Elliptic Curves and Iwasawa Theory

Karl Rubin

Department of Mathematics

Stanford University

Stanford CA 94305, USA

`rubin@math.stanford.edu`

22 August 2002

The problem

Given an elliptic curve E, understand how the Mordell-Weil group $E(F)$ varies as F varies.

Restrict to:

- subfields F of $\mathbf{Z}_p$ (or $\mathbf{Z}_p^d$) extensions of a base field K (Iwasawa theory).
- $K = \mathbf{Q}$ or imaginary quadratic field (explicit constructions).

This lecture

This talk describes joint work with Barry Mazur.

It is a sequel to Mazur's 1983 ICM lecture in Warsaw. We will survey the progress since then, due to many people including:

Bertolini & Darmon
Cornut
Greenberg
Gross & Zagier
Haran
Hida
Kato
Kolyvagin
Nekovář
Perrin-Riou
Vatsal

Example

Let E be the elliptic curve

$$y^2 + y = x^3 - x,$$

- $K = \mathbf{Q}(\sqrt{-7})$,
- $\mathbf{K}_\infty$ is the unique $\mathbf{Z}_5^2$-extension of K,
- $K \subset F \subset \mathbf{K}_\infty$.

Let K_∞^+ and K_∞^- be the cyclotomic and anticyclotomic $\mathbf{Z}_5$-extensions of K.

Theorem. $\operatorname{rank} E(F) = [F \cap K_\infty^- : K]$.

In particular

- $\operatorname{rank} E(K_\infty^-) = \operatorname{rank} E(\mathbf{K}_\infty) = \infty$,
- $\operatorname{rank} E(K_\infty^+) = \operatorname{rank} E(K) = 1$.

Example

Keep the same E, but now

- $K = \mathbf{Q}(\sqrt{-26})$.
- $\mathbf{K}_\infty$, K_∞^+, and K_∞^- are the $\mathbf{Z}_5^2$-extension and cyclotomic and anticyclotomic $\mathbf{Z}_5$-extensions of K,
- $K \subset F \subset \mathbf{K}_\infty$.

Conjecture.

$$\operatorname{rank} E(F) \ = \ [F \cap K_\infty^- : K] + 2.$$

This conjecture seems to be out of reach of current technology.

Method

Conjecture (Birch & Swinnerton-Dyer)
If F is a number field,

(i) rank $E(F) = \mathrm{ord}_{s=1} L(E_{/F}, s)$,

(ii) *a prediction for the first nonvanishing derivative $L^{(r)}(E_{/F}, 1)$ in terms of periods, heights of rational points, and other arithmetic information.*

Iwasawa theory packages this kind of information, for *all* subfields of a $\mathbf{Z}_p^d$-extension, in p-*adic* L-functions.

This will be our approach.

The setup

Fix:

- an elliptic curve $E_{/\mathbf{Q}}$ of conductor N,
- a prime number $p > 2$,
- an imaginary quadratic field K of discriminant $D < -4$.

Assume:

- N, p, D are pairwise relatively prime,
- E has good, ordinary reduction at p,
- every prime dividing N splits in K,
- the Shafarevich-Tate groups of E over all number fields are finite.

Theorem (Nekovář). *Under these assumptions,* $\operatorname{rank} E(K)$ *is odd.*

The setup

- $\mathbf{K}_\infty$: the (unique) $\mathbf{Z}_p^2$-extension of K,
- $K_\infty^+, K_\infty^- \subset \mathbf{K}_\infty$ the cyclotomic and anticyclotomic $\mathbf{Z}_p$-extensions of K:

$$\begin{tikzcd}
& \mathbf{K}_\infty \arrow[dl, dash, "\mathbf{Z}_p"'] \arrow[dd, dash, "\boldsymbol{\Gamma}"', "\mathbf{Z}_p^2"] \arrow[dr, dash, "\mathbf{Z}_p"] & \\
K_\infty^- \arrow[dr, dash, "\Gamma_-"'] & & K_\infty^+ \arrow[dl, dash, "\Gamma_+"] \\
& K \arrow[d, dash, "\{1,\tau\}"] & \\
& \mathbf{Q} &
\end{tikzcd}$$

- $\Gamma_\pm$ is the maximal quotient of $\boldsymbol{\Gamma}$ on which τ acts via ± 1.
- $K_\infty^+ \subset K(\boldsymbol{\mu}_{p^\infty})$ is abelian over $\mathbf{Q}$.

