

A p -ADIC ANALOGUE OF THE CONJECTURE OF BIRCH AND SWINNERTON-DYER FOR MODULAR ABELIAN VARIETIES

JENNIFER S. BALAKRISHNAN, J. STEFFEN MÜLLER, AND WILLIAM A. STEIN

ABSTRACT. Mazur, Tate, and Teitelbaum gave a p -adic analogue of the Birch and Swinnerton-Dyer conjecture for elliptic curves. We provide a generalization of their conjecture in the good ordinary case to higher dimensional modular abelian varieties over the rationals by constructing the p -adic L -function of a modular abelian variety and showing it satisfies the appropriate interpolation property. We describe the techniques used to formulate the conjecture and give evidence supporting the conjecture in the case when the modular abelian variety is of dimension 2.

1. INTRODUCTION

The Birch and Swinnerton-Dyer (BSD) conjecture gives a precise relationship between several arithmetic invariants of an abelian variety A over a number field K . As formulated by Tate [45], the conjecture states the following:

Conjecture 1.1 (BSD conjecture for abelian varieties). *Let A be an abelian variety of dimension g over a number field K , and let A^\vee be its dual. Then the Mordell-Weil rank r of $A(K)$ is equal to the analytic rank $\text{ord}_{s=1} L(A, s)$ of A and*

$$\lim_{s \rightarrow 1} (s-1)^{-r} L(A, s) = \frac{\Omega_A \cdot |\text{III}(A/K)| \cdot \text{Reg}(A) \cdot \prod_v c_v}{\sqrt{|D_K|^g} |A(K)_{\text{tors}}| \cdot |A^\vee(K)_{\text{tors}}|},$$

where D_K is the absolute discriminant of K , Ω_A is the real period, $\text{Reg}(A)$ is the regulator, c_v is the Tamagawa number at a finite place v of K , $\text{III}(A/K)$ the Shafarevich-Tate group of A and $A(K)_{\text{tors}}$ is the torsion subgroup of $A(K)$.

Note that this conjecture relies on two assumptions: that the Shafarevich-Tate group III is finite and that the L -series can be analytically continued to $s = 1$. An analytic continuation is known to exist for modular abelian varieties over \mathbb{Q} , where an abelian variety is said to be *modular* if it is a quotient of $J_1(N)$ for some level N . In particular, for an elliptic curve E/\mathbb{Q} of rank r , the BSD conjecture predicts

Conjecture 1.2 (BSD conjecture for elliptic curves). *Let E be an elliptic curve over \mathbb{Q} . Then the Mordell-Weil rank r of $E(\mathbb{Q})$ is equal to the analytic rank of E and*

$$\lim_{s \rightarrow 1} (s-1)^{-r} L(E, s) = \frac{\Omega_E \cdot |\text{III}(E/\mathbb{Q})| \cdot \text{Reg}(E) \cdot \prod_p c_p}{|E(\mathbb{Q})_{\text{tors}}|^2}.$$

In 1986, Mazur, Tate, and Teitelbaum [24] gave a p -adic analogue of this conjecture for an elliptic curve E over the rationals and a prime p of good ordinary or multiplicative reduction. Much work has been done towards a proof of the conjecture, and more is known about the p -adic conjecture than its classical counterpart. We give a brief overview of the circle of ideas involved; see also the recent work of Stein-Wuthrich [43]. For simplicity, we assume that $p > 2$.

Date: November 8, 2012.

Let ${}_{\infty}G$ denote the Galois group $\text{Gal}(\mathbb{Q}(\mu_{p^{\infty}})/\mathbb{Q})$, where $\mathbb{Q}(\mu_{p^{\infty}})$ is the cyclotomic extension of \mathbb{Q} obtained by adjoining all p -power roots of unity, let $\kappa : {}_{\infty}G \rightarrow \mathbb{Z}_p^{\times}$ denote the cyclotomic character and let γ be a topological generator of $\Gamma = {}_{\infty}G^{(p-1)}$. For an elliptic curve E/\mathbb{Q} and a prime p such that E has good or multiplicative reduction at p , we denote the p -adic regulator, divided by $\log_p(\kappa(\gamma))^r$, by $\text{Reg}_{\gamma}(E/\mathbb{Q})$ and we let $\mathcal{L}_p(E, T)$ denote the series expansion of the p -adic L -function $L_p(E, s)$ associated to E in $T = \kappa(\gamma)^{s-1} - 1$.

Conjecture 1.3 (*p -adic BSD conjecture for elliptic curves*). *Let E be an elliptic curve over \mathbb{Q} and let p be a prime number such that E has good ordinary or multiplicative reduction at p .*

- (i) *The order of vanishing $\text{ord}_T(\mathcal{L}_p(E, T))$ of $\mathcal{L}_p(E, T)$ at $T = 0$ is equal to the rank r of $E(\mathbb{Q})$ if E has good ordinary or nonsplit multiplicative reduction at p . If E has split multiplicative reduction at p , then $\text{ord}_T(\mathcal{L}_p(E, T)) = r + 1$.*
- (ii) *If E has good ordinary or nonsplit multiplicative reduction at p , then the leading term $\mathcal{L}_p^*(E, 0)$ satisfies*

$$(1.1) \quad \mathcal{L}_p^*(E, 0) = \epsilon_p(E) \cdot \frac{|\text{III}(E/\mathbb{Q})| \cdot \text{Reg}_{\gamma}(E) \cdot \prod_v c_v}{|E(\mathbb{Q})_{\text{tors}}|^2},$$

where $\epsilon_p(E) = (1 - \alpha^{-1})^b$ for a unit root α of $x^2 - a_p x + p \in \mathbb{Q}_p[x]$ (with a_p the Hecke eigenvalue of the newform associated to E) and b is 2 if E has good ordinary reduction at p and 1 if E has nonsplit multiplicative reduction at p .

If E has split multiplicative reduction at p , then

$$\mathcal{L}_p^*(E, 0) = \frac{\mathcal{S}_p}{\log_p(\kappa(\gamma))} \cdot \frac{|\text{III}(E/\mathbb{Q})| \cdot \text{Reg}_{\gamma}(E) \cdot \prod_v c_v}{|E(\mathbb{Q})_{\text{tors}}|^2},$$

where $\mathcal{S}_p = \frac{\log_p(q_E)}{\text{ord}_p(q_E)}$ and q_E is the Tate period of E over \mathbb{Q}_p .

For primes of supersingular reduction, the p -adic L -function and the p -adic regulator can also be defined, and a p -adic BSD conjecture has been formulated by Bernardi and Perrin-Riou [5].

Much work has been done toward a proof of Conjecture 1.3, but since most of it is also relevant for more general modular abelian varieties considered in the present paper, we defer a discussion of the known results to the end of this introduction.

We note that in the case of elliptic curves, the classical BSD conjecture (Conjecture 1.2) shares many of the same arithmetic quantities with the p -adic BSD conjecture (Conjecture 1.3); the main difference is that the regulator and L -series are replaced with p -adic analogues. In particular, the conjectures are equivalent if the rank is 0 and p has good ordinary or nonsplit multiplicative reduction. Consequently, one might expect that a statement like Conjecture 1.1 could be formulated and studied for a modular abelian variety A/\mathbb{Q} associated to a newform f ; this is the goal of the present paper.

One of the main difficulties in formulating the conjecture is that the correct definition of the p -adic L -function of A involves some subtleties to get the precise normalization. By the general motivic framework outlined by Coates [10], the p -adic L -series of A should interpolate the complex L -series $L(A, s)$ at special values, so it seems plausible that it can be defined, similar to $L(A, s)$, as the product of p -adic L -functions $L_p(f^{\sigma}, s)$ associated to the Galois conjugates f^{σ} of f . However, there is no obvious canonical choice for $L_p(f^{\sigma}, s)$, since picking a p -adic L -function associated to f^{σ} requires picking a Shimura period (see Theorem 2.2) for each f^{σ} , that is, a complex number $\Omega_{f^{\sigma}}^+$ such that $L(f^{\sigma}, 1)/\Omega_{f^{\sigma}}^+$ is algebraic. In the case of elliptic curves, this is not an issue, since we can choose Ω_f^+ to be the real period Ω_E^+ of the associated elliptic curve E .

On the other hand, an extension of Conjecture 1.3 to modular abelian varieties should be equivalent to Conjecture 1.1 in rank 0. Since the latter involves the real period Ω_A^+ associated to A , we normalize our Shimura period $\Omega_{f^{\sigma}}^+$, and hence our p -adic L -function, by requiring that the product of the

Shimura periods equals Ω_A^+ ; that we can do this is a consequence of a result we prove later (see Theorem 2.3).

In this way we are able to explicitly construct, essentially generalizing the treatment in [24], a p -adic L -function associated to A with the expected interpolation property, in the case where p is a prime of good ordinary reduction (see (2.10) and (2.11)). We keep the notation introduced prior to Conjecture 1.3 and extend it to the case of modular abelian varieties. We also define the p -adic multiplier $\epsilon_p(A)$ as follows: fix a prime $\wp \mid p$ of the number field K_f generated by the Hecke eigenvalues of f and let α^σ denote the unit root of $x^2 - \sigma(a_p)x + p \in (K_f)_\wp[x]$, where $\sigma : K_f \hookrightarrow \mathbb{C}$ is an embedding. For a Galois conjugate f^σ of f define $\epsilon_p(f^\sigma) = (1 - 1/(\alpha^\sigma))^2$ and define $\epsilon_p(A)$ to be the product of the p -adic multipliers $\epsilon_p(f^\sigma)$ over all distinct Galois conjugates of f .

We make the following p -adic BSD conjecture:

Conjecture 1.4. *Let A/\mathbb{Q} be a modular abelian variety associated to a newform f and let p be a prime number such that A has good ordinary reduction at p . Then the Mordell-Weil rank r of A equals $\text{ord}_T(\mathcal{L}_p(A, T))$ and*

$$(1.2) \quad \mathcal{L}_p^*(A, 0) = \epsilon_p(A) \cdot \frac{|\text{III}(A/\mathbb{Q})| \cdot \text{Reg}_\gamma(A) \cdot \prod_v c_v}{|A(\mathbb{Q})_{\text{tors}}| \cdot |A^\vee(\mathbb{Q})_{\text{tors}}|},$$

where $\mathcal{L}_p^*(A, 0)$ is the leading coefficient of the p -adic L -series $\mathcal{L}_p(A, T)$.

Note that the conjecture of Mazur-Tate-Teitelbaum in the good ordinary case is a special case of Conjecture 1.4. Moreover, if the rank of A/\mathbb{Q} is zero, then our conjecture is equivalent to the classical BSD conjecture due to the interpolation property

$$\mathcal{L}_p(A, 0) = L_p(A, 1) = \epsilon_p(A) \cdot \frac{L(A, 1)}{\Omega_A^+}.$$

Most progress toward proving the Mazur-Tate-Teitelbaum conjecture uses Iwasawa theory and many results remain valid in our setup. Unfortunately, Iwasawa-theoretic results typically only assert equality up to a p -adic unit, whereas our Conjecture 1.4 asserts full equality. We restrict to the good ordinary case from now on, although most results have supersingular or multiplicative analogues. See [43, §6,7] for a summary of such analogues in the elliptic curves case.

Let $X(A/\infty\mathbb{Q})$ denote the Pontryagin dual of the p -Selmer group of A and let Λ be the completed group algebra $\mathbb{Z}_p[[\Gamma]]$. Using p -adic Hodge theory, Kato [18] has shown that $X(A/\infty\mathbb{Q})$ is a torsion Λ -module. Hence we can associate a characteristic series $f_A(T) \in \mathbb{Z}_p[[T]]$, well-defined up to a factor in $\mathbb{Z}_p[[T]]^\times$, to $X(A/\infty\mathbb{Q})$.

Conjecture 1.5. *(Main conjecture of Iwasawa theory for abelian varieties with good ordinary reduction) There exists an element $u(T) \in \Lambda^\times$ such that*

$$\mathcal{L}_p(A, T) = f_A(T) \cdot u(T).$$

If $A = E$ is an elliptic curve, then the main conjecture is known to be a theorem in many cases. If E has complex multiplication, then a proof is due to Rubin [35]. Many other cases have been proven, culminating in the work [40] of Skinner and Urban. See [43, §7] for an overview. The following unconditional result is due to Kato [18]:

Theorem 1.6. *(Kato) Let A be an elliptic curve. There is an integer $m \geq 0$ such that $f_A(T)$ divides $p^m \mathcal{L}_p(A, T)$.*

The following result of Perrin-Riou [31] and Schneider [37] relates $f_A(T)$ to the right hand side of (1.2):

Theorem 1.7. (*Perrin-Riou, Schneider*) *The order of vanishing $\text{ord}_{T=0} f_A(T)$ is greater than or equal to the rank r of A/\mathbb{Q} . Equality holds if and only if the p -adic height pairing on A is nondegenerate and the p -primary part $\text{III}(A/\mathbb{Q})(p)$ of the Shafarevich-Tate group of A is finite, in which case the leading coefficient of $f_A(T)$ has the same valuation as*

$$\epsilon_p(A) \cdot \frac{|\text{III}(A/\mathbb{Q})(p)| \cdot \text{Reg}_\gamma(A) \cdot \prod_v c_v}{|A(\mathbb{Q})_{\text{tors}}| \cdot |A^\vee(\mathbb{Q})_{\text{tors}}|}.$$

See for instance [37, Theorem 2'], noting that we have $\text{ord}_p(\epsilon_p(A)) = 2 \text{ord}_p(N_p)$, where N_p is the number of \mathbb{F}_p -rational points on the reduction of A over \mathbb{F}_p .

As a corollary of Theorem 1.6 and Theorem 1.7, we have that

$$(1.3) \quad \text{ord}_{T=0} \mathcal{L}_p(A, T) \geq \text{ord}_{T=0} f_A(T) \geq r = \text{rank}(A(\mathbb{Q})),$$

if A is an elliptic curve, so one direction of the first part of Conjecture 1.3 (with (1.3) suitably modified in the case of multiplicative reduction) is already known. Moreover, the second part of our Conjecture 1.4 is consistent with the Main Conjecture, since the latter implies that the leading coefficients of the p -adic L -series and the characteristic series have the same valuation. If $\mathcal{L}_p(E, 0) \neq 0$, then Conjecture 1.3, part (ii) is also known up to a rational factor (see [18], [31], and also the exposition in [43, §8]). The primes appearing in this factor can be determined explicitly using [40]. In the good ordinary case a similar result also holds when the p -adic analytic rank is 1, under an additional hypothesis; see [43, §9]. This follows from work of Perrin-Riou [32] and Kato [18].

Historically speaking, numerical evidence played a crucial role in the formulation of Conjecture 1.3 [24, §II.12]. Gathering evidence for Conjecture 1.4 would require two computations independent of the usual Birch and Swinnerton-Dyer conjecture: the computation of p -adic regulators of A , as well as the computation of special values of the p -adic L -function attached to A . We give algorithms to compute these quantities and provide the first numerical verification for Conjecture 1.4 by considering the modular abelian varieties of dimension 2 and rank 2 in [13] and the Jacobian of a twist of $X_0(31)$ of rank 4.

Our aim is to give a self-contained discussion of the p -adic Birch and Swinnerton-Dyer conjecture for modular abelian varieties. To that end, we discuss both the theoretical and the algorithmic aspects of p -adic special values and p -adic regulators. This paper is structured as follows: in §2, we give a construction of the p -adic L -series attached to modular abelian varieties, making explicit certain aspects of [24]. This allows us to compute p -adic special values. In §3, we take a look at the p -adic regulator attached to an abelian variety, focusing on the case when the abelian variety is the Jacobian of a hyperelliptic curve. We begin by reviewing the work of Coleman and Gross [12], which gives the p -adic height pairing on Jacobians of curves in terms of local height pairings. We discuss the two types of local height pairings which arise and give an algorithm to compute p -adic heights, which allows us to compute p -adic regulators. In §4 and §5 we present the evidence for the conjecture in dimension 2.

ACKNOWLEDGEMENTS

We thank Robert Pollack, Chris Wuthrich, Kiran Kedlaya, Shinichi Kobayashi, Bjorn Poonen, David Holmes and Michael Stoll for several helpful conversations and David Roe and Robert Pollack for their work implementing an algorithm to compute p -adic L -series. The first author was supported by NSF grant DMS-1103831. The second author was supported by DFG grants STO 299/5-1 and KU 2359/2-1. The third author was supported by NSF Grants DMS-1161226 and DMS-1147802.

