ICM 2002 · Vol. II · 185–195

Elliptic Curves and Class Field Theory

Barry Mazur* **Karl Rubin**†

Abstract

Suppose E is an elliptic curve defined over $\mathbf{Q}$. At the 1983 ICM the first author formulated some conjectures that propose a close relationship between the explicit class field theory construction of certain abelian extensions of imaginary quadratic fields and an explicit construction that (conjecturally) produces almost all of the rational points on E over those fields.

Those conjectures are to a large extent settled by recent work of Vatsal and of Cornut, building on work of Kolyvagin and others. In this paper we describe a collection of interrelated conjectures still open regarding the variation of Mordell-Weil groups of E over abelian extensions of imaginary quadratic fields, and suggest a possible algebraic framework to organize them.

2000 Mathematics Subject Classification: 11G05, 11R23.
Keywords and Phrases: Elliptic curves, Iwasawa theory, Heegner points.

1. Introduction

Eighty years have passed since Mordell proved that the (Mordell-Weil) group of rational points on an elliptic curve E is finitely generated, yet so limited is our knowledge that we still have no algorithm guaranteed to compute the rank of this group. If we want to ask even more ambitious questions about how the rank of the Mordell-Weil group $E(F)$ varies as F varies, it makes sense to restrict attention only to those fields for which we have an explicit construction, such as finite abelian extensions of a given imaginary quadratic field K. Taking our lead from the profound discovery of Iwasawa that the variational properties of certain arithmetic invariants are well-behaved if one restricts to subfields of $\mathbf{Z}_p^d$-extensions of number fields, we will focus on the following Mordell-Weil variation problem:

Fixing an elliptic curve E defined over $\mathbf{Q}$, an imaginary quadratic field K, and a prime number p, study the variation of the Mordell-Weil group of E over finite subfields of the (unique) $\mathbf{Z}_p^2$-extension of K in $\bar{K}$.

*Department of Mathematics, Harvard University, Cambridge, MA 02138, USA. E-mail: mazur@math.harvard.edu
†Department of Mathematics, Stanford University, Stanford, CA 94305, USA. E-mail: rubin@math.stanford.edu

This problem was the subject of some conjectures formulated by the first author at the 1983 ICM [8], conjectures which have recently been largely settled by work of Vatsal [15] and Cornut [1] building on work of Kolyvagin and others.

Example. Let E be the elliptic curve $y^2+y=x^3-x$, $p=5$, and let $K=\mathbf{Q}(\sqrt{-7})$. If F is a finite extension of K, contained in the $\mathbf{Z}_5^2$ extension of K, then $\operatorname{rank} E(F) = [F\cap K_\infty^{\mathrm{anti}} : K]$ where K_∞^{anti} is the anticyclotomic $\mathbf{Z}_5$-extension of K (see §2 for the definition). One only has an answer like this in the very simplest cases.

Now with the same E and p, take $K=\mathbf{Q}(\sqrt{-26})$. A guess here would be that $\operatorname{rank} E(F) = [F\cap K_\infty^{\mathrm{anti}} : K]+2$, but this seems to be beyond present technology.

The object of this article is to sketch a package of still-outstanding conjectures in hopes that it offers an even more precise picture of this piece of arithmetic. These conjectures are in some cases due to, and in other cases build on ideas of, Bertolini & Darmon, Greenberg, Gross & Zagier, Haran, Hida, Iwasawa, Kolyvagin, Nekovář, Perrin-Riou, and the authors, among others.

In sections 3 through 5 we describe the three parts of our picture: the *arithmetic theory* (the study of the Selmer modules over Iwasawa rings that contain the information we seek), the *analytic theory* (the construction and study of the relevant L-functions, both classical and p-adic), and the *universal norm theory* which arises from purely arithmetic considerations, but provides analytic invariants.

In the final section we suggest the beginnings of a new algebraic structure to organize these conjectures. This structure should not be viewed as a conjecture, but rather as a mnemonic to collect our conjectures and perhaps predict new ones.

More details and proofs will appear in a forthcoming paper.

2. Running hypotheses and notation

Fix a triple (E,K,p) where E is an elliptic curve of conductor N over $\mathbf{Q}$, K is an imaginary quadratic field of discriminant $D<-4$, and p is a prime number. To keep our discussion focused and as succinct as possible, we make the following hypotheses and conventions.

Assume that p is odd, that N, p and D are pairwise relatively prime, and that if E has complex multiplication, then K is *not* its field of complex multiplication. Let $\mathcal{O}_K\subset K$ denote the ring of integers of K. Assume further that there exists an ideal $\mathcal{N}\subset\mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N}$ is cyclic of order N (this is sometimes called the **Heegner Hypothesis**), and that p is a prime of ordinary reduction for E. For simplicity we will assume throughout this article that the p-primary subgroups of the Shafarevich-Tate groups of E over the number fields we consider are all finite.

Proposition 1. *Under the assumptions above,* $\operatorname{rank} E(K)$ *is odd.*

Proof. This follows from the Parity Conjecture recently proved by Nekovář [11].

