010. MR2801688

[MSD74] Barry Mazur and Peter Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), 1–61. MR0354674 (50:7152)

[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). MR2290599 (2007i:11089)

[MT91] Barry Mazur and John Tate, *The p-adic sigma function*, Duke Math. J. **62** (1991), no. 3, 663–688. MR1104813 (93d:11059)

[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. MR830037 (87e:11076)

[PAR11] The PARI Group, Bordeaux, *PARI/GP, version* `2.5`, 2011, 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. MR1983040 (2004e:11050)

[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. MR683689 (85e:11040)

[PR87] ———, *Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner*, Bull. Soc. Math. France **115** (1987), no. 4, 399–456. MR928018 (89d:11094)

[PR93] ———, *Fonctions L p-adiques d'une courbe elliptique et points rationnels*, Ann. Inst. Fourier (Grenoble) **43** (1993), no. 4, 945–995. MR1252935 (95d:11081)

[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. MR1248080 (95c:11082)

[PR03] ———, *Arithmétique des courbes elliptiques à réduction supersingulière en p*, Experiment. Math. **12** (2003), no. 2, 155–186. MR2016704 (2005h:11138)

[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. MR2052361 (2005g:11097)

[PS11] Robert Pollack and Glenn Stevens, *Overconvergent modular symbols and p-adic L-functions*, Ann. Sci. Éc. Norm. Supér. (4) **44** (2011), no. 1, 1–42. MR2760194

[Roh84] David E. Rohrlich, *On L-functions of elliptic curves and cyclotomic towers*, Invent. Math. **75** (1984), no. 3, 409–423. MR735333 (86g:11038b)

[RS01] K. A. Ribet and W. A. Stein, *Lectures on Serre's conjectures*, Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Math. Ser., vol. 9, Amer. Math. Soc., Providence, RI, 2001, `http://wstein.org/papers/serre/`, pp. 143–232. MR2002h:11047

[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. MR1754688 (2001j:11050)

[Rub00] ———, *Euler systems*, Annals of Mathematics Studies, vol. 147, Princeton University Press, Princeton, NJ, 2000, Hermann Weyl Lectures. The Institute for Advanced Study. MR1749177 (2001g:11170)

[S11a] W. A. Stein et al., *Psage Library*, 2011, `http://code.google.com/p/purplesage/`.

[S11b] ———, *Sage Mathematics Software (Version 4.6.2)*, The Sage Development Team, 2011, `http://www.sagemath.org`.

[Sch82] Peter Schneider, *p-adic height pairings. I*, Invent. Math. **69** (1982), no. 3, 401–409. MR679765 (84e:14034)

[Sch85] ———, *p-adic height pairings. II*, Invent. Math. **79** (1985), no. 2, 329–374. MR778132 (86j:11063)

[Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331. MR0387283 (52:8126)

[Ser96] ———, *Travaux de Wiles (et Taylor, ...). I*, Astérisque (1996), no. 237, Exp. No. 803, 5, 319–332, Séminaire Bourbaki, Vol. 1994/95. MR1423630 (97m:11076)

[Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR1312368 (96b:11074)

[Sim02] Denis Simon, *Computing the rank of elliptic curves over number fields*, LMS J. Comput. Math. **5** (2002), 7–17 (electronic). MR1916919 (2003g:11060)

[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. MR2021618 (2004g:11045)

[Ste07a] William Stein, *The Birch and Swinnerton-Dyer Conjecture, a Computational Approach*, 2007, `http://wstein.org/books/bsd/`.

[Ste07b] ———, *Modular forms, a computational approach*, Graduate Studies in Mathematics, vol. 79, American Mathematical Society, Providence, RI, 2007, With an appendix by Paul E. Gunnells. MR2289048

[SU10] C. Skinner and D. Urban, *The Iwasawa Main Conjecture for* GL_2, `http://www.math.columbia.edu/%7Eurban/eurp/MC.pdf`.

[Wer98] Annette Werner, *Local heights on abelian varieties and rigid analytic uniformization*, Doc. Math. **3** (1998), 301–319. MR1662481 (99k:11086)

[Wil95] Andrew Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551. MR1333035 (96d:11071)

[Wut04] Christian Wuthrich, *On p-adic heights in families of elliptic curves*, J. London Math. Soc. (2) **70** (2004), no. 1, 23–40. MR2064750 (2006h:11079)

[Wut07] ———, *Iwasawa theory of the fine Selmer group*, J. Algebraic Geom. **16** (2007), 83–108. MR2257321 (2008c:11148)

Department of Mathematics, University of Washington, Seattle, Washington
E-mail address: `wstein@uw.edu`

School of Mathematical Sciences, University of Nottingham, University Park Nottingham NG7 2RD, United Kingdom
E-mail address: `christian.wuthrich@nottingham.ac.uk`