Heegner points on Mumford-Tate curves

M. Bertolini and H. Darmon

September 9, 2007

Contents

Let $E/\mathbb{Q}$ be a modular elliptic curve of conductor N, and let p be a prime number. In [MTT], Mazur, Tate and Teitelbaum formulate a p-adic analogue of the conjecture of Birch and Swinnerton-Dyer, relating the p-adic L-function of $E/\mathbb{Q}$ to certain arithmetic invariants of E, such as the order of its Shafarevich-Tate group, the rank of its Mordell-Weil group, and a regulator made from the canonical p-adic height pairing.

An intriguing and unexpected feature of their study is the phenomenon of "exceptional zeroes" that have no counterpart in the classical setting, and arise purely from the p-adic interpolation process. This phenomenon occurs only when E has split multiplicative reduction at p. In that case, the authors of [MTT] are led to conjecture that the order of vanishing of the p-adic L-function $L_p(E/\mathbb{Q}, s)$ is exactly one more than that of its complex counterpart, and that the difference between the classical and p-adic special values at $s = 1$ is accounted for by a somewhat mysterious factor (which they call the $\mathcal{L}$-invariant)

$$\mathcal{L} = \frac{\log q}{\mathrm{ord}_p q},$$

where q is Tate's p-adic period associated to E.

The p-adic L-function in [MTT] is defined (building on the work of Manin-Vishik and Amice-Velu) as a p-adic Mellin transform of a measure on the group $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) = \mathbb{Z}_p^*$ taking values in the module $H_1(E(\mathbb{C}), \mathbb{Z})$. This measure is constructed from so-called *modular symbols*. For more details on this construction, see [MTT].

Now, let K be a quadratic imaginary field of discriminant D, and let K_∞ be the compositum of all the ring class fields K_n of conductor p^n, which contains the anticyclotomic $\mathbb{Z}_p$-extension of K. By making a slight generalization of the constructions explained in [GZ] and [Gr2], we show how to associate to the data (N, K, p) a "Heegner distribution" on $G_\infty = \mathrm{Gal}(K_\infty/K)$ with values in $\mathrm{Pic}(X)$. Here X is a Shimura curve corresponding to a (definite or indefinite) quaternion algebra, whose definition depends on the data (N, K, p).

The Heegner distribution behaves formally like the p-adic L-function constructed from modular symbols. In particular it interpolates special values – or, sometimes, *first derivatives* – of the complex L-function $L(E/K, \chi, s)$ at $s = 1$, twisted by characters χ of G_∞. It seems natural to formulate generalizations of the Mazur-Tate-Teitelbaum conjectures for these Heegner distributions. We show that the "exceptional zero" phenomena also occur in the context of Heegner distributions, and that they lead to new insights into the arithmetic behaviour of Heegner points on Shimura curves.

Following Mazur, Tate and Teitelbaum, we say that we are in an *exceptional case* if E/K has split multiplicative reduction at a prime above p. Let $K_p = K \otimes \mathbb{Q}_p$, and $K_{n,p} = K_n \otimes \mathbb{Q}_p$. In the exceptional case the p-adic analytic uniformization of Tate:

$$\Phi_{Tate} : \mathbf{G}_{m/K_p} \longrightarrow E_{/K_p}$$

plays a key role in the formulation of the conjectures.

We say that we are in the *split* (resp. *non-split*) exceptional case if $p||N$ is split (resp. inert) in $K/\mathbb{Q}$. The split exceptional case resembles the exceptional zero situation studied by Mazur, Tate and Teitelbaum: in that case our conjecture expresses the p-adic periods of E in terms of the derivatives of the anti-cyclotomic p-adic L-function. The non-split exceptional case seems to have no direct analogue in the setting studied in [MTT], and offers the most surprises. For the convenience of the reader we will spend the rest of the introduction summarizing the main features of the non-split exceptional case.

The first unusual phenomenon that occurs in this setting is that the sign ϵ in the functional equation for the classical L-function $L(E/K, s)$, and the sign for the twisted L-function $L(E/K, \chi, s)$, where χ is a ramified character of finite order of G_∞, are *opposite*. The shape of the conjecture depends on the sign ϵ.

If $\epsilon = 1$, then $L(E/K, \chi, 1) = 0$ whenever χ is a ramified character of G_∞. The Birch Swinnerton-Dyer conjecture leads one to expect that the Mordell-Weil group $E(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ has corank at least one over the Iwasawa algebra $\mathbb{Z}_p[[G_\infty]]$ (i.e., its Pontryagin dual has rank at least one over $\mathbb{Z}_p[[G_\infty]]$). In this case one expects a systematic supply of algebraic points over the anticyclotomic tower. Indeed, a norm-compatible system of points $P_n \in E(K_n)$ can be obtained by a Heegner point construction, and it can be shown that these points satisfy

$$\mathrm{Norm}_{K_n/K}(P_n) = 0, \tag{1}$$

where the trace is taken on the Mordell-Weil group $E(K_n)$. Let $\tilde{P}_n \in K_{n,p}^*$ be elements such that $\Phi_{Tate}(\tilde{P}_n) = P_n$. Then, by equation (1), the element

$Q_n = \mathrm{Norm}_{K_{n,p}/K_p}(\tilde{P}_n)$ of K_p^* is a power of the Tate period q, and $\log_q(Q_n)$ is an integer which is well defined mod $(p+1)p^n$ (i.e., does not depend on the choice of lift $\tilde{P}_n$). Our conjecture predicts that

$$\log_q(Q_n)^2 \stackrel{?}{=} \begin{cases} 0 \text{ if } \#E(\mathbb{Q}) = \infty, \\ \#\underline{III}(E/K)m^2/\#E(\mathbb{Q})^2 \pmod{(p+1)p^n} \text{ otherwise,} \end{cases}$$

where m is an integer related to the bad reduction of E/K. Combining this with the classical Birch and Swinnerton-Dyer conjecture suggests a direct relation between the quantity $\log_q(Q_n)^2$ and the special value $L(E/K,1)$. Indeed in [BD4] we prove the formula:

$$\log_q(Q_n)^2 = \frac{L(E/K,1)\sqrt{D}}{\Omega}\delta \pmod{(p+1)p^n}, \tag{2}$$

where $\Omega = \int_{E(\mathbb{C})} \omega \wedge \bar{\omega}$ is the complex period attached to E and δ is a non-zero rational number which measures the difference between the degrees of the modular curve and a certain Shimura curve parametrization of E. The proof uses a mild generalization of a formula of Gross [Gr2] for the special value $L(E/K,1)$, and a precise recipe of Edixhoven [Ed] for the natural projection map to the group of connected components of the Néron models of Jacobians of Shimura curves. Equation (2) can be viewed simultaneously as an analogue of the Gross-Zagier formula [GZ] in a rigid analytic setting, and of a theorem of Greenberg-Stevens [GS] in an anticyclotomic setting. It can be used to prove the implication (for curves having a prime of multiplicative reduction):

$$L(E/\mathbb{Q},1) \neq 0 \text{ implies } E(\mathbb{Q}) \text{ finite.}$$

This statement was originally proved (for all modular elliptic curves) by Kolyvagin, building on the Gross-Zagier formula [GZ], and on non-vanishing results of Bump-Friedberg-Hoffstein [BFH] and Murty-Murty [MM]. Our proof does not appeal to the rather involved calculations of [GZ], but only to the simpler formula of [Gr2]. Furthermore, it does not require non-vanishing results for derivatives of L-series[1].

[1]The formula (2) and its proof also carry over, mutatis mutandis, to the more general context of eigenforms f of weight 2 and trivial Nebentypus character, and yields a proof of the implication $L(f,1) \neq 0 \Rightarrow A_f(\mathbb{Q})$ is finite, where A_f is the abelian variety in $J_0(N)$ "cut out" by f. Such an implication (for prime conductor) plays a key role in Merel's recent proof [Me] of the uniform boundedness conjecture.

Kolyvagin's approach required the choice of an auxiliary imaginary quadratic field K for which $L(E/K,1) = 0$ and $L'(E/K,1) \neq 0$. Our approach works directly with a field K for which $L(E/K,1) \neq 0$. If K is such a field, $\rho : \mathrm{Gal}(L/K) \longrightarrow \mathbb{C}^*$ is an anticyclotomic character of K of conductor prime to N, and $(E(L)\otimes\mathbb{C})^\rho$ is the ρ-eigenspace of $\mathrm{Gal}(L/K)$ acting on the Mordell-Weil group $E(L) \otimes \mathbb{C}$, then a twisted form of equation (2) combined with a direct generalization of Kolyvagin's argument explained in [BD1], yield a proof of the new result

$$L(E/K, \rho, 1) \neq 0 \Rightarrow \dim_{\mathbb{C}}(E(L) \otimes \mathbb{C})^\rho = 0, \tag{3}$$

for *semistable* elliptic curves over $\mathbb{Q}$. We can then establish (assuming an analytic non-vanishing hypothesis) that the Mordell-Weil groups $E(L_\infty)$ are finitely generated, for certain anticyclotomic $\mathbb{Z}_\ell$-extensions of K. The methods of [B2], building directly on Kolyvagin's theory, allowed one to exhibit pairs (E, L_∞) for which $E(L_\infty) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell$ could be proved to be of corank 1 over the Iwasawa algebra $\mathbb{Z}_\ell[[\mathrm{Gal}(L_\infty/K)]]$. The proof of formulas (2) and (3) and the above arithmetic applications are given in [BD4].

When $\epsilon = -1$, our conjecture predicts a p-adic analytic construction of a rational point on $E(K)$ in terms of the special values of the p-adic L-function $L_p(E/K)^2$. In fact, it suggests a precise recipe for computing the Heegner divisor class in the Jacobian of a Shimura curve associated to an indefinite quaternion algebra B ramified at p. In that case the Shimura curve is a *Mumford curve* and its Jacobian has purely toric reduction at p. We express the Heegner class as the image, via the Cerednik-Drinfeld p-adic uniformization map, of a p-adic limit of "special points" generalizing those defined in [Gr2], which belong to *another* Shimura curve related to the definite quaternion algebra obtained from B by Cerednik's interchange of invariants. We give a precise statement, and numerical evidence for the conjecture, in sec. 5.3. The calculations of this section suggest a reasonably practical, purely p-adic analytic algorithm for computing Heegner points arising from Shimura curve parametrizations, in terms of derivatives of p-adic L-functions. A proof of the main formula (conj. 5.6) of sec. 5.3 will be given in [BD5]. The main ingredients in this proof are the Cerednik-Drinfeld theory of p-adic uniformization

[2] This conjecture has the same flavour as a construction of Karl Rubin [Ru] for curves with complex multiplication. However, the settings are quite disjoint, since complex multiplication curves have integral j-invariants. It would be interesting to fit these two formulae into a common picture. In this connection, see also [PR]

of Shimura curves, and an explicit description of the p-adic Abel-Jacobi map for Mumford curves in terms of automorphy factors of p-adic theta-functions.

The first section of this paper contains a brief review of background material on quaternion algebras and Shimura curves. The second section explains the construction of Heegner points and the p-adic L function associated to certain Heegner distributions (which enters in the "left hand side" of our Birch Swinnerton-Dyer type conjecture) based on a mild generalization of ideas of Gross, Mazur, and others. The third section is devoted to the "right hand side": it introduces the p-adic regulator[3] associated to the extended Mordell-Weil group. The fourth section puts the two previous sections together and formulates the p-adic analogue of the Birch Swinnerton-Dyer conjecture. Finally, section 5 makes explicit some special cases and applications of our conjecture, and summarizes the evidence that we have gathered in their support.

1 Shimura curves

1.1 Quaternion algebras

We briefly recall some basic facts on the arithmetic of quaternion algebras over $\mathbb{Q}$. A good reference for this material, where all the results stated here are proved, often in greater generality, is [Vi].

Let $\hat{\mathbb{Z}} := \prod_{\ell\neq\infty} \mathbb{Z}_\ell$ be the profinite completion of $\mathbb{Z}$ and let $\hat{\mathbb{Q}} = \hat{\mathbb{Z}} \otimes \mathbb{Q}$ denote the ring of finite adèles. Let B be a quaternion algebra over $\mathbb{Q}$: it is a central simple algebra of rank 4, satisfying $B \otimes \mathbb{C} \simeq M_2(\mathbb{C})$. For each place ℓ of $\mathbb{Q}$ (including $\ell = \infty$), we let $B_\ell = B \otimes \mathbb{Q}_\ell$, and let $\hat{B} = B \otimes \hat{\mathbb{Q}}$ be the "adèlization" of B. If B_ℓ is isomorphic to the split algebra $\simeq M_2(\mathbb{Q}_\ell)$, we say that B is split at ℓ, and that it is ramified otherwise. In the latter case B_ℓ is isomorphic to the (unique, up to isomorphism) quaternion division algebra over $\mathbb{Q}_\ell$. By Hilbert's reciprocity law – due, in this special case, to Lagrange

[3]In the anti-cyclotomic situation, degeneracies in the height pairings tend to cause extra vanishing of a type not experienced in the original Mazur-Tate-Teitelbaum setting, where a conjecture of Schneider predicts that the p-adic height is always non degenerate. In certain cases, our regulator can vanish. A more satisfying definition of the p-adic regulator in the anticyclotomic context might build on the theory of "derived p-adic heights" developed elsewhere by the authors [BD3]. To lighten the exposition, we have avoided the machinery of derived heights.

– the set S of ramified places of B (possibly including ∞) is finite and has even cardinality. Conversely, given any set S of places of even cardinality, there is a unique quaternion algebra ramified exactly at the places of S. Let N^- be the product of all the finite primes in S. We say that B is indefinite if $B_\infty = B \otimes \mathbb{R}$ is isomorphic to $M_2(\mathbb{R})$, i.e., B is split at ∞, and that it is definite if B_∞ is isomorphic to the algebra of Hamilton quaternions, i.e,. B is ramified at ∞.

For each $\ell \notin S$, choose an isomorphism $\phi_\ell : B_\ell \longrightarrow M_2(\mathbb{Q}_\ell)$. The order $R_\ell = \phi_\ell^{-1}(M_2(\mathbb{Z}_\ell))$ is a maximal order of B_ℓ which depends on the choice of ϕ_ℓ. If ℓ is in S, then B_ℓ has a unique maximal order R_ℓ ([Vi], p. 34, lemme 1.5). Define the global order $R = R_{1,N^-}$ by

$$R = B \cap \prod_\ell R_\ell,$$

(where we have identified B with a subalgebra of $\hat{B}$ by the diagonal embedding). The order R is a maximal order of B. (Note that its definition depends on the choice of the isomorphisms ϕ_ℓ.) More generally, if N^+ is a (square-free) integer prime to the elements of S, we define an Eichler order R_{N^+,N^-} of level N^+ by

$$R_{N^+,N^-} = \left\{ x \in R \quad | \quad \phi_\ell(x) \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{\ell} \text{ for all } \ell | N^+ \right\},$$

and write $\hat{R}_{N^+,N^-} = R_{N^+,N^-} \otimes \hat{\mathbb{Z}} = \prod (R_{N^+,N^-} \otimes \mathbb{Z}_\ell)$.

A left ideal $I \subset R_{N^+,N^-}$ is an additive subgroup of R_{N^+,N^-} which is stable under left multiplication by elements of R_{N^+,N^-}, and is of rank 4 as a $\mathbb{Z}$-module.

Two left ideals I and J are said to be in the same *class* if there exists α in B^* such that $I\alpha = J$. The set of left ideal classes admits an adelic interpretation as the set of double cosets

$$\hat{R}^*_{N^+,N^-} \backslash \hat{B}^* / B^*.$$

(Cf. [Vi], p. 87.) The number of such left ideal classes depends very much on whether B is definite or indefinite.

Proposition 1.1 .

1. If B is an indefinite quaternion algebra, then $\#(\hat{R}^*_{N^+,N^-}\backslash\hat{B}^*/B^*) = 1$.

2. If B is a definite quaternion algebra, then $\#(\hat{R}^*_{N^+,N^-}\backslash\hat{B}^*/B^*) < \infty$.

Proof: This is a direct consequence of "strong approximation" ([Vi], p. 61, théorème 4.3, and p. 89, corollaire 5.7 (1)).

In all cases we let $h(R_{N^+,N^-})$ denote the number of left ideal classes for R_{N^+,N^-}; it is called the class number of R_{N^+,N^-}. Unlike the case for Dedekind domains, the left ideal classes do not form a group; also, the class number can be expressed by a simple closed formula, which shows in particular that its size is roughly $N/12$ in the definite case, where $N = N^+N^-$, and N^- is the product of the primes in S. (Cf. [Vi], p. 146, proposition 3.2.)

Orientations: If ℓ divides N^+, then there are exactly two distinct surjective algebra homomorphisms $R_{N^+,N^-} \otimes \mathbb{F}_\ell \longrightarrow \mathbb{F}_\ell$. If ℓ divides N^-, then there are exactly two distinct algebra homomorphisms $R_{N^+,N^-} \otimes \mathbb{F}_\ell \longrightarrow \mathbb{F}_{\ell^2}$. We fix a choice of such algebra homomorphisms

$$\mathfrak{o}_\ell^+ : R_{N^+,N^-} \otimes \mathbb{F}_\ell \longrightarrow \mathbb{F}_\ell, \quad \mathfrak{o}_\ell^- : R_{N^+,N^-} \otimes \mathbb{F}_\ell \longrightarrow \mathbb{F}_{\ell^2}.$$

The data $\mathfrak{o}_\ell^+$ (with $\ell|N^+$) and $\mathfrak{o}_\ell^-$ (with $\ell|N^-$) is called an *orientation* for R_{N^+,N^-}, and the order R_{N^+,N^-} equipped with this extra structure is sometimes called an *oriented Eichler order*. (Cf. [Ro].)

1.2 Homogeneous spaces

We define a homogenous space $\mathbb{P}$ on which the group B^* acts. This definition depends in an essential way on whether B is indefinite or definite.

Case 1: B is indefinite. We set

$$\mathbb{P} = \mathbb{P}_1(\mathbb{C}) - \mathbb{P}_1(\mathbb{R}) = \mathbb{C} - \mathbb{R}.$$

The isomorphism ϕ_∞ identifies B^*_∞ with $\mathbf{GL_2}(\mathbb{R})$; we let B^* act on $\mathbb{P}$ via the natural action of $\mathbf{GL_2}(\mathbb{R})$ on $\mathbb{P}$ by fractional linear transformations.