The setup

Iwasawa algebras:

- $\mathbf{\Lambda} := \mathbf{Z}_p[[\Gamma]] \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, and if $K \subset F \subset \mathbf{K}_\infty$

$$\Lambda_F := \mathbf{Z}_p[[\mathrm{Gal}(F/K)]] \otimes_{\mathbf{Z}_p} \mathbf{Q}_p,$$

- $\mathbf{I}_F := \ker[\mathbf{\Lambda} \to \Lambda_F]$,
- $\Lambda_+ := \Lambda_{K_\infty^+}, \qquad \Lambda_- := \Lambda_{K_\infty^-}$.

We have tensored the usual Iwasawa algebras with $\mathbf{Q}_p$.

- $\mathbf{\Lambda} \cong \mathbf{Z}_p[[T_1, T_1]] \otimes \mathbf{Q}_p$.
- If F is a $\mathbf{Z}_p$-extension of K in $\mathbf{K}_\infty$ then $\Lambda_F \cong \mathbf{Z}_p[[T]] \otimes \mathbf{Q}_p$ is a PID.

Growth of Mordell-Weil

Theorem (Mazur). *If F is a $\mathbf{Z}_p$-extension of K, there is an integer $r(F) \geq 0$ (the "growth number") such that*

$$\operatorname{rank} E(L) - r(F)[L:K]$$

is bounded for $K \subset L \subset F$.

Conjecture (Mazur). *$r(K_\infty^-) = 1$, and $r(F) = 0$ if $F \neq K_\infty^-$.*

New tools (late 1980's):

- Gross-Zagier Theorem, relating Heegner points to derivatives of L-functions
- Kolyvagin's method of Euler systems, giving upper bounds for Selmer groups.

Growth of Mordell-Weil

Theorem (Kato, Rohrlich). $r(K_\infty^+) = 0$.

Corollary. $r(F) = 0$ *for all but finitely many* $\mathbf{Z}_p$*-extensions* F *of* K*.*

Theorem (Cornut, Vatsal). $r(K_\infty^-) = 1$.

Both theorems use Kolyvagin's theory of Euler systems to get upper bounds for $r(K_\infty^+)$ and $r(K_\infty^-)$.

The second theorem uses Heegner points to obtain a lower bound for $r(K_\infty^-)$.

Universal norms

If $K \subset F \subset \mathbf{K}_\infty$, the *universal norm module*

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

is the projective limit with respect to norm maps, over finite extensions of K in F.

The anticyclotomic universal norm subgroup in $E(K) \otimes \mathbf{Q}_p$ is

$E(K)^{\text{univ}} := \text{image}[U(K_\infty^-) \to E(K) \otimes \mathbf{Q}_p]$.

Corollary. (i) $U(\mathbf{K}_\infty) = U(K_\infty^+) = 0$,

(ii) $U(K_\infty^-)$ *is free of rank one over* Λ_-,

(iii) $\dim_{\mathbf{Q}_p}(E(K)^{\text{univ}}) = 1$.

Universal norms

Let $\epsilon(E) = \pm 1$ be the sign of the action of complex conjugation τ on $E(K)^{\text{univ}}$.

Let $r^{\pm}$ be the rank of the ± 1 eigenspace of τ on $E(K)$:

- $\operatorname{rank} E(\mathbf{Q}) = r^{+}$,
- $\operatorname{rank} E(K) = r^{+} + r^{-}$,
- since $\operatorname{rank} E(K)$ is odd, $r^{+} \neq r^{-}$.