2. p -ADIC L -FUNCTIONS ATTACHED TO MODULAR ABELIAN VARIETIES

In this section, we construct the p -adic L -function attached to a newform $f \in S_2(\Gamma_1(N))$ with trivial Dirichlet character, making explicit a few aspects of [24, §I.10]. This depends on the choice

of a Shimura period as in Theorem 2.2. In order to pin down the p -adic L -function we want, we relate the Shimura periods of f and its Galois conjugates to the real period of the abelian variety A_f attached to f . This leads to a definition of a p -adic L -function for A_f which satisfies the expected interpolation property (2.13). Finally, we discuss how this p -adic L -function can be computed in practice.

2.1. Periods. Let N be a positive integer and let $X_1(N)$ be the modular curve of level N . The Jacobian $J_1(N)$ of $X_1(N)$ is an abelian variety over \mathbb{Q} of dimension equal to the genus of $X_1(N)$, which is equipped with an action of the Hecke algebra \mathbb{T} . The space $S := S_2(\Gamma_1(N))$ of cusp forms of weight 2 on $\Gamma_1(N)$ with trivial Dirichlet character is a module over \mathbb{T} . Let $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z} \in S$ be a newform, let K_f be the totally real number field $\mathbb{Q}(\dots, a_n, \dots)$, and let I_f denote the annihilator $\text{Ann}_{\mathbb{T}}(f)$ of f in \mathbb{T} . Following Shimura [38], we have that the quotient

$$A_f = J_1(N)/I_f J_1(N)$$

is an abelian variety over \mathbb{Q} of dimension $g = [K_f : \mathbb{Q}]$ which is equipped with a faithful action of \mathbb{T}/I_f . Moreover, A_f is an *optimal quotient* of $J_1(N)$ in the sense that the kernel of $J_1(N) \rightarrow A_f$ is connected. For ease of notation, we will drop the subscript f and write $A = A_f$.

Remark 2.1. We assume that f has trivial character for convenience, because we need that K_f is totally real in order for Theorem 2.2 and Theorem 2.3 to hold precisely as stated. However, in the case where K_f is a CM-field, Shimura [39] has proved that a slightly modified version of Theorem 2.2 continues to hold. Using this, one can prove a result that is analogous to Theorem 2.3 for arbitrary newforms $f \in S_2(\Gamma_1(N))$.

There is a complex-valued pairing $\langle \cdot, \cdot \rangle$ on $S \times H_1(X_1(N), \mathbb{Z})$, given by integration:

$$\langle h, \gamma \rangle = 2\pi i \int_{\gamma} h(z) dz.$$

This pairing induces a natural \mathbb{T} -module homomorphism

$$\Phi : H_1(X_1(N), \mathbb{Z}) \rightarrow \text{Hom}_{\mathbb{C}}(S, \mathbb{C}),$$

called the *period mapping*.

Let G_f be the set of embeddings $\sigma : K_f \rightarrow \mathbb{C}$. If $\sigma \in G_f$, we let f^σ denote the conjugate of f by σ . We denote the complex vector space generated by the Galois conjugates of f by S_f . Let $\Phi_f : H_1(X_1(N), \mathbb{Z}) \rightarrow \text{Hom}_{\mathbb{C}}(S_f, \mathbb{C})$ be given by Φ composed with restriction to S_f . Then $\Phi_f(H_1(X_1(N), \mathbb{Z}))$ is a lattice in $\text{Hom}_{\mathbb{C}}(S_f, \mathbb{C})$ and we have an isomorphism

$$A(\mathbb{C}) \cong \text{Hom}_{\mathbb{C}}(S_f, \mathbb{C}) / \Phi_f(H_1(X_1(N), \mathbb{Z})).$$

A choice of basis \mathcal{B} of S_f induces an isomorphism $\text{Hom}_{\mathbb{C}}(S_f, \mathbb{C}) \cong \mathbb{C}^g$ and \mathcal{B} maps via Φ_f to a lattice $\Lambda_{\mathcal{B}} \subset \mathbb{C}^g$ such that

$$A(\mathbb{C}) \cong \mathbb{C}^g / \Lambda_{\mathcal{B}}.$$

For a basis \mathcal{B} of S_f we let $\Lambda_{\mathcal{B}}^+$ (resp. $\Lambda_{\mathcal{B}}^-$) be the fixed points of $\Lambda_{\mathcal{B}}$ under complex conjugation (resp. under minus complex conjugation).

We define the *real period* Ω_A^+ (resp. the *minus period* Ω_A^-) of A as follows: Let ω_A be the pullback of a generator of the nontrivial global relative differential g -forms on the Néron model \mathcal{A} of A over $\text{Spec}(\mathbb{Z})$ to A . We call ω_A a *Néron differential* on A . Then we define

$$\Omega_A^{\pm} := \int_{A(\mathbb{C})^{\pm}} |\omega_A|.$$

where $A(\mathbb{C})^{\pm}$ denotes the set of points of $A(\mathbb{C})$ on which complex conjugation acts as multiplication by ± 1 .

Let \mathcal{B} be a \mathbb{Z} -basis of the finitely generated free \mathbb{Z} -module consisting of elements of S_f with Fourier coefficients in \mathbb{Z} . Then we have (see [1, §3.2])

$$\Omega_A^\pm = \rho \cdot c_A \cdot \text{vol}(\Lambda_{\mathcal{B}}^\pm),$$

where c_A is the Manin constant of A , defined, for instance, in [1, §3.1] and $\rho \in \mathbb{C}$ is i^g if $\pm = -$ and 1 otherwise. It is known that c_A is an integer and conjectured that it is always 1 (cf. [1, §3.3]). There is no known algorithm to *compute* the Manin constant in general, which complicates much of what we do below. The evidence that $c_A = 1$ is compelling, and we make the following:

Running Hypothesis: *We assume for the rest of this paper that $c_A = 1$.*

Let $H_1(X_1(N), \mathbb{Z})^\pm$ denote the part of $H_1(X_1(N), \mathbb{Z})$ fixed by complex conjugation (resp. minus complex conjugation). If $w, z \in \mathbb{C}$, then we write $w \sim z$ if w and z differ by a rational factor. We have that

$$\Omega_A^\pm \sim \rho \cdot \text{vol}(\widetilde{\Lambda}_{\mathcal{B}}^\pm),$$

where $\widetilde{\Lambda}_{\mathcal{B}}^\pm$ is the lattice $\Phi_f(H_1(X_1(N), \mathbb{Z})^\pm)$, Φ_f is induced by the choice of basis \mathcal{B} as above, and the rational factor is the number of components of $A(\mathbb{R})$ (resp. $A(\mathbb{C})^-$).

We denote the complex L -series of f by

$$L(f, s) = \sum_{n \geq 1} \frac{a_n}{n^s}.$$

If ψ is a Dirichlet character, we denote its Gauss sum by $\tau(\psi)$ and its conjugate character by $\bar{\psi}$. We also let f_ψ denote the newform f twisted by ψ and K_ψ the field generated over \mathbb{Q} by the values of ψ .

Theorem 2.2. (Shimura, [39, Theorem 1]) *For all $\sigma \in G_f$ there exist $\Omega_{f\sigma}^+ \in \mathbb{R}$ and $\Omega_{f\sigma}^- \in i \cdot \mathbb{R}$ such that the following properties are satisfied:*

(i) *We have*

$$\frac{\pi i}{\Omega_{f\sigma}^\pm} \left(\int_r^{i\infty} f^\sigma(z) dz \pm \int_{-r}^{i\infty} f^\sigma(z) dz \right) \in K_f$$

for all $r \in \mathbb{Q}$.

(ii) *If ψ is a Dirichlet character, then*

$$\frac{L(f_{\bar{\psi}}, 1)}{\tau(\psi) \cdot \Omega_f^{\text{sign } \psi}} \in K_f \cdot K_\psi.$$

(iii) *If ψ is a Dirichlet character, then*

$$\sigma \left(\frac{L(f_{\bar{\psi}}, 1)}{\tau(\psi) \cdot \Omega_f^{\text{sign}(\psi)}} \right) = \frac{L(f_{\bar{\psi}^\sigma}, 1)}{\tau(\psi^\sigma) \cdot \Omega_{f\sigma}^{\text{sign}(\psi^\sigma)}}.$$

We call a set $\{\Omega_{f\sigma}^\pm\}_{\sigma \in G_f}$ as in Theorem 2.2 a set of *Shimura periods* for f . Note that the conditions of Theorem 2.2 do not determine the sets $\{\Omega_{f\sigma}^\pm\}_{\sigma \in G_f}$. Indeed, if $\{\Omega_{f\sigma}^\pm\}_{\sigma \in G_f}$ satisfy the assertions of the theorem, then this also holds for $\{\sigma(b) \cdot \Omega_{f\sigma}^\pm\}_{\sigma \in G_f}$, where $b \in K_f^\times$.

According to Shimura [39, §2], the periods $\Omega_{f\sigma}^\pm$ are related to a certain period lattice, which gives us a way to compare them to the periods Ω_A^\pm .

Theorem 2.3. *Let $\{\Omega_{f\sigma}^\pm\}_{\sigma \in G_f}$ be any choice of Shimura periods as in Theorem 2.2. Then we have*

$$\Omega_A^\pm \sim \prod_{\sigma \in G_f} \Omega_{f\sigma}^\pm.$$

Proof. Fix a \mathbb{Z} -basis $\mathcal{B} = (h_1, \dots, h_g)$ of the free \mathbb{Z} -module consisting of elements of S_f with Fourier coefficients in \mathbb{Z} . Then there are $b_1, \dots, b_g \in K$ such that

$$f = \sum_{i=1}^g b_i h_i.$$

If $\sigma \in G_f$, then

$$f^\sigma = \sum_{i=1}^g \sigma(b_i) h_i$$

and hence we have

$$(2.1) \quad \langle f^\sigma, \gamma \rangle = \sum_{i=1}^g \sigma(b_i) \cdot \langle h_i, \gamma \rangle$$

for each $\gamma \in H_1(X_1(N), \mathbb{Z})$.

Now fix some ordering $\sigma_1, \dots, \sigma_g$ of G_f and let $B = (b_{ij})$ be the $g \times g$ -matrix with entries $b_{ij} = \sigma_j(b_i)$. We have that $\mathcal{B}' = (f^\sigma)_{\sigma \in G_f}$ forms a basis of the complex vector space S_f . We will compute $\text{vol}(\Lambda_{\mathcal{B}'}^\pm)$ in two different ways and the desired equality up to a rational number will fall out.

First we express $\text{vol}(\Lambda_{\mathcal{B}'}^\pm)$ in terms of Ω_A^\pm . Note that (2.1) implies

$$(2.2) \quad \rho \cdot \text{vol}(\Lambda_{\mathcal{B}'}^\pm) \sim \rho \cdot \text{vol}(\widetilde{\Lambda_{\mathcal{B}'}}^\pm) \sim \rho \cdot |\det(B)| \cdot \text{vol}(\widetilde{\Lambda_{\mathcal{B}}}^\pm) \sim |\det(B)| \cdot \Omega_A^\pm.$$

By [39, §2], we can also relate the lattice $\Lambda_{\mathcal{B}'}$ to the Shimura periods $\Omega_{f^\sigma}^\pm$. Namely, we let K_f act on \mathbb{C}^g as follows: if $a \in K_f$, then the action of a on \mathbb{C}^g is represented by the diagonal matrix $\text{diag}((\sigma_i(a))_i)$. We can decompose

$$\Lambda_{\mathcal{B}'} \otimes \mathbb{Q} = (\Lambda_{\mathcal{B}'} \otimes \mathbb{Q})^+ \oplus (\Lambda_{\mathcal{B}'} \otimes \mathbb{Q})^-,$$

where $(\Lambda_{\mathcal{B}'} \otimes \mathbb{Q})^\pm$ is the set of elements of $\Lambda_{\mathcal{B}'}$ fixed by \pm complex conjugation. Then we have

$$(\Lambda_{\mathcal{B}'} \otimes \mathbb{Q})^\pm = K_f \Omega^\pm,$$

where $\Omega^\pm \in \mathbb{C}^g$ is the vector whose i -th entry is $\Omega_{f^{\sigma_i}}^\pm$. Hence $(\Lambda_{\mathcal{B}'} \otimes \mathbb{Q})^\pm$ is a one-dimensional K_f -vector space.

Since $\det(B) \neq 0$, the elements b_1, \dots, b_g of K_f form a basis for K_f over \mathbb{Q} and therefore a basis of $(\Lambda_{\mathcal{B}'} \otimes \mathbb{Q})^\pm$ as a \mathbb{Q} -vector space is given by

$$\left(\left(\sigma_1(b_i) \Omega_{f^{\sigma_i}}^\pm, \dots, \sigma_g(b_i) \Omega_{f^{\sigma_g}}^\pm \right)_{i=1, \dots, g} \right).$$

Hence we have

$$(2.3) \quad \rho \cdot \text{vol}(\Lambda_{\mathcal{B}'}^\pm) \sim |\det(B)| \cdot \prod_{\sigma} \Omega_{f^\sigma}^\pm,$$

since

$$(\Lambda_{\mathcal{B}'} \otimes \mathbb{Q})^\pm = (\Lambda_{\mathcal{B}'}^\pm) \otimes \mathbb{Q}.$$

The proof of the theorem now follows from (2.2) and (2.3). \square

Remark 2.4. If $L(f, 1) \neq 0$, then we can also argue as follows: We have

$$\frac{L(A, 1)}{\prod_{\sigma \in G_f} \Omega_{f^\sigma}^\pm} \in \mathbb{Q}$$

by Theorem 2.2. But on the other hand, the quotient $\frac{L(A,1)}{\Omega_A^+}$ is a rational number as well by [2, Theorem 4.5]. Hence we get $\prod_{\sigma \in G_f} \Omega_{f\sigma}^+ \sim \Omega_A^+$.

Remark 2.5. In [46], Vatsal defines canonical Shimura periods associated to cuspforms. It would be interesting to determine whether his periods satisfy Theorem 2.3.

From now on, we fix some choice $\{\Omega_{f\sigma}^\pm\}_{\sigma \in G_f}$ such that

$$(2.4) \quad \prod_{\sigma \in G_f} \Omega_{f\sigma}^\pm = \Omega_A^\pm.$$

If $\{\Psi_{f\sigma}^\pm\}_{\sigma \in G_f}$ is another set of Shimura periods satisfying (2.4), then there is a unit $b \in \mathcal{O}_{K_f}$ such that $\Psi_{f\sigma}^\pm = \sigma(b)\Omega_{f\sigma}^\pm$ for all $\sigma \in G_f$. For our intended applications, this ambiguity is not serious, see Remark 2.9.

In order to *compute* $\{\Omega_{f\sigma}^\pm\}_{\sigma \in G_f}$ we can find a Dirichlet character ψ of sign \pm such that $L(f_\psi, 1) \neq 0$ and use equation (11) of [39]. Alternatively, we can fix some nonzero element $\gamma \in H_1(X_1(N), \mathbb{Z})[I_f]^\pm$ and define

$$\Omega_{f\sigma}^\pm = \sigma(b) \cdot \langle f^\sigma, \gamma \rangle,$$

for each $\sigma \in G_f$, where $b \in K_f$ is chosen to make (2.4) hold. See [41, Ch. 10] for a description of how to compute the integration pairing in practice.

As an application of Theorem 2.3, we can prove a relation between the real and minus period of A and the corresponding periods of A twisted by a Dirichlet character ψ .

Corollary 2.6. *Let ψ be a Dirichlet character such that $L(f_\psi, 1) \neq 0$. Then there exists $\eta_\psi \in K_\psi^*$ such that*

$$\Omega_A^{\text{sign } \psi} \cdot \prod_{\sigma \in G_f} \tau(\psi^\sigma) = \eta_\psi \cdot \Omega_{A_\psi}^+.$$

In particular, if ψ takes values in \mathbb{Q} , then there exists $\eta_\psi \in \mathbb{Q}^$ such that*

$$\Omega_A^{\text{sign } \psi} \cdot \tau(\psi)^g = \eta_\psi \cdot \Omega_{A_\psi}^+.$$

Proof. This follows from Theorem 2.3 and Theorem 2.2. □

Remark 2.7. If A is the Jacobian of a hyperelliptic curve of genus at most 2 and ψ is a quadratic Dirichlet character such that $\psi(N) \neq 0$, then one can show that the statement of Corollary 2.6 holds without the assumption $L(f_\psi, 1) \neq 0$ using quite concrete arguments. For elliptic curves and quadratic ψ , Corollary 2.6 was already used in [24, §II.11]. Note, however, that their claim that $\eta_\psi \in \{1, 2\}$ is incorrect; see [30], where the correct value of η_ψ is determined in all cases.