Let $\mathbf{K}_\infty$ denote the (unique) $\mathbf{Z}_p^2$-extension of K and $\mathbf{\Gamma} := \operatorname{Gal}(\mathbf{K}_\infty/K)$, so $\mathbf{\Gamma}\cong\mathbf{Z}_p^2$. We define the Iwasawa ring

$$\mathbf{\Lambda} := \mathbf{Z}_p[[\mathbf{\Gamma}]]\otimes_{\mathbf{Z}_p}\mathbf{Q}_p.$$

(To simplify notation and to avoid some complications, we will often work with $\mathbf{Q}_p$-vector spaces instead of natural $\mathbf{Z}_p$-modules; in particular we have tensored the usual Iwasawa ring with $\mathbf{Q}_p$.) For every (finite or infinite) extension F of K in $\mathbf{K}_\infty$ we also define

$$\Lambda_F := \mathbf{Z}_p[[\mathrm{Gal}(F/K)]] \otimes_{\mathbf{Z}_p} \mathbf{Q}_p, \qquad \mathbf{I}_F := \ker\{\boldsymbol{\Lambda} \twoheadrightarrow \Lambda_F\}.$$

Then $\mathbf{I}_K$ is the augmentation ideal of $\boldsymbol{\Lambda}$, and if $[F:K]$ is finite then Λ_F is just the group ring $\mathbf{Q}_p[\mathrm{Gal}(F/K)]$. If $\mathrm{Gal}(F/K)$ is $\mathbf{Z}_p$ or $\mathbf{Z}_p^2$, and M is a finitely generated torsion Λ_F-module, then $\mathrm{char}_{\Lambda_F}(M)$ will denote the characteristic ideal of M. In particular $\mathrm{char}_{\Lambda_F}(M)$ is a principal ideal of Λ_F.

There is a $\mathbf{Q}_p$-projective line of $\mathbf{Z}_p$-extensions of K, all contained in $\mathbf{K}_\infty$. Among these are two distinguished $\mathbf{Z}_p$-extensions:

- the **cyclotomic** $\mathbf{Z}_p$-extension K_∞^{cycl}, the compositum of K with the unique (cyclotomic) $\mathbf{Z}_p$-extension of $\mathbf{Q}$ (write $\Gamma_{\mathrm{cycl}} = \mathrm{Gal}(K_\infty^{\mathrm{cycl}}/K)$, $\Lambda_{\mathrm{cycl}} = \Lambda_{K_\infty^{\mathrm{cycl}}}$),
- the **anticyclotomic** $\mathbf{Z}_p$-extension K_∞^{anti}, the unique $\mathbf{Z}_p$-extension of K that is Galois over $\mathbf{Q}$ with non-abelian, and in fact dihedral, Galois group (write $\Gamma_{\mathrm{anti}} = \mathrm{Gal}(K_\infty^{\mathrm{anti}}/K)$, $\Lambda_{\mathrm{anti}} = \Lambda_{K_\infty^{\mathrm{anti}}}$).

Then $\boldsymbol{\Gamma} = \Gamma_{\mathrm{cycl}} \oplus \Gamma_{\mathrm{anti}}$ and $\boldsymbol{\Lambda} = \Lambda_{\mathrm{cycl}} \otimes_{\mathbf{Z}_p} \Lambda_{\mathrm{anti}}$.

Complex conjugation $\tau : K \to K$ acts on $\boldsymbol{\Gamma}$, acting as $+1$ on Γ_{cycl} and -1 on Γ_{anti}. This induces nontrivial involutions of $\boldsymbol{\Lambda}$ and Λ_{anti}, which we also denote by τ. If M is a module over $\boldsymbol{\Lambda}$ (or similarly over Λ_{anti}), let $M^{(\tau)}$ denote the module whose underlying abelian group is M but where the new action of $\gamma \in \boldsymbol{\Gamma}$ on $m \in M^{(\tau)}$ is given by the old action of γ^τ on m.

Our $\boldsymbol{\Lambda}$-modules will usually come with a natural action of $\mathrm{Gal}(\mathbf{K}_\infty/\mathbf{Q})$. These actions are continuous and $\mathbf{Z}_p$-linear, and satisfy the formula $\tilde{\tau}(\gamma \cdot m) = \gamma^\tau \cdot \tilde{\tau}(m)$ for every lift $\tilde{\tau}$ of τ to $\mathrm{Gal}(\mathbf{K}_\infty/\mathbf{Q})$. Thus the action of any lift $\tilde{\tau}$ induces an isomorphism $M \xrightarrow{\sim} M^{(\tau)}$. We will refer to such $\boldsymbol{\Lambda}$ or Λ_{anti}-modules as **semi-linear τ-modules**. If M is a semi-linear τ-module and is free of rank one over Λ_{anti}, we define the **sign** of M to be the sign ± 1 of the action of τ on the one-dimensional $\mathbf{Q}_p$-vector space $M \otimes_{\Lambda_{\mathrm{anti}}} \Lambda_K$. Such an M is completely determined (up to isomorphism preserving its structure) by its sign.

Definition 2. *If M and A are semi-linear τ-modules, then a ($\boldsymbol{\Lambda}$-bilinear) A-valued* **τ-Hermitian pairing** *π is a $\boldsymbol{\Lambda}$-module homomorphism $\pi : M \otimes_{\boldsymbol{\Lambda}} M^{(\tau)} \to A$ such that for every lift $\tilde{\tau}$ of τ to* $\mathrm{Gal}(\mathbf{K}_\infty/\mathbf{Q})$

$$\pi(m \otimes n) = \pi(n \otimes m)^{\tilde{\tau}} = \pi(\tilde{\tau} n \otimes \tilde{\tau} m).$$

3. Universal norms

Definition 3. *If $K \subset F \subset \mathbf{K}_\infty$, the* **universal norm module** *$U(F)$ is the projective limit*

$$U(F) := \mathbf{Q}_p \otimes \varprojlim_{K \subset L \subset F} (E(L) \otimes \mathbf{Z}_p)$$

(projective limit with respect to traces, over finite *extensions L of K in F) with its natural Λ_F-structure. If F is a finite extension of K, then $U(F)$ is simply $E(F) \otimes \mathbf{Q}_p$.*

If F is a $\mathbf{Z}_p$-extension of K, then $U(F)$ is a free Λ_F-module of finite rank, and is zero if and only if the Mordell-Weil ranks of E over subfields of F are bounded (cf. [8] §18 or [12] §2.2). The first author conjectured some time ago [8] that for $\mathbf{Z}_p$-extensions F/K, and under our running hypotheses, $U(F) = 0$ if $F \neq K_\infty^{\mathrm{anti}}$ and $U(K_\infty^{\mathrm{anti}})$ is free of rank one over Λ_{anti}. The following theorem follows from recent work of Kato [6] for K_∞^{cycl} and Vatsal [15] and Cornut [1] for K_∞^{anti}.