Conjecture (Sign Conjecture).

$$r^{\epsilon(E)} > r^{-\epsilon(E)}.$$

I.e., the anticyclotomic universal norms in $E(K) \otimes \mathbf{Z}_p$ are contained in the larger of $(E(K) \otimes \mathbf{Z}_p)^{+}$ and $(E(K) \otimes \mathbf{Z}_p)^{-}$.

$\mathbf{\Lambda}$-modules

If M is a finitely generated Λ_F-module, then

$$M \xrightarrow{\sim} \bigoplus_i \Lambda_F / f_i \Lambda_F \qquad (*)$$

with $f_i \in \Lambda_F$. The *characteristic ideal*

$$\mathrm{char}(M) := (\prod_i f_i)\Lambda_F$$

of M is well-defined independently of the choice of the f_i in (*).

If M is a finitely generated over $\mathbf{\Lambda}$, then we have the same definition except that the map (*) may have a kernel and cokernel which are finite dimensional over $\mathbf{Q}_p$.

$\mathbf{\Lambda}$-modules

Every homomorphism χ : Gal$(F/K) \to \bar{\mathbf{Z}}_p^\times$ extends to a homomorphism $\chi : \Lambda_F \to \bar{\mathbf{Q}}_p$.

A *p-adic L-function* will typically be an element of some Λ_F, which when evaluated on characters in this way gives special values of L-functions.

Complex conjugation τ acts naturally on $\mathbf{\Gamma}$, Γ_+, and Γ_-.

If M is a $\mathbf{\Lambda}$- (or Λ_--) module, let $M^{(\tau)}$ be the abelian group M with new action of $\gamma \in \mathbf{\Gamma}$ given by the old action of γ^τ.

p-adic heights

Let $\mathcal{U} = U(K_\infty^-)$. The canonical (cyclotomic) p-adic height pairing $\langle\ ,\ \rangle_{\mathrm{cyc}}$ induces a homomorphism

$$\mathcal{U} \otimes_{\Lambda_-} \mathcal{U}^{(\tau)} \longrightarrow \Gamma_+ \otimes_{\mathbf{Z}_p} \Lambda_- \qquad (*)$$

which is "τ-Hermitian": for every lift $\tilde{\tau}$ of τ to $\mathrm{Gal}(\mathbf{K}_\infty/K)$ we have

$$\langle \tilde{\tau}u, \tilde{\tau}v\rangle_{\mathrm{cyc}} = \tilde{\tau}\langle u, v\rangle_{\mathrm{cyc}}.$$

Conjecture (Height Conjecture). *The map* (*) *is an isomorphism.*

Heegner points

Fix a modular parametrization $X_0(N) \to E$.

The theory of complex multiplication provides a family of points in $X_0(N)(K^{\mathrm{ab}})$.

These points give a free rank-one submodule of Heegner points $\mathcal{H} \subset U(K_\infty^-)$.

$\mathcal{H}$ has a Λ_--generator c, well-defined up to multiplication by ± 1 and by $\gamma \in \Gamma_-$.

The free, rank-one module $\mathcal{H} \otimes_{\Lambda_-} \mathcal{H}^{(\tau)}$ has a canonical generator

$$c \otimes c^{(\tau)} \ \in \ \mathcal{H} \otimes_{\Lambda_-} \mathcal{H}^{(\tau)} \ \subset \ \mathcal{U} \otimes_{\Lambda_-} \mathcal{U}^{(\tau)}.$$

Heegner points

Define the *Heegner L-function*

$$\mathcal{L} := \langle c, c^{(\tau)} \rangle_{\mathrm{cyc}} \in \Gamma_+ \otimes_{\mathbf{Z}_p} \Lambda_-$$

where $c \otimes c^{(\tau)}$ is the canonical generator of $\mathcal{H} \otimes_{\Lambda_-} \mathcal{H}^{(\tau)}$.