2.2. Modular symbols, measures, and the p -adic L -function of a newform. In this subsection we define the p -adic L -function associated to f , following [24]. See also the treatment in [33]. The definitions for f^σ , where $\sigma \in G_f$, are entirely analogous.

Recall that we fixed a choice of Shimura periods $\Omega_{f\sigma}^\pm$ above. The *plus modular symbol map* associated to f is the map

$$[\]_f^+ : \mathbb{Q} \rightarrow K_f$$

$$r \mapsto [r]_f^+ = -\frac{\pi i}{\Omega_f^+} \left(\int_r^{i\infty} f(z) dz + \int_{-r}^{i\infty} f(z) dz \right)$$

and the *minus modular symbol map* associated to f is the map

$$\begin{aligned} [\]_f^- : \mathbb{Q} &\rightarrow K_f \\ r &\mapsto [r]_f^- = \frac{\pi i}{\Omega_f^-} \left(\int_r^{i\infty} f(z) dz - \int_{-r}^{i\infty} f(z) dz \right). \end{aligned}$$

Note that we have $[0]_f^+ = \frac{L(f,1)}{\Omega_f^+}$. More generally, if m is a positive integer and ψ is a Dirichlet character modulo m , then [24, §I.8] implies

$$(2.5) \quad \frac{L(f_{\bar{\psi}}, 1)}{\Omega_f^{\text{sign } \psi}} = \frac{\psi(-1)}{\tau(\psi)} \sum_{u \bmod m} \psi(a) \cdot \left[\frac{u}{m} \right]_f^{\text{sign } \psi} \in K_f.$$

Let p be a prime of good ordinary reduction for A . We fix, once and for all, a prime \wp of K_f lying above p . The modular symbol maps allow us to define two measures on \mathbb{Z}_p^\times which depend on the unit root of the polynomial $h(x) := x^2 - a_p x + p \in (K_f)_\wp[x]$, where $(K_f)_\wp$ is the completion of K_f at \wp . The construction of the p -adic L -function depends, in turn, on these measures. Since A is ordinary at p , the polynomial h has a unique unit root $\alpha \in (K_f)_\wp$, i.e., a root with $\text{ord}_\wp(\alpha) = 0$.

Using the modular symbol maps $[\]_f^\pm$, we define two measures $\mu_{f,\alpha}^\pm$ on \mathbb{Z}_p^\times by

$$\mu_{f,\alpha}^\pm(a + p^n \mathbb{Z}_p) = \frac{1}{\alpha^n} \left[\frac{a}{p^n} \right]_f^\pm - \frac{1}{\alpha^{n+1}} \left[\frac{a}{p^{n-1}} \right]_f^\pm.$$

For a continuous character χ on \mathbb{Z}_p^\times with values in \mathbb{C}_p , we may integrate χ against $\mu_{f,\alpha}$. Following [24, §I.13], we write $x \in \mathbb{Z}_p^\times$ as $\omega(x) \cdot \langle x \rangle$ where $\omega(x)$ is a $(p-1)$ -st root of unity and $\langle x \rangle$ belongs to $1 + p\mathbb{Z}_p$. The element ω is known as the Teichmüller character.

We define the analytic p -adic L -function associated to f by

$$(2.6) \quad L_p(f, s) = \int_{\mathbb{Z}_p^\times} \langle x \rangle^{s-1} d\mu_{f,\alpha}^+(x) \quad \text{for all } s \in \mathbb{Z}_p,$$

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, respectively. The function $L_p(f, s)$ extends to a locally analytic function in s on the disc defined by $|s-1| < 1$, as in the first proposition of [24, §I.13].

Let ${}_\infty G$ be the Galois group $\text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$. The cyclotomic character $\kappa : {}_\infty G \rightarrow \mathbb{Z}_p^\times$ induces an isomorphism from ${}_\infty G$ to \mathbb{Z}_p^\times that sends a topological generator γ in ${}_\infty G^{(p-1)}$ to a generator $\kappa(\gamma)$ of $1 + p\mathbb{Z}_p^\times$. This identification allows us to give a series expansion of the p -adic L -function in terms of $T = \kappa(\gamma)^{s-1} - 1$. That is, we have

$$(2.7) \quad \mathcal{L}_p(f, T) = \int_{\mathbb{Z}_p^\times} (1+T)^{\frac{\log_p(\langle x \rangle)}{\log_p(\kappa(\gamma))}} d\mu_{f,\alpha}^+(x).$$

Now for each $n \geq 1$, let $P_n(f, T)$ be the following polynomial:

$$(2.8) \quad P_n(f, T) = \sum_{a=1}^{p-1} \left(\sum_{j=0}^{p^{n-1}-1} \mu_{f,\alpha}^+(\omega(a)(1+p)^j + p^n \mathbb{Z}_p) \cdot (1+T)^j \right).$$

We have that (2.8) gives us a Riemann sum for the integral (2.7), by summing over residue classes mod p^n ; in other words:

Proposition 2.8. *We have that the p -adic limit of these polynomials is the p -adic L -series:*

$$\lim_{n \rightarrow \infty} P_n(f, T) = \mathcal{L}_p(f, T).$$

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

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

Proof. This is a straightforward generalization of [43, Proposition 3.1]. The upper bounds we obtain are the same as the upper bounds in the proof of [43, Proposition 3.1], which enables us to compute the p -adic L -series to any desired precision. \square

We define the p -adic multiplier $\epsilon_p(f)$ by

$$\epsilon_p(f) = (1 - \alpha^{-1})^2.$$

The p -adic L -series of f satisfies an interpolation property with respect to the complex L -series of f [24, §I.14]:

$$(2.9) \quad \mathcal{L}_p(f, 0) = L_p(f, 1) = \int_{\mathbb{Z}_p^\times} d\mu_{f,\alpha}^+ = \epsilon_p(f) \cdot [0]_f^+ = \epsilon_p(f) \cdot \frac{L(f, 1)}{\Omega_f^+}.$$

2.3. p -adic L -function associated to A . The p -adic L -series $\mathcal{L}_p(f, s)$ associated to f that we constructed in the previous subsection depends on the Shimura periods $\Omega_{f^\sigma}^+$ and on the prime \wp . In the present section we define a p -adic L -function associated to the abelian variety A which is independent of the choices of the Shimura periods (provided they satisfy (2.4)) and of \wp .

The abelian variety A has an associated complex L -series, given by

$$L(A, s) = \prod_{\sigma \in G_f} L(f^\sigma, s),$$

which can be extended analytically to the whole complex plane.

We define the p -adic L -function associated to A by

$$(2.10) \quad L_p(A, s) = \prod_{\sigma \in G_f} L_p(f^\sigma, s)$$

for $s \in \mathbb{Z}_p$.

Remark 2.9. Since we require our Shimura periods $\{\Omega_{f^\sigma}^\pm\}_{\sigma \in G_f}$ to satisfy (2.4), the p -adic L -function $L_p(A, s)$ does not depend on the choice of period for each f^σ , although the individual p -adic L -functions $L_p(f^\sigma, s)$ do.

Furthermore, we define

$$(2.11) \quad \mathcal{L}_p(A, T) = \prod_{\sigma \in G_f} \mathcal{L}_p(f^\sigma, T)$$

and the p -adic multiplier of A by

$$\epsilon_p(A) = \prod_{\sigma \in G_f} \epsilon_p(f^\sigma).$$

For $r \in \mathbb{Q}$ we set

$$(2.12) \quad [r]_A^\pm := \prod_{\sigma \in G_f} [r]_{f^\sigma}^\pm.$$

Corollary 2.10. *Let $\{\Omega_{f^\sigma}^\pm\}_{\sigma \in G_f}$ be a set of Shimura periods satisfying (2.4). Then (2.9) immediately implies*

$$(2.13) \quad \mathcal{L}_p(A, 0) = L_p(A, 1) = \epsilon_p(A) \cdot [0]_A^+ = \epsilon_p(A) \cdot \frac{L(A, 1)}{\Omega_A^+}.$$

2.4. Quadratic twists and normalization. Modular symbols can be computed up to a rational multiple purely algebraically (cf. [41]) using (mostly sparse) linear algebra over fields. Computing the exact modular symbol (not just up to a rational factor) requires doing linear algebra over \mathbb{Z} , which is much slower. In this section we describe a method to determine the correct normalization of the modular symbol map by using special values of quadratic twists, which is potentially much faster than using linear algebra over \mathbb{Z} .

In order to find the correct normalization, we use the fact that the p -adic L -series associated to A interpolates the Hasse-Weil L -function $L(A, s)$ associated to A at special values. Algorithms for the computation of $\frac{L(A,1)}{\Omega_A^+}$, $L(A, 1)$ and Ω_A^+ are discussed in [2, 13, 41]. So if $L(A, 1) \neq 0$, then we can find the correct normalization factor δ^+ for $\mathcal{L}_p(A, T)$ by computing $[0]_A^+$ and comparing it to $\frac{L(A,1)}{\Omega_A^+}$. Note that the quotient $\frac{L(A,1)}{\Omega_A^+}$ can be computed purely algebraically as a certain lattice index, without computing either of the real numbers $L(A, 1)$ or Ω_A^+ .

In order to discuss the strategy for the case $L(A, 1) = 0$, we begin by considering modular symbols associated to quadratic twists of f . Let D be a fundamental discriminant of a quadratic number field such that $\gcd(pN, D) = 1$ and let ψ denote the Dirichlet character associated to $\mathbb{Q}(\sqrt{D})$. We assume that $L(f_\psi, 1) \neq 0$. Using Corollary 2.6 we see that there exists $\eta_\psi \in K_f^*$ such that

$$\Omega_A^{\text{sign}(D)} \cdot D^{g/2} = \eta_\psi \cdot \Omega_{A_\psi}^+.$$

A computation analogous to [43, §3.7] yields

$$(2.14) \quad [r]_{A_\psi}^+ = \prod_{\sigma \in G_f} [r]_{f_\psi^\sigma}^+ = \frac{\text{sign}(D)^g}{\eta_\psi} \prod_{\sigma \in G_f} \sum_{u=1}^{|D|-1} \psi(u) \cdot \left[r + \frac{u}{D} \right]_{f^\sigma}^{\text{sign}(D)}.$$

Therefore we can compute the product of the plus modular symbols for f_ψ and its conjugates in terms of modular symbols for f and its conjugates. The same holds for the p -adic L -function of the twist A_ψ of A by ψ .

Now suppose that $\mathcal{L}_p(A, 0) = 0$ and we want to find the correct normalization factor for $[]_f^+$. We can use that for a fundamental discriminant D with Dirichlet character ψ , the modular symbols $[]_f^+$ and $[]_{f_\psi}^{\text{sign}(D)}$ are related by (2.14). Hence the same normalization factor δ^+ will yield the correct value $[r]_{A_\psi}^+$ for all $D > 0$ such that $\gcd(pN, D) = 1$.

We can compute δ^+ by finding a fundamental discriminant $D > 0$ such that $\gcd(pN, D) = 1$ and such that A_ψ has analytic rank 0 over \mathbb{Q} , where ψ is the quadratic character associated to $\mathbb{Q}(\sqrt{D})$, and comparing $[0]_{A_\psi}^+$ to

$$\frac{\eta_\psi \cdot L(A_\psi, 1)}{D^{g/2} \cdot \Omega_A^+}.$$

An analogous approach can be used to find the correct normalization factor δ^- for the minus modular symbol. It follows from [9] that in both cases a fundamental discriminant D as above always exists.

Remark 2.11. Suppose that A is the Jacobian of a hyperelliptic curve X/\mathbb{Q} of genus g given by an equation

$$y^2 + h_1(x)y = f_1(x)$$

which is minimal in the sense of [20]. Often it is not necessary to compute $\Omega_{A_\psi}^{\text{sign } D}$ (or even Ω_A^+) to compute η_ψ . Let $y^2 + h_2(x)y = f_2(x)$ be a minimal equation for X_ψ , and consider the differentials $\omega_i = \frac{x^i dx}{2y+h_1(x)}$ on X and $\omega'_i = \frac{x^i dx}{2y+h_2(x)}$ on X_ψ . It frequently happens that $(\omega_1, \dots, \omega_g)$ is a basis of the integral 1-forms on A and $(\omega'_1, \dots, \omega'_g)$ is also a basis for the integral 1-forms on A_ψ . In that case we always have $\eta_\psi \in \{\pm 1\}$; this follows from [13, §3.5]. It is easy to determine the sign using a

straightforward generalization of [19, §1.3]. More generally, a similar approach can also be used to compute η_ψ directly if we know how to express a basis for the integral 1-forms in terms of $\omega_1, \dots, \omega_g$.

2.5. The algorithm. We implemented the following algorithm for the computation of the p -adic L -series of A in Sage [42].

Algorithm 2.12 (p -adic L -series).

Input: Good ordinary prime p , A modular abelian variety attached to newform f , precision n .

Output: n th approximation to the p -adic L -series $\mathcal{L}_p(A, T)$.

- (1) Fix a prime \wp of the field K_f generated by the Hecke eigenvalues of f lying above p and compute the unit root α of $h(x) \in (K_f)_\wp[x]$.
- (2) Find a fundamental discriminant $D > 0$ such that $\gcd(pN, D) = 1$ and A_ψ has analytic rank 0 over \mathbb{Q} , where ψ is the quadratic character associated to $\mathbb{Q}(\sqrt{D})$.
- (3) Compute η_ψ .
- (4) For each $\sigma \in G_f$, define measures $\mu_{f^\sigma, \alpha}^\pm$.
- (5) For each $\sigma \in G_f$, compute $[0]_{f^\sigma}^+$ and set $[0]_{A_\psi}^+ = \prod_{\sigma \in G_f} [0]_{f^\sigma}^+$.
- (6) Compute $\frac{L(A_\psi, 1)}{D^{g/2} \Omega_A^+}$ and deduce the normalization factor δ^+ using (2.13).
- (7) For each σ , compute $P_n(f^\sigma, T)$.
- (8) Return $\delta^+ \cdot \prod_\sigma P_n(f^\sigma, T)$.

Remark 2.13. Note that Step (7) of Algorithm 2.12 is exponential in p ; see the following subsection for an alternative method.

2.6. Overconvergent modular symbols. Here we outline an alternative method for Step (7) of Algorithm 2.12. This method is due to Pollack and Stevens [34] and has running time polynomial in p and in the desired number of digits of precision.

The idea is to use Stevens's overconvergent modular symbols; these are constructed using certain p -adic distributions, and they can be specialized to classical modular symbols. More precisely, any classical modular eigensymbol can be lifted uniquely to an overconvergent modular Hecke-eigensymbol, which can be approximated using finite data. Note that in order to do this, we first have to p -stabilize the symbol to a symbol for $\Gamma_0(Np)$ which is an eigensymbol away from p .

The plus modular symbol we start with is only determined up to multiplication by a scalar, so the corresponding overconvergent eigenlift is also only determined up to multiplication by a scalar. Hence we cannot dispense with Steps (2), (3), (5) and (6) of Algorithm 2.12.

Once this desired lift has been computed, writing down the p -adic L -series associated to the modular symbol and its quadratic twists by ψ for suitable D is rather easy, cf. [34, §9]. Together with David Roe and Robert Pollack, we have implemented Algorithm 2.12 with Step (7) replaced by the algorithm from [34] in Sage as well, building on an implementation due to Pollack.

3. THE p -ADIC HEIGHT PAIRING OF COLEMAN-GROSS AND p -ADIC REGULATORS

We now shift our attention to the remaining p -adic quantity appearing in Conjecture 1.4, the p -adic regulator. To discuss p -adic regulators, we begin, in this section, by describing one construction of the global p -adic height pairing relevant to our setting. We give an algorithm to compute the height pairing in the case when the abelian variety A is the Jacobian of a hyperelliptic curve and show how we use it to compute p -adic regulators.

Let A be an abelian variety defined over a number field K and let A^\vee denote the dual abelian variety to A . There are several definitions of p -adic height pairings on abelian varieties in the literature. Schneider [36] and Mazur-Tate [23] were the first to construct the p -adic height pairing on abelian varieties defined over number fields. This was extended to motives by Nekovář [29]. There

are also more specialized definitions: in the case when $\dim A = 1$, $K = \mathbb{Q}$, and p is a prime of good, ordinary reduction, Mazur, Stein, and Tate [22] gave an explicit formula for the p -adic height which relies on an understanding of the p -adic sigma function. When A is the Jacobian of a curve, Coleman and Gross [12] described the p -adic height pairing on A as a sum of local height pairings. Note that in the range where all of these constructions apply, they are known to be equivalent by the work of Coleman [11] and Besser [6] (where the equivalence is possibly up to sign, e.g., in the supersingular case). For all of these definitions, the p -adic height pairing is known to be bilinear and, in the principally polarized case, symmetric.