Theorem 4. *$U(K_\infty^{\mathrm{cycl}}) = 0$ and $U(K_\infty^{\mathrm{anti}})$ is free of rank one over Λ_{anti}.*

For the rest of this paper we will write $\mathcal{U}$ for the anticyclotomic universal norm module $U(K_\infty^{\mathrm{anti}})$. Complex conjugation gives $\mathcal{U}$ a natural semi-linear τ-module structure. Since $\mathcal{U}$ is free of rank one over Λ_{anti}, we conclude that $\mathcal{U}$ is completely determined (up to isomorphism preserving its τ-structure) by its sign.

Let $r^{\pm}$ be the rank of the ± 1 eigenspace of τ acting on $E(K)$, so $\operatorname{rank} E(\mathbf{Q}) = r^+$ and $\operatorname{rank} E(K) = r^+ + r^-$. By Proposition 1, $\operatorname{rank} E(K)$ is odd so $r^+ \neq r^-$.

Conjecture 5 (Sign Conjecture). *The sign of the semi-linear τ-module $\mathcal{U}$ is $+1$ if $r^+ > r^-$, and is -1 if $r^- > r^+$.*

Remark. Equivalently, the Sign Conjecture asserts that the sign of $\mathcal{U}$ is $+1$ if twice $\operatorname{rank} E(\mathbf{Q})$ is greater than $\operatorname{rank} E(K)$, and -1 otherwise.

As we discuss below in §4, the Sign Conjecture is related to the nondegeneracy of the p-adic height pairing (see the remark after Conjecture 11).

The Λ_{anti}-module $\mathcal{U}$ comes with a canonical Hermitian structure. That is, the canonical (cyclotomic) p-adic height pairing (see [10] and [12] §2.3)

$$\mathrm{h} : \mathcal{U} \otimes_{\Lambda_{\mathrm{anti}}} \mathcal{U}^{(\tau)} \longrightarrow \Gamma_{\mathrm{cycl}} \otimes_{\mathbf{Z}_p} \Lambda_{\mathrm{anti}}$$

is a τ-Hermitian pairing in the sense of Definition 2.

Conjecture 6 (Height Conjecture). *The homomorphism* h *is an isomorphism of free Λ_{anti}-modules of rank one*

$$\mathrm{h} : \mathcal{U} \otimes_{\Lambda_{\mathrm{anti}}} \mathcal{U}^{(\tau)} \xrightarrow{\sim} \Gamma_{\mathrm{cycl}} \otimes_{\mathbf{Z}_p} \Lambda_{\mathrm{anti}}.$$

The Λ_{anti}-module $\mathcal{U}$ has an important submodule, the **Heegner submodule** $\mathcal{H} \subset \mathcal{U}$. Fix a modular parameterization $X_0(N) \to E$. The Heegner submodule $\mathcal{H}$ is the cyclic Λ_{anti}-module generated by a trace-compatible sequence $c = \{c_L\}$ of Heegner points $c_L \in E(L) \otimes \mathbf{Z}_p$ for finite extensions L of K in K_∞^{anti}. See for example [8] §19 or [12] §3. Call such a $c \in \mathcal{H}$ a **Heegner generator**. The Heegner generators of $\mathcal{H}$ are well-defined up to multiplication by an element of $\pm\Gamma \subset (\Lambda_{\mathrm{anti}})^\times$. The Λ_{anti}-submodule $\mathcal{H} \subset \mathcal{U}$ is stable under the semi-linear τ-structure of $\mathcal{U}$, so the action of τ gives an isomorphism $\mathcal{U}/\mathcal{H} \xrightarrow{\sim} (\mathcal{U}/\mathcal{H})^{(\tau)} \cong \mathcal{U}^{(\tau)}/\mathcal{H}^{(\tau)}$.

Let $c^{(\tau)}$ denote the element c viewed in the Λ_{anti}-module $\mathcal{H}^{(\tau)}$. Since

$$(\pm\gamma c) \otimes_{\Lambda_{\mathrm{anti}}} (\pm\gamma c)^{(\tau)} = c \otimes_{\Lambda_{\mathrm{anti}}} c^{(\tau)}$$

for every $\pm\gamma \in \pm\Gamma$, the element $c \otimes c^{(\tau)} \in \mathcal{H} \otimes_{\Lambda_{\mathrm{anti}}} \mathcal{H}^{(\tau)}$ is independent of the choice of Heegner generator, and is therefore a totally canonical generator of the free, rank one Λ_{anti}-module $\mathcal{H} \otimes_{\Lambda_{\mathrm{anti}}} \mathcal{H}^{(\tau)}$.