We observe (and this will be important for later constructions) that $\mathbb{P}$ can be identified with the set of algebra homomorphisms $\mathrm{Hom}(\mathbb{C}, B_\infty)$ in a natural way. For, any $f \in \mathrm{Hom}(\mathbb{C}, B_\infty)$ gives rise to a group action of $\mathbb{C}^*$ on $\mathbb{P}$. There are exactly two fixed points P^+ and P^- in $\mathbb{P}$ for this action. We order P^+ and P^- so that the induced action of $\mathbb{C}^*$ on the complex cotangent space $T^*_{P^+}(\mathbb{P})$ (resp. $T^*_{P^-}(\mathbb{P})$) is via the character $z \mapsto \bar{z}/z$ (resp. $z \mapsto z/\bar{z}$). The reader will check that this can always be done. To each $f \in \mathrm{Hom}(\mathbb{C}, B_\infty)$ we associate the fixed point $P^+ \in \mathbb{P}$. This sets up a bijection

$$\mathrm{Hom}(\mathbb{C}, B_\infty) \xrightarrow{\simeq} \mathbb{P}.$$

Case 2: B is definite. We let $\mathbb{P}$ denote the conic (curve of genus 0) defined over $\mathbb{Q}$ by:

$$\mathbb{P}(K) = \{x \in B \otimes K \quad | \quad \mathrm{Norm}(x) = \mathrm{trace}(x) = 0\},$$

for all $\mathbb{Q}$-algebras K. The group B^* acts naturally on $\mathbb{P}$ by conjugation, and this action is algebraic and defined over $\mathbb{Q}$. In fact, we have $\mathrm{Aut}(\mathbb{P}) = B^*$ canonically, as algebraic groups over $\mathbb{Q}$.

Exactly as in case 1, we identify $\mathrm{Hom}(\mathbb{C}, B_\infty)$ with $\mathbb{P}(\mathbb{C})$. In fact, if K is a quadratic imaginary field, then $\mathbb{P}(K)$ becomes identified with $\mathrm{Hom}(K, B)$, using the obvious recipe. For more details, see [Gr2], p. 131.

1.3 Shimura curves

Basic Reference: [Ro]. We recall the definition of the Shimura curves that we will use. For a nice treatment of this material (in a more general setting) the reader may consult [Ro].

Let $N = N^+N^-$ be a square free integer. Let B be the quaternion algebra ramified exactly at the primes dividing N^-, together with ∞, if N^- has an odd number of prime factors. Let R_{N^+,N^-} be the Eichler order defined as above. We associate to this data the open Shimura curve Y_{N^+,N^-}, as follows:

$$Y_{N^+,N^-} = \hat{R}^*_{N^+,N^-} \backslash (\hat{B}^* \times \mathbb{P})/B^*.$$

Using the remarks of sec. 1.2, we note that $Y_{N^+N^-}$ can also be identified with the space

$$Y_{N^+,N^-} = \hat{R}^*_{N^+,N^-} \backslash (\hat{B}^* \times \mathrm{Hom}(\mathbb{C}, B_\infty))/B^*,$$

where the action of B^* on $\mathrm{Hom}(\mathbb{C}, B_\infty)$ is by conjugation.

Although we have strived through our notations to make the definitions appear uniform, the nature of Y_{N^+,N^-} depends greatly on whether the algebra

B is indefinite or definite (i.e., on whether the integer N^- has an even or an odd number of prime divisors). We treat each case in turn.

Case 1: B is indefinite. The group $\Gamma = \phi_\infty(R^*_{N^+,N^-})$ is a discrete subgroup of $\mathbf{GL_2}(\mathbb{R})$. (The matrices in Γ have determinant 1 or -1.) It follows directly from prop. 1.1 that

$$Y_{N^+,N^-} \simeq \mathbb{P}/\Gamma \simeq \mathcal{H}/\Gamma^+,$$

where $\mathcal{H}$ is the classical upper half plane and Γ^+ is the subgroup of matrices in Γ of determinant 1. This gives an *analytic* description of the curves Y_{N^+,N^-}. It is a deep fact due to Shimura that these curves can actually be defined over $\mathbb{Q}$.

If $B = M_2(\mathbb{Q})$ is the usual matrix algebra (so that $N^- = 1$), the curve $Y_{N,1}$ is equal to $\mathcal{H}/\Gamma_0(N)$, the classical open modular curve of level N which can be compactified by adjoining a finite set of cusps. Let $X_{N,1}$ $(= X_0(N))$ denote the compactified curve. If B is a division algebra, (i.e., $N^- \neq 1$), then Y_{N^+,N^-} is already compact and we write $X_{N^+,N^-} = Y_{N^+,N^-}$.

Case 2: B is definite. In this case the fact that $X_{N^+,N^-} := Y_{N^+,N^-}$ is a complete algebraic curve defined over $\mathbb{Q}$ is built into the definitions. More precisely, let $n = h(R_{N^+,N^-})$ be the class number of R_{N^+,N^-}, and choose representatives $g_1, \dots, g_n$ for the double coset space $\hat{R}^*_{N^+,N^-}\backslash\hat{B}^*/B^*$. The groups $\Gamma_i = (g_i^{-1}\hat{R}^*_{N^+,N^-}g_i \cap B^*)/\langle\pm1\rangle$ are finite subgroups of $B^*/\langle\pm1\rangle$, and the curves $Y_i = \mathbb{P}/\Gamma_i$ are curves of genus 0 defined over $\mathbb{Q}$ (i.e., conics). The curve X_{N^+,N^-} is expressed as a finite disjoint union of these curves of genus 0:

$$X_{N^+,N^-} = \bigcup_{i=1}^{n} Y_i.$$

For more details on this construction, see [Gr2] and [Ro].

We will call the Shimura curve X_{N^+,N^-} *definite* or *indefinite* depending on whether the associated quaternion algebra is definite or indefinite.

1.4 Jacobians and height parings

Let $J_{N^+,N^-} := \mathrm{Pic}(X_{N^+,N^-})$ be the group of divisor classes on the curve X_{N^+,N^-}.

Case 1: B is indefinite. In that case J_{N^+,N^-} is an extension of $\mathbb{Z}$ by an abelian variety of dimension $g \simeq N/12$. We define $J_{N^+,N^-}(L)$ in the obvious way, for any number field L; it is a finitely generated abelian group, by the Mordel-Weil theorem. By Néron's theory [Ne], the group $J_{N^+,N^-}(L)$ is equipped with the (normalized) Néron-Tate canonical height which takes values in $\mathbb{R}$ and is positive definite and non degenerate on $J_{N^+,N^-}(L)/\text{torsion}$. We denote by $\langle P, Q\rangle$ the Néron-Tate height of points P, Q in $J_{N^+,N^-}(L)$.

Case 2: B is definite. Then J_{N^+,N^-} is isomorphic to the lattice of elements in

$$\mathbb{Z}e_1 + \mathbb{Z}e_2 + \cdots + \mathbb{Z}e_n,$$

where e_i corresponds to the class in $\mathrm{Pic}(X_{N^+,N^-})$ generated by a single point supported on the ith component $Y_i = \mathbb{P}/\Gamma_i$.

Let $w_i = \#\Gamma_i$. Following [Gr2], we define a symmetric positive definite inner product on J_{N^+,N^-} by the rule

$$\langle e_i, e_j\rangle = w_i\delta_{ij}.$$

Unlike the indefinite case, this pairing takes values in $\mathbb{Z}$, and defines a natural injection

$$J_{N^+,N^-} \longrightarrow J^{dual}_{N^+,N^-},$$

where the *dual* here means $\mathbb{Z}$-dual.

1.5 Hecke Operators

Since $\mathbb{Q}$ has class number 1, we have $\mathbb{Q}^*\hat{\mathbb{Z}}^* = \hat{\mathbb{Q}}^*$. Hence the curve Y_{N^+,N^-} can be written as

$$(\hat{R}^*_{N^+,N^-}\backslash\hat{B}^*/\hat{\mathbb{Q}}^* \times \mathbb{P})/B^*.$$

The space $(\hat{R}^*_{N^+,N^-}\backslash\hat{B}^*/\hat{\mathbb{Q}}^*)$ is the product of local spaces

$$((R_{N^+,N^-}\otimes\mathbb{Z}_\ell)^*\backslash B^*_\ell/\mathbb{Q}^*_\ell).$$

The Hecke operators T_ℓ: When ℓ does not divide N, then

$$((R_{N^+,N^-}\otimes\mathbb{Z}_\ell)^*\backslash B^*_\ell/\mathbb{Q}^*_\ell) \simeq \mathbf{PGL_2}(\mathbb{Z}_\ell)\backslash\mathbf{PGL_2}(\mathbb{Q}_\ell)$$

is the Bruhat-Tits tree of $\mathbf{PGL_2}(\mathbb{Q}_\ell)$, whose vertices correspond to similarity classes of rank two $\mathbb{Z}_\ell$-lattices in $\mathbb{Q}_\ell^2$. It is a homogenous tree of degree $\ell+1$;

more precisely, if $g \in \mathbf{PGL_2}(\mathbb{Z}_\ell)\backslash\mathbf{PGL_2}(\mathbb{Q}_\ell)$ is a vertex, its $\ell+1$ neighbours $g_0, \dots, g_{\ell-1}, g_\infty$ are given by the formulae

$$g_i = \begin{pmatrix} 1 & i \\ 0 & \ell \end{pmatrix} g, \quad i = 0, \cdots, \ell-1, \qquad g_\infty = \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} g.$$

The tree of $\mathbf{PGL_2}(\mathbb{Q}_\ell)$ is equipped with a correspondence T_ℓ of degree $\ell+1$ sending a vertex g to the formal sum of its $\ell+1$ neighbours in the tree:

$$T_\ell(g) = \sum_{i=0}^{\ell-1} g_i + g_\infty.$$

(Note that the values of the elements g_i and g_∞ depend on the choice of representative for g, but that the collection $\{g_0, \dots, g_{\ell-1}, g_\infty\}$ does not.)

One extends the correspondence to the product tree $(\hat{R}^*_{N^+,N^-}\backslash\hat{B}^*/\hat{\mathbb{Q}}^*)$. Since right multiplication by B acts by isometries on the tree, T_ℓ naturally gives rise to a well-defined correspondence on the curve X_{N^+,N^-}.

The Hecke operator U_p: If p divides N^+, then

$$((R_{N^+,N^-} \otimes \mathbb{Z}_p)^*\backslash B_p^*/\mathbb{Q}_p^*) \simeq \Gamma_0(p)\backslash\mathbf{PGL_2}(\mathbb{Q}_\mathbf{p})$$

can be identified with the set of edges on the Bruhat-Tits tree of $\mathbf{PGL_2}(\mathbb{Q}_\mathbf{p})$. This set is equipped with a correspondence U_p of degree p sending an edge g to the formal sum of the p other edges emanating from its target:

$$U_p(g) = \sum_{i=0}^{p-1} g_i,$$

where the g_i are defined in the same way as for the Hecke operator T_ℓ.

The Atkin Lehner involutions W_p^+: If p divides N^+, then the space

$$((R_{N^+,N^-} \otimes \mathbb{Z}_p)^*\backslash B_p^*/\mathbb{Q}_p^*) \simeq \Gamma_0(p)\backslash\mathbf{PGL_2}(\mathbb{Q}_\mathbf{p})$$

is equipped with the standard involution

$$g \mapsto \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix} g.$$

This involution gives rise in a natural way to an involution on X_{N^+,N^-}, which we call W_p^+.

The Atkin Lehner involutions W_p^-: If p divides N^-, then the space

$$((R_{N^+,N^-} \otimes \mathbb{Z}_p)^* \backslash B_p^* / \mathbb{Q}_p^*)$$

consists of exactly two elements. Let W_p^- be the (only) non-trivial involution on this set. This involution gives rise in a natural way to an involution on X_{N^+,N^-}, which we call W_p^-.

Given any factorization $N = N^+N^-$, we let $\mathbb{T}_{N^+,N^-}$ be the ring of Hecke operators acting as endomorphisms of J_{N^+,N^-}. It is generated by the operators T_ℓ, with $(\ell, N) = 1$, together with the involutions W_p^+, with $p|N^+$ and W_p^-, with $p|N^-$.

1.6 The Jacquet-Langlands correspondence

Let f be a normalized newform on $\Gamma_0(N)$, with Fourier expansion

$$f = \sum a_n q^n.$$

Such a newform is an eigenform for the Hecke operators T_ℓ and the Atkin Lehner involutions W_p^+ $(p|N)$ acting on $S_2(X_0(N))$, and we have

$$T_\ell f = a_\ell f, \qquad W_p^+ f = -a_p f.$$

Let K_f be the field generated by the Fourier coefficients a_n and let $\mathcal{O}_f$ be its ring of integers.

The form f gives rise to an algebra homomorphism

$$\phi_f : \mathbb{T}_{N,1} \longrightarrow \mathcal{O}_f,$$

satisfying $\phi_f(T_\ell) = a_\ell$, and $\phi_f(W_p^+) = -a_p$.

The result of Jacquet-Langlands [JL] establishing a correspondence between forms on $\mathbf{GL_2}$ and on quaternion algebras, can be formulated in our context as follows:

Theorem 1.2 (Jacquet-Langlands) *For any factorization $N = N^+N^-$, there is an algebra homomorphism $\phi_f : \mathbb{T}_{N^+,N^-} \longrightarrow \mathcal{O}_f$, satisfying*

$$\phi_f(T_\ell) = a_\ell, \quad \phi_f(W_p^+) = -a_p \;\; \text{if} \;\; p|N^+, \quad \phi_f(W_p^-) = a_p \;\; \text{if} \;\; p|N^-.$$

Note the slight abuse of notation, in denoting the various homomorphisms associated to f by the same letter ϕ_f. In general the context will make it clear which algebra of Hecke operators we are working with.

1.7 The Cerednik-Drinfeld uniformization

If $N^+N^- = N$ is a factorization of N, and if p divides N^+, then there are two degeneracy maps

$$\nu_1, \nu_2 : X_{N^+,N^-} \longrightarrow X_{N^+/p,N^-}.$$

The map ν_1 is induced by the natural projection, and $\nu_2 = \nu_1 W_p^+$. These induce maps by Pic (i.e., contravariant) functoriality (which we call ν_1^* and ν_2^*) from $J_{N^+/p,N^-}$ to J_{N^+,N^-}. Define J_{N^+,N^-}^{p-new} by the exact sequence

$$0 \longrightarrow J_{N^+/p,N^-} \oplus J_{N^+/p,N^-} \stackrel{\nu_1^* \oplus \nu_2^*}{\longrightarrow} J_{N^+,N^-} \longrightarrow J_{N^+,N^-}^{p-new} \longrightarrow 0.$$

Suppose that X_{N^+,N^-} corresponds to an indefinite quaternion algebra, and let p be a prime dividing N^-. In that case, the curve $(X_{N^+,N^-})_{/\mathbb{Q}_p}$ is a *Mumford curve*: the special fiber of its mod p reduction is a finite union of copies of $\mathbb{P}_1$ intersecting transversally in certain points. By Mumford's theory [G-VdP] the curve X_{N^+,N^-} has a p-adic uniformization expressing it as a quotient of the p-adic upper half plane by the action of a discrete subgroup Γ.

The theory of Cerednik-Drinfeld (cf. for example [BC], especially ch. III) gives an explicit description of this p-adic uniformization. More precisely, let $N_*^+ = N^+p$, and $N_*^- = N^-/p$, so that $N = N_*^+ N_*^-$ is another factorization of N. Let $R_{N_*^+,N_*^-}$ be the Eichler order defined as in sec. 1.1, and let Γ be the group of elements in $(R_{N_*^+,N_*^-}[\frac{1}{p}])^*$ whose reduced norm is an even power of p. The group Γ acts properly discontinuously on the p-adic upper half plane $\mathcal{H}_p := \mathbb{P}_1(\mathbb{C}_p) - \mathbb{P}_1(\mathbb{Q}_p)$, and the quotient $\mathcal{H}_p/\Gamma$ is a Mumford curve defined over $\mathbb{Q}_p$. Let K_p be the unique unramified quadratic extension of $\mathbb{Q}_p$, and let X'_{N^+,N^-} be the curve over $\mathbb{Q}_p$ obtained by twisting X_{N^+,N^-} by the cocycle in $H^1(\mathrm{Gal}(K_p/\mathbb{Q}_p), \mathrm{Aut}(X_{N^+,N^-}))$ which sends the generator of $\mathrm{Gal}(K_p/\mathbb{Q}_p)$ to the Atkin Lehner involution W_p^-. Then we have:

Theorem 1.3 (Cerednik, Drinfeld) *The curves X'_{N^+,N^-} and $\mathcal{H}_p/\Gamma$ are isomorphic over $\mathbb{Q}_p$. In particular, the curves X_{N^+,N^-} and $\mathcal{H}_p/\Gamma$ are isomorphic over K_p.*

It follows from the general theory [G-VdP] that the Jacobian $J_{N^+,N^-}/K_p$ is purely toric at p and admits a uniformization by the p-adic torus $\mathrm{Hom}(\Gamma, K_p^*)$. In [BD5] we will describe a natural Hecke-equivariant map

$$\Gamma^{ab} \longrightarrow J^{p-new,dual}_{N_*^+,N_*^-},$$

where the *dual* in the superscript means $\mathbb{Z}$-dual. Combining these two remarks, we obtain:

Corollary 1.4 *There is a canonical, Hecke equivariant, p-adic analytic uniformization*

$$\Phi_{CD} : (J^{p-new}_{N_*^+,N_*^-}) \otimes K_p^* \longrightarrow (J_{N^+,N^-})_{/K_p}.$$

Note that the curve $X_{N_*^+,N_*^-}$ corresponds to a definite quaternion algebra, so that its Picard group $J_{N_*^+,N_*^-}$ is a finitely generated free $\mathbb{Z}$-module.

1.8 Signs

We define the *Fricke involution* W_{N^+,N^-} on X_{N^+,N^-} by

$$W_{N^+,N^-} = \prod_{p|N^+} W_p^+ \prod_{p|N^-} W_p^-.$$

We will also have a use for the involutions W'_{N^+,N^-}, whose definition depends on a fixed prime p, and is given by

$$W'_{N^+,N^-} = W_{N^+,N^-}, \text{ if } p \text{ does not divide } N,$$

$$W'_{N^+,N^-} = W_{N^+/p,N^-}, \text{ if } p \text{ divides } N^+,$$
$$W'_{N^+,N^-} = W_{N^+,N^-/p}, \text{ if } p \text{ divides } N^-.$$

Let ϕ_f be the map from the Hecke ring $\mathbb{T}_{N^+,N^-}$ to $\mathbb{Z}$ associated to f, defined in sec. 1.6. Let $w_{N^+,N^-} = \phi_f(W_{N^+,N^-})$ be the eigenvalue of the Fricke involution W_{N^+,N^-} acting on the f-isotypic component of J_{N^+,N^-}, and let w'_{N^+,N^-} be the eigenvalue of the involution W'_{N^+,N^-}. As a shorthand notation we let $w = \phi_f(W_{N,1})$, and $w' = \phi_f(W'_{N,1})$ be the signs of these Atkin-Lehner involutions acting on the modular form f on $X_0(N)$. (Where now ϕ_f is defines on $\mathbb{T}_{N,1}$.) It follows from thm. 1.2 of sec. 1.6 that $w'_{N_*^+,N_*^-} = (-1)^{\#\{\ell|N'\}}w'$.