Let p be a prime number such that A has good ordinary reduction at all primes of K above p . We denote the p -adic height pairing by

$$h : A \times A^\vee \longrightarrow \mathbb{Q}_p$$

$$(P, Q) \mapsto h(P, Q).$$

Now we want to define the p -adic regulator with respect to h . In the literature, one usually defines this quantity as the determinant of the height pairing matrix with respect to set of generators of the free part of $A(K)$ and $A^\vee(K)$, respectively. This, however, is only well-defined up to sign. Since results in Iwasawa theory are typically only up to a p -adic unit, this is usually not a serious problem, but in order to state Conjecture 1.4, we need a canonical well-defined p -adic regulator. First note that if $\phi : A \rightarrow A^\vee$ is an isogeny and P_1, \dots, P_r generate the free part of $A(K)$, then

$$\text{Reg}_\phi(A/K) := \det \left((h(P_i, \phi(P_j)))_{i,j} \right)$$

does not depend on the choice of generators P_1, \dots, P_r .

Lemma 3.1. *Let $c, c' \in \text{Pic}^0(A)$ and let $\phi_c, \phi_{c'} : A \rightarrow A^\vee$ be the corresponding isogenies. If P_1, \dots, P_r is a set of generators for the free part of $A(K)$, then we have*

$$\frac{1}{[A^\vee(K) : \phi_c(A(K))]} \text{Reg}_{\phi_c}(A/K) = \frac{1}{[A^\vee(K) : \phi_{c'}(A(K))]} \text{Reg}_{\phi_{c'}}(A/K).$$

Proof. We set $m = [A^\vee(K) : \phi_c(A(K))]$ and $m' = [A^\vee(K) : \phi_{c'}(A(K))]$. Let Q_1, \dots, Q_r denote a set of generators of the free part of $A^\vee(K)$ such that

$$\det \left((h(P_i, Q_j))_{i,j} \right) = \frac{1}{m} \text{Reg}_{\phi_c}(A/K).$$

There are integers $m_{ij}, m'_{ij} \in \mathbb{Z}$ such that

$$\phi_c(P_i) = \sum_{j=1}^r m_{ij} Q_j \quad \text{and} \quad \phi_{c'}(P_i) = \sum_{j=1}^r m'_{ij} Q_j.$$

Since $\det \left((m_{ij})_{i,j} \right) = m$ and $\det \left((h(P_i, Q_j))_{i,j} \right) = \pm \frac{1}{m'} \text{Reg}_{\phi_c}(A/K)$, it suffices to show that $\det \left((m'_{ij})_{i,j} \right) = m'$ (and not $-m'$).

To show this, we use classical Néron-Tate heights. The Néron-Tate regulator is defined as

$$\text{Reg}(A/K) = \left| \det \left((\langle P_i, Q_j \rangle_{\mathcal{P}})_{i,j} \right) \right|,$$

where the bilinear pairing $\langle P_i, Q_j \rangle_{\mathcal{P}} = \hat{h}_{\mathcal{P}}(P_i, Q_j)$ is defined in terms of the Néron-Tate height $\hat{h}_{\mathcal{P}}$ with respect to the Poincaré bundle on $A \times A^\vee$. See [16, Remark F.4.1]. On the other hand, it is easy to see that

$$\langle P_i, \phi_c(P_j) \rangle_{\mathcal{P}} = \langle P_i, P_j \rangle_c,$$

where $\langle \cdot, \cdot \rangle_c$ is the Néron-Tate height pairing on A with respect to c , and similarly for c' . This implies that

$$0 < \det \left((\langle P_i, P_j \rangle_c)_{i,j} \right) = \det(M) \cdot \det \left((\langle P_i, Q_j \rangle_{\mathcal{P}})_{i,j} \right).$$

Since $\det(M) = m > 0$ and $\text{Reg}(A/K) = \frac{1}{m} \text{Reg}_c(A/K)$, we have

$$\text{Reg}(A/K) = \det \left((\langle P_i, Q_j \rangle_{\mathcal{P}})_{i,j} \right),$$

and hence

$$\text{Reg}(A/K) = \frac{1}{\det(M')} \det \left((\langle P_i, \phi_{c'}(P_j) \rangle_{\mathcal{P}})_{i,j} \right) = \frac{1}{\det(M')} \det \left((\langle P_i, P_j \rangle_{c'})_{i,j} \right).$$

Therefore we find $\det(M') = m'$. \square

Definition 3.2. Let A be an abelian variety defined over a number field K and let A^\vee denote its dual. Let P_1, \dots, P_r be a set of generators of $A(K)/A(K)_{\text{tors}}$. Fix some $c \in \text{Pic}^0(A)$ and let $\phi_c : A \rightarrow A^\vee$ denote the corresponding isogeny. The p -adic regulator of A , denoted $\text{Reg}_p(A)$, is defined by

$$\text{Reg}_p(A) := \frac{1}{[A^\vee(K) : \phi_c(A(K))]} \text{Reg}_{\phi_c}(A/K)$$

The p -adic regulator is well-defined by Lemma 3.1. It has been conjectured by Schneider [36] that the p -adic height pairing is nondegenerate, however, in contrast to the classical case of Néron-Tate heights, this is not known in general.

Among the aforementioned definitions of the p -adic height pairing, the Coleman-Gross construction of the p -adic height pairing is fairly explicit in nature, and for that reason, lends itself nicely to computation. Thus we take it as our working definition of the p -adic height. We start by giving a brief overview of the work of Coleman and Gross.

Suppose X/K is a curve defined over a number field K , with good reduction at primes above p . To define the p -adic height pairing

$$h : \text{Div}^0(X) \times \text{Div}^0(X) \rightarrow \mathbb{Q}_p,$$

where $\text{Div}^0(X)$ denotes the divisors on X of degree zero, one needs the following data:

- A “global log”- a continuous idele class character $\ell : \mathbb{A}_K^*/K^* \rightarrow \mathbb{Q}_p$.
- For each $v \mid p$ a choice of a subspace $W_v \subset H_{\text{dR}}^1((X \otimes K_v)/K_v)$ complementary to the space of holomorphic forms.

We require that the local characters ℓ_v induced by ℓ , for $v \mid p$, are ramified in the sense that they do not vanish on the units in K_v . From ℓ one deduces the following data:

- For any place $v \nmid p$ we have $\ell_v(\mathcal{O}_{K_v}^*) = 0$ for continuity reasons, which implies that ℓ_v is completely determined by the number $\ell_v(\pi_v)$, where π_v is any uniformizer in K_v .
- For any place $v \mid p$ we can decompose ℓ_v as a composition

$$(3.1) \quad \begin{array}{ccc} \mathcal{O}_{K_v}^* & \xrightarrow{\ell_v} & \mathbb{Q}_p \\ & \searrow \log_v & \nearrow t_v \\ & & K_v \end{array}$$

where t_v is a \mathbb{Q}_p -linear map. Since we assume that ℓ_v is ramified it is then possible to extend \log_v to $\log_v : K_v^* \rightarrow K_v$ in such a way that the diagram remains commutative.

We will later need to choose a branch of the p -adic logarithm, since the Coleman integral of a form with residue depends on such a choice. We will fix this choice for the computation of the local height pairing to be the one determined above.

Let us now describe the p -adic height pairing $h(D, E)$ for a pair of degree zero divisors D and E with disjoint support. The height pairing is a sum of local terms

$$h(D, E) = \sum_v h_v(D, E)$$

over all finite places v . The local terms depend only on the completion at v of K . Thus, let K_v be the completion of K at a place v , with valuation ring \mathcal{O} , uniformizer π and let $k_v = \mathcal{O}/\pi\mathcal{O}$ be the residue field, with order q . Let C denote the curve X over the local field K_v . We shall assume that C has a K_v -rational point and that C has good reduction at π .

Let $\chi : K_v^* \rightarrow \mathbb{Q}_p$ be the local component of ℓ , which is a continuous homomorphism.

Proposition 3.3. *If $\text{char } k_v \neq p$, there exists a unique function $\langle D, E \rangle$ defined for all $D, E \in \text{Div}^0(C)$ of disjoint support that is continuous, symmetric, bi-additive, takes values in \mathbb{Q}_p , and satisfies*

$$(3.2) \quad \langle (f), E \rangle = \chi(f(E))$$

for $f \in K_v(C)^*$.

Proof. See [12, Prop 1.2]. □

We will discuss how to compute this in practice in Section 3.1.

3.1. Computing p -adic heights away from p . We keep the notation of the previous section, but assume, in addition, that X is hyperelliptic of genus g , given by an equation $y^2 = f(x)$, where $f \in \mathcal{O}[x]$ is separable. Let v be a fixed non-archimedean place of K not dividing p .

The arithmetic geometry needed in the present section can be found in [21, Chapters 8,9]. We fix a proper regular model \mathcal{C} of $C = X \times_K K_v$ over $\text{Spec}(\mathcal{O})$ with special fiber \mathcal{C}_v . If D is a prime divisor on C , then we let \overline{D} denote the Zariski closure of D on \mathcal{C} and we extend this to all of $\text{Div}(C)$ by linearity. It was shown by Hriljac [17] that if $D \in \text{Div}^0(C)$, then there exists a vertical \mathbb{Q} -divisor $\Phi(D)$ on \mathcal{C} such that the intersection multiplicity of $\overline{D} + \Phi(D)$ with any irreducible components of \mathcal{C}_v is trivial.

If $D, E \in \text{Div}^0(C)$ have disjoint support, then according to [12, Prop 1.2] the local height pairing between D and E at v is given by

$$(3.3) \quad h_v(D, E) = \ell_v(\pi_v) \cdot i_v(\overline{D} + \Phi(D), \overline{E}),$$

where i_v denotes the (rational-valued) intersection pairing on \mathcal{C} . This does not depend on the choice of $\Phi(D)$ or of \mathcal{C} .

As in [26], the following steps are sufficient to compute the local p -adic height pairing at v .

- (1) Compute a desingularization \mathcal{C} in the strong sense of the Zariski closure \overline{C} of C over $\text{Spec}(\mathcal{O})$;
- (2) Compute $i_v(\overline{D}, \overline{E})$;
- (3) Compute $i_v(\Phi(D), \overline{E})$.

These steps are dealt with in detail and greater generality in [26]. For the convenience of the reader, we provide a brief summary in the present case of hyperelliptic curves.

Step (1) can be done using a desingularization algorithm implemented by Steve Donnelly in **Magma** [8]. Recall that a desingularization \mathcal{C} of the Zariski closure \overline{C} of C over $\text{Spec}(\mathcal{O})$ in the strong sense is a proper regular model of C over $\text{Spec}(\mathcal{O})$ such that there exists a morphism $\xi : \mathcal{C} \rightarrow \overline{C}$ that is an isomorphism above regular points of \overline{C} . From now on we will assume that our model \mathcal{C} is of this type, as this property is needed in order for some of the other steps to work. See [26, §4.3] for details.

For Step (2), we write our divisors D and E as differences of effective divisors

$$D = D_1 - D_2, \quad E = E_1 - E_2.$$

By bilinearity of the intersection pairing it suffices to discuss the computation of $i_v(\overline{D_1}, \overline{E_1})$.

For now we assume that the points on \mathcal{C}_v where $\overline{D_1}$ and $\overline{E_1}$ intersect all lie on a single affine piece \mathcal{C}^a of \mathcal{C} . Suppose that $\mathcal{C}^a = \text{Spec}(\mathcal{O}[x_1, \dots, x_n]/J)$ for some ideal J and that $I_{\overline{D_1}}$ (resp. $I_{\overline{E_1}}$) represents $\overline{D_1}$ (resp. $\overline{E_1}$) on \mathcal{C} . Then we have

$$(3.4) \quad i_v(\overline{D_1}, \overline{E_1}) = \text{length}_{\mathcal{O}_{\mathcal{C}^a}} \left((\mathcal{O}[x_1, \dots, x_n]/J + I_{\overline{D_1}} + I_{\overline{E_1}})_{(\pi_v)} \right).$$

The computation of the right hand side of (3.4) can be reduced to (essentially) the computation of Gröbner bases over $\text{Spec}(\mathcal{O})$, cf. [26, Algorithm 1].

In order to find the representing ideals $I_{\overline{D_1}}$ and $I_{\overline{E_1}}$ the strategy is to first find representing ideals for the Zariski closures of D_1 and E_1 on $\overline{\mathcal{C}}$ and lift these to \mathcal{C} through the blow-up process. We can guarantee that the intersection of these closures has support only in one of the two standard affine pieces of $\overline{\mathcal{C}}$ by decomposing D_1 and E_1 into prime divisors over a finite extension M of K_v ; in the present case of hyperelliptic curves this is possible using factorisation of univariate polynomials over M as described in [26, §5.3].

So it remains to discuss how to represent Zariski closures of prime divisors on \mathcal{C} on the affine piece

$$\mathcal{C}^a = \text{Spec}(\mathcal{O}[x, y]/(y^2 - f(x))).$$

If $D_1 = \sum_{i=1}^d (P_i)$ is reduced, then we can use a representing ideal

$$(a(x), y - b(x)),$$

where $a(x) \in \mathcal{O}[x]$ has roots $x(P_1), \dots, x(P_d)$ and does not vanish modulo π_v and $b(x) \in \mathcal{O}[x]$ does not vanish modulo π_v and satisfies $y(P_i) = b(x(P_i))$ for $i \in \{1, \dots, d\}$. This is commonly referred to as Mumford representation, see [27, 3.19]. In particular, if $D_1 = (P_1)$, where $P_1 \in C(K_v)$, then we can take the ideal

$$(x - x(P_1), y - y(P_1)).$$

The other case we have to consider is the case $D_1 = (P_1) + (P_1^-)$, where P_1 is defined over an extension of K_v of degree at most 2 and P_1^- is the image of P_1 under the hyperelliptic involution. Then we can simply use the ideal

$$(x - x(P_1)).$$

For Step (3) we refer to [26, §4.5]. In brief, we first compute the intersection matrix M of \mathcal{C}_v and its Moore-Penrose pseudoinverse M^+ . Suppose that the special fiber \mathcal{C}_v is given by $\sum_{i=0}^m n_i \Gamma_i$, where $\Gamma_0, \dots, \Gamma_m$ are the irreducible components of \mathcal{C}_v . We also need the vectors $s(D)$ and $s(E)$ of intersection multiplicities, where

$$s(D) = (n_0 \cdot i_v(\overline{D}, \Gamma_0), \dots, n_m \cdot i_v(\overline{D}, \Gamma_m))^T;$$

and $s(E)$ is defined similarly. These can be computed using the techniques introduced in Step (2) above. Then we have

$$i_v(\Phi(D), \overline{E}) = -s(E)^T \cdot M^+ \cdot s(D).$$

We have not discussed how we can compute a finite set U of places of K such that we have $h_v(D, E) = 0$ for all $v \notin U$. This is discussed in [26, §4.2, §5.2]. Here we only mention that it suffices to compute U containing all bad places (that is, all places v such that $\text{ord}_v(2 \cdot \text{disc}(f)) > 0$) and all places v such that D and E have nontrivial common support modulo π_v . The latter can be computed as follows, where $D = D_1 - D_2$ and $E = E_1 - E_2$ are as above.

We only discuss the computation of all v such that D_1 and E_1 have nontrivial common support modulo π_v . Let I_{D_1} and I_{E_1} denote representing ideals of the Zariski closures of D_1 and E_1 on the affine piece

$$\text{Spec}(\mathcal{O}_K[x, y]/(y^2 - f(x)))$$

of the Zariski closure of X over $\text{Spec}(\mathcal{O}_K)$. We assume that \mathcal{O}_K is Euclidean; the general case can be reduced to this situation using a straightforward trick discussed in [26, §4.2]. If B is a Gröbner basis of the ideal

$$(y^2 - f(x)) + I_{D_1} + I_{E_1},$$

over \mathcal{O}_K , then B contains a unique element $q \in \mathcal{O}_K$ (cf. [26, Lemma 4.3]). Factoring (q) yields a set of places containing all places such that D_1 and E_1 have nontrivial common support on the reduction of the affine piece given by $y^2 = f(x)$. Repeating this process for the other standard affine piece $y^2 = x^{2g-2}f(1/x)$ yields all places v such that D_1 and E_1 intersect nontrivially modulo π_v .