Definition 7. *The* **Heegner L-function** *(for the triple (E, K, p) satisfying our running hypotheses) is the element*

$$\mathcal{L} := \mathrm{h}(c \otimes c^{(\tau)}) \in \Gamma_{\mathrm{cycl}} \otimes_{\mathbf{Z}_p} \Lambda_{\mathrm{anti}}.$$

Conjecture 8. $\Gamma_{\mathrm{cycl}} \otimes \mathrm{char}(\mathcal{U}/\mathcal{H})^2 = \Lambda_{\mathrm{anti}}\mathcal{L}$ *inside* $\Gamma_{\mathrm{cycl}} \otimes \Lambda_{\mathrm{anti}}$.

One sees easily that $\Gamma_{\mathrm{cycl}} \otimes \mathrm{char}(\mathcal{U}/\mathcal{H})^2 \supset \Lambda_{\mathrm{anti}}\mathcal{L}$, and that Conjecture 8 is equivalent to the Height Conjecture (Conjecture 6).

4. The analytic theory

The ("two-variable") p-adic L-function for E over K is an element $\mathbf{L} \in \mathbf{\Lambda}$ constructed by Haran [3] and by a different, more general, method by Hida [4] (see also the papers of Perrin-Riou [13, 14]). The L-function $\mathbf{L}$ is characterized by the fact that it interpolates special values of the classical Hasse-Weil L-function of twists of E over K. More precisely, embedding $\bar{\mathbf{Q}}$ both in $\mathbf{C}$ and $\bar{\mathbf{Q}}_p$, if $\chi : \mathbf{\Gamma} \to \bar{\mathbf{Z}}^\times \subset \bar{\mathbf{Z}}_p^\times$ is a character of finite order then

$$\chi(\mathbf{L}) = c(\chi)\frac{L_{\mathrm{classical}}(E_{/K}, \chi, 1)}{8\pi^2 ||f_E||^2} \tag{4.1}$$

where $L_{\mathrm{classical}}(E_{/K}, \chi, s)$ is the Hasse-Weil L-function of the twist of $E_{/K}$ by χ, $c(\chi)$ is an explicit algebraic number (cf. [13] Théorème 1.1), f_E is the modular form on $\Gamma_0(N)$ corresponding to E, and $||f_E||$ is its Petersson norm.

Projecting $\mathbf{L} \in \mathbf{\Lambda}$ to the cyclotomic or the anticyclotomic line via the natural projections $\mathbf{\Lambda} \to \Lambda_{\mathrm{cycl}}$ and $\mathbf{\Lambda} \to \Lambda_{\mathrm{anti}}$, we get "one-variable" p-adic L-functions

$$\mathbf{L} \mapsto L_{\mathrm{cycl}} \in \Lambda_{\mathrm{cycl}} \qquad \text{and} \qquad \mathbf{L} \mapsto L_{\mathrm{anti}} \in \Lambda_{\mathrm{anti}}.$$

It follows from the functional equation satisfied by $\mathbf{L}$ ([13] Théorème 1.1) and the Heegner Hypothesis that $L_{\mathrm{anti}} = 0$. In other words, viewing $\mathbf{\Lambda} = \Lambda_{\mathrm{anti}}[[\Gamma_{\mathrm{cycl}}]]$ as the completed group ring of Γ_{cycl} with coefficients in Λ_{anti}, we have that the "constant term" of $\mathbf{L} \in \Lambda_{\mathrm{anti}}[[\Gamma_{\mathrm{cycl}}]]$ vanishes. We now consider its "linear term."

There is a canonical isomorphism of (free, rank one) Λ_{anti}-modules

$$\Gamma_{\mathrm{cycl}} \otimes_{\mathbf{Z}_p} \Lambda_{\mathrm{anti}} \cong \mathbf{I}_{K_\infty^{\mathrm{anti}}}/\mathbf{I}^2_{K_\infty^{\mathrm{anti}}}$$

which sends $\gamma \otimes 1 \in \Gamma_{\mathrm{cycl}} \otimes_{\mathbf{Z}_p} \Lambda_{\mathrm{anti}}$ to $\gamma - 1 \in \mathbf{I}_{K_\infty^{\mathrm{anti}}}/\mathbf{I}^2_{K_\infty^{\mathrm{anti}}}$.

Conjecture 9 (Λ-adic Gross-Zagier Conjecture). *Let L' denote the image of $\mathbf{L}$ under the map $\mathbf{I}_{K_\infty^{\mathrm{anti}}}/\mathbf{I}^2_{K_\infty^{\mathrm{anti}}} \xrightarrow{\sim} \Gamma_{\mathrm{cycl}} \otimes_{\mathbf{Z}_p} \Lambda_{\mathrm{anti}}$. Then*

$$L' = d^{-1}\mathcal{L}$$

where d is the degree of the modular parametrization $X_0(N) \to E$.

Remark. Perrin-Riou [13] proved that if p splits in K and the discriminant D of K is odd, then L' and $d^{-1}\mathcal{L}$ have the same image under the projection $\Lambda_{\mathrm{anti}} \to \Lambda_K = \mathbf{Q}_p$.