1.9 Elliptic curves and modular parametrizations

Let E be an elliptic curve of square-free conductor N, and let

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

be its minimal Weierstrass model over $\mathbb{Q}$.

Thanks to the fundamental work of Wiles [Wi] and Taylor-Wiles [TW], we now know that E is modular, i.e., there is a parametrization

$$\pi_E : X_0(N) \longrightarrow E.$$

This map induces maps $\pi_{E*} : J_{N,1} \longrightarrow E$ and $\pi_E^* : E \longrightarrow J_{N,1}$ by Albanese and Pic functoriality respectively. The pullback of a Néron differential on E is a multiple of a normalized newform f which is an eigenform for all the Hecke operators.

More generally, if X_{N^+,N^-} is a Shimura curve associated to an indefinite quaternion algebra, then the Jacquet-Langlands correspondence explained in sec. 1.6, combined with the Eichler-Shimura theory and the isogeny conjecture proved by Serre in this case, implies the existence of maps π_{E*} and π_E^* (which by abuse of notation we also denote by the same letters, relying on the context to make it clear which Shimura curve we are working with):

$$\pi_{E*} : J_{N^+,N^-} \longrightarrow E, \quad \pi_E^* : E \longrightarrow J_{N^+,N^-},$$

which are dual to each other. Of course, the map π_{E*} is not uniquely defined, since it can always be composed with an isogeny of E. We say that E is a strong Weil curve, and that π_{E*} is a strong Weil parametrization, relative to the Shimura curve X_{N^+,N^-}, if the map π_{E*} has connected kernel (or, equivalently, if π_E^* is injective, so that E is a sub-abelian variety of J_{N^+,N^-}). If E is a strong Weil curve, then the map π_{E*} is well-defined, up to composition by -1.

At the cost of replacing E by an isogenous curve, we will always assume from now on that E is the strong Weil curve associated to X_{N^+,N^-}, and that π_{E*} is a strong Weil parametrization.

If X_{N^+,N^-} corresponds to a definite quaternion algebra, then we let $J^f_{N^+,N^-}$ be the sublattice of J_{N^+,N^-} on which $\mathbb{T}_{N^+,N^-}$ acts via the homomorphism ϕ_f of sec. 1.6. By the multiplicity 1 theorem, $J^f_{N^+,N^-}$ is a $\mathbb{Z}$-module of rank 1;

let v_f be a generator of this $\mathbb{Z}$-module, and define $\pi_{E*} : J_{N^+,N^-} \longrightarrow \mathbb{Z}$ and $\pi_E^* : \mathbb{Z} \longrightarrow J_{N^+,N^-}$ by the formulae

$$\pi_{E*}(D) = \langle D, v_f \rangle, \qquad \pi_E^*(1) = v_f,$$

where the pairing here is the one introduced in sec. 1.4. Note that there is an ambiguity of sign in the definition of π_{E*} and π_E^*.

1.10 The extended Mordell-Weil group

Suppose that p divides N, so that E has (split or non-split) multiplicative reduction at p. Let M be any finite extension of K, and let $M_p = M \otimes \mathbb{Q}_p = \oplus M_{\mathfrak{p}}$, where the sum is taken over all primes of M lying above p. Define

$$M_p' = \oplus_{\mathfrak{p}} M_{\mathfrak{p}},$$

where the sum now is taken over all primes $\mathfrak{p}$ for which $E/M_{\mathfrak{p}}$ has *split* multiplicative reduction. If there are such primes, then we have the Tate analytic uniformization:

$$\Phi_{Tate} : (M_p')^* \longrightarrow E(M_p').$$

We define the extended Mordell-Weil group

$$E^\dagger(M) = \{(\tilde{P}, P) \text{ such that } P \in E(M), \tilde{P} \in (M_p')^*, \text{ and } \Phi_{Tate}(\tilde{P}) = P\}.$$

In other words, a point in $E^\dagger(M)$ is an M-rational point P of $E(M)$, together with a distinguished lift, $\tilde{P}$, of P to $(M_p')^*$. Often, we will simply use the letter P to denote a point in $E^\dagger(M)$, keeping in mind that this point P comes equipped with a distinguished choice of lift $\tilde{P}$.

If there are no primes of M above p at which E has split multiplicative reduction (e.g., if p does not divide N) then by convention we set $E^\dagger(M) := E(M)$.

Action of complex conjugation:
Let $z \mapsto \bar{z}$ be the complex conjugation acting on $K_p = K \otimes \mathbb{Q}_p$. We define an action of complex conjugation τ on $E^\dagger(K)$ which extends the Galois action on $E(K)$, as follows:

1. If $E/\mathbb{Q}_p$ has good ordinary or split multiplicative reduction at p, then the action of τ is induced from the natural action of complex conjugation on $E(K)$ and K_p^*, i.e.,

$$\tau((z,P)) = (\bar{z}, \tau P)$$

This action is well-defined and consistent, because the Tate parametrization Φ_{Tate} is defined over $\mathbb{Q}_p$.
2. If $E/\mathbb{Q}_p$ has non-split multiplicative reduction, and p is inert in $K/\mathbb{Q}$, then we make τ act on $E^\dagger(K)$ by the rule

$$\tau((z,P)) = (\bar{z}^{-1}, \tau P).$$

One checks that this defines an action of τ on $E^\dagger(K)$ also. The twisting in the action of τ is necessary in this case because the Tate parametrization is not defined over $\mathbb{Q}_p$ (cf. [Si1], ch. V).

Let r be the rank of the Mordell-Weil group $E(K)$, and let $\tilde{r}$ be the rank of the extended Mordell-Weil group $E^\dagger(K)$.The vector spaces $E(K)\otimes\mathbb{Q}_p$ and $E^\dagger(K)\otimes\mathbb{Q}_p$ can be decomposed into $+$ and $-$ eigenspaces for this action. Let r^+ and r^- denote the ranks of $(E(K)\otimes\mathbb{Q})^+$ and $(E(K)\otimes\mathbb{Q})^-$, and let $\tilde{r}^+$ and $\tilde{r}^-$ denote the analogous ranks for $E^\dagger(K)$, so that

$$r = r^+ + r^-, \quad \tilde{r} = \tilde{r}^+ + \tilde{r}^-.$$

We recall the relation between r and $\tilde{r}$:

The non-exceptional case: $\tilde{r} = r, \quad \tilde{r}^+ = r^+, \quad \tilde{r}^- = r^-.$

The split exceptional case: $\tilde{r} = r + 2, \quad \tilde{r}^+ = r^+ + 1, \quad \tilde{r}^- = r^- + 1.$

The non-split exceptional case:

$$\tilde{r} = r+1, \begin{cases} \tilde{r}^+ = r^+ + 1, & \tilde{r}^- = r^- & \text{if } a_p = 1, \\ \tilde{r}^+ = r^+, & \tilde{r}^- = r^- + 1 & \text{if } a_p = -1. \end{cases}$$

1.11 Examples

We now discuss some examples that will be used in the numerical verifications of sec. 5.

The curves $X_0(14)$ and $X_{7,2}$:

Let $E = X_0(14)$ be the modular curve of level 14. It is an elliptic curve given in minimal Weierstrass form by the equation

$$y^2 + xy + y = x^3 + 4x - 6.$$

The maps π_{E*} and π_E^* are the identity maps.

We now turn to the study of the curve $X_{7,2}$ associated to an Eichler order of level 7 in the algebra of (rational) Hamilton quaternions $B = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$. Let R be Hurwitz's ring of integral quaternions:

$$R = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}\omega,$$

where $\omega = \frac{1+i+j+k}{2}$. Hurwitz showed that R is the unique maximal order in B up to conjugacy, and that every left R-ideal is principal.

Fix an embedding $\phi_7 = \phi$ of B_7 into $M_2(\mathbb{Q}_7)$ which has the property that $\phi^{-1}(M_2(\mathbb{Z}_7)) = R \otimes \mathbb{Z}_7$. For our calculations, we will take

$$\phi(i) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \phi(j) = \begin{pmatrix} \rho & \rho+1 \\ \rho+1 & -\rho \end{pmatrix}, \quad \phi(k) = \begin{pmatrix} \rho+1 & -\rho \\ -\rho & -\rho-1 \end{pmatrix},$$

where $\rho = \lim_{n\longrightarrow\infty} 2^{7^n}$ is a primitive cube root of unity in $\mathbb{Z}_7$. We define the Eichler order $R_{7,2}$ and the curve $X_{7,2}$ as in sec. 1.1 and sec. 1.3.

Lemma 1.5 *The curve $X_{7,2}$ has two components Y_1 and Y_2, which are isomorphic to $\mathbb{P}/\Gamma_i$, where Γ_1 and Γ_2 are subgroups of $R^*/\langle\pm 1\rangle$ of order 3, and $\mathbb{P}$ is the conic associated to B as in sec. 1.2.*

Proof: The components of $X_{7,2}$ are indexed by elements (g_ℓ) (with $g_\ell \in B_\ell^*$) in the double coset space $\hat{R}_{7,2}^*\backslash\hat{B}^*/B^*$. Without loss of generality, we may assume that g_ℓ belongs to R_ℓ^*, since R has class number 1. The idèle (g_ℓ) is then uniquely represented by the element $\phi(g_7)$ in the coset space $(R_{7,2} \otimes \mathbb{Z}_7)^*\backslash\mathbf{GL_2}(\mathbb{Z}_\mathbf{7})/\phi(\mathbf{R}^*)$. The space $(R_{7,2} \otimes \mathbb{Z}_7)^*\backslash\mathbf{GL_2}(\mathbb{Z}_\mathbf{7})$ can be identified with $\mathbb{P}_1(\mathbb{F}_7)$ via the map $\gamma \mapsto \gamma^{-1}(\infty)$. The group R^* is a group of order 24, generated by i, j, and ω, and $\phi(R^*)$ acts on $\mathbb{P}_1(\mathbb{F}_7)$ in the obvious way. This action breaks $\mathbb{P}_1(\mathbb{F}_7)$ into two orbits, $\{\infty, 0, 2, 3\}$ and $\{1, 4, 5, 6\}$, and the stabilizers Γ_1 and Γ_2 of each orbit element are of order 3 in $R^*/\{\pm 1\}$. So if $P = (g_\ell) \times y$, with $g_\ell \in R_\ell^*$, we have:

$$P \in \begin{cases} Y_1 & \text{if} \quad \phi(g_7^{-1})(\infty) = 0, 2, 3, \text{ or } \infty, \\ Y_2 & \text{if} \quad \phi(g_7^{-1})(\infty) = 1, 4, 5, \text{ or } 6. \end{cases}$$

Let e_1 and e_2 be the divisor classes generated by a single point supported on each component. Then $J_{7,2} = \mathbb{Z}e_1 + \mathbb{Z}e_2$, and, following sec. 1.4, the inner product on $J_{7,2}$ is defined as

$$\langle e_1, e_2 \rangle = 0, \quad \langle e_1, e_1 \rangle = \langle e_2, e_2 \rangle = 3.$$

The Hecke operator T_3 acts on e_1, e_2 by

$$T_3 e_1 = e_1 + 3e_2, \quad T_3 e_2 = 3e_1 + e_2.$$

By diagonalizing the operator T_3, one finds that the vectors

$$v_{eis} = e_1 + e_2, \quad v_1 = e_1 - e_2,$$

give an eigenbasis for $J_{7,2}$ under the Hecke action. If $p \neq 2, 7$ is prime, then the eigenvalue of T_p acting on v_{eis} is $p + 1$; the vector v_{eis} corresponds to an Eisenstein series of weight 2. The eigenvalues of T_p acting on v_1 are the Fourier coefficients a_p of the unique cusp form on $X_0(14)$.

The curves $X_0(26)$ and $X_{13,2}$:
The curve $X_0(26)$ is a curve of genus 2. There are two isogeny classes of elliptic curves of conductor 26, which are labelled $26A$ and $26B$ in the Antwerp tables; their minimal Weierstrass equations are

$$26A : y^2 + xy + y = x^3 - 5x - 8, \quad 26B : y^2 + xy + y = x^3 - x^2 - 3x + 3.$$

Now we analyze the curve $X_{13,2}$ corresponding to an Eichler order of level 13 in the algebra of rational Hamilton quaternions. Let R denote as before the Hurwitz order. The embedding $\phi = \phi_{13}$ of R in $M_2(\mathbb{Z}_{13})$, given by the rule

$$\phi(i) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \phi(j) = \begin{pmatrix} \rho & \rho+1 \\ \rho+1 & -\rho \end{pmatrix}, \quad \phi(k) = \begin{pmatrix} \rho+1 & -\rho \\ -\rho & -\rho-1 \end{pmatrix},$$

where $\rho = \lim_{n \longrightarrow \infty} 3^{13^n}$ is a primitive cube root of unity in $\mathbb{Z}_{13}$, can be used to define the Eichler order $R_{13,2}$ and the curve $X_{13,2}$, as before.

Lemma 1.6 *The curve $X_{13,2}$ has three components Y_1, Y_2, and Y_3, which are isomorphic to $\mathbb{P}/\Gamma_i$, where Γ_1, Γ_2 and Γ_3 are subgroups of $R^*/\langle \pm 1 \rangle$ of orders 3, 3 and 2 respectively, and $\mathbb{P}$ is the conic associated to B.*

Proof: This proceeds exactly as for lemma 1.5. The components of $X_{13,2}$ are indexed by elements in the double coset space:

$$\hat{R}^*_{13,2}\backslash\hat{B}^*/B^* = \hat{R}^*_{13,2}\backslash\hat{R}^*/R^* = (R_{13,2}\otimes\mathbb{Z}_{13})^*\backslash\mathbf{GL_2}(\mathbb{Z}_{\mathbf{13}})/\phi(\mathbf{R}^*)$$

$$= \mathbb{P}_1(\mathbb{F}_{13})/\phi(R^*).$$

The action of $\phi(R^*)$ breaks $\mathbb{P}_1(\mathbb{F}_{13})$ into three orbits,

$$\{\infty, 0, 4, 3\}, \{1, 7, 11, 12\}, \text{ and } \{2, 5, 6, 8, 9, 10\},$$

and the stabilizers Γ_1, Γ_2 and Γ_3 of each orbit element are of order 3, 3, and 2 respectively in $R^*/\langle\pm1\rangle$. So if $P = (g_\ell)\times y$, with $g_\ell \in R^*_\ell$, we have:

$$P \in \begin{cases} Y_1 & \text{if} \quad \phi(g_{13}^{-1})(\infty) = \infty, 0, 3, \text{ or } 4, \\ Y_2 & \text{if} \quad \phi(g_{13}^{-1})(\infty) = 1, 7, 11, \text{ or } 12, \\ Y_3 & \text{if} \quad \phi(g_{13}^{-1})(\infty) = 2, 5, 6, 8, 9, \text{ or } 10. \end{cases}$$

Let e_1, e_2 and e_3 be the divisor classes in $J_{13,2}$ generated by a single point supported on each component Y_1, Y_2 and Y_3. Then $J_{13,2} = \mathbb{Z}e_1 + \mathbb{Z}e_2 + \mathbb{Z}e_3$, and the inner product on $J_{13,2}$ is defined as

$$\langle e_i, e_j\rangle = w_i\delta_{ij}, \quad w_1 = w_2 = 3, \quad w_3 = 2.$$

The Hecke operator T_3 acts on $J_{13,2}$ by

$$T_3(e_1) = e_1 + 3e_3, \quad T_3(e_2) = e_2 + 3e_3, \quad T_3(e_3) = 2e_1 + 2e_2.$$

Diagonalizing T_3 decomposes $J_{13,2}$ into a sum of three distinct eigenspaces spanned by the vectors

$$v_{eis} = 2e_1 + 2e_2 + 3e_3, \quad v_1 = e_1 - e_2, \quad v_2 = e_1 + e_2 - 2e_3.$$

If $p \neq 2, 13$ is prime, then the eigenvalues of T_p on v_{eis} are $p+1$, so that v_{eis} corresponds to an Eisenstein series of weight 2. The Hecke eigenvalues for v_1 (resp. v_2) are the Fourier coefficients of the form of weight 2 corresponding to the curve $26A$ (resp. $26B$).

2 Heegner Points

2.1 Definition

Let K be a quadratic imaginary field, satisfying $(\mathrm{Disc}(K), N) = 1$, and let $\epsilon : (\mathbb{Z}/D\mathbb{Z})^* \longrightarrow \pm 1$ be the associated primitive Dirichlet character. There is a natural map from $\mathrm{Hom}(K, B)$ to $\mathrm{Hom}(\mathbb{C}, B_\infty)$ given by extension of scalars. We say that a point $P \in X_{N^+,N^-}$ is a *Heegner point associated to* K if $P \in \hat{R}^*_{N^+,N^-}\backslash(\hat{B}^* \times \mathrm{Hom}(\mathbb{C}, B_\infty))/B^*$ is the image of an element $(g \times f) \in \hat{R}^*_{N^+,N^-}\backslash(\hat{B}^* \times \mathrm{Hom}(K, B))/B^*$ by the natural inclusion. We will often describe Heegner points by writing down a representative $(g \times f)$ in $\hat{B}^* \times \mathrm{Hom}(K, B)$.

Let $\mathcal{O}$ be a (not necessarily maximal) order of K. If $\mathcal{O}_K = \mathbb{Z}[\omega]$ is the maximal order of K, then $\mathcal{O} = \mathbb{Z}[c\omega]$, where c is a positive integer called the conductor of $\mathcal{O}$. We say that $P = (g \times f)$ is a Heegner point of conductor c associated to K, or is a Heegner point associated to $\mathcal{O}$, if

$$f(K) \cap g^{-1}\hat{R}_{N^+,N^-}g = f(\mathcal{O}).$$

We let $H_{N^+,N^-}(K, c) = H_{N^+,N^-}(\mathcal{O})$ denote the set of Heegner points of conductor c on X_{N^+,N^-}. We call f an *optimal embedding* of $\mathcal{O}$ into the Eichler order $B \cap g\hat{R}_{N^+,N^-}g^{-1}$. The Heegner points of conductor c in $H_{N^+,N^-}(K, c)$ thus correspond to (conjugacy classes of) optimal embeddings of $\mathcal{O}$ into R_{N^+,N^-}.