3.2. Computing p -adic heights above p . We now describe the local contribution at a place $v \mid p$.

Definition 3.4. Let $D, E \in \text{Div}^0(C)$ have disjoint support. The local height pairing at a place $v \mid p$ is given by the following Coleman integral:

$$h_v(D, E) := t_v \left(\int_E \omega_D \right),$$

where t_v is the trace map determined by the decomposition of ℓ_v (see (3.1)), and ω_D is a differential associated to D .

We start by reviewing the construction of ω_D . Let $T(K_v)$ denote the subgroup of differentials on C of the third kind. We are interested in a particular subgroup of $T(K_v)$ whose elements are the logarithmic differentials, i.e., those of the form $\frac{df}{f}$ for $f \in K_v(C)^*$. We denote this subgroup as $T_l(K_v)$. Letting $H_{\text{dR}}^{1,0}(C/K_v)$ denote the space of holomorphic differentials and $A = \text{Pic}^0(C)$, we have the short exact sequence

$$0 \longrightarrow H_{\text{dR}}^{1,0}(C/K_v) \longrightarrow T(K_v)/T_l(K_v) \longrightarrow A(K_v) \longrightarrow 0.$$

This sequence has a natural identification with the K_v -rational points of an exact sequence of commutative algebraic groups over K_v :

$$0 \longrightarrow H_{\text{dR}}^{1,0}(C/K_v) \longrightarrow \mathcal{U} \longrightarrow A \longrightarrow 0,$$

where \mathcal{U} is the universal extension of A by a vector group and $H_{\text{dR}}^{1,0}(C/K_v) \cong \mathbb{G}_a^g$.

Now as K_v is p -adic, we will make use of the fact that we have a logarithmic homomorphism defined on an open subgroup of the points of any commutative p -adic Lie group, G , to the points of its Lie algebra $\text{Lie}(G)$. When $G = \mathcal{U}$ or A , the open subgroup on which the logarithm converges has finite index, so the homomorphism can be uniquely extended to the entire group. We denote this extension as $\log_{\mathcal{U}}$ or \log_A , respectively. Since the logarithm is functorial and equal to the identity on $H_{\text{dR}}^{1,0}(C/K_v)$, we have the following:

Proposition 3.5. *There is a canonical homomorphism*

$$\Psi : T(K_v)/T_l(K_v) \longrightarrow H_{\text{dR}}^1(C/K_v)$$

which is the identity on differentials of the first kind and makes the following diagram commute:

$$\begin{array}{ccccccc} 0 & \longrightarrow & H_{\text{dR}}^{1,0}(C/K_v) & \longrightarrow & \mathcal{U}(K_v) & \longrightarrow & A(K_v) \longrightarrow 0 \\ & & \parallel & & \downarrow \Psi = \log_{\mathcal{U}} & & \downarrow \log_A \\ 0 & \longrightarrow & H_{\text{dR}}^{1,0}(C/K_v) & \longrightarrow & H_{\text{dR}}^1(C/K_v) & \longrightarrow & H^1(C, \mathcal{O}_{C/K_v}) \longrightarrow 0 \end{array}$$

Note that the map Ψ takes a differential of the third kind on C to a differential of the second kind modulo exact differentials, sending log differentials to 0. It can be extended to a linear map from the K_v -vector space of all differentials on C/K_v to $H_{dR}^1(C/K_v)$ by writing an arbitrary differential ν as a linear combination $\nu = \sum \alpha_i \mu_i + \gamma$, where μ_i is of the third kind, $\alpha_i \in \overline{K_v}$, and γ is of the second kind on C . We then define $\Psi(\nu) = \sum \alpha_i \Psi(\mu_i) + [\gamma]$.

Now recall that we have at our disposal the complementary subspace $W = W_v$. It allows us to isolate a canonical form ω_D with residue divisor D as follows:

Definition 3.6. Let $D \in \text{Div}^0(C)$. Then ω_D is the unique form of the third kind satisfying

$$\text{res}(\omega_D) = D, \quad \Psi(\omega_D) \in W.$$

3.3. Computing the global p -adic height. Using the material in Sections 3.1 and 3.2, we may now give an algorithm to compute global p -adic heights on Jacobians of hyperelliptic curves.

Algorithm 3.7 (Global p -adic height pairing).

Input:

- Genus g hyperelliptic curve X over \mathbb{Q} of the form $y^2 = f(x)$, with f separable, $\deg f = 2g+1$,
- Prime p of good ordinary reduction for X ,
- Divisors $D, E \in \text{Div}^0(X)$ with disjoint support.

Output:

- Global p -adic height pairing $h(D, E) = \sum_v h_v(D, E)$

Algorithm:

(1) **Heights away from p**

(a) **Find relevant places.** Compute the following set U of non-archimedean places of K :

$$U = \{v : v \mid 2 \text{disc}(f)\} \cup \{v : \text{supp}(D \bmod v) \cap \text{supp}(E \bmod v) \neq \emptyset\}.$$

(b) **Local computations.** For each $v \in U$ go through the following steps.

- (i) **Regular models.** Compute a desingularization \mathcal{C} of the Zariski closure of $X \times_K K_v$ over $\mathcal{O} = \mathcal{O}_v$ in the strong sense.
- (ii) **Ideal representatives.** Write $D = D_1 - D_2$ and $E = E_1 - E_2$, where D_i, E_j are effective and find representatives $I_{\overline{D}_i}$ and $I_{\overline{E}_j}$ of the Zariski closures $\overline{D}_i, \overline{E}_j$ of D_i, E_j , respectively, on an affine piece of \mathcal{C} containing $\text{supp}(D) \cap \text{supp}(E)$.
- (iii) **Horizontal data.** Compute $i_v(\overline{D}_i, \overline{E}_j)$ for $i, j \in \{1, 2\}$ using (3.4).
- (iv) **Vertical data.** Compute the Moore-Penrose pseudoinverse M^+ of the intersection matrix of the special fiber $\mathcal{C}_v = \sum_{i=0}^m n_i \Gamma_i$ and for $H \in \{D, E\}$, the vectors

$$s(H) = (n_0 \cdot i_v(\overline{H}, \Gamma_0), \dots, n_m \cdot i_v(\overline{H}, \Gamma_m))^T.$$

(v) **Local height pairing.** Let k_v be the residue field at v and set

$$h_v(D, E) = \left(s(E) \cdot M^+ \cdot s(D)^T - \sum_{i,j} i_v(\overline{D}_i, \overline{E}_j) \right) \cdot \log(\#k_v).$$

(c) **Global height pairing away from p .** Compute $\sum_{v \nmid p} h_v(D, E)$.

(2) **Height above p**

(a) **From D to ω_D .** Choose ω a differential of the third kind with $\text{Res}(\omega) = D$ and compute $\log(\omega) = \Psi(\omega)$ for ω . Using the decomposition

$$H_{dR}^1(C/K_v) \simeq H_{dR}^{1,0}(C/K_v) \oplus W,$$

write

$$\log(\omega) = \eta + \log(\omega_D),$$

where η is holomorphic, and $\log(\omega_D) \in W$. Now, using this holomorphic component η , we have

$$\omega_D := \omega - \eta.$$

(b) **Coleman integration**

- (i) ...of a holomorphic differential. Compute $\int_E \eta$, as in [4].
- (ii) ...of a meromorphic differential. Let ϕ be a p -power lift of Frobenius and set $\alpha := \phi^* \omega - p\omega$. Write $E = \sum_i E_i$, where $E_i = (R_i) - (S_i)$ for points R_i, S_i on X . Then for β_i a differential with residue divisor E_i , we compute

$$\begin{aligned} \int_E \omega &= \sum_i \int_{E_i} \omega \\ &= \sum_i \frac{1}{1-p} \left(\Psi(\alpha) \cup \Psi(\beta_i) + \sum \text{Res} \left(\alpha \int \beta_i \right) - \int_{\phi(S_i)}^{S_i} \omega - \int_{R_i}^{\phi(R_i)} \omega \right), \end{aligned}$$

as described in [3].

- (c) **Height pairing above p .** Subtract the integrals to recover the pairing at p :

$$h_p(D, E) = \int_E \omega_D = \int_E \omega - \int_E \eta.$$

- (3) **Global p -adic height pairing.** Return the sum of 1(c) and 2(c).

Remark 3.8. Note that our current implementation of Algorithm 3.7 further assumes, in Step 2(b)(ii), that $R_i, S_i \in C(\mathbb{Q}_p)$.

3.4. Computing the p -adic regulator. In this section, we explain how we use Algorithm 3.7, in practice, to compute the p -adic regulator of A/\mathbb{Q} , where A is a Jacobian surface of a curve X/\mathbb{Q} of genus 2 and p is a prime such that A has good ordinary reduction at p .

Suppose that $P, Q \in A(\mathbb{Q})$ are distinct and that we want to compute the p -adic height pairing of P and Q . If we can find representatives $D_1 = (P_1) - (P_2)$ and $D_2 = (Q_1) - (Q_2)$ of P and Q , respectively, where $P_1, P_2, Q_1, Q_2 \in X(\mathbb{Q})$ are all distinct, then we can simply apply Algorithm 3.7 directly to compute $h_p(D_1, D_2)$.

However, in many situations, it is not possible to find representatives of P and Q whose support consists of \mathbb{Q} -rational points. We can still compute the p -adic height pairing if we can find representatives $D_1, D_2 \in \text{Div}^0(X)(\mathbb{Q})$ of P and Q , respectively, such that

$$D_1 \times_{\mathbb{Q}} \mathbb{Q}_p = (P_1) + (P_2) - (R) - (R^-),$$

$$D_2 \times_{\mathbb{Q}} \mathbb{Q}_p = (Q_1) + (Q_2) - (S) - (S^-),$$

where $P_1, P_2, Q_1, Q_2, R, S \in C(\mathbb{Q}_p)$ are pairwise distinct. It is explained in Section 3.1 how to find ideal representations of the positive and negative parts of D_1 and D_2 , respectively, which is all we need to compute the local height pairings away from p . The latter is very similar to the computation of canonical real-valued height pairings on Jacobians of hyperelliptic curves as discussed in [26] and has been implemented in **Magma**.

If we want to compute the p -adic height pairing of P with itself, then we simply compute minus the p -adic height pairing of P with $-P$ using the techniques discussed above.

Remark 3.9. In principle this algorithm can be generalized immediately to hyperelliptic curves over \mathbb{Q} of arbitrary genus, with minor subtleties if the genus is odd and the degree is even. See the discussion in [26]. However, to find the p -adic regulator precisely (and not only up to a rational square), we first need a set of generators for $A(\mathbb{Q})/A(\mathbb{Q})_{\text{tors}}$. Given generators of a finite index subgroup of $A(\mathbb{Q})/A(\mathbb{Q})_{\text{tors}}$, a general algorithm for this computation is presented by Stoll in [44], but currently it is only feasible if the rank is zero or X has genus 2 (using current work in progress due to Stoll this can be extended to genus 3). Hence we can only hope to compute the p -adic regulator up to a rational square in general.

Remark 3.10. It is useful to note that in order to compute the p -adic regulator in the genus 2 case, we need not work with generators of the free part of the Mordell-Weil group itself. Indeed, if we have a set of points generating a subgroup G of finite index, then we can easily compute the index of G by computing and comparing the real-valued regulators of G and of $A(\mathbb{Q})/A(\mathbb{Q})_{\text{tors}}$, see Remark 3.9. Since the p -adic height is quadratic, it suffices to compute the p -adic regulator of G in order to deduce the p -adic regulator. This helps in finding points with representatives of the required form.

Remark 3.11. Suppose that X is hyperelliptic and defined over a number field K . Then we can still compute the p -adic regulator exactly as above if all completions K_v at places $v \mid p$ satisfy $K_v \cong \mathbb{Q}_p$.

Finally, following [43], we note that the p -adic regulator has a natural normalization from Iwasawa theory, coming from the choice of topological generator γ . This is done so that the global p -adic height depends only on the choice of isomorphism $\Gamma \rightarrow \mathbb{Z}_p$, instead of on the \mathbb{Z}_p -extension. This normalization is carried out by dividing $h(P_i, P_j)$ by $\log_p(\kappa(\gamma))$, or, alternatively, since the p -adic regulator involves a basis of dimension r , by taking

$$\text{Reg}_\gamma(A) = \frac{\text{Reg}_p(A)}{(\log_p(\kappa(\gamma)))^r}.$$

4. EVIDENCE FOR RANK 2 JACOBIANS OF GENUS 2 CURVES

As we now have algorithms to compute the p -adic regulator and p -adic L -series, we proceed to verify Conjecture 1.4 for specific abelian varieties, using BSD data from [13, Table 2]. We take as our list of candidate modular abelian varieties A those appearing in [13] of rank 2.

We were able to find generators represented by divisors whose support consists only of \mathbb{Q} -rational points for each of the rank 2 Jacobians taken from [13] except for the one with level 167. Hence we used the easier first approach outlined in Section 3.4 to compute the p -adic regulator for all Jacobians except for the one associated to level 167.

In order to compute the special values $\mathcal{L}_p^*(A, 0)$, we used an implementation in Sage of the algorithm outlined in Section 2.6. Previously, we had used Algorithm 3.7 obtaining fewer digits of precision. The results agreed up to the precision obtained using the latter.

Table 4.1 is taken from [13] and contains minimal models (in the sense of [19]) for each curve from [13] whose Jacobian variety has Mordell-Weil rank 2 over \mathbb{Q} , as well as the corresponding level N .

The data presented in this section proves the following:

Theorem 4.1. *Assume that for the Jacobians of all curves in Table 4.1 the Shafarevich-Tate group over \mathbb{Q} is 2-torsion. Then Conjecture 1.4 is satisfied up to the respective precision specified in the tables below for the Jacobians of all curves in Table 4.1 at all good ordinary $p < 100$ satisfying the hypotheses of our algorithms.*

Remark 4.2. The assertion that all Shafarevich-Tate groups are 2-torsion for these abelian varieties follows from the classical conjecture of Birch and Swinnerton-Dyer by [13].

For our algorithms, we take the integral models in [13, Table 1] and do a change of coordinates to obtain the corresponding models of the form $y^2 = f(x)$. We record both models in Table 4.1

N	$(g(x), h(x))$ for integral model	$f(x)$ for $y^2 = f(x)$ model
67	$(x^5 - x, x^3 + x + 1)$	$x^6 + 4x^5 + 2x^4 + 2x^3 + x^2 - 2x + 1$
73	$(-x^5 - 2x^3 + x, x^3 + x^2 + 1)$	$x^6 - 2x^5 + x^4 - 6x^3 + 2x^2 + 4x + 1$
85	$(x^4 + x^3 + 3x^2 - 2x + 1, x^3 + x^2 + x)$	$x^6 + 2x^5 + 7x^4 + 6x^3 + 13x^2 - 8x + 4$
93	$(-2x^5 + x^4 + x^3, x^3 + x^2 + 1)$	$x^6 - 6x^5 + 5x^4 + 6x^3 + 2x^2 + 1$
103	$(x^5 + x^4, x^3 + x^2 + 1)$	$x^6 + 6x^5 + 5x^4 + 2x^3 + 2x^2 + 1$
107	$(x^4 - x^2 - x - 1, x^3 + x^2 + 1)$	$x^6 + 2x^5 + 5x^4 + 2x^3 - 2x^2 - 4x - 3$
115	$(2x^3 + x^2 + x, x^3 + x + 1)$	$x^6 + 2x^4 + 10x^3 + 5x^2 + 6x + 1$
125,A	$(x^5 + 2x^4 + 2x^3 + x^2 - x - 1, x^3 + x + 1)$	$x^6 + 4x^5 + 10x^4 + 10x^3 + 5x^2 - 2x - 3$
133,B	$(-x^5 + x^4 - 2x^3 + 2x^2 - 2x, x^3 + x^2 + 1)$	$x^6 - 2x^5 + 5x^4 - 6x^3 + 10x^2 - 8x + 1$
147	$(x^5 + 2x^4 + x^3 + x^2 + 1, x^3 + x^2 + x)$	$x^6 + 6x^5 + 11x^4 + 6x^3 + 5x^2 + 4$
161	$(x^3 + 4x^2 + 4x + 1, x^3 + x + 1)$	$x^6 + 2x^4 + 6x^3 + 17x^2 + 18x + 5$
165	$(x^5 + 2x^4 + 3x^3 + x^2 - 3x, x^3 + x^2 + x)$	$x^5 + 5x^4 - 168x^3 + 1584x^2 - 10368x + 20736$
167	$(-x^5 - x^3 - x^2 - 1, x^3 + x + 1)$	$x^6 - 4x^5 + 2x^4 - 2x^3 - 3x^2 + 2x - 3$
177	$(x^5 + x^4 + x^3, x^3 + x^2 + 1)$	$x^6 + 6x^5 + 5x^4 + 6x^3 + 2x^2 + 1$
188	$(x^5 - x^4 + x^3 + x^2 - 2x + 1, 0)$	$x^5 - x^4 + x^3 + x^2 - 2x + 1$
191	$(-x^3 + x^2 + x, x^3 + x + 1)$	$x^6 + 2x^4 - 2x^3 + 5x^2 + 6x + 1$

TABLE 4.1. Levels, integral models $y^2 + h(x)y = g(x)$, simplified models $y^2 = f(x)$

Let us recall what is known about computing the quantities appearing on the right side of Equation 1.2 which we have not addressed so far. As described in [13], the order of the torsion subgroups and the Tamagawa numbers are computable. For the Jacobians of the curves in Table 4.1, we list these values, taken from [13, Table 2], in Table 4.2. While no general algorithm has yet been developed and implemented to compute the order of the Shafarevich-Tate group $\text{III}(A/\mathbb{Q})$ for the Jacobians of each of the curves in Table 4.1, the conjectural order $\text{III}^?$ of the group is also given, conditional on the classical BSD conjecture 1.1 (and equal to the order of $\text{III}(A/\mathbb{Q})[2]$).