The Height Conjecture is equivalent to:

Conjecture. *$\mathcal{L}$ is a generator of the submodule*

$$\Gamma_+ \otimes \mathrm{char}(\mathcal{U}/\mathcal{H})^2 \subset \Gamma_+ \otimes \Lambda_-.$$

The analytic theory

The "two-variable" p-adic L-function (Haran, Hida) is an element $\mathbf{L} \in \mathbf{\Lambda}$ such that for $\chi : \mathbf{\Gamma} \to \bar{\mathbf{Z}}^{\times} \subset \bar{\mathbf{Z}}_p^{\times}$,

$$\chi(\mathbf{L}) \;=\; c(\chi)\frac{L_{\text{H-W}}(E_{/K}, \chi, 1)}{\pi^2 \|f_E\|^2}$$

where

- $L_{\text{H-W}}(E_{/K}, \chi, s)$ is the Hasse-Weil L-function,
- $c(\chi)$ is an explicit algebraic number,
- f_E is the modular form corresponding to E and $\|f_E\|$ is its Petersson norm.

The analytic theory

The image of $\mathbf{L} \in \mathbf{\Lambda}$ under the natural projections $\mathbf{\Lambda} \to \Lambda_+$ and $\mathbf{\Lambda} \to \Lambda_-$ gives "one-variable" p-adic L-functions

$$L_+ \in \Lambda_+ \qquad \text{and} \qquad L_- \in \Lambda_-.$$

It follows from a functional equation satisfied by $\mathbf{L}$ that $L_- = 0$, i.e.,

$$\mathbf{L} \in \mathbf{I}_{K_\infty^-} = \ker[\mathbf{\Lambda} \to \Lambda_-].$$

- $\mathbf{L}$ "vanishes on the anticyclotomic line"
- the image of $\mathbf{L}$ in $\mathbf{I}_{K_\infty^-}/\mathbf{I}^2_{K_\infty^-}$ is the "first derivative of $\mathbf{L}$ in the cyclotomic direction".

Λ-adic Gross-Zagier Conjecture

Recall the Heegner L-function

$$\mathcal{L} = \langle c, c^{(\tau)} \rangle_{\mathrm{cyc}} \in \Gamma_+ \otimes \Lambda_-.$$

There is a natural Λ_--isomorphism

$$\begin{array}{ccc} \Gamma_+ \otimes_{\mathbf{Z}_p} \Lambda_- & \xrightarrow{\sim} & \mathbf{I}_{K_\infty^-}/\mathbf{I}^2_{K_\infty^-} \\ \gamma \otimes 1 & \mapsto & \gamma - 1. \end{array} \qquad (*)$$

Conjecture (Perrin-Riou) "Λ-adic Gross-Zagier Conjecture." *The inverse image of* $\mathbf{L}$ *under* $(*)$ *is* $d^{-1}\mathcal{L}$*, where* d *is the degree of the parametrization* $X_0(N) \to E$*.*

Λ-adic Gross-Zagier Conjecture

Theorem (Perrin-Riou). "p-adic Gross-Zagier." *The images of* $d^{-1}\mathcal{L}$ *and* $\mathbf{L}$ *are identifed by the bottom map in*

$$\begin{array}{ccc}
\Gamma_+ \otimes_{\mathbf{Z}_p} \Lambda_- & \xrightarrow{\sim} & \mathbf{I}_{K_\infty^-}/\mathbf{I}^2_{K_\infty^-} \\
\downarrow & & \downarrow \\
\Gamma_+ \otimes_{\mathbf{Z}_p} \Lambda_K & \hookrightarrow & \mathbf{I}_K/\mathbf{I}_K^2 \\
|| & & || \\
\Gamma_+ \otimes \mathbf{Q}_p & \hookrightarrow & \mathbf{\Gamma} \otimes \mathbf{Q}_p
\end{array}$$

The image of $\mathbf{L}$ in the two-dimensional $\mathbf{Q}_p$-vector space $\mathbf{\Gamma}$ is the derivative of $\mathbf{L}$. This theorem expresses that derivative as the height of a Heegner point.