2.2 Orientations and the Heegner condition

Orientations: Let $P = g \times f$ be a Heegner point of conductor c. For each ℓ dividing N^+ the map $\kappa_\ell^+ = \mathfrak{o}_\ell^+ \circ gfg^{-1}$ gives a surjective $\mathbb{Z}_\ell$-algebra homomorphism from $\mathcal{O} \otimes \mathbb{Z}_\ell$ to $\mathbb{F}_\ell$. Likewise, if ℓ divides N^-, the map $\kappa_\ell^- = \mathfrak{o}_\ell^- \circ gfg^{-1}$ gives a surjective $\mathbb{Z}_\ell$-algebra homomorphism from $\mathcal{O} \otimes \mathbb{Z}_\ell$ to $\mathbb{F}_{\ell^2}$. We call the set of maps $\{\kappa_l^+, \kappa_l^-\}$ the *orientation* of $\mathcal{O}$ induced from the orientation $\{\mathfrak{o}_\ell^+, \mathfrak{o}_\ell^-\}$ of R_{N^+,N^-}. Each Heegner point of conductor c gives rise to an associated orientation of $\mathcal{O}$.

The Heegner condition: Define a factorization of the square-free integer N, $N = N^+N^-$, by setting

$$N^+ = \prod_{\epsilon(\ell)=1} \ell, \quad N^- = \prod_{\epsilon(\ell)=-1} \ell.$$

Fix a conductor c. The following lemma explains the significance of the factorization N^+N^- of N associated to K.

Lemma 2.1 *Let M^+M^- be an arbitrary factorization of N, and suppose that c is prime to N. Then the set $H_{M^+,M^-}(K,c)$ is non-empty if and only if $(M^+,M^-)=(N^+,N^-)$.*

Sketch of proof: Suppose that $H_{M^+,M^-}(K,c)$ is non-empty. A Heegner point in $H_{M^+,M^-}(K,c)$ gives rise to an orientation $\kappa_\ell^+ : \mathcal{O} \longrightarrow \mathbb{F}_\ell$, (with ℓ dividing M^+) and $\kappa_\ell^- : \mathcal{O} \longrightarrow \mathbb{F}_{\ell^2}$ (with ℓ dividing M^-). It follows that all ℓ dividing M^+ are split in $K/\mathbb{Q}$, and that all ℓ dividing M^- are inert in $K/\mathbb{Q}$, so that $(M^+,M^-)=(N^+,N^-)$. Conversely, if $(M^+,M^-)=(N^+,N^-)$, the theory of local embeddings (cf. [Gr2], or [Vi]) shows that $H_{M^+,M^-}(K,c)$ is non-empty.

Lemma 2.1 shows that the Heegner points associated to an order of K of conductor c prime to N always belong to *precisely one* Shimura curve X_{N^+,N^-} of level $N=N^+N^-$. Hence, we can use without ambiguity the notation $H_N(K,c)$ to denote $H_{N^+,N^-}(K,c)$, where N^+N^- is the only factorization of N for which $H_{N^+,N^-}(K,c)$ is non-empty. We will adopt this notation from now on.

In our conjectures, we will also be studying Heegner points of conductor cp^n, where $(c,NpD)=1$ and p is a prime which is not necessarily prime to N. (In fact, the case $p|N$ will be of *particular interest* to us.) Given any prime p, we define

$$\begin{aligned} N_*^+ &= N^+, \quad N_*^- = N^-, \qquad \text{if } (p,N^-)=1,\\ N_*^+ &= N^+p, \quad N_*^- = N^-/p, \qquad \text{if } p|N^-. \end{aligned}$$

Note that, if p divides N^-, this factorization is the same one as was defined in sec. 1.7.

Lemma 2.2 *Let M^+M^- be an arbitrary factorization of N. Then the set $H_{M^+,M^-}(K,cp^n)$ ($n \geq 1$) is non-empty if and only if $(M^+,M^-)=(N_*^+,N_*^-)$.*

The proof proceeds similarly as for lemma 2.1. For details see [Vi].

As before, we can write $H_N(K,cp^n)$ to denote $H_{N_*^+,N_*^-}(K,cp^n)$, since the data (K,cp^n) determines the factorization $N_*^+N_*^-$ without ambiguity. Note that, when p divides N^-, the sets $H_N(K,c)$ and $H_N(K,cp^n)$ are defined on different Shimura curves corresponding to quaternion algebras which have opposite ramification types at ∞. Moreover, if X_{N^+,N^-} corresponds to an indefinite quaternion algebra, then $X_{N_*^+,N_*^-}$ is the curve whose Jacobian appears in the statement of the Cerednik-Drinfeld theorem of sec. 1.7.

Definition 2.3 *We say that the pair* (E, K) *corresponds to a* definite *(resp.* indefinite*)* case *if the curve* $X_{N_*^+,N_*^-}$ *is associated to a definite (resp. indefinite) quaternion algebra.*

2.3 The action of Pic($\mathcal{O}$)

Let $\mathcal{O}$ be the order of K of conductor c, as in the previous section, but do not assume that c is prime to N. Let $\mathrm{Pic}(\mathcal{O}) = \hat{\mathcal{O}}^* \backslash \hat{K}^*/K^*$ be the Picard group of $\mathcal{O}$.

If f belongs to $\mathrm{Hom}(K, B)$, let $\hat{f} \in \mathrm{Hom}(\hat{K}, \hat{B})$ be the homomorphism deduced from f by extension of scalars. The set $H_N(K, c)$ of all Heegner points $(g \times f)$ of conductor c is endowed with a natural action of $\mathrm{Pic}(\mathcal{O})$ by the rule:

$$\sigma(g \times f) = (g\hat{f}(\sigma) \times f). \tag{4}$$

The reader will check that this action is well-defined and free (cf. [Gr2], sec. 3), and that

Lemma 2.4 *The action of Pic*($\mathcal{O}$) *preserves the orientations on the Heegner points defined in sec. 2.2*

Proof: This follows from a direct calculation.

Suppose now for simplicity that c is prime to $N\mathrm{Disc}(K)$, and that p is a prime not dividing $c\mathrm{Disc}(K)$ (but which may divide N).

The action (4) can be used to compute the exact number of Heegner points of conductor c (resp. cp^n) on X_{N^+,N^-} (resp. $X_{N_*^+,N_*^-}$) as in [Gr2]. Suppose that N is a product of t primes. Let h denote the cardinality of $\mathrm{Pic}(\mathcal{O})$, and let $u = \frac{1}{2}\#\mathcal{O}^*$. (In particular, $u = 1$ unless $c = 1$ and $K = \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$.) Let $\mathcal{O}_n$ denote the order of K of conductor cp^n. Note that if $n \geq 1$, then $\#\mathrm{Pic}(\mathcal{O}_n) = hu^{-1}p^{n-1}(p - \epsilon(p))$.

Lemma 2.5 .

1. *There are exactly* $2^t h$ *Heegner points of conductor* c *on* X_{N^+,N^-}*, if* (N^+, N^-) *is the factorization satisfying the Heegner condition of sec. 2.2.*

2. *If $n \geq 1$, then there are exactly $2^t h u^{-1} p^{n-1}(p - \epsilon(p))$ Heegner points of conductor cp^n on $X_{N_*^+,N_*^-}$, if (N_*^+, N_*^-) is the factorization satisfying the Heegner condition of sec. 2.2.*

Proof (sketch): In case 1, let $\mathcal{W}$ be the Atkin-Lehner group $\langle W_\ell^+, W_\ell^- \rangle$ of order 2^t generated by all the Atkin-Lehner involutions W_ℓ^+ with $\ell | N^+$ and W_ℓ^- with $\ell | N^-$. One can see by a direct calculation that the involution W_ℓ^+ or W_ℓ^- sends a Heegner point P to one with the oposite orientation at ℓ, (and the same orientation at all the other primes dividing N). In fact, it can be shown (cf. [Vi], or [Gr2]) that the group $\mathrm{Pic}(\mathcal{O}) \times \mathcal{W}$ acts simply transitively on the set $H_N(K, c)$ of Heegner points, and that the orbits of Heegner points under the action of $\mathrm{Pic}(\mathcal{O})$ correspond exactly to sets of Heegner points with a given orientation. A similar proof works, *mutatis mutandis*, for $H_N(K, cp^n)$, where $\mathcal{O}$ is replaced by $\mathcal{O}_n$, the order of conductor cp^n in K. For details see [Vi], cor. 5.12, p. 94.

Class field theory: Let $G_n = \mathrm{Pic}(\mathcal{O}_n)$. This group can be identified by class field theory with the Galois group of a certain abelian extension of K: the ring class field of K of conductor cp^n. Let K_n denote this field extension, so that $G_n = \mathrm{Gal}(K_n/K)$. The group $\mathrm{Gal}(K_n/K_0)$ is canonically isomorphic to $\mathcal{O}^* \backslash (\mathcal{O}_K \otimes \mathbb{Z}/p^n\mathbb{Z})^* / (\mathbb{Z}/p^n\mathbb{Z})^*$, and $G_\infty^0 = \mathrm{Gal}(K_\infty/K_0)$ is isomorphic to $\mathcal{O}^* \backslash (\mathcal{O}_K \otimes \mathbb{Z}_p)^* / \mathbb{Z}_p^*$.

Heegner points on indefinite Shimura curves: If X_{N^+,N^-} (resp. $X_{N_*^+,N_*^-}$) is associated to an indefinite quaternion algebra, then the definition of the Heegner points in $H_N(K, c)$ (resp. $H_N(K, cp^n)$) given in sec. 2.1 is purely analytic. It is a remarkable fact, which follows from the theory of complex multiplication, that the points in $H_N(K, c)$ (resp. $H_N(K, cp^n)$) are actually defined over the field K_0 (resp. K_n). The action of $\mathrm{Pic}(\mathcal{O})$ on $H_N(K, c)$ which was defined above corresponds, via the identification of class field theory, to the Galois action on the set of Heegner points. This is the content of the Shimura reciprocity law.

Heegner points on definite Shimura curves: Here the theory of Heegner points is considerably simpler and less deep. Suppose that $X = X_{N^+,N^-}$ (resp. $X_{N_*^+,N_*^-}$) is associated to a definite quaternion algebra. Unlike Heegner points in the indefinite case, the points in $H_N(K, c)$ (resp. $H_N(K, cp^n)$) are all defined over K, by construction, and the action of $\mathrm{Pic}(\mathcal{O})$ (resp. $\mathrm{Pic}(\mathcal{O}_n)$) that was defined above does not correspond to any Galois action.

2.4 Formal properties

A compatible system of points: Let σ be a generator of $\mathrm{Gal}(K_n/K_{n-1})$, and write

$$\mathrm{Norm}_{K_n/K_{n-1}} = \sum \sigma^i$$

for the norm operator. If $p \not| N$, then given $P = (g \times f)$ a Heegner point of conductor cp^n ($n \geq 1$), the points

$$(g_\infty \times f), (g_i \times f), i = 0, \ldots, p-1$$

are a collection of $p+1$ Heegner points, of which p are of conductor cp^{n+1}, and one is of conductor cp^{n-1}. Let $\bar{P}$ be this unique point of conductor cp^{n-1}. Likewise, if $p|N$ (and hence, N_*^+), one defines a map $H_N(K, cp^n) \longrightarrow H_N(K, cp^{n-1})$, by letting $\bar{P}$ be the unique point such that $\mathrm{Norm}_{K_n/K_{n-1}}(P) = U_p(\bar{P})$.

Choose points $P_n \in H_N(K, cp^n)$ which are compatible under these maps:

$$\bar{P}_{n+1} = P_n.$$

Behaviour of the P_n under norms: Recall that u denotes the order of the finite group $\mathcal{O}^*/\langle \pm 1 \rangle$. (And thus, $u = 1$ if $K \neq \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$, or if $c > 1$.) If p is split in $K/\mathbb{Q}$, let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be the two distinct prime ideals of K above p, and let $\sigma_{\mathfrak{p}_1}$ and $\sigma_{\mathfrak{p}_2}$ be the Frobenius elements in $\mathrm{Gal}(\bar{K}/K)$ corresponding to $\mathfrak{p}_1$ and $\mathfrak{p}_2$. We have the following norm relations in the Picard groups J_{N^+,N^-} of X_{N^+,N^-}:

- If p does not divide N, then

$$\begin{aligned} \mathrm{Norm}_{K_{n+1}/K_n}(P_{n+1}) &= T_p P_n - P_{n-1}, \text{ if } n \geq 1, \\ u\mathrm{Norm}_{K_1/K_0}(P_1) &= \begin{cases} T_p P_0 & \text{if } \epsilon(p) = -1, \\ (T_p - \sigma_{\mathfrak{p}_1} - \sigma_{\mathfrak{p}_2}) P_0 & \text{if } \epsilon(p) = 1. \end{cases} \end{aligned}$$

We denote by $J^{old}_{M^+,M^-}$ the old subvariety of J_{M^+,M^-}, which is the image of the map

$$\oplus_{q|M^+} J_{M^+/q,M^-} \oplus J_{M^+/q,M^-} \longrightarrow J_{M^+,M^-},$$

where the sum is taken over all primes q dividing M^+, and the homomorphism from $J_{M^+/q,M^-} \oplus J_{M^+/q,M^-}$ to J_{M^+,M^-} is induced from the two natural maps obtained by Pic (contravariant) functoriality on the Picard groups from the two degeneracy maps $X_{M^+,M^-} \longrightarrow X_{M^+/q,M^-}$.

• If p divides N (and hence N_*^+), then

$$\begin{array}{rcl} \mathrm{Norm}_{K_{n+1}/K_n}(P_{n+1}) & = & U_p P_n, \text{ if } n \geq 1, \\ u\mathrm{Norm}_{K_1/K_0}(P_1) & = & \begin{cases} P_0 \in J^{old}_{N_*^+,N_*^-} & \text{if } \epsilon(p) = -1, \\ (U_p - \sigma)P_0, (\sigma \in \mathrm{Gal}(K_0/K)) & \text{if } \epsilon(p) = 1. \end{cases} \end{array}$$

Action of complex conjugation: Let $W_{N_*^+,N_*^-}$ and $W'_{N_*^+,N_*^-}$ be the Fricke involutions introduced in sec. 1.5 acting on $X_{N_*^+,N_*^-}$, and let $P_n \in H_N(K, cp^n)$ be a given Heegner point belonging to $X_{N_*^+,N_*^-}$. Consider the involution τ acting on $X_{N_*^+,N_*^-}$ by sending $(g \times f)$ to $(g \times \bar{f})$, where $\bar{f}(x) := f(\bar{x})$. If $X_{N_*^+,N_*^-}$ corresponds to an indefinite quaternion algebra, then τ acts like complex conjugation on the complex points of $X_{N_*^+,N_*^-}$. If $X_{N_*^+,N_*^-}$ corresponds to a definite quaternion algebra, then τ acts trivially on $J_{N_*^+,N_*^-}$.

Proposition 2.6 *There exists $\gamma \in G_n$ (depending on the choice of P_n) such that*

1. $\tau(P_0) = \gamma W_{N^+,N^-}(P_0)$, *if* $n = 0$.
2. $\tau(P_n) = \gamma W'_{N_*^+,N_*^-}(P_n)$, *if* $n > 0$.

Proof: The reader may check that τ reverses all the orientations associated to the Heegner point P_0, for each ℓ dividing N. So does the involution W_{N^+,N^-}. Hence $\tau(P_0)$ and $W_{N^+,N^-}(P_0)$ belong to the same orbit under the action of $\mathrm{Pic}(\mathcal{O})$. (See the discussion in the proof of lemma 2.5.) This proves 1. The assertion 2 is proved similarly.

For more details, the reader may also wish to consult [Gr1].

2.5 Heegner points on elliptic curves

From now on, K_n denotes the ring class field of conductor cp^n, and K_∞ the compositum of all these ring class fields. The Galois group G_∞ of K_∞ over K is an extension of $\mathrm{Gal}(K_0/K) = \mathrm{Pic}(\mathcal{O})$ by the subgroup

$$G_\infty^0 = \mathrm{Gal}(K_\infty/K_0) = \mathcal{O}^* \backslash (\mathcal{O}_K \otimes \mathbb{Z}_p)^*/\mathbb{Z}_p^*.$$

Denote also by $G_{n,m}$ the Galois group of K_n over K_m, if $n > m$. We define the "Heegner point" y_n associated to E by

$$y_n = \pi_{E*}(P_n),$$

where π_{E*} is the map defined in sec. 1.9. Thus, y_n belongs to $E(K_n) \subset E(K_\infty)$ if $X_{N_*^+,N_*^-}$ corresponds to an indefinite quaternion algebra (the indefinite case), and y_n belongs to $\mathbb{Z}$ if $X_{N_*^+,N_*^-}$ corresponds to a definite quaternion algebra (the definite case). Let Z be the module $E(K_\infty)$ in the indefinite case, and the module $\mathbb{Z}$ in the definite case, and let $Z_p := Z \otimes \mathbb{Z}_p$. We also write $y_n^\sigma := \pi_E(P_n^\sigma)$ for all $\sigma \in G_n$, and define

$$\mathrm{Norm}_{K_n/K_{n-1}}(y_n) := \sum_{\sigma \in G_{n,n-1}} y_n^\sigma.$$

(In the indefinite case, when y_n belongs to $E(K_n)$, this is just the usual trace.)

Regularized Heegner points: We make the crucial hypothesis from now on that E is ordinary at p, i.e., the coefficient a_p is not divisible by p (and hence, is non-zero, if $p > 3$). We can then replace the Heegner points y_n by certain "regularized" Heegner points z_n in Z_p. This construction is introduced to make the points norm-compatible.