Remark 4.3. There is a general approach to computing $\text{III}(A/\mathbb{Q})$ for the rank 2 Jacobians in Table 4.1, which is to use Heegner points and Kolyvagin’s Euler system to give an explicit upper bound, then compute the remaining Selmer groups. It would be an interesting project to systematically develop this approach, by generalizing [15, 25] to this new setting.

Table 4.3 below provides the local height pairings away from p for $N \neq 167$. The global generators for $A(\mathbb{Q})/A(\mathbb{Q})_{\text{tors}}$ that we used are given as divisor classes $[P - Q], [R - S]$, where $P, Q, R, S \in C(\mathbb{Q})$. Points at infinity are denoted by ∞_a , where a is equal to y/x^3 evaluated at ∞_a . The heights list has three entries giving the nontrivial local height pairings $h_v((P) - (Q), (R) - (S))$, $h_v((P) - (Q), (-Q) - (-P))$ and $h_v((R) - (S), (-S) - (-R))$ for $v \neq p$. For two divisors D and E , this data is returned as a list of pairs $[v, d_v]$, where v is a prime and $h_v(D, E) = d_v \cdot \log_p(v)$.

Remark 4.4. The generators given for $N = 125, A$ are actually generators for an index 2 subgroup of $A(\mathbb{Q})/A(\mathbb{Q})_{\text{tors}}$, since an actual set of generators for the full group $A(\mathbb{Q})/A(\mathbb{Q})_{\text{tors}}$ whose support solely consisted of non-Weierstrass points was not readily available. For $N = 167$, we had to use generators (of finite index subgroups) represented by divisors with pointwise \mathbb{Q}_p -rational support; see Section 3.4.

N	c_v 's	$ A(\mathbb{Q})_{\text{tors}} $	III?
67	1	1	1
73	1	1	1
85	4,2	2	1
93	4,1	1	1
103	1	1	1
107	1	1	1
115	4,1	1	1
125,A	1	1	1
133,B	1,1	1	1
147	2,2	2	1
161	4,1	1	1
165	4,2,2	4	1
167	1	1	1
177	1,1	1	1
188	9,1	1	1
191	1	1	1

TABLE 4.2. BSD data for rank 2 Jacobians of genus 2 curves

N	global generators for $A(\mathbb{Q})/A(\mathbb{Q})_{\text{tors}}$	heights $[[v, h_v]]$
67	$[(-1, 0) - \infty_{-1}], [(0, -1) - \infty_0]$	$[], [], []$
73	$[(-1, -2) - \infty_{-1}], [(0, -1) - \infty_0]$	$[], [[3, 1]], []$
85	$[(-1, -2) - \infty_{-1}], [(1, -4) - \infty_0]$	$[[2, -1]], [[5, \frac{1}{2}]], [[5, \frac{1}{2}]]$
93	$[(-1, -2) - \infty_{-1}], [(1, -3) - \infty_0]$	$[], [[3, \frac{1}{2}]], [[3, \frac{1}{2}]]$
103	$[(-1, -1) - \infty_{-1}], [(0, -1) - \infty_0]$	$[], [], []$
107	$[(-1, -1) - \infty_{-1}], [(1, -2) - \infty_0]$	$[], [], []$
115	$[(1, -4) - \infty_{-1}], [(-2, 2) - \infty_0]$	$[[3, -1]], [[5, \frac{1}{2}]], [[5, \frac{1}{2}]]$
125,A	$[(-1, 0) - \infty_{-1}], [(1, -4) - \infty_0]$	$[[2, -1]], [], [[5, 1]]$
133,B	$[(0, -1) - \infty_{-1}], [(1, -2) - \infty_0]$	$[], [], []$
147	$[(-1, -1) - \infty_{-1}], [(-3, 7) - \infty_0]$	$[[2, -1]], [[3, \frac{1}{2}]], [[7, \frac{1}{2}]]$
161	$[(1, -5) - \infty_{-1}], [(\frac{2}{3}, -3) - \infty_0]$	$[], [[7, \frac{1}{2}]], [[5, 1]], [7, \frac{1}{2}]$
165	$[(-8, -528) - (0, -144)], [(8, 80) - (0, 144)]$	$[[2, 2], [3, -\frac{1}{2}]], [[2, -2], [11, \frac{1}{2}], [3, \frac{3}{2}]],$ $[[2, -2], [5, \frac{1}{2}], [3, \frac{1}{2}]]$
177	$[(0, 0) - \infty_{-1}], [(-\frac{2}{3}, -\frac{7}{27}) - \infty_0]$	$[[3, 1]], [], [[3, -2], [17, 1]]$
188	$[(0, 1) - \infty_{-1}], [(-1, -1) - (2, 5)]$	$[[2, 1]], [[2, \frac{2}{3}]], [[2, \frac{2}{3}], [5, 1]]$
191	$[(0, -1) - \infty_{-1}], [(-2, 10) - \infty_0]$	$[], [], [[11, 1]]$

TABLE 4.3. Global generators and intersection data

For the computation of the special values $\mathcal{L}_p(A, 0)$, we need the normalization factor δ^+ , so we have to find a fundamental discriminant $D > 0$ such that for some good ordinary p_0 we have $\gcd(p_0 N, D) = 1$ and the analytic rank of A_ψ is zero, where ψ is the quadratic character associated to $\mathbb{Q}(\sqrt{D})$. See Subsection 2.4. The real period Ω_A^+ for our Jacobians can be found in [13]; there it was computed using the observation that (ω_1, ω_2) as in Remark 2.11 is a basis of integral 1-forms for all abelian varieties we consider. It is not difficult to show that the corresponding fact also holds for

all A_ψ and hence, using Remark 2.11, we found that $\eta_\psi = 1$ in all 16 cases. We list, for each level, the quantities needed to find δ^+ in Table 4.4.

N	D	η_ψ	p_0	$[0]_{A_\psi}^+$	$\frac{\eta_\psi \cdot L(A_\psi, 1)}{D \cdot \Omega_A^+}$	δ^+	$c_v(A_\psi)'s$	$ A_\psi(\mathbb{Q})_{\text{tors}} $	$\text{III}_\psi?$
67	5	1	19	16	4	1/4	1,1	1	4
73	5	1	11	16	4	1/4	1,1	1	4
85	61	1	41	64	16	1/4	4,2,8	2	1
93	5	1	11	-16	4	-1/4	4,1,1	1	1
103	5	1	11	16	4	1/4	1,1	1	4
107	5	1	19	16	4	1/4	1,1	1	4
115	89	1	11	64	16	1/4	4,1,4	1	1
125,A	17	1	19	16	4	1/4	1,1	1	4
133,B	5	1	29	-16	4	-1/4	1,1,1	1	4
147	5	1	31	-16	4	-1/4	2,2,2	2	2
161	53	1	11	64	16	1/4	4,1,4	1	1
165	89	1	17	64	16	1/4	4,2,2,16	4	1
167	5	1	31	-16	4	-1/4	1,1	1	4
177	5	1	19	16	4	1/4	1,1,1	1	4
188	233	1	19	144	36	1/4	9,1,4	1	1
191	33	1	31	16	4	1/4	1,1	1	4

TABLE 4.4. Rank zero twist data

For good measure, we also verified:

Proposition 4.5. *The classical (and hence, for all primes p of good ordinary reduction, the p -adic) Birch and Swinnerton-Dyer conjecture holds for all 16 twists A_ψ in Table 4.4 under the assumption that $\text{III}(A_\psi/\mathbb{Q})$ is 2-torsion.*

Proof. See Table 4.4, noting that $\text{III}_\psi?$ is equal to $|\text{III}(A_\psi/\mathbb{Q})[2]|$. □

Remark 4.6. For the computation of the Tamagawa numbers we used [7, Theorem 1.17]. Suppose that $v \mid D$, but that v does not divide the conductor of A . Then the twisted curve X_ψ has bad reduction at v , but acquires good reduction over a quadratic extension. The classification of Namikawa and Ueno [28] shows that in this case X_ψ must have reduction type $[I_{0^*}^*_{-0-0}]$ at v . Since the geometric component group of the Néron model is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$ for this reduction type, we always have $c_v(A_\psi) \mid 16$.

The tables below show the specific primes p and precision $O(p^n)$ for each level N for which we have tested Conjecture 1.4.

Remark 4.7. A note on our models and choices of primes. Since our p -adic heights algorithm requires that the curve be given by an odd degree model, for each curve $y^2 = g(x)$, we consider those good ordinary primes p for which $g(x)$ has a \mathbb{Q}_p -rational zero and do another change of coordinates to obtain the odd model $y^2 = f(x)$, with $f(x) \in \mathbb{Q}_p[x]$. We compute the p -adic regulators and p -adic L -values for these primes.

4.1. $N = 67$. We have the following data:

p -adic regulator $\text{Reg}_p(A)$	p -adic L -value	p -adic multiplier $\epsilon_p(A)$
$905422 + O(7^8)$	$4616447 + O(7^8)$	$953283 + O(7^8)$
$655636176 + O(13^8)$	$3718847 + O(13^8)$	$121846702 + O(13^8)$
$6411910349 + O(17^8)$	$490126740 + O(17^8)$	$2996208382 + O(17^8)$
$1955457580 + O(19^8)$	$205789013 + O(19^8)$	$6722090086 + O(19^8)$
$6490501114813 + O(37^9)$	$1520740814200 + O(37^8)$	$1763856795912 + O(37^8)$
$119112862323467 + O(41^9)$	$6899026979535 + O(41^8)$	$604530321123 + O(41^8)$
$231768637543452 + O(43^9)$	$11662319738050 + O(43^8)$	$11664993765232 + O(43^8)$
$258343847102710 + O(47^9)$	$6617527122585 + O(47^8)$	$21577206386081 + O(47^8)$
$7291679100956850 + O(59^9)$	$72703739307529 + O(59^8)$	$77184936742982 + O(59^8)$
$6048812062982476 + O(61^9)$	$174305066216353 + O(61^8)$	$133406272889885 + O(61^8)$
$53277934412195075 + O(73^9)$	$552479201354189 + O(73^8)$	$460739420635942 + O(73^8)$
$9278983589215557 + O(79^9)$	$88027589402068 + O(79^8)$	$801037408797804 + O(79^8)$
$157708559779041510 + O(83^9)$	$1578704504708054 + O(83^8)$	$162512920516158 + O(83^8)$

4.2. $N = 73$. We have the following data:

p -adic regulator $\text{Reg}_p(A)$	p -adic L -value	p -adic multiplier $\epsilon_p(A)$
$163731997 + O(11^8)$	$183868925 + O(11^8)$	$192773925 + O(11^8)$
$482988818 + O(13^8)$	$522787644 + O(13^8)$	$757562196 + O(13^8)$
$51174691892 + O(23^8)$	$46581832325 + O(23^8)$	$48224542827 + O(23^8)$
$553299007790 + O(31^8)$	$440555494391 + O(31^8)$	$850258335981 + O(31^8)$
$5421948177967 + O(41^8)$	$5077531013725 + O(41^8)$	$5384419950679 + O(41^8)$
$38176784853304 + O(59^8)$	$63020796753579 + O(59^8)$	$113039802800992 + O(59^8)$
$70602302343232 + O(61^8)$	$139895606364222 + O(61^8)$	$79733480381568 + O(61^8)$
$433639741922965 + O(71^8)$	$576931954734067 + O(71^8)$	$8989266238661 + O(71^8)$
$589304115938460 + O(83^8)$	$347866087087015 + O(83^8)$	$720001059253854 + O(83^8)$
$6769596692483671 + O(97^8)$	$4269348271 + O(97^5)$	$3993521258998096 + O(97^8)$

4.3. $N = 85$. We have the following data:

p -adic regulator $\text{Reg}_p(A)$	p -adic L -value	p -adic multiplier $\epsilon_p(A)$
$1015073423894 + O(37^8)$	$167411116045 + O(37^8)$	$1002150510104 + O(37^8)$
$6819810980339 + O(41^8)$	$7975900636623 + O(41^8)$	$7153783865856 + O(41^8)$
$8962714100713 + O(53^8)$	$1069648287223 + O(53^7)$	$44683460285079 + O(53^8)$
$43568329449 + O(61^6)$	$3136884016567 + O(61^7)$	$72019680061615 + O(61^8)$
$119416997911215 + O(73^8)$	$683019204724944 + O(73^8)$	$32602153132641 + O(73^8)$
$1942338381733272 + O(89^8)$	$3482744225118281 + O(89^8)$	$1038134293650945 + O(89^8)$
$5147606270477176 + O(97^8)$	$2836855197 + O(97^5)$	$3784121167774074 + O(97^8)$

4.4. $N = 93$. We have the following data:

p -adic regulator $\text{Reg}_p(A)$	p -adic L -value	p -adic multiplier $\epsilon_p(A)$
$185741420 + O(11^8)$	$151839057 + O(11^8)$	$11051656 + O(11^8)$
$405483221 + O(13^8)$	$670790176 + O(13^8)$	$230057694 + O(13^8)$
$43885519955 + O(23^8)$	$26161319539 + O(23^8)$	$47769373949 + O(23^8)$
$336788503314 + O(29^8)$	$484038257980 + O(29^8)$	$222828561623 + O(29^8)$
$1678741468628 + O(37^8)$	$2569674002391 + O(37^8)$	$1378603735422 + O(37^8)$
$5324074002210 + O(43^8)$	$8725984878581 + O(43^8)$	$3160248767946 + O(43^8)$
$16824305598488 + O(47^8)$	$15669575995471 + O(47^8)$	$8286455636222 + O(47^8)$
$4960862919215 + O(53^8)$	$49317038818954 + O(53^8)$	$23178143892193 + O(53^8)$
$143070222270789 + O(61^8)$	$92506965732666 + O(61^8)$	$122923764909639 + O(61^8)$
$279322082363042 + O(67^8)$	$74111413499770 + O(67^8)$	$180555937022120 + O(67^8)$
$430169136747961 + O(73^8)$	$471513912864315 + O(73^8)$	$411163460552347 + O(73^8)$
$1384453915387035 + O(79^8)$	$1232301086171477 + O(79^8)$	$503819572894975 + O(79^8)$
$2228621109604011 + O(83^8)$	$1304530016876211 + O(83^8)$	$1071794429225898 + O(83^8)$
$1081659147745931 + O(89^8)$	$1330994142123689 + O(89^8)$	$1518075886594725 + O(89^8)$