Let $\mathbf{I} := \mathbf{I}_K$, the augmentation ideal of $\mathbf{\Lambda}$. For every integer $r \geq 0$ we have $\mathbf{I}^r/\mathbf{I}^{r+1} \cong \mathrm{Sym}^r_{\mathbf{Z}_p}(\mathbf{\Gamma}) \otimes \mathbf{Q}_p$. Using the direct sum decomposition $\mathbf{\Gamma} = \Gamma_{\mathrm{cycl}} \oplus \Gamma_{\mathrm{anti}}$ we get a canonical direct sum decomposition

$$\mathrm{Sym}^r_{\mathbf{Z}_p}(\mathbf{\Gamma}) = \bigoplus_{j=0}^{r} \Gamma^{r-j,j} \quad \text{where } \Gamma^{i,j} := (\Gamma_{\mathrm{cycl}})^{\otimes i} \otimes_{\mathbf{Z}_p} (\Gamma_{\mathrm{anti}})^{\otimes j}. \tag{4.2}$$

Consider the canonical (two-variable) p-adic height pairing

$$\langle\ ,\ \rangle \ :\ E(K) \times E(K) \longrightarrow \mathbf{\Gamma} \otimes \mathbf{Q}_p. \tag{4.3}$$

Set $r = \operatorname{rank} E(K)$, which is odd by Proposition 1. Define the **two-variable p-adic regulator** $R_p(E,K)$ to be the discriminant of this pairing:

$$R_p(E,K) := t^{-2} \det\langle P_i, P_j\rangle \in \mathrm{Sym}^r_{\mathbf{Z}_p}(\mathbf{\Gamma}) \otimes \mathbf{Q}_p \cong \mathbf{I}^r/\mathbf{I}^{r+1},$$

where $\{P_1, \ldots, P_r\}$ generates a subgroup of $E(K)$ of finite index t. For each integer $j = 0, \ldots, r$ let $R_p(E,K)^{r-j,j}$ be the projection of $R_p(E,K)$ into $\Gamma^{r-j,j} \otimes \mathbf{Q}_p$ under (4.2), so that

$$R_p(E,K) = \bigoplus_{j=0}^{r} R_p(E,K)^{r-j,j}.$$

Recall that $r^{\pm}$ is the rank of the ± 1-eigenspace $E(K)^{\pm}$ of τ acting on $E(K)$.

Proposition 10. *$R_p(E,K)^{r-j,j} = 0$ unless j is even and $j \leq 2\min(r^+, r^-)$.*

Proof. This follows from the fact that the height pairing (4.3) is τ-Hermitian, so $\langle \tau x, \tau y\rangle = \langle x, y\rangle^{\tau}$, and therefore the induced height pairings

$$E(K)^{\pm} \times E(K)^{\pm} \to \Gamma_{\mathrm{anti}} \otimes \mathbf{Q}_p, \quad E(K)^{+} \times E(K)^{-} \to \Gamma_{\mathrm{cycl}} \otimes \mathbf{Q}_p$$

vanish.

Conjecture 11 (Maximal nondegeneracy of the height pairing). *If j is even and $0 \leq j \leq 2\min(r^+, r^-)$ then $R_p(E,K)^{r-j,j} \neq 0$.*

Remark. Conjecture 11, or more specifically the nonvanishing of $R_p(E,K)^{r-j,j}$ when $j = 2\min(r^+, r^-)$, implies the Sign Conjecture (Conjecture 5). This is proved in the same way as Proposition 10, using the additional fact that the anticyclotomic universal norms in $E(K) \otimes \mathbf{Z}_p$ are in the kernel of the anticyclotomic p-adic height pairing $(E(K) \otimes \mathbf{Z}_p) \times (E(K) \otimes \mathbf{Z}_p) \to \Gamma_{\mathrm{anti}} \otimes \mathbf{Q}_p$.

5. The arithmetic theory

For every algebraic extension F of K, let $\mathrm{Sel}_p(E_{/F})$ denote the p-power Selmer group of E over F, the subgroup of $H^1(G_F, E[p^\infty])$ that sits in an exact sequence

$$0 \longrightarrow E(F) \otimes \mathbf{Q}_p/\mathbf{Z}_p \longrightarrow \mathrm{Sel}_p(E_{/F}) \longrightarrow Ш(E_{/F})[p^\infty] \longrightarrow 0$$

where $Ш(E_{/F})$ is the Shafarevich-Tate group of E over F. Also write

$$\mathcal{S}_p(E_{/F}) = \mathrm{Hom}(\mathrm{Sel}_p(E_{/F}), \mathbf{Q}_p/\mathbf{Z}_p) \otimes \mathbf{Q}_p$$

for the tensor product of $\mathbf{Q}_p$ with the Pontrjagin dual of the Selmer group.

The following theorem is proved using techniques which go back to [7]; see [2] and [12] Lemme 5, §2.2.

Theorem 12 (Control Theorem). *Suppose $K \subset F \subset \mathbf{K}_\infty$.*

(i) *The natural restriction map $H^1(F, E[p^\infty]) \to H^1(\mathbf{K}_\infty, E[p^\infty])$ induces an isomorphism $\mathcal{S}_p(E_{/\mathbf{K}_\infty}) \otimes_{\mathbf{\Lambda}} \Lambda_F \xrightarrow{\sim} \mathcal{S}_p(E_{/F})$.*

(ii) *There is a canonical isomorphism $U(F) \xrightarrow{\sim} \mathrm{Hom}_{\Lambda_F}(\mathcal{S}_p(E_{/F}), \Lambda_F)$.*

Conjecture 13 (Two-variable main conjecture [8, 12]). *The two-variable p-adic L-function $\mathbf{L}$ generates the ideal $\mathrm{char}_{\mathbf{\Lambda}}(\mathcal{S}_p(E_{/\mathbf{K}_\infty}))$ of $\mathbf{\Lambda}$.*

Restricting the two-variable main conjecture to the cyclotomic and anticyclotomic lines leads to the following "one-variable" conjectures originally formulated in [9] and [12], respectively. Let L' denote the image of $\mathbf{L}$ in $\Gamma_{\mathrm{cycl}} \otimes_{\mathbf{Z}_p} \Lambda_{\mathrm{anti}}$ as in Conjecture 9, and $\mathcal{S}_p(E_{/K_\infty^{\mathrm{anti}}})_{\mathrm{tors}}$ the Λ_{anti}-torsion submodule of $\mathcal{S}_p(E_{/K_\infty^{\mathrm{anti}}})$.