Case 1: p does not divide N. Then the equations of sec. 2.4 tell us that

$$\begin{aligned} \mathrm{Norm}_{K_{n+1}/K_n}(y_{n+1}) &= a_p y_n - y_{n-1}, \quad \text{if} \quad n \geq 1, &(5)\\ u\mathrm{Norm}_{K_1/K_0}(y_1) &= \begin{cases} a_p y_0 & \text{if } \epsilon(p) = -1, \\ (a_p - \sigma_{\mathfrak{p}_1} - \sigma_{\mathfrak{p}_2}) y_0 & \text{if } \epsilon(p) = 1. \end{cases} &(6) \end{aligned}$$

Let α be the unit root of the polynomial $x^2 - a_p x + p$, which exists since E has good ordinary reduction. Define the *regularized Heegner points* $z_n \in Z_p$ by the rule

$$\begin{aligned} z_n &= \frac{1}{\alpha^n} y_n - \frac{1}{\alpha^{n+1}} y_{n-1}, \text{ if } n \geq 1, \\ z_0 &= \begin{cases} u^{-1}(1 - \alpha^{-2}) y_0 & \text{if } \epsilon(p) = -1, \\ u^{-1}(1 - (\sigma_{\mathfrak{p}_1} + \sigma_{\mathfrak{p}_2})\alpha^{-1} + \alpha^{-2}) y_0 & \text{if } \epsilon(p) = 1. \end{cases} \end{aligned}$$

Case 2: p divides N. Then the equations of sec. 2.4 tell us that

$$\begin{aligned}
\mathrm{Norm}_{K_{n+1}/K_n}(y_{n+1}) &= a_p y_n, \quad \text{if} \quad n \geq 1, &(7)\\
u\mathrm{Norm}_{K_1/K_0}(y_1) &= \begin{cases} 0 & \text{if } \epsilon(p) = -1, \\ (a_p - \sigma)y_0 & \text{if } \epsilon(p) = 1. \end{cases} &(8)
\end{aligned}$$

Let $\alpha = a_p$ be the unit root of $x^2 - a_p x$. Note that $\alpha = \pm 1$ in this case.

$$\begin{aligned}
z_n &= \frac{1}{\alpha^n} y_n \quad \text{if } n \geq 1, \\
z_0 &= \begin{cases} 0 & \text{if } \epsilon(p) = -1, \\ u^{-1}(1 - \alpha^{-1}\sigma)y_0 & \text{if } \epsilon(p) = 1. \end{cases}
\end{aligned}$$

Note here that the regularized Heegner points z_n actually belong to Z and not just Z_p.

Proposition 2.7 *In all cases, the points $z_n \in Z_p$ are norm-compatible, i.e.,*

$$\sum_{\sigma \in G_{n+1,n}} z_{n+1}^{\sigma} = z_n.$$

Proof: A direct calculation.

2.6 Heegner points in the extended Mordell-Weil group

Let $E^\dagger(K_n)$ denote the extended Mordell-Weil group which is defined in sec. 1.10. Thus $E^\dagger(K_n)$ fits into an exact sequence

$$0 \longrightarrow Q \longrightarrow E^\dagger(K_n) \longrightarrow E(K_n) \longrightarrow 0,$$

where $Q \subset (K_0 \otimes \mathbb{Q}_p)^*$ is a discrete subgroup whose rank, t, is equal to:
a) Zero, if p does not divide N.
b) The number of primes of K_0 above p, if p divides N^-. This number is always equal to $[K_0 : K]$.
c) The number of primes of K_0 above p, if p divides N^+ and $E_{/\mathbb{Q}_p}$ has split multiplicative reduction.
d) The number of primes of even degree of K_0 above p, if p divides N^+ and $E_{/\mathbb{Q}_p}$ has non-split multiplicative reduction.

Suppose we are in the indefinite case, so that the regularized points z_n belong to $E(K_n) \otimes \mathbb{Z}_p$. Let $\tilde{z}_n^0$ be an arbitrary lift of z_n to $E^\dagger(K_n) \otimes \mathbb{Z}_p$ for each n. Then, if $m > n$, the points $\mathrm{Norm}_{K_m/K_n}(\tilde{z}_m^0)$ are well-defined in $E^\dagger(K_n) \otimes \mathbb{Z}_p$, modulo $p^{m-n}Q$, and form a Cauchy sequence. Hence, the limit

$$\tilde{z}_n = \lim_{m \longrightarrow \infty} \mathrm{Norm}_{K_m/K_n}(\tilde{z}_m^0)$$

exists in $E^\dagger(K_n) \otimes \mathbb{Z}_p$. In the definite case, we make the convention that $\tilde{z}_n := z_n$.
Remark: It will follow from the results of [BD4] that the points $\tilde{z}_n$ belong to $E^\dagger(K_n) \subset E^\dagger(K_n) \otimes \mathbb{Z}_p$ when $\epsilon(N) = -1$ and $p|N^-$ (i.e., in the indefinite, non-split exceptional case). When $\epsilon(N) = -1$ and $p|N^+$ (in the indefinite, split exceptional case), one does not expect such a rationality statement for the points $\tilde{z}_n$.

From prop. 2.7, it follows immediately that:

Corollary 2.8 *In all cases, the points $\tilde{z}_n$ are norm-compatible, i.e.,*

$$\sum_{\sigma \in G_{n+1,n}} \tilde{z}_{n+1}^\sigma = \tilde{z}_n.$$

2.7 The theta-elements and p-adic L-functions

If Z is any $\mathbb{Z}$-module, we let as in the previous section $Z_p := Z \otimes \mathbb{Z}_p$. Furthermore we denote by $Z_p[G_n]$ the induced module $Z_p \otimes \mathbb{Z}[G_n]$, and by $Z_p[[G_\infty]] = \lim_{\leftarrow} Z_p[G_n]$ the completed group ring tensored with Z_p, where the inverse limit is taken with respect to the natural homomorphisms $Z_p[G_n] \longrightarrow Z_p[G_m]$ induced from the projections $G_n \longrightarrow G_m$ for $n \geq m$.

Using the regularized Heegner points $\tilde{z}_n$ introduced in the previous section, we define the theta-elements

$$\theta_n = \sum_{\sigma \in G_n} (\tilde{z}_n^\sigma) \cdot \sigma^{-1} \in Z_p[G_n].$$

(Recall that $Z_p = \mathbb{Z}_p$ in the definite case, and that $Z_p = E^\dagger(K_\infty) \otimes \mathbb{Z}_p$ in the indefinite case. Recall also that here we are assuming that the curve E is ordinary at p.)

Cor. 2.8 shows that the elements θ_n are compatible under the natural projections $\nu_{n+1,n} : Z_p[G_{n+1}] \longrightarrow Z_p[G_n]$ induced by the homomorphisms $G_{n+1} \longrightarrow G_n$.

Hence, we can define

$$\theta = \theta_\infty = \lim_{\leftarrow} \theta_n \in Z_p[[G_\infty]].$$

Let $x \mapsto x^*$ be the involution on $Z_p[G_n]$ induced by $\sigma \mapsto \sigma^{-1}$ on group-like elements. Consider the tensor product of $Z_p[[G_\infty]]$ with itself, taken over the ring $\mathbb{Z}_p[[G_\infty]]$. This is naturally isomorphic to $Z_p^{\otimes 2}[[G_\infty]]$. We define the "$p$-adic L-function" $\mathcal{L}$ in $Z_p^{\otimes 2}[[G_\infty]]$ by the formula

$$\mathcal{L}_n = \theta_n \otimes \theta_n^*, \quad \mathcal{L} = \lim_{\leftarrow} \mathcal{L}_n,$$

where the product is taken formally.

2.8 Classical L-functions and parity conjectures

Let $L(E/\mathbb{Q}, s) = \prod_{\ell \nmid N}(1 - a_\ell \ell^{-s} + \ell^{1-2s})^{-1} \prod_{\ell | N}(1 - a_\ell \ell^{-s})^{-1}$ be the complex (Hasse-Weil) L-function of E over $\mathbb{Q}$. By Wiles's theorem this L-function is the L-series of an eigenform f on $\Gamma_0(N)$, and the work of Hecke shows that the function $\Lambda(E/\mathbb{Q}, s) = (2\pi)^{-s} N^{s/2} \Gamma(s) L(E/\mathbb{Q}, s)$ extends to an entire function and satisfies the functional equation

$$\Lambda(E/\mathbb{Q}, s) = -w\Lambda(E/\mathbb{Q}, 2 - s),$$

where w is the eigenvalue of the Atkin-Lehner involution $W_{N,1}$ acting on f in $S_2(\Gamma_0(N))$.

Likewise, let

$$L(E/K, s) = \prod_{v \nmid N}(1 - a_v N v^{-s} + N v^{1-2s})^{-1} \prod_{v | N}(1 - a_v N v^{-s})^{-1},$$

where the product is taken over all finite places v of K. By defining

$$\Lambda(E/K, s) = (2\pi)^{-2s} N^s |D|^s \Gamma(s)^2 L(E/K, s),$$

we find (cf. [GZ], p. 71) that $L(E/K, s)$ satisfies the functional equation

$$\Lambda(E/K, s) = -\epsilon(N)\Lambda(E/K, 2 - s). \quad (9)$$

Note that the sign in the functional equation (9) is 1 if X_{N^+,N^-} corresponds to a definite quaternion algebra, and is -1 if X_{N^+,N^-} corresponds to an indefinite quaternion algebra.

Let $E(K)^+$ and $E(K)^-$ be the $+$ and $-$ eigenspaces for complex conjugation acting on the Mordell-Weil groups $E(K)$, let r^+ and r^- denote their ranks over $\mathbb{Z}$, and let r be the rank of $E(K)$. The functional equations allow us to predict the parity of the order of vanishing of $L(E/K,s)$ and $L(E/\mathbb{Q},s)$, and hence the Birch Swinnerton-Dyer conjecture can be used to predict the parities of r, r^+ and r^-.

Conjecture 2.9 *1. If $\epsilon(N)=1$, then r is odd. More precisely, r^+ is even and r^- is odd, if $w=-1$, and r^+ is odd and r^- is even, if $w=1$.*

2. If $\epsilon(N)=-1$, then r is even. More precisely, r^+ and r^- are both even if $w=-1$, and r^+ and r^- are both odd if $w=1$.

More generally, let $\chi : G_n \longrightarrow \mathbb{C}^*$ be a complex valued character, and let $\chi(\theta_n) \in Z_p \otimes \mathbb{C}$ be the natural image of θ_n by χ.

One also has the twisted L-function

$$L(E/K,\chi,s)=\prod_{v\nmid N}(1-\chi(v)a_vNv^{-s}+\chi^2(v)Nv^{1-2s})^{-1}\prod_{v|N}(1-\chi(v)a_vNv^{-s})^{-1},$$

which has a functional equation analogous to (9) relating its value at s and $2-s$. The sign in this functional equation is $-\epsilon(N)$ as in formula (9) if χ is unramified at p, and is $-\epsilon(N')$ otherwise, where N' is the prime-to p part of N:

$$N'=\begin{cases} N/p \text{ if } p|N,\\ N \text{ otherwise.}\end{cases}$$

Note here that the sign in the functional equation is 1 if $X_{N_*^+,N_*^-}$ corresponds to a definite quaternion algebra, and is -1 if $X_{N_*^+,N_*^-}$ corresponds to an indefinite quaternion algebra. Notice also that the signs for $L(E/K,s)$ and $L(E/K,\chi,s)$ are the same, *except* in the case where p divides N and $\epsilon(p)=-1$ (i.e., in the non-split exceptional case), which is precisely the case when X_{N^+,N^-} and $X_{N_*^+,N_*^-}$ are different Shimura curves, corresponding to quaternion algebras with opposite ramification types at ∞.

The space $(E(K_n)\otimes\mathbb{C})$ is a finite dimensional complex vector space endowed with an action of the Galois group G_n. Let r_χ be the dimension of the χ-eigenspace $(E(K_n)\otimes\mathbb{C})^\chi$ for this action. The parity conjecture allows us to predict the parity of r_χ. It is reasonable to expect that the values of r_χ are equal to 0 or 1 for almost all values of χ as χ varies over the anticyclotomic characters of all the G_n. The following is a slight generalization of a conjecture of Mazur [Ma2]:

Conjecture 2.10 *1. If $\epsilon(N') = 1$, then $E(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ has corank 1 over the Iwasawa algebra $\mathbb{Z}_p[[G_\infty]]$.*

2. If $\epsilon(N') = -1$, then $E(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is of corank 0 over the Iwasawa algebra $\mathbb{Z}_p[[G_\infty]]$. (I.e., $E(K_\infty)$ is a finitely generated $\mathbb{Z}$-module.)

2.9 Parity conjectures for the extended Mordell-Weil group

Conjecture 2.9 immediately implies the following:

Conjecture 2.11 *1. If $\epsilon(N') = 1$, then $\tilde{r}$ is odd. More precisely, $\tilde{r}^+$ is even and $\tilde{r}^-$ is odd, if $w' = -1$, and $\tilde{r}^+$ is odd and $\tilde{r}^-$ is even, if $w' = 1$.*

2. If $\epsilon(N') = -1$, then $\tilde{r}$ is even. More precisely, $\tilde{r}^+$ and $\tilde{r}^-$ are both even if $w' = -1$, and $\tilde{r}^+$ and $\tilde{r}^-$ are both odd if $w' = 1$.

2.10 Relation with classical L-values

In this section we explain how θ and $\mathcal{L}$ ought to be related to special values of the classical L-functions $L(E/K, \chi, s)$. This section is intended for *motivation only*, and will not be used elsewhere.

Choose an embedding $\mathbb{Z}_p \longrightarrow \mathbb{C}$, and let α denote, by abuse of notation, the complex root of $x^2 - a_p x + p$ (or $x^2 - a_p x$) which is the image of the $\alpha \in \mathbb{Z}_p$ chosen previously, and let $\bar{\alpha}$ denote the non-unit root. Suppose that χ is a primitive character on G_n for some n. Define the local multiplier $L_p(\chi)$ by the formula:

$$L_p(\chi) = \begin{cases} \alpha^{-n} & \text{if } n \geq 1, \\ (1 - \alpha^{-2}) & \text{if } n = 0, \epsilon(p) = -1, \\ (1 - \alpha^{-1}\chi(\sigma_{\mathfrak{p}_1}))(1 - \alpha^{-1}\chi(\sigma_{\mathfrak{p}_2})) & \text{if } n = 0, \epsilon(p) = 1, p \nmid N, \\ (1 - \alpha^{-1}\chi(\sigma)) & \text{if } n = 0, \epsilon(p) = 1, p | N. \end{cases} \tag{10}$$

The embedding $\mathbb{Z}_p \longrightarrow \mathbb{C}$ gives rise to a natural linear map $Z_p^{\otimes 2} \longrightarrow \mathbb{C}$ induced by the normalized Néron-Tate height in the indefinite case (when

$Z_p = E^\dagger(K_\infty)\otimes\mathbb{Z}_p$) and by multiplication in the definite case (when $Z_p = \mathbb{Z}_p$). Let $\mathcal{L}_{\mathbb{C}} \in \mathbb{C}[[G_\infty]]$ be the element deduced from $\mathcal{L}$ by applying this map to the coefficients. Then we have:

Conjecture 2.12 *Let $\chi(\mathcal{L}_{\mathbb{C}}) \in \mathbb{C}$ be the element obtained by applying χ to the element $\mathcal{L}_{\mathbb{C}}$.*

1. *In the indefinite case,*

$$\chi(\mathcal{L}_{\mathbb{C}}) = L_p(\chi)^2 \cdot \frac{L'(E/K,\chi,1)}{\Omega} \cdot \sqrt{D} \cdot \prod_{\ell|N^-} m_\ell^{-1},$$

   where $D = Disc(\mathcal{O})$.

2. *In the definite case,*

$$\chi(\mathcal{L}_{\mathbb{C}}) = L_p(\chi)^2 \cdot \frac{L(E/K,\chi,1)}{\Omega} \cdot \sqrt{D} \cdot \prod_{\ell|N^-} m_\ell^{-1}.$$

A number of cases of this conjecture have been established, thanks to the work of Gross-Zagier [GZ] and Gross [Gr2].
Case 1: The indefinite case. In [GZ], the formula relating the heights of Heegner points to derivatives of L-series at $s = 1$ is established when $X_{N^+,N^-} = X_{N,1} = X_0(N)$ is the modular curve of level N (i.e., when all primes dividing the conductor N are split in $K/\mathbb{Q}$), and when χ is an unramified character of $\mathrm{Gal}(K^{ab}/K)$ (i.e., when the conductor c that was fixed in sec. 2.1 is equal to 1, so that K_0 is the Hilbert class field of K, and when χ factors through G_0). However, it seems likely that the methods of Gross and Zagier would extend to prove the general case. For more details, see the discussion in [GZ], p. 130-133, and forthcoming work of Keating and Kudla.
Case 2: The definite case. Here, the formula has been proved, for forms of weight 2 and prime conductor, and for unramified characters of K, by Gross in [Gr2]. The methods of [Gr2] should extend to arbitrary levels.

Although the Gross-Zagier formulas are not completely worked out in the generality in which we formulate them in conjecture 2.12, we mention this conjecture for *motivation only*, and will not require the precise result at any stage of our calculations.

Conj. 2.12 suggests the following philosophy. When $\mathcal{L}$ is constructed from Heegner points attached to an indefinite Shimura curve, then the element $\mathcal{L}_{\mathbb{C}}$ is interpolating the special values of $L'(E/K,\chi,1)$. When $\mathcal{L}$ comes from a definite Shimura curve, then $\mathcal{L}_{\mathbb{C}}$ interpolates the special values of $L(E/K,\chi,1)$. Hence the "p-adic analytic" properties of $\mathcal{L}$ should be similar to those of $L'(E/K,s)$ (resp. $L(E/K,s)$) in the indefinite (resp. definite) case, in a manner which is consistent with the classical Birch Swinnerton-Dyer conjectures. This is the philosophy that has guided us in formulating our conjectures of Mazur-Tate-Teitelbaum type.

2.11 Extra zeroes

Conjecture 2.12 predicts that $\chi(\mathcal{L}_{\mathbb{C}})$ is equal to zero when the L-functions $L(E/K,\chi,1)$ (resp. $L'(E/K,\chi,1)$) vanish in the definite (resp. indefinite) cases *or* when the p-adic multiplier term $L_p(\chi)$ is equal to zero. This vanishing of the p-adic multiplier term occurs if and only if $n=0$, and

1. p divides N^+, and $a_p=\chi(\mathrm{Frob}_p)$, or
2. p divides N^-.

In particular, if χ is the trivial character, then $L_p(\chi)$ vanishes precisely in the following two situations:

1. In the split exceptional case, i.e., when p divides N^+, and $a_p=1$.
2. In the non-split exceptional case, i.e., p divides N^-.

2.12 The functional equation for θ

Let $x\mapsto x^*$ be the involution on $Z_p[G_n]$ sending $\sum_\sigma a_\sigma\cdot\sigma$ to $\sum_\sigma a_\sigma\cdot\sigma^{-1}$. Let $x\mapsto \tau x$ be the involution induced by complex conjugation on Z_p. (Thus, τ is the identity when $Z_p=\mathbb{Z}_p$, and is complex conjugation on $E(K_n)\otimes\mathbb{Z}_p$ in the indefinite case.)