The conjecture extends this to the entire anticyclotomic $\mathbf{Z}_p$-extension.

Two-variable p-adic regulator

Let $\mathbf{I} = \mathbf{I}_K$, the augmentation ideal of $\mathbf{\Lambda}$, and recall $\mathbf{\Gamma} \cong \Gamma_+ \oplus \Gamma_-$.

For every $r \geq 0$

$$\mathbf{I}^r/\mathbf{I}^{r+1} \cong \mathrm{Sym}^r_{\mathbf{Z}_p}(\mathbf{\Gamma}) \otimes \mathbf{Q}_p \cong \bigoplus_{j=0}^{r} \Gamma^{r-j,j}$$

where $\Gamma^{i,j} = \mathbf{Q}_p \otimes (\Gamma_+^{\otimes i} \otimes \Gamma_-^{\otimes j})$.

Suppose $r = \operatorname{rank} E(F)$. Fix $P_1, \ldots, P_r \in E(F)$ which generate a subgroup of finite index t.

Two-variable p-adic regulator

Using the two-variable p-adic height pairing

$$\langle\ ,\ \rangle_{\mathbf{\Gamma}}\ :\ E(K)\times E(K)\longrightarrow \mathbf{\Gamma}\otimes\mathbf{Q}_p,$$

define the *two-variable p-adic regulator*

$$\begin{aligned} R_p(E,K) &:= t^{-2}\,\mathrm{det}\langle P_i,P_j\rangle_{\mathbf{\Gamma}} \\ &\in \mathrm{Sym}^r_{\mathbf{Z}_p}(\mathbf{\Gamma})\otimes\mathbf{Q}_p \\ &\cong \bigoplus_{j=0}^{r}\Gamma^{r-j,j}\cong \mathbf{I}^r/\mathbf{I}^{r+1}, \end{aligned}$$

If $0\le j\le r$ let $R_p(E,K)^{r-j,j}$ be the projection of $R_p(E,K)$ into $\Gamma^{r-j,j}$, so that

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

Nondegeneracy of the height pairing

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

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

Conjecture (Maximal Nondegeneracy of the Height Pairing). *If j is even and $j \le 2\min(r^+, r^-)$, then $R_p(E,K)^{r-j,j} \neq 0$.*

The Maximal Nondegeneracy Conjecture, or more specifically the nonvanishing of $R_p(E,K)^{r-j,j}$ when $j = 2\min(r^+, r^-)$, implies the Sign Conjecture.

Selmer groups

If $K \subset F \subset \mathbf{K}_\infty$, let

$$\mathrm{Sel}_p(E_{/F}) \;\subset\; H^1(G_F, E[p^\infty])$$

be the p-power Selmer group and $\text{Ш}(E_{/F})$ the Shafarevich-Tate group. Thus

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

Also write

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

If $[F:K] < \infty$ then (since $|\text{Ш}(E_{/F})| < \infty$)

$$\mathcal{S}_p(E_{/F}) \;=\; \mathrm{Hom}(E(F), \mathbf{Q}_p).$$

Selmer groups

Theorem (Control Theorem).
If $K \subset F \subset \mathbf{K}_\infty$

(i) *the natural restriction map 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*

$$U(F) \xrightarrow{\sim} \mathrm{Hom}_{\Lambda_F}(\mathcal{S}_p(E_{/F}), \Lambda_F).$$

Let $\mathcal{S}_p(E_{/K_\infty^-})_{\text{tors}}$ denote the Λ_--torsion submodule of $\mathcal{S}_p(E_{/K_\infty^-})$).

Main Conjectures

Conjecture (Mazur,Perrin-Riou). "Two-Variable Main Conjecture." *The two-variable p-adic L-function $\mathbf{L}$ generates the ideal* $\mathrm{char}_{\mathbf{\Lambda}}(\mathcal{S}_p(E_{/\mathbf{K}_\infty}))$ *of* $\mathbf{\Lambda}$.