4.5. $N = 103$. We have the following data:

p -adic regulator $\text{Reg}_p(A)$	p -adic L -value	p -adic multiplier $\epsilon_p(A)$
$147377758 + O(11^8)$	$86486502 + O(11^8)$	$192773925 + O(11^8)$
$489193484 + O(13^8)$	$67428377 + O(13^8)$	$337691501 + O(13^8)$
$15204606664 + O(19^8)$	$10638300382 + O(19^8)$	$12173049603 + O(19^8)$
$66216995216 + O(23^8)$	$18109392006 + O(23^8)$	$45043095109 + O(23^8)$
$5372718408 + O(29^8)$	$76731347688 + O(29^8)$	$12536647436 + O(29^8)$
$6799091682040 + O(41^8)$	$4391281006909 + O(41^8)$	$5303120857798 + O(41^8)$
$23467041445332 + O(47^8)$	$5937816898560 + O(47^8)$	$1847891549858 + O(47^8)$
$9449958206985 + O(53^8)$	$6585582284426 + O(53^8)$	$47071170371848 + O(53^8)$
$55788681659810 + O(59^8)$	$58416917952322 + O(59^8)$	$134523844728309 + O(59^8)$
$180708198470076 + O(61^8)$	$86273076603078 + O(61^8)$	$91320952633362 + O(61^8)$
$304798054862709 + O(71^8)$	$23644536785282 + O(71^8)$	$318837731560077 + O(71^8)$
$651632900917334 + O(73^8)$	$128186925484 + O(73^6)$	$86431680403618 + O(73^8)$
$1422073004111088 + O(79^8)$	$162819364440040 + O(79^8)$	$1353067258168647 + O(79^8)$
$2204776989584744 + O(83^8)$	$290525162365 + O(83^6)$	$1489257165084816 + O(83^8)$
$3419478873681093 + O(89^8)$	$13722104837501 + O(89^7)$	$2011257469143583 + O(89^8)$
$5187359554281130 + O(97^8)$	$588713923936 + O(97^6)$	$291254315420391 + O(97^8)$

4.6. $N = 107$. We have the following data:

p -adic regulator $\text{Reg}_p(A)$	p -adic L -value	p -adic multiplier $\epsilon_p(A)$
$100037184 + O(13^8)$	$381034778 + O(13^8)$	$725504508 + O(13^8)$
$5164824485 + O(17^8)$	$2251756830 + O(17^8)$	$6548185060 + O(17^8)$
$4948122310 + O(19^8)$	$410682533 + O(19^8)$	$11770828305 + O(19^8)$
$2233155353996 + O(37^8)$	$782254360600 + O(37^8)$	$499167048517 + O(37^8)$
$7693933727093 + O(41^8)$	$1126806110759 + O(41^8)$	$941047246375 + O(41^8)$
$1985728518871 + O(43^8)$	$11350309489829 + O(43^8)$	$1490080422844 + O(43^8)$
$9236325503676 + O(47^8)$	$9352977397857 + O(47^8)$	$3877324130340 + O(47^8)$
$66592510503713 + O(59^8)$	$126498662012390 + O(59^8)$	$66521146158463 + O(59^8)$
$73605475872145 + O(61^8)$	$67998854641813 + O(61^8)$	$149495311709314 + O(61^8)$
$215631855830774 + O(67^8)$	$276136144242399 + O(67^8)$	$300204582979356 + O(67^8)$
$235988007934369 + O(71^8)$	$4203263257242 + O(71^7)$	$297538516047502 + O(71^8)$
$1405009654786451 + O(79^8)$	$1425538781612665 + O(79^8)$	$637219753066297 + O(79^8)$
$966246807067004 + O(83^8)$	$29073683 + O(83^5)$	$122301722091732 + O(83^8)$

4.7. $N = 115$. We have the following data:

p -adic regulator $\text{Reg}_p(A)$	p -adic L -value	p -adic multiplier $\epsilon_p(A)$
$151819184 + O(11^8)$	$96031694 + O(11^8)$	$55470083 + O(11^8)$
$6070540659 + O(17^8)$	$2602174031 + O(17^8)$	$2479111430 + O(17^8)$
$443043366998 + O(37^8)$	$3207000318071 + O(37^8)$	$518402902203 + O(37^8)$
$10506890337861 + O(43^8)$	$466034248434 + O(43^8)$	$3160248767946 + O(43^8)$
$25938666299194 + O(53^8)$	$43404652273198 + O(53^8)$	$24704105954182 + O(53^8)$
$68828469915327 + O(59^8)$	$15822514736163 + O(59^8)$	$112268718282797 + O(59^8)$
$117125015025879 + O(61^8)$	$99513360280408 + O(61^8)$	$144234417021077 + O(61^8)$
$117261157211649 + O(67^8)$	$369365142758789 + O(67^8)$	$388573100762289 + O(67^8)$
$38346420175144 + O(79^8)$	$1042744621946608 + O(79^8)$	$856522414733559 + O(79^8)$
$232154244720909 + O(83^8)$	$1238796074898239 + O(83^8)$	$2232922964727286 + O(83^8)$
$3680613169329886 + O(89^8)$	$1982664616252635 + O(89^8)$	$1447736508567520 + O(89^8)$
$337111037730418 + O(97^8)$	$5523549952859660 + O(97^8)$	$5537610452725212 + O(97^8)$

4.8. $N = 125, A$. We have the following data:

p -adic regulator $\text{Reg}_p(A)$	p -adic L -value	p -adic multiplier $\epsilon_p(A)$
$298562498 + O(13^8)$	$592894408 + O(13^8)$	$337691501 + O(13^8)$
$6712555657 + O(19^8)$	$7153379737 + O(19^8)$	$7352726322 + O(19^8)$
$28761182485 + O(23^8)$	$19244567041 + O(23^8)$	$47769373949 + O(23^8)$
$1610334394992 + O(37^8)$	$2619837199442 + O(37^8)$	$518402902203 + O(37^8)$
$5827125727855 + O(47^8)$	$2438975823319 + O(47^8)$	$20137488978024 + O(47^8)$
$43827481404730 + O(53^8)$	$12237145144494 + O(53^8)$	$45444073360562 + O(53^8)$
$934069839446 + O(59^8)$	$138331812786050 + O(59^8)$	$119463235911829 + O(59^8)$
$94940897306587 + O(61^8)$	$86820693223899 + O(61^8)$	$134545325721836 + O(61^8)$
$344652595573416 + O(67^8)$	$285200220171958 + O(67^8)$	$55395450190703 + O(67^8)$
$494778091759992 + O(73^8)$	$211635131306627 + O(73^8)$	$338214791799846 + O(73^8)$
$911058348384486 + O(83^8)$	$15062127863580 + O(83^7)$	$1695835531921770 + O(83^8)$
$3812663593637783 + O(89^8)$	$140584030153 + O(89^6)$	$3229221353736449 + O(89^8)$
$7743507247513256 + O(97^8)$	$72751227747664 + O(97^7)$	$6602401135477806 + O(97^8)$

4.9. $N = 133, B$. We have the following data:

p -adic regulator $\text{Reg}_p(A)$	p -adic L -value	p -adic multiplier $\epsilon_p(A)$
$4554714851 + O(17^8)$	$1400369830 + O(17^8)$	$1530767973 + O(17^8)$
$482641533 + O(29^6)$	$224834369110 + O(29^8)$	$188246220652 + O(29^8)$
$285247284517 + O(31^8)$	$644745508559 + O(31^8)$	$65426082523 + O(31^8)$
$873461875052 + O(41^8)$	$5913841764921 + O(41^8)$	$5173622706020 + O(41^8)$
$6395433286380 + O(43^8)$	$5250591893580 + O(43^8)$	$7173815953060 + O(43^8)$
$40174155934745 + O(53^8)$	$9436443664 + O(53^6)$	$47071170371848 + O(53^8)$
$388303423009987 + O(67^8)$	$74275805470 + O(67^6)$	$287829738202699 + O(67^8)$
$582542046575002 + O(73^8)$	$47404160292 + O(73^6)$	$214334244118640 + O(73^8)$
$997934987934019 + O(79^8)$	$1692929332309 + O(79^7)$	$85649658584845 + O(79^8)$
$337083794306147 + O(83^8)$	$8815903470 + O(83^6)$	$1446666792043837 + O(83^8)$
$3826161118964265 + O(89^8)$	$689438763 + O(89^5)$	$1571471061650586 + O(89^8)$

4.10. $N = 147$. We have the following data:

p -adic regulator $\text{Reg}_p(A)$	p -adic L -value	p -adic multiplier $\epsilon_p(A)$
$434194800 + O(13^8)$	$772553365 + O(13^8)$	$69777210 + O(13^8)$
$3085885399 + O(19^8)$	$14351355419 + O(19^8)$	$10124513344 + O(19^8)$
$57105870 + O(23^6)$	$56314647135 + O(23^8)$	$77688619426 + O(23^8)$
$598807495296 + O(31^8)$	$500890389807 + O(31^8)$	$226083261470 + O(31^8)$
$1255556858069 + O(37^8)$	$728534804896 + O(37^8)$	$925099803678 + O(37^8)$
$3028914438423 + O(43^8)$	$5310811645878 + O(43^8)$	$1448245155768 + O(43^8)$
$21722415097178 + O(53^8)$	$32574036544128 + O(53^8)$	$14098536063957 + O(53^8)$
$9696531871680 + O(61^8)$	$147051772023912 + O(61^8)$	$127085340697404 + O(61^8)$
$252460432397529 + O(67^8)$	$2933215623449 + O(67^7)$	$15805729099128 + O(67^8)$
$319985315705867 + O(71^8)$	$4744056079140 + O(71^7)$	$454718387048106 + O(71^8)$
$696485497462517 + O(73^8)$	$75645384726 + O(73^6)$	$263081220212640 + O(73^8)$
$1036811888178773 + O(79^8)$	$965207536 + O(79^5)$	$74020902743243 + O(79^8)$
$4273472549945572 + O(97^8)$	$6770845150 + O(97^5)$	$7422648274246094 + O(97^8)$

4.11. $N = 161$. We have the following data:

p -adic regulator $\text{Reg}_p(A)$	p -adic L -value	p -adic multiplier $\epsilon_p(A)$
$171933135 + O(11^8)$	$104178769 + O(11^8)$	$48803991 + O(11^8)$
$16676191757 + O(19^8)$	$8396822512 + O(19^8)$	$10186228540 + O(19^8)$
$3000539180980 + O(37^8)$	$2959738471101 + O(37^8)$	$1378603735422 + O(37^8)$
$4799012913812 + O(43^8)$	$820015420 + O(43^6)$	$7358928540810 + O(43^8)$
$33038825747471 + O(53^8)$	$14752347930 + O(53^6)$	$37415160388754 + O(53^8)$
$144048375212404 + O(59^8)$	$67829338510607 + O(59^8)$	$113039802800992 + O(59^8)$
$989091293021 + O(61^8)$	$62763431617869 + O(61^8)$	$191252449121304 + O(61^8)$
$93625125465306 + O(67^8)$	$43269028077 + O(67^6)$	$228681540167106 + O(67^8)$
$372742847896101 + O(79^8)$	$16260012523515 + O(79^7)$	$1380060506871347 + O(79^8)$
$133689266642605 + O(83^8)$	$27328857470 + O(83^6)$	$1997163923487638 + O(83^8)$
$109602346601919 + O(89^8)$	$3775670578 + O(89^5)$	$404117712562583 + O(89^8)$
$4449889265258731 + O(97^8)$	$8056056109 + O(97^5)$	$3796862465389610 + O(97^8)$

4.12. $N = 165$. We have the following data:

p -adic regulator $\text{Reg}_p(A)$	p -adic L -value	p -adic multiplier $\epsilon_p(A)$
$2478665 + O(7^9)$	$988615 + O(7^8)$	$2047938 + O(7^8)$
$7577669996 + O(13^9)$	$546478360 + O(13^8)$	$19120487 + O(13^8)$
$1345832 + O(17^5)$	$115518752 + O(17^8)$	$6743866153 + O(17^8)$
$317314039860 + O(19^9)$	$15454527827 + O(19^8)$	$16701261693 + O(19^8)$
$1197529401836 + O(23^9)$	$21430827992 + O(23^8)$	$32283075894 + O(23^8)$
$182820405709 + O(29^9)$	$462793840863 + O(29^8)$	$167834932128 + O(29^8)$
$30402585606264 + O(37^9)$	$145763317789 + O(37^8)$	$1905855970461 + O(37^8)$
$300867423531184 + O(41^9)$	$4638175450295 + O(41^8)$	$7243944162192 + O(41^8)$
$453491841293220 + O(43^9)$	$10502890759714 + O(43^8)$	$981850330755 + O(43^8)$
$841500704008115 + O(47^9)$	$22177682954670 + O(47^8)$	$15840901508219 + O(47^8)$
$108480654690546 + O(53^9)$	$812837848921 + O(53^7)$	$17925543534180 + O(53^8)$
$5924946879989069 + O(59^9)$	$2021593887077 + O(59^7)$	$32899436516884 + O(59^8)$
$11004676059690151 + O(61^9)$	$1114772875983 + O(61^7)$	$102536167075224 + O(61^8)$
$6402333518135195 + O(67^9)$	$1539009404714 + O(67^7)$	$15805729099128 + O(67^8)$
$18266464992713450 + O(71^9)$	$98457973781 + O(71^6)$	$34536869719889 + O(71^8)$
$42183534718264644 + O(73^9)$	$6514036760733 + O(73^7)$	$39739465931437 + O(73^8)$
$1224455456912234 + O(79^8)$	$1812891052 + O(79^5)$	$186442021878008 + O(79^8)$
$124036966428761339 + O(83^9)$	$203487283131 + O(83^6)$	$1504086404024377 + O(83^8)$
$243696118400513337 + O(89^9)$	$2097535192 + O(89^5)$	$1826662988317474 + O(89^8)$
$635540819872824429 + O(97^9)$	$1063985237 + O(97^5)$	$4391966065852909 + O(97^8)$

4.13. $N = 167$. We have the following data:

p -adic regulator $\text{Reg}_p(A)$	p -adic L -value	p -adic multiplier $\epsilon_p(A)$
$19432714 + O(7^9)$	$2251 + O(7^4)$	$307185 + O(7^8)$
$13117611 + O(13^7)$	$666390377 + O(13^8)$	$526042526 + O(13^8)$
$1908862518313 + O(17^{10})$	$2314174880 + O(17^8)$	$5234654956 + O(17^8)$
$2053675284265 + O(19^{10})$	$7656154501 + O(19^8)$	$14340680958 + O(19^8)$
$27719111127295 + O(23^{10})$	$41736439730 + O(23^8)$	$16647712571 + O(23^8)$
$405640880151858 + O(31^{10})$	$714765172682 + O(31^8)$	$358709025654 + O(31^8)$
$57769565310991429 + O(53^{10})$	$19704952386 + O(53^6)$	$17681237786119 + O(53^8)$
$501328316424338015 + O(59^{10})$	$64487204069600 + O(59^8)$	$140344643451642 + O(59^8)$
$1243828341260907954 + O(71^{10})$	$56573288611 + O(71^6)$	$557648531014830 + O(71^8)$
$2079988387733147685 + O(73^{10})$	$4104591 + O(73^4)$	$759308640111719 + O(73^8)$
$20365783254113182401 + O(89^{10})$	$5065696436 + O(89^5)$	$1447017073110591 + O(89^8)$
$67990777180272953115 + O(97^{10})$	$23364634 + O(97^4)$	$6376229493766338 + O(97^8)$

4.14. $N = 177$. We have the following data:

p -adic regulator $\text{Reg}_p(A)$	p -adic L -value	p -adic multiplier $\epsilon_p(A)$
$1072267 + O(7^8)$	$1192 + O(7^4)$	$507488 + O(7^8)$
$9772408 + O(19^6)$	$2558009183 + O(19^8)$	$11268267357 + O(19^8)$
$27690468499 + O(23^8)$	$51308343838 + O(23^8)$	$3788873485 + O(23^8)$
$141718660962 + O(29^8)$	$391909937451 + O(29^8)$	$65127401733 + O(29^8)$
$265288097732 + O(31^8)$	$167635394515 + O(31^8)$	$519021947371 + O(31^8)$
$1019326123826 + O(37^8)$	$2370016933013 + O(37^8)$	$1021993916814 + O(37^8)$
$952644023485 + O(41^8)$	$5888249521909 + O(41^8)$	$5919384948361 + O(41^8)$
$21867793727731 + O(47^8)$	$3399186192198 + O(47^8)$	$18039627327365 + O(47^8)$
$54813744728211 + O(61^8)$	$136070004398022 + O(61^8)$	$149495311709314 + O(61^8)$
$374976464608823 + O(73^8)$	$92506712920 + O(73^6)$	$469524064138469 + O(73^8)$
$2024750045809193 + O(83^8)$	$1537698302 + O(83^6)$	$2034477952337988 + O(83^8)$