Proposition 2.13 *There exists $\gamma\in G_\infty$ such that*

$$\tau\theta = w'_{N_*^+,N_*^-}\theta^*\gamma = \epsilon(N')w'\theta^*\gamma.$$

Proof: Let n be greater than or equal to 1. Using the fact that $\tau\sigma = \sigma^{-1}\tau$ for all $\sigma \in G_n$, together with prop. 2.6, we have:

$$\tau\theta_n = \tau \sum_{\sigma \in G_n} \tilde{z}_n^{\sigma} \cdot \sigma^{-1} = \sum_{\sigma \in G_n} (\tau \tilde{z}_n)^{\sigma^{-1}} \cdot \sigma^{-1}$$

$$= \sum \gamma_n W'_{N_*^+, N_*^-}(\tilde{z}_n^{\sigma^{-1}}) \cdot \sigma^{-1} = w'_{N_*^+, N_*^-} \theta^* \gamma_n.$$

This proposition can be viewed as giving a "functional equation" for the p-adic L-function corresponding to θ. We spell it out in the various special cases:

Case 1: The definite case: In that case complex conjugation τ acts trivially on Z_p, and $\epsilon(N') = -1$. Hence the functional equation becomes

$$\theta = -w'\theta^* \pmod{G_\infty}. \tag{11}$$

Case 2: The indefinite case: In that case $\epsilon(N') = 1$, so the functional equation becomes

$$\tau\theta = w'\theta^* \pmod{G_\infty}. \tag{12}$$

Let I_n be the augmentation ideal in the group ring $\mathbb{Z}_p[G_n]$. We say that θ_n vanishes to order ρ if θ_n belongs to $Z_p \otimes I_n^\rho$, and that θ vanishes to order ρ if θ_n vanishes to order ρ for all n. The *order of vanishing* of θ is the greatest ρ such that θ vanishes to order ρ. If ρ is the order of vanishing of θ, we let $\bar{\theta}$ denote the projection of θ to $Z_p \otimes I^\rho / I^{\rho+1}$.

Lemma 2.14 *In the indefinite case, $\bar{\theta}$ belongs to $(E^\dagger(K_\infty) \otimes I^\rho/I^{\rho+1})^{G_\infty}$.*

This is readily checked.

As in the classical case, the functional equation allows us to deduce some information about the parity of ρ and the nature of the leading term $\bar{\theta}$.

Corollary 2.15 *Let ρ be the order of vanishing of θ.*

1. *In the definite case, ρ is even if $w' = -1$, and ρ is odd if $w' = 1$.*

2. *In the indefinite case, $\bar{\theta}$ belongs to the $(-1)^\rho w'$- eigenspace for complex conjugation acting on $(E^\dagger(K_\infty) \otimes I^\rho/I^{\rho+1})^{G_\infty}$.*

Proof: Let ρ be the order of vanishing of θ, and let $\bar{\theta}$ be the image of θ in $Z_p \otimes I^\rho/I^{\rho+1}$. The involution $*$ acts by multiplication by $(-1)^\rho$ on $Z \otimes (I^\rho/I^{\rho+1})$. In the definite case, equation (11) implies

$$\bar{\theta} = -w'(-1)^\rho \bar{\theta}.$$

Since $\bar{\theta}$ is non-zero, we have $-w'(-1)^\rho = 1$, which implies the parity statement for ρ. In the indefinite case, equation (12) implies

$$t\bar{\theta} = w'(-1)^\rho \bar{\theta},$$

where t is the eigenvalue for τ acting on $\bar{\theta}$. Hence $t = w'(-1)^\rho$.

3 The regulator term

3.1 p-adic heights

For the rest of this paper, assume to simplify matters that $c = 1$, so that G_∞ is an extension of the class group of K by $G_\infty^0 = (\mathcal{O}_K^*)\backslash(\mathcal{O}_K \otimes \mathbb{Z}_p)^*/\mathbb{Z}_p^*$. Let I be the augmentation ideal in the completed group ring $\mathbb{Z}[[G_\infty]]$. The map $G_\infty \longrightarrow I/I^2$ which sends g to $(g-1)$ identifies G_∞ with I/I^2. For any place v of K, let $\mathrm{rec}_v : K_v^* \longrightarrow I/I^2$ be the reciprocity law map of local class field theory. Finally let

$$\mathrm{rec} : \mathbb{A}_K^* \longrightarrow I/I^2$$

be the reciprocity law map of global class field theory (where $\mathbb{A}_K$ denotes the ring of adèles of K).

Let $E^0(K)$ denote the subgroup of points of $E(K)$ that reduce to the connected component of the Néron model of E over $\mathrm{Spec}(\mathbb{Z})$ and let $E_0^\dagger(K)$ denote the full inverse image of $E^0(K)$ in $E^\dagger(K)$. Let $\mathcal{P}$ denote the set of primes above p in K at which E has split multiplicative reduction (this set has cardinality 0 in the non-exceptional case, 1 in the non-split exceptional case, and 2 in the split exceptional case), and denote by $\mathbb{Z}^\mathcal{P}$ the set of maps from $\mathcal{P}$ to $\mathbb{Z}$. For each $\mathfrak{p} \in \mathcal{P}$, let $q_\mathfrak{p}$ denote the Tate period for E at $\mathfrak{p}$.

There is an exact sequence

$$0 \longrightarrow \mathbb{Z}^\mathcal{P} \longrightarrow E_0^\dagger(K) \longrightarrow E^0(K) \longrightarrow 0. \tag{13}$$

The map $E_0^\dagger(K) \longrightarrow E^0(K)$ is the natural projection sending $(\tilde{P}, P)$ to P, and the map from $\mathbb{Z}^{\mathcal{P}}$ to $E_0^\dagger(K)$ sends $h \in \mathbb{Z}^{\mathcal{P}}$ to the point $(\tilde{P}, P)$ given by $P = 0$ and

$$\tilde{P} = \prod_{\mathfrak{p} \in \mathcal{P}} q_{\mathfrak{p}}^{h(\mathfrak{p})}.$$

The exact sequence (13) has a natural splitting $E^0(K) \longrightarrow E_0^\dagger(K)$ by sending P to $(\tilde{P}_{unit}, P)$ where $\tilde{P}_{unit}$ is a unit in K_p^* at all places $\mathfrak{p}$ of $\mathcal{P}$. In this way we can identify $E_0^\dagger(K)$ with $\mathbb{Z}^{\mathcal{P}} \times E^0(K)$.

We define bilinear pairings

$$\begin{aligned} \langle\ ,\ \rangle_1 : &\quad E^0(K) \times E^0(K) \longrightarrow I/I^2, \\ \langle\ ,\ \rangle_2 : &\quad \mathbb{Z}^{\mathcal{P}} \times E^0(K) \longrightarrow (I/I^2) \otimes \mathbb{Q}_p, \\ \langle\ ,\ \rangle_3 : &\quad \mathbb{Z}^{\mathcal{P}} \times \mathbb{Z}^{\mathcal{P}} \longrightarrow (I/I^2) \otimes \mathbb{Q}_p, \end{aligned}$$

as follows:

1. $\langle P, P \rangle_1 = \mathrm{rec}((\alpha_v))$, where (α_v) is an idèle in $\lim_{\leftarrow} \hat{\mathcal{O}}_{p^n}^* \backslash \hat{K}^*/K^*$ defined by

$$\alpha_v = \pi_v^{\max(0, -ord_v(x(P_v)))}, \text{ for } v \not| p, \quad \alpha_v = \sigma^2(P), \text{ for } v|p,$$

where σ is the p-adic σ-function (cf. [MTT], p. 30-33 or [MT1]), π_v is a uniformizer at v, and $x(P_v)$ is the x coordinate of the point P, in the minimal Weierstrass model for E over K_v.

2. $\langle g, P \rangle_2 = \sum_{\mathfrak{p} \in \mathcal{P}} g(\mathfrak{p}) \mathrm{ord}_{\mathfrak{p}}(q_{\mathfrak{p}})^{-1} \mathrm{rec}_{\mathfrak{p}}(\tilde{P}_{unit})$.

3. $\langle g, h \rangle_3 = \sum_{\mathfrak{p} \in \mathcal{P}} \mathrm{ord}_{\mathfrak{p}}(q_{\mathfrak{p}})^{-1} g(\mathfrak{p}) h(\mathfrak{p}) \mathrm{rec}_{\mathfrak{p}}(q_{\mathfrak{p}})$.

Following [MTT], we combine the pairings $\langle\ ,\ \rangle_1$, $\langle\ ,\ \rangle_2$, and $\langle\ ,\ \rangle_3$ to obtain the symmetric bilinear Mazur-Tate pairing on $\mathbb{Z}^{\mathcal{P}} \times E^0(K) = E_0^\dagger(K)$ with values in $(I/I^2) \otimes \mathbb{Q}_p$. Since the value group is divisible, and since $E_0^\dagger(K)$ has finite index in $E^\dagger(K)$, we can extend this pairing uniquely to a pairing

$$\langle\ ,\ \rangle_{MTT} : E^\dagger(K) \times E^\dagger(K) \longrightarrow (I/I^2) \otimes \mathbb{Q}_p.$$

Let ϵ be a formal element satisfying $\epsilon^2 = 0$; following [Da2], §3.1, we set

$$\langle P, Q \rangle = \langle P, Q \rangle_{MTT} + \epsilon(P \otimes Q).$$

This pairing takes values in the module $M \otimes \mathbb{Q}_p$, where

$$M = (I/I^2) \oplus \epsilon(E^\dagger(K)^{\otimes 2}).$$

Behaviour under complex conjugation: If γ is any Galois automorphism, it acts on $E^\dagger(K)$ in the natural way (using the action of complex conjugation on $E^\dagger(K)$ that was defined in sec. 1.10) and acts on $I/I^2 = G_\infty$ by conjugation. The pairing $\langle\ ,\ \rangle_{MTT}$ has the Galois-equivariance property:

$$\langle \gamma P, \gamma Q \rangle_{MTT} = \langle P, Q \rangle_{MTT}^{\gamma}.$$

In particular, if $\gamma = \tau$ is complex conjugation, we find:

$$\langle \tau P, \tau Q \rangle_{MTT} = -\langle P, Q \rangle_{MTT},$$

since τ acts on $I/I^2 = G_\infty$ as multiplication by -1.

Corollary 3.1 *The subspaces $E^\dagger(K)^+$ and $E^\dagger(K)^-$ are isotropic for the Mazur-Tate pairing $\langle\ ,\ \rangle_{MTT}$.*

3.2 The regulator

Let Λ_M be the formal graded commutative algebra having M as module of degree 1 elements. Thus,

$$\Lambda_M = \oplus_{k=0}^{\infty} \Lambda_M^{(k)},$$

$$\Lambda_M^{(0)} = \mathbb{Z}, \quad \Lambda_M^{(k)} = (I^k/I^{k+1}) \oplus \epsilon(I^{k-1}/I^k \otimes E^\dagger(K)^{\otimes 2}).$$

Given an $r \times r$ matrix with entries in M, its determinant can be defined to be the obvious element in $\Lambda_M^{(r)}$.

Let $P_1, \ldots, P_{\tilde{r}}$ be a $\mathbb{Z}$-basis for the group $E^\dagger(K)$ modulo torsion, and let t denote the index of the $\mathbb{Z}$-module generated by $P_1, \ldots, P_{\tilde{r}}$ in the full extended Mordell-Weil group $E^\dagger(K)$. We define the regulator $\mathcal{R}$ by the formula

$$\mathcal{R} = \frac{1}{t^2} \det(\langle P_i, P_j \rangle) \in \Lambda_M^{(\tilde{r})} \otimes \mathbb{Q}_p,$$

and we write

$$\mathcal{R} = R_{MTT} + \epsilon R'_{MTT}.$$

The notation is justified, as the reader will verify: the term R_{MTT} is the original Mazur-Tate regulator obtained by taking the determinant of the p-adic pairing of Mazur and Tate, with the anticyclotomic p-adic height replacing the cyclotomic height pairing. The term R'_{MTT} can be thought of as a "formal deformation" of the Mazur-Tate regulator. It belongs to $(I^{\tilde{r}-1}/I^{\tilde{r}}) \otimes E^{\dagger}(K)^{\otimes 2} \otimes \mathbb{Q}_p$. We now give a more explicit description. Let R_{ij} be the (i,j)-th minor of the pairing matrix $(\langle P_i, P_j \rangle_{MTT})_{i,j \leq \tilde{r}}$, in $I^{\tilde{r}-1}/I^{\tilde{r}}$. Then we have:

$$R'_{MTT} = \frac{1}{t^2} \sum_{i,j=1}^{\tilde{r}} (-1)^{i+j} P_i \otimes P_j \otimes R_{ij}.$$

For more details, see [Da1] and [Da2].

The regulator when $\tilde{r}$ is even: In that case, we have

Lemma 3.2 *If $\tilde{r}^+ \neq \tilde{r}^-$, then the term R_{MTT} vanishes, and so does R'_{MTT}.*

Proof: If $\tilde{r}^+ \neq \tilde{r}^-$, then the ranks of these spaces differ by at least 2. Hence by cor. 3.1 $E^{\dagger}(K)$ contains an isotropic subspace of rank $> \tilde{r}/2$. Therefore the determinant of the pairing matrix $(\langle P, Q \rangle_{MTT})$, and its $(\tilde{r}-1) \times (\tilde{r}-1)$ minors, vanish.

Let $P_1^+, \dots P_a^+$ be a basis for $E^{\dagger}(K)^+$ modulo torsion, and let $P_1^-, \dots, P_b^-$ be a basis for $E^{\dagger}(K)^-$ modulo torsion. Let t denote the index of the group generated by these points in $E^{\dagger}(K)$. A direct computation shows:

Lemma 3.3 *If $\tilde{r}^+ = \tilde{r}^-$, then*

$$R_{MTT} = -\frac{1}{t^2} \det(\langle P_i^+, P_j^- \rangle_{MTT})^2.$$

Since the expression for R_{MTT} is essentially a square, we set $R_{MTT}^{1/2} := \frac{1}{t} \det(\langle P_i^+, P_j^- \rangle_{MTT})$ when $\tilde{r}^+ = \tilde{r}^-$, and $R_{MTT}^{1/2} = 0$ otherwise. Note that $R_{MTT}^{1/2}$ is only defined up to sign. The p-adic height pairing in the cyclotomic setting is conjectured to be non-degenerate (cf. [MTT], p. 38). This motivates the following:

Conjecture 3.4 *The regulator $R_{MTT}^{1/2}$, and hence also R_{MTT}, is always non-zero when $\tilde{r}^+ = \tilde{r}^-$.*

The regulator when $\tilde{r}$ is odd: In that case, we have

Lemma 3.5 *The term R_{MTT} always vanishes. If $|\tilde{r}^+ - \tilde{r}^-| > 1$, then R'_{MTT} also vanishes.*

Proof: It is the same as for lemma 3.2.

We now give a more explicit description of the regulator R'_{MTT} in the case where $|\tilde{r}^+ - \tilde{r}^-| = 1$. Consider the pairing

$$(E^\dagger(K) \otimes \mathbb{Z}_p)^+ \times (E^\dagger(K) \otimes \mathbb{Z}_p)^- \longrightarrow (I/I^2) \otimes \mathbb{Q}$$

induced by $\langle\ ,\ \rangle_{MTT}$. Let P be an element of $E^\dagger(K) \otimes \mathbb{Z}_p$ such that

1. P belongs to the largest eigenspace for complex conjugation, and belongs to the radical of the pairing $\langle\ ,\ \rangle_{MTT}$.
2. P is not divisible by p in $E^\dagger(K) \otimes \mathbb{Z}_p$.

Complete P to a basis $(P, P_1^+, \ldots, P_s^+, P_1^-, \ldots, P_s^-)$ of $E^\dagger(K) \otimes \mathbb{Z}_p$, where $s = (\tilde{r}-1)/2$, and the $P_i^\pm$ belong to $(E^\dagger(K) \otimes \mathbb{Z}_p)^\pm$. Assume furthermore that the basis is chosen so that it is equivalent, by a transformation in $\mathbf{GL}_{\tilde{\mathbf{r}}}(\mathbb{Z}_\mathbf{p})$ of determinant 1, to an integral basis for $E^\dagger(K)$ modulo torsion. A direct computation shows

Lemma 3.6 *If $|\tilde{r}^+ - \tilde{r}^-| = 1$, then*

$$R'_{MTT} = -\frac{1}{t^2}(P \otimes P) \otimes \det(\langle P_i^+, P_j^- \rangle_{MTT})^2.$$

Since the expression for R'_{MTT} is essentially a square, we set

$$R_{MTT}^{'1/2} := \frac{1}{t} P \otimes \det(\langle P_i^+, P_j^- \rangle_{MTT})$$

when $\tilde{r}^+$ and $\tilde{r}^-$ differ by at most 1, and set $R_{MTT}^{'1/2} = 0$ otherwise. The term $R_{MTT}^{'1/2}$ belongs to $E^\dagger(K) \otimes (I^s/I^{s+1}) \otimes \mathbb{Q}$, and is only well defined up to sign.

The following conjecture is a natural generalization of a conjecture of Mazur [Ma3].

Conjecture 3.7 *The pairing*

$$(E^\dagger(K) \otimes \mathbb{Z}_p)^+ \times (E^\dagger(K) \otimes \mathbb{Z}_p)^- \longrightarrow (I/I^2) \otimes \mathbb{Q}$$

induced by $\langle\ ,\ \rangle_{MTT}$ is either left or right non-degenerate.

This conjecture implies that if $|\tilde{r}^+ - \tilde{r}^-| = 1$, the radical of the pairing is of rank 1 over $\mathbb{Z}_p$, and belongs to the larger of the two eigenspaces under complex conjugation. It implies also that the regulator R'_{MTT} is always non-zero when $|\tilde{r}^+ - \tilde{r}^-| = 1$.

We say that we are in an *unbalanced case* if $|\tilde{r}^+ - \tilde{r}^-| > 1$. In the unbalanced case we always have $\mathcal{R} = 0$.

4 The conjecture

4.1 Orders of vanishing

Conjecture 4.1 *Let ρ be the exact order of vanishing of θ.*

1. *In the definite case, ρ is equal to* $\max(\tilde{r}^+, \tilde{r}^-)$.
2. *In the indefinite case, ρ is equal to* $\max(\tilde{r}^+, \tilde{r}^-) - 1$.

This conjecture may appear somewhat unmotivated. Evidence for it is given in [B1], [B2], [Da1], [Da3], and [BD2].