Conjecture (Mazur&Swinnerton-Dyer, Perrin-Riou). "Cyclotomic and Anticyclotomic One-Variable Main Conjectures"

(i) L_+ *generates the ideal*

$$\mathrm{char}_{\Lambda_+}(\mathcal{S}_p(E_{/K_\infty^+})) \subset \Lambda_+.$$

(ii) *The image of* $\mathbf{L}$ *under*

$$\mathbf{I}_{K_\infty^-} \to \mathbf{I}_{K_\infty^-}/\mathbf{I}^2_{K_\infty^-} \xrightarrow{\sim} \Gamma_+ \otimes_{\mathbf{Z}_p} \Lambda_-$$

generates

$$\Gamma_+ \otimes \mathrm{char}_{\Lambda_-}(\mathcal{S}_p(E_{/K_\infty^-})_{\mathrm{tors}}).$$

Main Conjectures

Theorem (Kato, Rubin, Howard, Kolyvagin). *Under mild additional hypotheses,*

(i) $L_+\Lambda_+ \subset \mathrm{char}_{\Lambda_+}(\mathcal{S}_p(E_{/K_\infty^+}))$, *and if E has complex multiplication then equality holds.*

(ii) $\mathrm{char}_{\Lambda_-}(\mathcal{U}/\mathcal{H})^2$
$$\subset \mathrm{char}_{\Lambda_-}(\mathcal{S}_p(E_{/K_\infty^+})_{\mathrm{tors}}).$$

Note: the Height Conjecture and the Λ-adic Gross-Zagier Conjecture predict that

$$\Gamma_+ \otimes \mathrm{char}_{\Lambda_-}(\mathcal{U}/\mathcal{H})^2 = L'\Lambda_-$$

where L' is the image of $\mathbf{L}$ in $\Gamma_+ \otimes_{\mathbf{Z}_p} \Lambda_-$.

Orthogonal $\mathbf{\Lambda}$-modules

Let V be a $\mathbf{Z}_p[[\mathrm{Gal}(\mathbf{K}_\infty/K)]] \otimes \mathbf{Q}_p$-module which is free of finite rank over $\mathbf{\Lambda}$.

- $V^{(\tau)}$ denotes V with $\mathbf{\Lambda}$-module structure obtained by composition with the action of τ,
- $V^* = \mathrm{Hom}_{\mathbf{\Lambda}}(V, \mathbf{\Lambda})$.

An *orthogonal $\mathbf{\Lambda}$-module* is such a V with

- an isomorphism

$$\delta \ : \ \det_{\mathbf{\Lambda}}(V^*) \ \xrightarrow{\sim} \ \det_{\mathbf{\Lambda}}(V^{(\tau)})$$

- a $\mathbf{\Lambda}$-bilinear τ-Hermitian pairing

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

  or equivalently a map $V^{(\tau)} \to V^*$.

Orthogonal Λ-modules

The *discriminant*

$$\mathrm{disc}(V) = \mathrm{disc}(V, \delta, \pi) \in \mathbf{\Lambda}$$

is the composition $\delta \circ \mathrm{det}_{\mathbf{\Lambda}}(\pi)$

$$\mathrm{det}_{\mathbf{\Lambda}}(V^{(\tau)}) \to \mathrm{det}_{\mathbf{\Lambda}}(V^*) \to \mathrm{det}_{\mathbf{\Lambda}}(V^{(\tau)}).$$

Let $M = M(V, \pi)$ be the cokernel of

$$0 \longrightarrow V^{(\tau)} \xrightarrow{\pi} V^* \longrightarrow M \longrightarrow 0.$$

We assume that $\mathrm{disc}(V) \neq 0$, so M is a torsion module.