Conjecture 14 (Cyclotomic and anticyclotomic main conjectures).

(i) *L_{cycl} generates the ideal $\mathrm{char}_{\Lambda_{\mathrm{cycl}}}(\mathcal{S}_p(E_{/K_\infty^{\mathrm{cycl}}}))$ of Λ_{cycl}.*

(ii) *L' generates $\Gamma_{\mathrm{cycl}} \otimes \mathrm{char}_{\Lambda_{\mathrm{anti}}}(\mathcal{S}_p(E_{/K_\infty^{\mathrm{anti}}})_{\mathrm{tors}})$ inside $\Gamma_{\mathrm{cycl}} \otimes \Lambda_{\mathrm{anti}}$.*

Remark. Using Euler systems, Kato [6] and Howard [5] have proved (under some mild additional hypotheses) divisibilities related to the cyclotomic and anticyclotomic main conjectures, respectively, namely

$$L_{\mathrm{cycl}} \in \mathrm{char}_{\Lambda_{\mathrm{cycl}}}(\mathcal{S}_p(E_{/K_\infty^{\mathrm{cycl}}})), \quad \mathrm{char}_{\Lambda_{\mathrm{anti}}}(\mathcal{U}/\mathcal{H})^2 \subset \mathrm{char}_{\Lambda_{\mathrm{anti}}}(\mathcal{S}_p(E_{/K_\infty^{\mathrm{cycl}}})_{\mathrm{tors}})$$

(note that Conjectures 8 and 9 predict that $\Gamma_{\mathrm{cycl}} \otimes \mathrm{char}_{\Lambda_{\mathrm{anti}}}(\mathcal{U}/\mathcal{H})^2 = L'\Lambda_{\mathrm{anti}}$).

Conjecture 15 (Two-variable p-adic BSD conjecture). *Let $r = \mathrm{rank}\, E(K)$. The two-variable p-adic L-function $\mathbf{L} \in \mathbf{\Lambda}$ is contained $\mathbf{I}^r$ and*

$$\mathbf{L} \equiv c(\chi_{\mathrm{triv}})\#(Ш(E_{/K}))\prod_v c_v \cdot R_p(E,K) \pmod{\mathbf{I}^{r+1}}$$

where $c(\chi_{\mathrm{triv}})$ is the rational number in the interpolation formula (4.1) for the trivial character, $Ш(E_{/K})$ is the Shafarevich-Tate group of E over K, and the c_v are the Tamagawa factors in the (usual) Birch and Swinnerton-Dyer conjecture for E over K.

6. Orthogonal $\mathbf{\Lambda}$-modules

In this final section we introduce a purely algebraic template which, when it "fits", gives rise to many of the properties conjectured in the previous sections.

Keep the notation of the previous sections. In particular $\tau : \mathbf{\Lambda} \to \mathbf{\Lambda}$ is the involution of $\mathbf{\Lambda}$ induced by complex conjugation on K, and if V is a $\mathbf{\Lambda}$-module, then $V^{(\tau)}$ denotes V with $\mathbf{\Lambda}$-module structure obtained by composition with τ. Let $V^* = \mathrm{Hom}_{\mathbf{\Lambda}}(V, \mathbf{\Lambda})$. If V is a free $\mathbf{\Lambda}$-module of rank r, then $\det_{\mathbf{\Lambda}}(V^\tau)$ will denote the r-th exterior power of V and a **τ-gauge** on V is a $\mathbf{\Lambda}$-isomorphism between the free $\mathbf{\Lambda}$-modules of rank one

$$t_V \ : \ \det_{\mathbf{\Lambda}}(V^*) \cong \det_{\mathbf{\Lambda}}(V^{(\tau)})$$

or equivalently an isomorphism $\det_{\mathbf{\Lambda}}(V) \otimes \det_{\mathbf{\Lambda}}(V^{(\tau)}) \xrightarrow{\sim} \mathbf{\Lambda}$.

By an **orthogonal $\mathbf{\Lambda}$**-module we mean a free $\mathbf{\Lambda}$-module V with semi-linear τ-structure endowed with a τ-gauge t_V and a $\mathbf{\Lambda}$-bilinear τ-Hermitian pairing (Definition 2)

$$\pi : V \otimes_{\mathbf{\Lambda}} V^{(\tau)} \longrightarrow \mathbf{\Lambda}.$$

Viewing π as a $\mathbf{\Lambda}$-linear map $V^{(\tau)} \to V^*$, the composition

$$t_V \circ \det_{\mathbf{\Lambda}}(\pi) \ : \ \det_{\mathbf{\Lambda}}(V^{(\tau)}) \longrightarrow \det_{\mathbf{\Lambda}}(V^*) \longrightarrow \det_{\mathbf{\Lambda}}(V^{(\tau)})$$

must be multiplication by an element $\mathrm{disc}(V) \in \mathbf{\Lambda}$ that we call the **discriminant** of the orthogonal $\mathbf{\Lambda}$-module V. We further assume that $\mathrm{disc}(V) \neq 0$, and we define $M = M(V, \pi)$ to be the cokernel of the (injective) map $\pi : V^{(\tau)} \to V^*$, so we have

$$0 \longrightarrow V^{(\tau)} \longrightarrow V^* \longrightarrow M \longrightarrow 0. \tag{6.1}$$