Assume the parity conjecture. Then $\tilde{r}$ is even in the definite case and $2\max(\tilde{r}^+, \tilde{r}^-) \geq \tilde{r}$, with equality if and only if $\tilde{r}^+ = \tilde{r}^-$. In the indefinite case, $\tilde{r}$ is odd and $2(\max(\tilde{r}^+, \tilde{r}^-) - 1) \geq \tilde{r} - 1$, with equality if and only if $|\tilde{r}^+ - \tilde{r}^-| = 1$. Conjecture 4.1 can therefore be restated in terms of $\mathcal{L}$ in a weaker form, but which may appear more natural in light of the conjecture that will be made in sec. 4.2:

Conjecture 4.2 .

1. *In the definite case, $\mathcal{L}$ vanishes to order at least $\tilde{r}$, and vanishes to order exactly $\tilde{r}$ if and only if $\tilde{r}^+ = \tilde{r}^-$.*
2. *In the indefinite case, $\mathcal{L}$ vanishes to order at least $\tilde{r} - 1$, and vanishes to order exactly $\tilde{r} - 1$ if and only if $|\tilde{r}^+ - \tilde{r}^-| = 1$.*

4.2 The leading term

Motivated by conj. 4.2, define the leading coefficient $\bar{\mathcal{L}}$ to be the projection of $\mathcal{L}$ to the value group $I^{\tilde{r}}/I^{\tilde{r}+1}$ in the definite case, and to $Z^{\otimes 2} \otimes I^{\tilde{r}-1}/I^{\tilde{r}} =$

$E^\dagger(K)^{\otimes 2} \otimes (I^{\tilde{r}-1}/I^{\tilde{r}})$ in the indefinite case. For each rational prime q, let m_q denote the number of connected components in the Néron model of E over $\mathbb{F}_q$, and let $m = \prod_{q|N^+} m_q$.

The definite case: Then the parity conjecture 2.11 implies that $\tilde{r}$ is even, so that $\tilde{r}^+ \equiv \tilde{r}^- \pmod 2$. In that case, the regulator R_{MTT} defined in sec. 3.2 belongs to $(I^{\tilde{r}}/I^{\tilde{r}+1}) \otimes \mathbb{Q}$.

Conjecture 4.3 *The following equality holds in* $(I^{\tilde{r}}/I^{\tilde{r}+1}) \otimes \mathbb{Q}$*:*

1. *(Non-exceptional case):*

$$\bar{\mathcal{L}} = L_p(1)^2 \cdot \#\underline{III}(E/K) \cdot R_{MTT} \cdot m^2.$$

2. *(Exceptional case):*

$$\bar{\mathcal{L}} = \#\underline{III}(E/K) \cdot R_{MTT} \cdot m^2.$$

Let $s = \tilde{r}/2$. We observe that the leading coefficient $\bar{\mathcal{L}}$ is essentially the square of the element $\bar{\theta}$, the projection of θ to I^s/I^{s+1}. All the terms occuring on the right of our conjectured formula are also squares, so it is natural to reformulate conjecture 4.3 in terms of the square roots:

Conjecture 4.4 *The following equality holds in* $(I^s/I^{s+1}) \otimes \mathbb{Q}$*:*

1. *(Non-exceptional case):*

$$\bar{\theta} = \pm L_p(1) \cdot \sqrt{\#\underline{III}(E/K)} \cdot R_{MTT}^{1/2} \cdot m.$$

2. *(Exceptional case):*

$$\bar{\theta} = \pm \sqrt{\#\underline{III}(E/K)} \cdot R_{MTT}^{1/2} \cdot m.$$

The indefinite case: Suppose we are in the indefinite case. Then the parity conjecture 2.11 implies that $\tilde{r}$ is odd, so that $\tilde{r}^+ \not\equiv \tilde{r}^- \pmod 2$. In that case, the regulator R_{MTT} is always zero, and the regulator R'_{MTT} defined in sec. 3.2 belongs to $E^\dagger(K)^{\otimes 2} \otimes I^{\tilde{r}-1}/I^{\tilde{r}} \otimes \mathbb{Q}$. The leading coefficient $\bar{\mathcal{L}}$ belongs to $E^\dagger(K_\infty)^{\otimes 2} \otimes I^{\tilde{r}-1}/I^{\tilde{r}}$.

Conjecture 4.5 *The following equality holds in* $E^\dagger(K)^{\otimes 2} \otimes (I^{\tilde{r}-1}/I^{\tilde{r}})_{\otimes}\mathbb{Q}$*:*

1. *(Non-exceptional case):*

$$\bar{\mathcal{L}} = L_p(1)^2 \cdot \#\underline{III}(E/K) \cdot R'_{MTT} \cdot m^2.$$

2. *(Exceptional case):*

$$\bar{\mathcal{L}} = \#\underline{III}(E/K) \cdot R'_{MTT} \cdot m^2.$$

Let $s = (\tilde{r} - 1)/2$. We observe that the leading coefficient $\bar{\mathcal{L}}$ is essentially the square of the element $\bar{\theta}$, the projection of θ to $E^\dagger(K) \otimes I^s/I^{s+1}$. Hence conj. 4.5 can also be reformulated in terms of square roots:

Conjecture 4.6 *The following equality holds in* $E^\dagger(K)^{\otimes 2} \otimes (I^s/I^{s+1}) \otimes \mathbb{Q}$*:*

1. *(Non-exceptional case):*

$$\bar{\theta} = \pm L_p(1) \cdot \sqrt{\#\underline{III}(E/K)} \cdot R'^{1/2}_{MTT} \cdot m.$$

2. *(Exceptional case):*

$$\bar{\theta} = \pm\sqrt{\#\underline{III}(E/K)} \cdot R'^{1/2}_{MTT} \cdot m.$$

Remark on the unbalanced case: We say that the extended Mordell-Weil group is *unbalanced* if $|\tilde{r}^+ - \tilde{r}^-| > 1$. In that case, the regulator terms R_{MTT} and R'_{MTT} are both 0. In harmony with this fact, conj. 4.1 predicts that $\mathcal{L}$ vanishes to order strictly greater than $\tilde{r}$ (resp. $\tilde{r} - 1$) in the definite (resp. indefinite) case. Thus conj. 4.3 and 4.5 should reduce to the equality $0 = 0$ in the unbalanced case. This is not really very satisfying, and one would like an interpretation of the projection of $\mathcal{L}$ to $Z \otimes I^{2\rho}/I^{2\rho+1}$, where ρ is $\max(\tilde{r}^+, \tilde{r}^-)$ in the definite case, and is $\max(\tilde{r}^+, \tilde{r}^-) - 1$ in the indefinite case. Such an interpretation has been proposed in the generic case, (under certain mild technical assumptions), using the notion of derived p-adic height. (Cf. [BD2] and [BD3].) It would be of interest to extend the formalism of derived heights to cover exceptional zero situations.

5 Applications and refinements

5.1 p-adic periods and p-adic L-functions

In this section, we restrict our attention to the split exceptional case, i.e., we suppose that p divides N^+ and that E has split multiplicative reduction over $\mathbb{Q}_p$. We also assume that we are in the definite case, i.e., $\epsilon(N') = \epsilon(N) = -1$.

In this case, our conjecture predicts that we can recover the values of p-adic periods from special values of the p-adic L-functions, in a manner quite analogous to [MTT]. We describe precisely how, and present some numerical evidence.

The curve $X_{N^+,N^-} = X_{N_*^+,N_*^-}$ is associated to a definite quaternion algebra. Observe that the element $\mathcal{L}$ constructed in sec. 2.7 belongs to $\mathbb{Z}[[G_\infty]]$ (and not just $\mathbb{Z}_p[[G_\infty]]$ as in the non-exceptional case). Let now $I \subset \mathbb{Z}[[G_\infty]]$ be the augmentation ideal of $\mathbb{Z}[[G_\infty]]$.

Lemma 5.1 *The element θ belongs to I.*

Proof: This follows from equation (8) in sec. 2.5, since $a_p = \alpha$ is equal to 1 in our case.

We have the exact sequence

$$1 \longrightarrow Q \longrightarrow E^\dagger(K) \longrightarrow E(K) \longrightarrow 0,$$

where $Q \subset K_p^*$ is a $\mathbb{Z}$-module of rank 2. Let us identify K_p^* with the algebra $\mathbb{Q}_p^* \times \mathbb{Q}_p^*$ by choosing an ordering of the two places of K above p. Then a basis for the module Q is given by the elements $(q, 1)$ and $(1, q)$, where $q \in \mathbb{Q}_p^*$ denotes Tate's p-adic period associated to $E_{/\mathbb{Q}_p}$. Let $\mathrm{rec}_p : K_p^* \longrightarrow I/I^2 (= G_\infty)$ be the reciprocity law map of local class field theory.

Conjectures 2.9 and 2.11 predict that $E(K)$ and $E^\dagger(K)$ have even rank. Let us suppose further that the rank of $E(K)$ is 0, so that $E(K)$ is finite of order t.

Then the regulator R_{MTT} becomes the determinant of the matrix with entries in $(I/I^2) \otimes \mathbb{Q}$:

$$R_{MTT} = \frac{1}{t^2} \det \begin{pmatrix} \mathrm{ord}_p(q)^{-1}\mathrm{rec}_p(q,1) & 0 \\ 0 & \mathrm{ord}_p(q)^{-1}\mathrm{rec}_p(1,q) \end{pmatrix}.$$

Since $\mathrm{rec}_p(q,1) = -\mathrm{rec}_p(1,q)$, we find:

$$R_{MTT} = -t^{-2}\mathrm{ord}_p(q)^{-2}\mathrm{rec}_p(q,1)^2, \quad R_{MTT}^{1/2} = \pm t^{-1}\mathrm{ord}_p(q)^{-1}\mathrm{rec}_p(q,1).$$

Conjecture 5.2 *Suppose $E(K)$ has rank zero, and let $\bar{\theta}$ be the projection of θ to $I/I^2 = G_\infty$.*

1. *The following equality holds in $(I/I^2) \otimes \mathbb{Q}$:*

$$\bar{\theta} = \pm\sqrt{\#\underline{III}(E/K)} \cdot m \cdot t^{-1} \cdot \mathrm{ord}_p(q)^{-1} \cdot \mathrm{rec}_p(q, 1).$$

2. *The following equality holds in $(I/I^2) = G_\infty$:*

$$t \cdot \mathrm{ord}_p(q) \cdot \bar{\theta} = \pm\sqrt{\#\underline{III}(E/K)} \cdot m \cdot \mathrm{rec}_p(q, 1).$$

Remark: Part 1 of the conjecture is merely a specialization of conj. 4.4. Part 2 of the conjecture is stronger, since the map $(I/I^2) \longrightarrow (I/I^2) \otimes \mathbb{Q}$ has a kernel of order $(p-1)/u_K$. Part 2 can be viewed as a "refinement" of the p-adic conjecture analagous to the refinements proposed in [MT2]. This refinement amounts to an extra congruence modulo $(p-1)/u_K$. In all of our numerical verifications, we have always tested for the stronger refined conjecture.

Combined with the classical Birch Swinnerton-Dyer conjecture, conj. 5.2 can be restated without explicitly making the hypothesis $r = 0$ in terms of the classical L-function $L(E/K, s)$ at $s = 1$, as follows:

Conjecture 5.3 *Suppose we are in the split exceptional and definite case. Let θ_1 be the projection of θ to $I/I^2 \otimes \mathbb{Q}$. Then*

$$\theta_1 = \mathrm{ord}_p(q)^{-1} \cdot \mathrm{rec}_p(q, 1) \cdot \sqrt{L(E/K, 1) D^{1/2} \Omega^{-1} \prod_{q|N^-} m_q^{-1}}.$$

Of course, if $L(E/K, 1)$ is equal to zero, then conj. 4.1 combined with the classical Birch Swinnerton-Dyer conjecture implies that $\theta_1 = 0$, and the above equality reduces to the statement $0 = 0$. Conjecture 5.3 can be viewed as a direct anti-cyclotomic analogue of the p-adic formula proved by Greenberg and Stevens in the cyclotomic case [GS], together with the refinement proved recently by de Shalit [de Sh]. It would be of interest to see if the methods of [GS] and [de Sh] can be used to tackle the anti-cyclotomic formula of conj. 5.3.

Numerical verification:

Examples with $N = 14$ and $p = 7$

Let $K = \mathbb{Q}(w)$, with $w = \frac{1+\sqrt{-3}}{2}$ be the quadratic imaginary field of discriminant -3. The prime 2 is inert in K and 7 is split, so that $X_{N^+,N^-} = X_{N_*^+,N_*^-} = X_{7,2}$. The 7-adic Heegner distribution attached to the data $N = 14$, K, was computed up to level 7^5 using the programming package Pari.

The calculation yields an element θ in $\mathbb{Z}[G_5]$,

$$\theta = \sum_{i=1}^{2\cdot 7^4} a_i \sigma^i$$

where σ is a generator of G_5. Now, we verify that θ belongs to the augmentation ideal I of $\mathbb{Z}[G_5]$. Using the identifications

$$I/I^2 = G_5 = (\mathcal{O}_K \otimes \mathbb{Z}/7^5\mathbb{Z})^*/(\mathbb{Z}/7^5\mathbb{Z})^*\langle\zeta_3\rangle,$$

we find

$$\bar{\theta} = \prod_{i=1}^{2\cdot 7^4} \sigma^{ia_i} = (5+w)^{-1983} = 8313 + 16456w$$

Let $\pi = 2+w$ and $\bar{\pi} = 3-w$ be elements of $\mathcal{O}_K$ of norm 7 and let $\mathfrak{p} = (2+w)$ be one of the primes of $\mathcal{O}_K$ above 7. Projecting $\bar{\theta}$ onto the minus-part for complex conjugation, and working modulo $\mathfrak{p}^5$, we find:

$$\bar{\theta}^- := \bar{\theta}/\tau\bar{\theta} = 4073 \pmod{\mathfrak{p}^5}.$$

The 7-adic period of $X_0(14)$ is

$$q = 2700782 = 7874 \cdot 7^3 \pmod{7^8},$$

so that,

$$\operatorname{rec}(q,1) = \operatorname{rec}(q\cdot\pi^{-3}, \bar{\pi}^{-3}) = 174 \pmod{\mathfrak{p}^5}.$$

By consuting the tables of [Ant], we find that

$$t = 18, \quad \operatorname{ord}_p(q) = 3, \quad m = 18.$$

(The only point that does not follow directly from the tables is that

$$E(\mathbb{Q}(\sqrt{-3}))_{tors} \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.)$$

Hence conj. 5.2 (assuming $\#\underline{III}(E/K) = 1$) predicts that

$$(\bar{\theta}^-)^{\pm 3} = 174 = \mathrm{rec}_p(q,1) \pmod{7^5}.$$

One checks that this is indeed the case, namely, $(\bar{\theta}^-)^{-3} = 174$.

We have performed a similar calculation with the quadratic field of class number one and discriminant $D = -19$ in which 2 is inert and 7 is split, with a 7-adic precision of 7^{-5}. The results are summarized in the following table.

D	$\bar{\theta}^- \pmod{7^5}$	$q^- = q \cdot (\frac{\pi}{\bar{\pi}})^3 \pmod{7^5}$	n, such that $\bar{\theta}^- = (q^-)^n$
-3	12074	174	$-\frac{1}{3}$
-19	13145	13145	1

The curves $X_0(26)$ and $X_{13,2}$

We did similar verifications with $X_0(26)$, working now with quadratic fields of class number 1 in which 13 is split and 2 is inert. We recovered in this way the 13-adic periods of the curve $26A$, but not those of the curve $26B$ which has non-split multiplicative reduction at 13. The results are summarized in the following table.

D	$\bar{\theta}^- \pmod{13^4}$	$q^- = q \cdot (\frac{\pi}{\bar{\pi}})^3 \pmod{13^4}$	n, such that $\bar{\theta}^- = (q^-)^n$
-3	14893	11656	$\frac{1}{3}$
-43	13798	13798	1

5.2 A rigid analytic Gross-Zagier formula, and Kolyvagin's descent

In this section we place ourselves in the non-split exceptional case, i.e., $p|N$ is inert in K, and hence p divides N^-. Let $q \in \mathbb{Q}_p^*$ be as before the Tate period. Suppose also that we are in the indefinite case, i.e., that the curve $X_{N_*^+,N_*^-}$ corresponds to an indefinite quaternion algebra, so that θ belongs to $E^\dagger(K_\infty)[[G_\infty]]$. In that case $\epsilon(N) = -1$, so that the parity conjecture 2.9 predicts that $E(K)$ has even rank.

Assume that $E(K)$ has rank 0. Then $E^\dagger(K)$ has rank 1, and is generated by the Tate period $q \in K_p^*$, modulo torsion. Hence the regulator on the extended Mordell-Weil group is just the formal expression

$$R'_{MTT} = \frac{1}{t^2} q \otimes q \text{ in } E^\dagger(K)^{\otimes 2} \otimes \mathbb{Q}.$$

Conjecture 4.1 implies that $\mathcal{L}$, and θ, vanish to order 0, and the leading term $\bar{\theta}$ is just the term $\mathrm{Norm}_{K_0/K}(\tilde{z}_0)$, where $\tilde{z}_0$ is the Heegner point in the extended Mordell-Weil group defined in sec. 2.5. Hence conjecture 4.6 implies:

Conjecture 5.4 *If $E(K)$ has rank zero, then*

$$\mathrm{Norm}_{K_0/K}(\tilde{z}_0) = q^{\pm\sqrt{\#\underline{III}(E/K)mt^{-1}}}.$$

Let $y_n \in E(K_n)$ be the ("naive") Heegner points defined in sec. 2.5, and let $\tilde{y}_n \in K^*_{n,p}$ be elements such that $\Phi_{Tate}(\tilde{y}_n) = y_n$. Let $z_n = \mathrm{norm}(\tilde{y}_n)$. Then z_n is an integer power of the Tate period $q \in K_p^*$, and the integer $\log_q(z_n)$ is well defined modulo $[K_n : K_0] = (p+1)u^{-1}p^{n-1}$. Using the classical Birch Swinnerton-Dyer conjecture, conjecture 5.4 above can be restated directly in terms of the classical L-function $L(E/K, s)$ at $s = 1$, as follows:

Conjecture 5.5

$$\log_q(z_n)^2 = \frac{L(E/K,1)\sqrt{D}}{\Omega} \prod_{q|N^-} m_q^{-1} \pmod{(p+1)u^{-1}p^{n-1}}.$$

This formula can be viewed as a rigid analytic version of the Gross-Zagier formula, because it expresses special values of the classical L-function (which perhaps ought to be thought of as the *first derivative* of the p-adic L-function) in terms of Heegner points. The proof of a very closely related formula, and the arithmetic applications that were mentioned in the introduction, are given in [BD4].