Orthogonal Λ-modules

If $K \subset F \subset \mathbf{K}_\infty$, recall that

$$\mathbf{I}_F = \ker[\mathbf{\Lambda} \twoheadrightarrow \Lambda_F].$$

Define

$$\begin{aligned} V(F) &:= \ker[V \otimes \Lambda_F \xrightarrow{\pi \otimes 1} (V^{(\tau)})^* \otimes \Lambda_F] \\ &= \{x \in V : \pi(x, V^{(\tau)}) \subset \mathbf{I}_F\}/\mathbf{I}_F V \end{aligned}$$

and similarly

$$V^{(\tau)}(F) := \ker[V^{(\tau)} \otimes \Lambda_F \to V^* \otimes \Lambda_F].$$

We get an induced pairing

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

Packaging the conjectures

Recall the Selmer groups $\mathrm{Sel}_p(E_{/F})$ and

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

Proposition. *Suppose V is an orthogonal $\mathbf{\Lambda}$-module and $\varphi : M \xrightarrow{\sim} \mathcal{S}_p(E_{/\mathbf{K}_\infty})$ is an isomorphism. Then for every extension F of K in $\mathbf{K}_\infty$, φ induces an isomorphism*

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

where $U(F)$ is the module of universal norms.

Orthogonal Λ-modules

Now take $F = K_\infty^-$.

Let $\mathcal{A}$ be the largest ideal of Λ_- such that

- $\mathcal{A}^\tau = \mathcal{A}$,
- $\mathcal{A}^2 \subset \mathrm{char}_{\Lambda_-}(M \otimes \Lambda_-)_{\mathrm{tors}}$.

Define a submodule H of $V(K_\infty^-)$ by

$$H = \mathcal{A} V(K_\infty^-).$$

Packaging the conjectures

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

(a) disc$(V) = \mathbf{L} \in \mathbf{\Lambda}$,

(b) $M \cong \mathcal{S}_p(E_{/\mathbf{K}_\infty})$,

(c) the induced pairing

$$V(K_\infty^-) \otimes V(K_\infty^-)^{(\tau)} \to \mathbf{I}_{K_\infty^-}/\mathbf{I}^2_{K_\infty^-}$$

is surjective,

(d) the isomorphism $V(K_\infty^-) \cong U(K_\infty^-)$ induced by (b) identifies $H \subset V(K_\infty^-)$ with the Heegner submodule $\mathcal{H}$, and identifies the pairing of (c) with the p-adic height pairing.

Packaging the conjectures

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)?*

When E is $y^2 + y = x^3 - x$, $K = \mathbf{Q}(\sqrt{-7})$, $p = 5$, the answer is yes, with V free of rank one.

One could ask analogous questions with:

- $\mathbf{\Lambda}$ replaced by the localization of $\mathbf{\Lambda}$ at $\mathbf{I}$ (weaker),
- $\mathbf{\Lambda}$ replaced by $\mathbf{Z}_p[[\mathbf{\Gamma}]]$ (stronger).

Packaging the conjectures

Theorem. *Suppose there is an orthogonal* $\boldsymbol{\Lambda}$*-module* V *that organizes the anticyclotomic arithmetic of* (E, K, p)*. Then*

- *the Two-Variable Main Conjecture,*
- *the Cyclotomic Main Conjecture,*
- *the Anticyclotomic Main Conjecture,*
- *the Height Conjecture,*
- *the* Λ*-adic Gross-Zagier Conjecture*

all hold.

Some remarks about the proof

- The Two-Variable Main Conjecture follows immediately from (a) and (b).
- The Cyclotomic Main Conjecture follows from the Two-Variable Main Conjecture and the Control Theorem.
- The Height Conjecture is (c).
- The Anticyclotomic Main Conjecture and the Λ-adic Gross-Zagier Conjecture follow from (a), (b), (c), (d), and facts about the structure of $\mathcal{S}_p(E_{/K_\infty^-})$ proved by Howard and by Nekovář.
- The Maximal Nondegeneracy Conjecture Implies the Sign Conjecture, but not (immediately?) from the existence of an organizing orthogonal $\mathbf{\Lambda}$-module.