4.15. $N = 188$. We have the following data:

p -adic regulator $\text{Reg}_p(A)$	p -adic L -value	p -adic multiplier $\epsilon_p(A)$
$5623044 + O(7^8)$	$1259 + O(7^4)$	$507488 + O(7^8)$
$4478725 + O(11^7)$	$150222285 + O(11^8)$	$143254320 + O(11^8)$
$775568547 + O(13^8)$	$237088204 + O(13^8)$	$523887415 + O(13^8)$
$1129909080 + O(17^8)$	$6922098082 + O(17^8)$	$4494443586 + O(17^8)$
$14409374565 + O(19^8)$	$15793371104 + O(19^8)$	$4742010391 + O(19^8)$
$31414366115 + O(23^8)$	$210465118 + O(23^8)$	$45043095109 + O(23^8)$
$2114154456754 + O(37^8)$	$1652087821140 + O(37^8)$	$1881820314237 + O(37^8)$
$6279643012659 + O(41^8)$	$2066767021277 + O(41^8)$	$4367414685819 + O(41^8)$
$9585122287133 + O(43^8)$	$3309737400961 + O(43^8)$	$85925017348 + O(43^8)$
$3328142761956 + O(53^8)$	$5143002859 + O(53^6)$	$6112104707558 + O(53^8)$
$17411023818285 + O(59^8)$	$7961878705 + O(59^6)$	$98405729721193 + O(59^8)$
$102563258757138 + O(61^8)$	$216695090848 + O(61^7)$	$137187998566490 + O(61^8)$
$26014679325501 + O(67^8)$	$7767410995 + O(67^6)$	$38320151289262 + O(67^8)$
$490864897182147 + O(71^8)$	$16754252742 + O(71^6)$	$530974572239623 + O(71^8)$
$689452389265311 + O(73^8)$	$193236387 + O(73^5)$	$162807895476311 + O(73^8)$
$878760549863821 + O(79^8)$	$1745712500 + O(79^5)$	$1063642669147985 + O(79^8)$
$2070648686579466 + O(83^8)$	$2888081539 + O(83^5)$	$1103760059074178 + O(83^8)$
$3431343284115672 + O(89^8)$	$1591745960 + O(89^5)$	$1012791564080640 + O(89^8)$
$4259144286293285 + O(97^8)$	$21828881 + O(97^4)$	$6376229493766338 + O(97^8)$

4.16. $N = 191$. We have the following data:

p -adic regulator $\text{Reg}_p(A)$	p -adic L -value	p -adic multiplier $\epsilon_p(A)$
$4195478 + O(7^8)$	$1867 + O(7^4)$	$1638463 + O(7^8)$
$43495803539 + O(23^8)$	$62365909362 + O(23^8)$	$47598354917 + O(23^8)$
$276478270993 + O(31^8)$	$411081898951 + O(31^8)$	$611200443823 + O(31^8)$
$7847912037610 + O(43^8)$	$1839263047933 + O(43^8)$	$10085036614653 + O(43^8)$
$3701160666066 + O(47^8)$	$16594732090932 + O(47^8)$	$9836262988784 + O(47^8)$
$19837992635361 + O(53^8)$	$121641372 + O(53^5)$	$22289116823061 + O(53^8)$
$207820830309704 + O(71^8)$	$80098460638243 + O(71^8)$	$318837731560077 + O(71^8)$
$105659818394179 + O(73^8)$	$278456920 + O(73^5)$	$160255667550084 + O(73^8)$
$4330286071100495 + O(97^8)$	$12214648 + O(97^4)$	$1683523428082670 + O(97^8)$

5. EVIDENCE FOR A TWIST OF RANK 4

In this section, we present evidence for Conjecture 1.4 on a rank 4 twist of a rank 0 modular abelian surface for the primes 29, 61 and 79. Let $X = X_0(31)$. According to [14], an affine equation for X is given by

$$y^2 = (x^3 - 2x^2 - x + 3) \cdot (x^3 - 6x^2 - 5x - 1).$$

The Jacobian A of X has rank zero over \mathbb{Q} .

We search for quadratic twists of high rank by searching among quadratic twists ψ of small conductor D for some A_ψ whose complex L -series seems to vanish at $s = 1$ up to order at least 4. This is the case for $D = -47$. We then use a 2-descent on A_ψ as implemented in *Magma* to find that the rank is at most 4. Searching for \mathbb{Q} -rational points on A_ψ of small height quickly reveals subgroups of rank 4, such as the groups G_p described below, thus proving that the rank A_ψ over \mathbb{Q} is indeed 4.

Using [7, Theorem 1.17] we find that the potentially nontrivial Tamagawa numbers are $c_{31}(A_\psi) = 1$ and $c_{47}(A_\psi) = 16$. Moreover, the torsion subgroup is trivial as is the 2-torsion of $\text{III}(A_\psi/\mathbb{Q})$. Since the divisors supported in \mathbb{Q} -rational points of X_ψ do not generate a subgroup of finite index, we compute the p -adic regulator for $p \in \{29, 61, 79\}$ using the second method outlined in Section 3.4. Namely, for each p we find a finite index subgroup G_p of $A_\psi(\mathbb{Q})/A_\psi(\mathbb{Q})_{\text{tors}}$ generated by the classes of divisors D_1, \dots, D_4 such that each D_i has pointwise \mathbb{Q}_p -rational support. It is then enough to compute the p -adic regulator of G_p to find the p -adic regulator of $A_\psi(\mathbb{Q})/A_\psi(\mathbb{Q})_{\text{tors}}$.

The generators we used are given in Table 5.1 in Mumford representation, along with the index of G_p .

p	index	generators of G_p
29	2	$[x^2 - 7/2x + 49/16, 581/16x - 1305/32], [x^2 - 2x - 1/2, -47/2x],$ $[x^2 - 5/3x + 5/6, 47/18x - 517/18], [x^2 - 19/3x - 11/4, -517/36x - 47/12]$
61	4	$[x^2 - 7/2x + 49/16, 581/16x - 1305/32], [x^2 - 5x + 11/2, -235/2x + 423/2],$ $[x^2 - 5x - 7/3, 235/3x + 94/3], [x^2 - 5/3x + 5/6, -47/18x + 517/18]$
79	4	$[x^2 - 7/2x + 49/16, 581/16x - 1305/32], [x^2 - x - 1/3, -47/3x],$ $[x^2 - 3x - 5/3, 149/3x + 82/3], [x^2 - 19/7x + 3/7, -1363/49x - 564/49]$

TABLE 5.1. Indices and generators, $N = 31$ twisted by $D = -47$

In order to compute the special values of the p -adic L -series, we need to find out the correct normalization factor δ^- of the minus modular symbol map associated to A . The twist A_χ of A by

the quadratic character χ associated to $\mathbb{Q}(\sqrt{-19})$ has rank 0 over \mathbb{Q} . Comparing $[0]_{A_\psi}^+ = -4$ to $\frac{L(A_\chi, 1)}{\Omega_{A_\chi}^+} = 1$, we find that $\delta^- = -\frac{1}{4}$.

For the latter computation, we used that for a minimal equation of X_χ , a basis of the integral 1-forms on A_χ is given by (ω_1, ω_2) as in Remark 2.11. Since the corresponding fact also holds for A , we find that $\eta_\chi = 1$ using [19].

The data presented in this section proves:

Proposition 5.1. *Assume that $\text{III}(A_\psi/\mathbb{Q})$ consists entirely of 2-torsion, and that the conjectural order of $\text{III}(A_\psi/\mathbb{Q})$ is 1 (numerically it is 1.0000000... to as many digits as we care to compute). Then Conjecture 1.4 is satisfied for the twist A_ψ of $J_0(31)$ of rank 4 for the primes 29, 61 and 79.*

The special values of the p -adic L -series, the p -adic regulators and the p -adic multipliers for $p \in \{29, 61, 79\}$ are given in the following table:

p -adic regulator $\text{Reg}_p(A)$	p -adic L -value	p -adic multiplier $\epsilon_p(A)$
$351486231941615978 + O(29^{12})$	$202402009906 + O(29^8)$	$423952915488 + O(29^8)$
$1650697608489237057465 + O(61^{12})$	$4326648666405 + O(61^8)$	$10267186717780 + O(61^8)$
$8155329946924028539010 + O(79^{12})$	$1513185184992411 + O(79^8)$	$1431106352547896 + O(79^8)$

Remark 5.2. Assume that $\text{III}(A_\chi/\mathbb{Q})$ consists entirely of 2-torsion. Then we also verified the classical (and hence for good ordinary primes p the p -adic) conjecture of Birch and Swinnerton-Dyer for the rank 0 twist A_χ , since all Tamagawa numbers, the order of the torsion subgroup and the order of $\text{III}(A_\chi/\mathbb{Q})[2]$ are easily seen to be equal to 1.

REFERENCES

- [1] A. Agashe, K. Ribet, and W. A. Stein. The Manin constant. *Pure Appl. Math. Q.*, 2(2, part 2):617–636, 2006. <http://wstein.org/papers/ars-manin/>.
- [2] A. Agashe and W. A. Stein. Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero. *Math. Comp.*, 74(249):455–484 (electronic), 2005. With an appendix by J. Cremona and B. Mazur, <http://wstein.org/papers/shacomp/>.
- [3] J. S. Balakrishnan and A. Besser. Computing local p -adic height pairings on hyperelliptic curves. *IMRN*, 2012(11):2405–2444, 2012.
- [4] J. S. Balakrishnan, R. W. Bradshaw, and K. S. Kedlaya. Explicit Coleman integration for hyperelliptic curves. In G. Hanrot, F. Morain, and E. Thomé, editors, *Algorithmic Number Theory*, volume 6197 of *Lecture Notes in Computer Science*, pages 16–31. Springer, 2010.
- [5] D. Bernardi and B. 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(3):227–232, 1993.
- [6] A. Besser. The p -adic height pairings of Coleman-Gross and of Nekovář. In *Number Theory*, volume 36 of *CRM Proceedings & Lecture Notes*, pages 13–25. American Mathematical Society, 2004.
- [7] S. Bosch and Q. Liu. Rational points of the group of components of a Néron model. *Manuscripta Math*, 98:275–293, 1999.
- [8] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3–4):235–265, 1997. Computational algebra and number theory (London, 1993).
- [9] D. Bump, S. Friedberg, and J. Hoffstein. Eisenstein series on the metaplectic group and nonvanishing theorems for automorphic L -functions and their derivatives. *Ann. of Math. (2)*, 131(1):53–127, 1990.
- [10] J. Coates. On p -adic L -functions. *Astérisque*, (177-178):Exp. No. 701, 33–59, 1989. Séminaire Bourbaki, Vol. 1988/89.
- [11] R. F. Coleman. The universal vectorial bi-extension and p -adic heights. *Invent. Math.*, 103(3):631–650, 1991.
- [12] R. F. Coleman and B. H. Gross. p -adic heights on curves. In *Algebraic Number Theory – in honor of K. Iwasawa*, volume 17 of *Advanced Studies in Pure Mathematics*, pages 73–81, 1989.

- [13] E. V. Flynn, F. Leprévost, E. F. Schaefer, W. A. Stein, M. Stoll, and J. L. Wetherell. Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves. *Math. Comp.*, 70(236):1675–1697 (electronic), 2001.
- [14] S. D. Galbraith. Equations for modular curves. *Oxford Ph.D. thesis*, 1996.
- [15] 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.*, 78:2397–2425, 2009. <http://wstein.org/papers/bsdalg/>.
- [16] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*. Springer-Verlag, New York, 2000. An introduction.
- [17] P. Hriljac. Heights and Arakelov’s intersection theory. *Amer. J. Math.*, 107:23–38, 1985.
- [18] K. Kato. p -adic Hodge theory and values of zeta functions of modular forms. *Astérisque*, (295):ix, 117–290, 2004. Cohomologies p -adiques et applications arithmétiques. III.
- [19] Q. Liu. Conducteur et discriminant minimal de courbes de genre 2. *Compositio Math.*, 94(1):51–79, 1994.
- [20] Q. Liu. Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète. *Trans. Amer. Math. Soc.*, 348(11):4577–4610, 1996.
- [21] Q. Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002.
- [22] B. Mazur, W. Stein, and J. Tate. Computation of p -adic heights and log convergence. *Doc. Math.*, (Extra Vol.):577–614 (electronic), 2006.
- [23] B. Mazur and J. Tate. Canonical height pairings via biextensions. In *Arithmetic and geometry, Vol. I*, volume 35 of *Progr. Math.*, pages 195–237. Birkhäuser Boston, Boston, MA, 1983.
- [24] B. Mazur, J. Tate, and J. Teitelbaum. On p -adic analogues of the conjectures of Birch and Swinnerton-Dyer. *Invent. Math.*, 84(1):1–48, 1986.
- [25] R. 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.
- [26] J. S. Müller. Computing canonical heights using arithmetic intersection theory. *Math. Comp.*, to appear. <http://arxiv.org/abs/1105.1719>.
- [27] D. Mumford. *Tata lectures on theta I*. Birkhäuser, Boston, second edition, 1990.
- [28] Y. Namikawa and K. Ueno. The complete classification of fibres in pencils of curves of genus two. *Manuscripta Math.*, 9:143–186, 1973.
- [29] J. Nekovář. On p -adic height pairings. In *Séminaire de Théorie des Nombres, Paris, 1990–91*, volume 108 of *Progr. Math.*, pages 127–202. Birkhäuser Boston, Boston, MA, 1993.
- [30] V. Pal. Periods of quadratic twists of elliptic curves. *Proc. Amer. Math. Soc.*, 140(5):1513–1525, 2012. With an appendix by A. Agashe.
- [31] B. Perrin-Riou. Arithmétique des courbes elliptiques et théorie d’Iwasawa. *Mém. Soc. Math. France (N.S.)*, (17):130, 1984.
- [32] B. Perrin-Riou. Fonctions L p -adiques, théorie d’Iwasawa et points de Heegner. *Bull. Soc. Math. France*, 115(4):399–456, 1987.
- [33] R. Pollack. On the p -adic L -function of a modular form at a supersingular prime. *Duke Math. J.*, 118(3):523–558, 2003.
- [34] R. Pollack and G. Stevens. Overconvergent modular symbols and p -adic L -functions. *Ann. Sci. Éc. Norm. Supér. (4)*, 44(1):1–42, 2011.
- [35] K. Rubin. The “main conjectures” of Iwasawa theory for imaginary quadratic fields. *Invent. Math.*, 103(1):25–68, 1991.
- [36] P. Schneider. p -adic height pairings. I. *Invent. Math.*, 69(3):401–409, 1982.
- [37] P. Schneider. p -adic height pairings. II. *Invent. Math.*, 79(2):329–374, 1985.
- [38] G. Shimura. On the factors of the jacobian variety of a modular function field. *J. Math. Soc. Japan*, 25:523–544, 1973.
- [39] G. Shimura. On the periods of modular forms. *Math. Ann.*, 229(3):211–221, 1977.
- [40] C. Skinner and D. Urban. The Iwasawa Main Conjecture for GL_2 . 2010. <http://www.math.columbia.edu/~7Urban/eurp/MC.pdf>.
- [41] W. A. Stein. *Modular Forms, A Computational Approach*, volume 79 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2007. With an appendix by Paul E. Gunnells, <http://wstein.org/books/modform/>.
- [42] W. A. Stein et al. *Sage Mathematics Software (Version 5.1)*. The Sage Development Team, 2012. <http://www.sagemath.org>.
- [43] W. A. Stein and C. Wuthrich. Computing Tate-Shafarevich groups of elliptic curves using Iwasawa theory. *Math. Comp.*, to appear. <http://wstein.org/papers/shark/shark.pdf>.
- [44] M. Stoll. On the height constant for curves of genus two. II. *Acta Arith.*, 104:165–182, 2002.

- [45] J. Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. In *Séminaire Bourbaki, Vol. 9*, pages Exp. No. 306, 415–440. Soc. Math. France, Paris, 1965/66. <http://wstein.org/papers/bib/tate-bsd.pdf>.
- [46] V. Vatsal. Canonical periods and congruence formulae. *Duke Math. J.*, 98(2):397–419, 1999.

JENNIFER S. BALAKRISHNAN, DEPARTMENT OF MATHEMATICS, HARVARD UNIVERSITY, 1 OXFORD STREET, CAMBRIDGE, MA 02138, USA

E-mail address: jen@math.harvard.edu

J. STEFFEN MÜLLER, DEPARTMENT OF MATHEMATICS, UNIVERSITÄT HAMBURG, BUNDESSTRASSE 55, 20146 HAMBURG, GERMANY

E-mail address: jan.steffen.mueller@uni-hamburg.de

WILLIAM A. STEIN, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WASHINGTON, SEATTLE, BOX 354350 WA 98195, USA

E-mail address: wstein@uw.edu