If $K \subset F \subset \mathbf{K}_\infty$, recall that $\mathbf{I}_F = \ker\{\mathbf{\Lambda} \twoheadrightarrow \Lambda_F\}$ and define

$$V(F) := \{x \in V : \pi(x, V^{(\tau)}) \subset \mathbf{I}_F\}/\mathbf{I}_F V = \ker\{V \otimes_{\mathbf{\Lambda}} \Lambda_F \xrightarrow{\pi \otimes 1} (V^{(\tau)})^* \otimes_{\mathbf{\Lambda}} \Lambda_F\}$$

and similarly $V^{(\tau)}(F) := \ker\{V^{(\tau)} \otimes \Lambda_F \to V^* \otimes \Lambda_F\}$. Any lift $\tilde{\tau}$ of τ to $\mathrm{Gal}(\mathbf{K}_\infty/\mathbf{Q})$ induces an isomorphism $V(F) \to V^{(\tau)}(F)$. From (6.1) we obtain

$$0 \longrightarrow V^{(\tau)}(F) \longrightarrow V^{(\tau)} \otimes_{\mathbf{\Lambda}} \Lambda_F \longrightarrow V^* \otimes_{\mathbf{\Lambda}} \Lambda_F \longrightarrow M \otimes_{\mathbf{\Lambda}} \Lambda_F \longrightarrow 0 \tag{6.2}$$

and (applying $\mathrm{Hom}(\,\cdot\,, \Lambda_F)$ and using the Hermitian property of π)

$$V(F) \cong \mathrm{Hom}_{\Lambda_F}(M \otimes_{\mathbf{\Lambda}} \Lambda_F, \Lambda_F). \tag{6.3}$$

We have an induced pairing

$$\pi_F : V^{(\tau)}(F) \otimes_{\Lambda_F} V(F) \longrightarrow \mathbf{I}_F/\mathbf{I}_F^2,$$

which we call the F-derived pairing. If F is stable under complex conjugation then $V^{(\tau)}(F)$ is canonically isomorphic to $V(F)^{(\tau)}$ and π_F is τ-Hermitian.

Now suppose $F = K_\infty^{\rm anti}$. By (6.3), $V(K_\infty^{\rm anti})$ is free over $\Lambda_{\rm anti}$. Applying the determinant functor to (6.2), the τ-gauge t_V induces an isomorphism

$$\det_{\Lambda_{\rm anti}} V(K_\infty^{\rm anti})^{(\tau)} = \det_{\Lambda_{\rm anti}} V^{(\tau)}(K_\infty^{\rm anti}) \xrightarrow{\sim} \operatorname{Hom}(\det_{\Lambda_{\rm anti}}(M \otimes_{\mathbf{\Lambda}} \Lambda_{\rm anti}), \Lambda_{\rm anti}).$$

If $V(K_\infty^{\rm anti})$ has rank one over $\Lambda_{\rm anti}$, then $V(K_\infty^{\rm anti})$ contains a unique maximal τ-stable submodule H such that the map

$$\begin{aligned} V(K_\infty^{\rm anti})^{(\tau)} &\xrightarrow{\sim} \operatorname{Hom}(\det_{\Lambda_{\rm anti}}(M \otimes \Lambda_{\rm anti}), \Lambda_{\rm anti}) \\ &\qquad\supset \operatorname{Hom}(M \otimes \Lambda_{\rm anti}, \Lambda_{\rm anti}) \cong V(K_\infty^{\rm anti}) \end{aligned}$$

sends $H^{(\tau)}$ into H. (Namely, $H = JV(K_\infty^{\rm anti})$ where J is the largest ideal of $\Lambda_{\rm anti}$ such that $J^\tau = J$ and $J^2 \subset \operatorname{char}_{\Lambda_{\rm anti}}(M \otimes \Lambda_{\rm anti})_{\rm tors}$.)

Recall that $\operatorname{Sel}_p(E_{/F})$ denotes the p-power Selmer group of E over F and $\mathcal{S}_p(E_{/F}) = \operatorname{Hom}(\operatorname{Sel}_p(E_{/F}), \mathbf{Q}_p/\mathbf{Z}_p) \otimes \mathbf{Q}_p$.

Proposition 16. *With notation as above, suppose that V is an orthogonal $\mathbf{\Lambda}$-module and $\varphi_V : M \xrightarrow{\sim} \mathcal{S}_p(E_{/\mathbf{K}_\infty})$ is an isomorphism. Then for every extension F of K in $\mathbf{K}_\infty$, φ_V induces an isomorphism*

$$V(F) \xrightarrow{\sim} U(F)$$

where $U(F)$ is the universal norm module defined in §3.

proof. This follows directly from Theorem 12 and (6.3).

Definition 17. *We say that the orthogonal $\mathbf{\Lambda}$-module V* **organizes the anticyclotomic arithmetic of** (E, K, p) *if the following three properties hold.*

- *(a)* $\operatorname{disc}(V) = \mathbf{L}$, *the two-variable p-adic L-function of E.*
- *(b) There is an isomorphism $\varphi_V : M \xrightarrow{\sim} \mathcal{S}_p(E_{/\mathbf{K}_\infty})$.*
- *(c) The isomorphism $V(K_\infty^{\rm anti}) \cong \mathcal{U}$ of Proposition 16 identifies $H \subset V(K_\infty^{\rm anti})$ with the Heegner submodule $\mathcal{H} \subset \mathcal{U}$, and identifies the $K_\infty^{\rm anti}$-derived pairing with the canonical p-adic height pairing into $\mathbf{I}_{K_\infty^{\rm anti}}/\mathbf{I}^2_{K_\infty^{\rm anti}} \cong \Gamma_{\rm cycl} \otimes \Lambda_{\rm anti}$.*

Question. Given E, K, and p satisfying our running hypotheses, is there an orthogonal $\mathbf{\Lambda}$-module V that organizes the anticyclotomic arithmetic of (E, K, p)?