5.3 p-adic analytic construction of rational points

In this section we examine again the non-split exceptional case, but this time suppose that we are in the definite case, i.e., that the curve $X_{N_*^+, N_*^-}$ corresponds to a definite quaternion algebra, so that θ belongs to the integral group ring $\mathbb{Z}[[G_\infty]]$. In that case the sign $\epsilon(N') = -1$ and $\epsilon(N) = 1$. Hence the parity conjecture 2.9 predicts that $E(K)$ has odd rank. Assume that

$E(K)$ has rank 1, and let P be a generator for its Mordell-Weil group modulo torsion.

Then $E^\dagger(K)$ has rank 2, and is generated (up to torsion) by the point P and the Tate period q. We now compute the regulator on this extended Mordell-Weil group. Since $\langle q,q\rangle_{MTT} = \langle P,P\rangle_{MTT} = 0$ by cor. 3.1, the regulator has the form

$$R_{MTT} = \frac{1}{t^2}\det\begin{pmatrix} 0 & \mathrm{ord}_p(q)^{-1}\mathrm{rec}_p(\tilde{P}) \\ \mathrm{ord}_p(q)^{-1}\mathrm{rec}_p(\tilde{P}) & 0 \end{pmatrix},$$

where $\mathrm{rec}_p : K_p^* \longrightarrow (I/I^2)$ is the reciprocity law map of local class field theory, and $\tilde{P}$ is an arbitrary lift P to K_p^* by the Tate parametrization. (Note that rec_p factors through $K_p^*/\mathbb{Q}_p^*$, and that q belongs to $\mathbb{Q}_p^*$, so that the value of $\mathrm{rec}_p(\tilde{P})$ does not depend on the choice of $\tilde{P}$.) Note also that if P belongs to $E(\mathbb{Q})$ and E has split multiplicative reduction over $\mathbb{Q}_p$, or if P belongs to $E(K)^-$ and E has non-split multiplicative reduction over $\mathbb{Q}_p$, then $\mathrm{rec}_p(\tilde{P}) = 0$ and $R_{MTT} = 0$. These situations correspond to unbalanced cases, where one of the eigenspaces in $E^\dagger(K)$ for complex conjugation has rank 0 and the other has rank 2. Otherwise,

$$R_{MTT} = -t^{-2}\mathrm{ord}_p(q)^{-2}\mathrm{rec}_p(\tilde{P})^2 \in (I^2/I^3)\otimes\mathbb{Q},$$

$$R_{MTT}^{1/2} = \pm t^{-1}\mathrm{ord}_p(q)^{-1}\mathrm{rec}_p(\tilde{P}).$$

Conjecture 4.4 can thus be reformulated as:

Conjecture 5.6 *If $E(K)$ has rank one, let $\tilde{P}$ be a lift to of a generator $P \in E(K)$ to K_p^*.*

1. *The following identity holds in $I/I^2 \otimes \mathbb{Q}$:*

$$\bar{\theta} = \pm\sqrt{\#\underline{III}(E/K)}\cdot m\cdot t^{-1}\cdot \mathrm{ord}_p(q)^{-1}\cdot \mathrm{rec}_p(\tilde{P}).$$

2. *(Refined conjecture): The following identity holds in I/I^2:*

$$t\cdot\mathrm{ord}_p(q)\cdot\bar{\theta} = \pm\sqrt{\#\underline{III}(E/K)}\cdot m\cdot \mathrm{rec}_p(\tilde{P}).$$

It is of interest to reformulate the above conjecture directly in terms of the Jacobians J_{N^+,N^-}, as a relation between different Heegner point constructions via the Cerednik-Drinfeld uniformization.

Let us relax for now the assumption that $c = 1$, and allow ourselves to work over general ring class fields of conductor c, with $(c, pND) = 1$. We also assume, to lighten notations, that $D < -4$ or that $c > 1$, so that $\mathcal{O}^* = \langle \pm 1 \rangle$. We let $\theta_{N_*^+,N_*^-} \in J^{p-new}_{N_*^+,N_*^-}[[G_\infty]]$ denote the element

$$\theta_{N_*^+,N_*^-} = \lim_{n \longrightarrow \infty} \sum_{\sigma \in G_n} P_n^\sigma \cdot \sigma^{-1},$$

where $P_n \in J^{p-new}_{N_*^+,N_*^-}$ is the Heegner class in $J_{N_*^+,N_*^-}$ defined in sec. 2.4, projected onto $J^{p-new}_{N_*^+,N_*^-}$. We let I denote the kernel of the map $\mathbb{Z}[[G_\infty]] \longrightarrow \mathbb{Z}[G_0]$ induced from the natural projection $G_\infty \longrightarrow G_0$. Then we have

$$I/I^2 = \mathbb{Z}[G_0] \otimes G_\infty^0 = (K_p^*/\mathbb{Q}_p^*) \otimes \mathbb{Z}[G_0].$$

From equation (8) of sec. 2.5, we have:

Lemma 5.7 *The element $\theta_{N_*^+,N_*^-}$ belongs to $J^{p-new}_{N_*^+,N_*^-} \otimes I$.*

Let $\bar{\theta}_{N_*^+,N_*^-}$ be the projection of $\theta_{N_*^+,N_*^-}$ to

$$J^{p-new}_{N_*^+,N_*^-} \otimes (I/I^2) = J^{p-new}_{N_*^+,N_*^-} \otimes (K_p^*/\mathbb{Q}_p^*) \otimes \mathbb{Z}[G_0].$$

Multiplication by $(1-\tau)$ gives a map $(K_p^*/\mathbb{Q}_p^*) \longrightarrow (K_p^*)_1$, where $(K_p^*)_1$ denotes the elements of K_p^* of norm 1. Let $\bar{\theta}^-_{N_*^+,N_*^-}$ be the element $(1-\tau)\bar{\theta}_{N_*^+,N_*^-}$. This element belongs canonically to

$$J^{p-new}_{N_*^+,N_*^-} \otimes K_p^* \otimes \mathbb{Z}[G_0].$$

Let $P_0 \in J_{N^+,N^-}(K_0)$ be the Heegner point of conductor c, and let

$$\theta_{N^+,N^-} = \sum_{\sigma \in G_0} P_0^\sigma \cdot \sigma^{-1} \in J_{N^+,N^-}(K_0) \otimes \mathbb{Z}[G_0].$$

Choose a prime $\mathfrak{p}$ of K_0 above p, and let τ be the (unique) choice of complex conjugation in $\mathrm{Gal}(K_0/K)$ which fixes $\mathfrak{p}$. Let $\theta^-_{N^+,N^-}$ be the projection of θ_{N^+,N^-} to the eigenspace where τ acts by the involution $-W_p^-$, i.e.,

$$\theta^-_{N^+,N^-} = (\tau + W_p^-)\theta_{N^+,N^-}.$$

We view the element $\theta^-_{N^+,N^-}$ as belonging to the group of local points

$$J_{N^+,N^-}((K_0)_{\mathfrak{p}}) \otimes \mathbb{Z}[G_0] \simeq J_{N^+,N^-}(K_p) \otimes \mathbb{Z}[G_0].$$

(Note that p splits completely in K_0/K, and is inert in $K/\mathbb{Q}$.)

Recall the Cerednik-Drinfeld uniformization defined in sec. 1.7. It gives rise to a map

$$\Phi_{CD} : J^{p-new}_{N^+_*,N^-_*} \otimes K^*_p \otimes \mathbb{Z}[G_0] \longrightarrow J_{N^+,N^-}(K_p) \otimes \mathbb{Z}[G_0].$$

Conjecture 5.8 *There exists $\gamma \in G_0$ such that*

$$\Phi_{CD}(\bar{\theta}^-_{N^+_*,N^-_*}) = \theta^-_{N^+,N^-}\gamma.$$

Note that the left hand side is constructed as a p-adic limit of Heegner points on the Shimura curve $X_{N^+_*,N^-_*}$ which corresponds to a definite quaternion algebra. The right hand side is constructed from a genuine algebraic point in J_{N^+,N^-} defined over the ring class field K_0. The above conjecture allows one to compute directly, by a p-adic analytic process, a certain subgroup of the Heegner points in $J_{N^+,N^-}(K_0)$.

Numerical evidence
The curves $X_0(14)$ and $X_{7,2}$: Let E be the elliptic curve $X_0(14)$. We have tested our conjecture when $N = 14$ and $p = 7$, in a few cases where K is a quadratic imaginary field in which both 2 and 7 are inert, so that

$$X_{N^+,N^-} = X_{1,14}, \quad X_{N^+_*,N^-_*} = X_{7,2}.$$

For example, let $K = \mathbb{Q}(w)$, with $w = \frac{1+\sqrt{-11}}{2}$. The 7-adic Heegner distribution attached to the data $N = 14$, K, was computed up to level 7^5 using the programming package Pari. This took about 90 minutes of computer time on a Sparc workstation. (It is likely that the calculation could have been carried out more quickly, as no special effort was made to render the algorithms efficient.)

The calculation yields an element θ in $\mathbb{Z}[G_5]$,

$$\theta = \sum_{i=1}^{8\cdot 7^4} a_i \sigma^i$$

where σ is a generator of $G_5 = (\mathcal{O}_K \otimes \mathbb{Z}/7^5\mathbb{Z})^*/(\mathbb{Z}/7^5\mathbb{Z})^*$. Now, we verify that θ belongs to the augmentation ideal I of $\mathbb{Z}[G_5]$, and that

$$\bar{\theta} = \prod_{i=1}^{8\cdot 7^4} \sigma^{ia_i} = 1544 + 5249w \pmod{7^5, (\mathbb{Z}/7^5\mathbb{Z})^*}.$$

Let now $z_7 = \bar{\theta}/\tau\bar{\theta}$, where τ is complex conjugation. Applying the Tate 7-adic uniformization of E to the element z_7 gives the point

$$\Phi_{Tate}(z_7) = (10696, 6528 + 9861w) \pmod{7^5}$$

on E, with a 7-adic error of 7^{-5}. A short inspection reveals that this point is equal to the rational point

$$(7/11, -(41 + 116w)/121) \in E(K),$$

to within the specified 7-adic accuracy of 7^{-5}. By consulting the Antwerp tables [Ant], we find that the fudge factors in conj. 5.6 cancel out exactly in this case, so that we expect (assuming that $\underline{III}(E/K)$ is trivial) that this point is a generator of $E(K)$ modulo torsion.

The curves $X_0(26)$ and $X_{13,2}$
The quadratic imaginary field of smallest discriminant in which 2 and 13 are inert is again the field $K = \mathbb{Q}(w)$, with $w = \frac{1+\sqrt{-11}}{2}$. It is a field of class number one. The 13-adic Heegner distribution attached to the data $X_0(26)$, K, was computed up to level 13^3 using the programming package Pari. We computed the θ-element for the two new forms of level 26 at once, corresponding to the two strong Weil curves $26A$ and $26B$ of sec. 1.11. The calculation yielded an element θ in $\mathbb{Z}[e_1, e_2, e_3] \otimes \mathbb{Z}[G_3]$. We verified that $\theta_A := \pi_{26A*}(\theta)$ and $\theta_B := \pi_{26B*}(\theta)$ both belong to the augmentation ideal of $\mathbb{Z}[G_3]$: the image of θ by the augmentation map is a multiple of the Eisenstein vector v_{eis} which is orthogonal to the cuspidal vectors v_1 and v_2.

We find that

$$\bar{\theta}_A = 1596 + 2018w \pmod{I^2},$$

using the canonical identification of I/I^2 with G_3.

Applying Tate's 13-adic analytic parametrization, we get the point

$$(x, y) = (1995, 292 + 1814w) \pmod{13^3},$$

with a 13-adic precision of 13^{-3}. A short inspection reveals that this point is equal to the rational point

$$(-25/11, (180 - 206w)/121) \in E(K),$$

to within the specified 13-adic accuracy.

The element θ_B belongs to I^2, as follows from the functional equation for θ_B explained in sec. 2.9. The image of θ_B in I^2/I^3 is non-zero, but we are at a loss to supply even a conjectural interpretation for this leading term.

References

[Ant] *Numerical tables on elliptic curves*, in Modular Functions of one Variable IV, Springer Lecture Notes 476.

[B1] M. Bertolini, Iwasawa theory, L-functions and Heegner points, PhD Thesis, Columbia University, 1992.

[B2] M. Bertolini, *Selmer groups and Heegner points in anticyclotomic $\mathbb{Z}_p$-extensions*, Compositio Math, to appear.

[BC] J-F. Boutot, H. Carayol, *Uniformisation p-adique des courbes de Shimura: les théorèmes de Cerednik et de Drinfeld*, Astérisque 196-197 (1991) pp. 45-158.

[BD1] M. Bertolini and H. Darmon, *Kolyvagin's descent and Mordell-Weil groups over ring class fields*, Journal für die reine und angewandte Mathematik 412 (1990), pp. 63-74.

[BD2] M. Bertolini and H. Darmon, *Derived heights and generalized Mazur-Tate regulators*, Duke Math. J., October 1994, Vol. 76, No. 1, pp. 75-111.

[BD3] M. Bertolini and H. Darmon, *Derived p-adic heights*, Am. J. of Math., to appear.

[BD4] M. Bertolini and H. Darmon (with an appendix by B. Edixhoven) *A rigid analytic Gross-Zagier formula and arithmetic applications*, CICMA preprint; submitted.

[BD5] M. Bertolini and H. Darmon, *Heegner points, p-adic L-functions and the Cerednik-Drinfeld uniformization*, in preparation.

[BFH] D. Bump, S. Friedberg, and J. Hoffstein, *Non-vanishing theorems for L-functions of modular forms and their derivatives*, Annals of Math., 1991.

[Cer] I.V. Cerednik, *Uniformization of algebraic curves by discrete arithmetic subgroups of* $\mathbf{PGL_2(k_w)}$ *with compact quotient* (in Russian) Math. Sbornik 100, 59-88, 1976. Transl. in Math. USSR Sb. 29, 55-78, 1976.

[Da1] H. Darmon, *A refined conjecture of Mazur-Tate type for Heegner points*, Inv. Math. 110, 123-146 (1992)

[Da2] H. Darmon, *Euler systems and refined conjectures of Birch and Swinnerton-Dyer type*, in proceedings of a Boston University Workshop on p-adic monodromy and the Birch Swinnerton-Dyer conjecture. August, 1992.

[Da3] H. Darmon, *Heegner points, Heegner cycles, and congruences*, Proceedings of Conference on elliptic curves and related topics, Ste-Adèle, Quebec, February, 1992.

[Dr] V.G. Drinfeld, *Coverings of p-adic symmetric regions*, (in Russian), Funkts. Anal. Prilozn. 10, 29-40, 1976. Transl. in Funct. Anal. Appl. 10, 107-115, 1976.

[de Sh] E. de Shalit, *p-adic periods and modular symbols of elliptic curves of prime conductor*, Invent. Math., to appear.

[Ed] B. Edixhoven, appendix to [BD4].

[G-VdP] L. Gerritzen, M. Van der Put, *Schottky groups and Mumford curves*, Lect. Notes in Math. 817, Springer-Verlag (1980).

[GS] R. Greenberg and G. Stevens, *p-adic L-functions and p-adic periods of modular forms*, Inv. Math. 111, 407-447 (1993).

[Gr1] B.H. Gross, *Heegner points on* $X_0(N)$, in Modular Forms, R.A. Rankin ed., p. 87-107, Ellis Horwood Ltd., 1984.

[Gr2] B.H. Gross, *Heights and the special values of L-series*, CMS conference proceedings, Volume 7 (1987).

[GZ] B.H. Gross, D.B. Zagier, *Heegner points and derivatives of L-series*, Inv. Math. (1986).

[JL] H. Jacquet, R.P. Langlands, *Automorphic forms on* $\mathbf{GL(2)}$, Springer Lecture Notes, v. 114, (1970).

[Ma1] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Inv. Math. 18, 183-266 (1972)

[Ma2] B. Mazur, *Modular curves and arithmetic*, Proceedings of the Int. Congress of Math., (1983), Warszawa.

[Ma3] B. Mazur, unpublished manuscript.

[MT1] B. Mazur and J. Tate, *Canonical height pairings via biextensions*, in Arithmetic and Geometry, Volume I, Michael Artin and John Tate, editors, Progress in Mathematics, Birkhauser, Boston, pp. 195-238.

[MT2] B. Mazur and J. Tate, *Refined conjectures of the "Birch and Swinnerton-Dyer type"*, Duke Math Journal, Vol. 54, No. 2, 1987, p. 711-750.

[MTT] B. Mazur, J. Tate, and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Inv. Math. 84, 1-48 (1986).

[Me] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Inventiones Math., to appear.

[Mi] J.S. Milne, Arithmetic duality theorems, Perspectives in Mathematics, Vol. 1, J. Coates, S. Helgason, eds., Academic Press 1986.

[Mu] Mumford, D., *An analytic construction of degenerating curves over complete local fields*, Compositio Math. 24, 129-174 (1972).

[MM] Murty, M.R., and Murty, V.K., *Mean values of derivatives of modular L-series*, Annals of Math. 133 (1991), 447-475.

[Ne] A. Neron, *Quasi-fonctions et hauteurs sur les variétés abéliennes*, Ann. of Math. 82, 249-331 (1965).

[PR] B. Perrin-Riou, *Fonctions L p-adiques, Théorie d'Iwasawa et points de Heegner*, Bull. Soc. Math. de France 115, 1987, 455-510.

[PR] B. Perrin-Riou, *Fonctions L p-adiques d'une courbe elliptique et points rationnels*, Annales de l'Institut Fourier, to appear.

[Ro] D. Roberts, Shimura curves analogous to $X_0(N)$, Harvard PhD. Thesis, 1989.

[Ru] K. Rubin, *p-adic L-functions and rational points on elliptic curves with complex multiplication*, Invent. Math. 107, 323-350 (1992).

[Sc1] P. Schneider, *Iwasawa L-functions of algebraic varieties over algebraic number fields*, Inv. Math. 71, 251-293, 1983.

[Sc2] P. Schneider, *p-adic height pairings II*, Inv. Math. 79, 329-374, 1985.

[Si1] J. Silverman, Advanced topics in the arithmetic of elliptic curves, Springer-Verlag, GTM 151.

[Tan] K.-S. Tan, p-adic pairings, proceedings of a conference on p-adic monodromy and the Birch Swinnerton-Dyer conjecture, Boston University, August 1992.

[Ta] J. Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Intern. Congress Math., Stockholm, pp. 234-241.

[TW] R. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Annals of Math. 141, No. 3, 1995, pp. 553-572.

[Vi] M-F. Vignéras, Arithmétique des algèbres de quaternions, Lecture Notes in Math. 800, Springer Verlag.

[Wi] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Annals of Math. 141, No. 3, 1995, pp. 443-551.