If one is not quite so (resp., much more) optimistic one could formulate an analogous question with the ring $\mathbf{\Lambda}$ replaced by the localization of $\mathbf{\Lambda}$ at $\mathbf{I}$ (resp., with $\mathbf{\Lambda}$ replaced by $\mathbf{Z}_p[[\mathbf{\Gamma}]]$).

Question. If V is an orthogonal $\mathbf{\Lambda}$-module V which organizes the anticyclotomic arithmetic of (E, K, p), then for every finite extension F of K in $\mathbf{K}_\infty$, we have an isomorphism $E(F) \otimes \mathbf{Q}_p = U(F) \cong V(F)$ as in Proposition 16, a p-adic height pairing on $E(F) \otimes \mathbf{Q}_p$, and the F-derived pairing on $V(F)$. How are these pairings related?

When $F = K_\infty^{\rm anti}$ condition (c) says that the two pairings are the same, but it seems that in general they cannot be the same for finite extensions F/K.

Theorem 18. *Suppose that there is an orthogonal* $\mathbf{\Lambda}$*-module* V *that organizes the anticyclotomic arithmetic of* (E, K, p)*. Then Conjectures 13 (the 2-variable main conjecture), and 14(i) (the cyclotomic main conjecture) hold.*

If further the induced pairing $V(K_\infty^{\mathrm{anti}}) \otimes V(K_\infty^{\mathrm{anti}})^{(\tau)} \to \Gamma_{\mathrm{cycl}} \otimes \Lambda_{\mathrm{anti}}$ *is surjective, then Conjectures 6 (the Height Conjecture), 8, 9 (the* Λ*-adic Gross-Zagier conjecture), and 14(ii) (the anticyclotomic main conjecture) also hold.*

Brief outline of the proof of Theorem 18. Since $\mathrm{disc}(V)$ is a generator of $\mathrm{char}_{\mathbf{\Lambda}}(M)$, the two-variable main conjecture follows immediately from (a) and (b) of Definition 17. The cyclotomic main conjecture follows from the two-variable main conjecture.

Now suppose that the induced pairing $V(K_\infty^{\mathrm{anti}}) \otimes V(K_\infty^{\mathrm{anti}})^{(\tau)} \to \Gamma_{\mathrm{cycl}} \otimes \Lambda_{\mathrm{anti}}$ is surjective. By (c) of Definition 17 this is equivalent to the Height Conjecture, which in turn is equivalent to Conjecture 8.

Howard proved in [5] that $\mathcal{S}_p(E_{/K_\infty^{\mathrm{anti}}})$ is pseudo-isomorphic to $\Lambda_{\mathrm{anti}} \oplus B^2$ where B is a τ-stable torsion Λ_{anti}-module. By Theorem 12(i) the same is true of $M \otimes \Lambda_{\mathrm{anti}}$, and so the remark at the end of the definition of H shows that $H = \mathrm{char}(B) V(K_\infty^{\mathrm{anti}})$. Using (6.2), (6.3), and our assumption that the induced pairing is surjective, one can show that the image of $\mathbf{L}$ in $\mathbf{I}_{K_\infty^{\mathrm{anti}}}/\mathbf{I}^2_{K_\infty^{\mathrm{anti}}}$ generates $\mathrm{char}(B)^2 \mathbf{I}_{K_\infty^{\mathrm{anti}}}/\mathbf{I}^2_{K_\infty^{\mathrm{anti}}}$. The Λ-adic Gross-Zagier conjecture and the anticyclotomic main conjecture follow from these facts and (c). □

References

[1] C. Cornut, Mazur's conjecture on higher Heegner points, *Invent. math.* **148** (2002), 495–523.

[2] R. Greenberg, Galois theory for the Selmer group of an abelian variety (preprint).

[3] S. Haran, p-adic L-functions for elliptic curves over CM fields, thesis, MIT 1983.

[4] H. Hida, A p-adic measure attached to the zeta functions associated with two elliptic modular forms. I, *Invent. Math.* **79** (1985), 159–195.

[5] B. Howard, *The Heegner point Kolyvagin system*, thesis, Stanford University 2002.

[6] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms (preprint).

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

[8] ———, Modular curves and arithmetic. In: *Proceedings of the International Congress of Mathematicians (Warsaw, 1983)*, PWN, Warsaw (1984), 185–211.

[9] B. Mazur, P. Swinnerton-Dyer, Arithmetic of Weil curves, *Invent. Math.* **25** (1974), 1–61.

[10] B. Mazur, J. Tate, Canonical height pairings via biextensions. In: *Arithmetic and Geometry*, Progr. Math. **35**, Birkhaüser, Boston (1983), 195–237.

[11] J. Nekovář, On the parity of ranks of Selmer groups. II, *C. R. Acad. Sci. Paris Sér. I Math.* **332** (2001), 99–104.

[12] B. Perrin-Riou, Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner, *Bull. Soc. Math. France* **115** (1987), 399–456.

[13] ———, Points de Heegner et dérivées de fonctions L p-adiques, *Invent. Math.* **89** (1987), 455–510.

[14] ———, Fonctions L p-adiques associées à une forme modulaire et à un corps quadratique imaginaire, *J. London Math. Soc.* **38** (1988), 1–32.

[15] V. Vatsal, Special values of anticyclotomic L-functions (preprint).