Traces of rationality of Darmon points

[BD09] Bertolini–Darmon, “The rationality of Stark–Heegner points over genus fields of real quadratic fields”

Seminari de Teoria de Nombres de Barcelona

Barcelona, January 2017

Marc Masdeu

University of Warwick

WARWICK
THE UNIVERSITY OF WARWICK

MARIE CURIE ACTIONS

Introduction

- $E/\mathbb{Q}$ an elliptic curve of conductor $N = pM$, with $p \nmid M$.
- $K/\mathbb{Q}$ a **real** quadratic field, satisfying:
  - p is inert in K
  - $\ell \mid M \implies \ell$ split in K.
- These conditions imply that $\operatorname{ord}_{s=1} L(E/K, s)$ is odd.
- BSD predicts $\exists P_K \in E(K)$ nontorsion...
- ...but Heegner points are not readily available, since K is real!
  - For example $\mathcal{H} \cap K = \emptyset$.
- **Darmon's insight:** consider $\mathcal{H}_p = \mathbb{P}^1(\mathbb{C}_p) \smallsetminus \mathbb{P}^1(\mathbb{Q}_p)$ instead.
  - Constructed a point $P_\psi \in E(\mathbb{C}_p)$ for each $\psi \colon \mathcal{O}_K \hookrightarrow M_2(\mathbb{Q})$.
- **Conjecture (2001):** $P_\psi \in E(K^{\text{ab}})$, and behave like Heegner points.
- In particular, he conjectured that $\sum_\psi P_\psi \in E(K)$.
  - This is (a particular case of) what Bertolini–Darmon proved in 2009.

Plan

1. Define Darmon points (a.k.a. Stark–Heegner points).
2. State the main result of [BD09].
3. Sketch the proof.

Measure-valued modular symbols and integration

- Let $\Gamma = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \in M_2(\mathbb{Z}[1/p]) \cap \mathrm{SL}_2(\mathbb{Q}) \colon N \mid c \right\}$.
- $\mathrm{Meas}^0(\mathbb{P}^1(\mathbb{Q}_p))$ = the Γ-module of measures on $\mathbb{P}^1(\mathbb{Q}_p)$ having total measure 0.
- From previous talks: $E \rightsquigarrow f \in S_2(\Gamma_0(N)) \rightsquigarrow I_f \in \mathrm{Symb}^{\text{new}}_{\Gamma_0(pM)}(\mathbb{Z})^+$.

Proposition

$\exists !\ \mu = \mu_f \in H^1(\Gamma, \mathrm{Meas}^0(\mathbb{P}^1(\mathbb{Q}_p)))$ satisfying:

$$\mu_\gamma(\mathbb{Z}_p) = I_f\{\infty \to \gamma\infty\} \text{ for all } \gamma \in \Gamma_0(N) \subset \Gamma.$$

- Recall $q = q_E \in p\mathbb{Z}_p$ the Tate period attached to $E/\mathbb{Q}_p$.
- There is a Γ-equivariant pairing $\mathrm{Meas}^0(\mathbb{P}^1(\mathbb{Q}_p)) \times \mathrm{Div}^0 \mathcal{H}_p \to \mathbb{C}_p$:

$$(\mu, \tau_2 - \tau_1) \mapsto \int_{\mathbb{P}^1(\mathbb{Q}_p)} \log_q \left(\frac{t - \tau_2}{t - \tau_1} \right) d\mu(t).$$

- Cap product induces a pairing

$$\langle \cdot, \cdot \rangle \colon H^1(\Gamma, \mathrm{Meas}^0(\mathbb{P}^1(\mathbb{Q}_p))) \times H_1(\Gamma, \mathrm{Div}^0 \mathcal{H}_p) \to \mathbb{C}_p.$$

Indefinite integrals

$$\langle\cdot,\cdot\rangle\colon H^1(\Gamma,\mathrm{Meas}^0(\mathbb{P}^1(\mathbb{Q}_p)))\times H_1(\Gamma,\mathrm{Div}^0\mathcal{H}_p)\to\mathbb{C}_p.$$

- Consider the short exact sequence of Γ-modules

$$0\to\mathrm{Div}^0\mathcal{H}_p\xrightarrow{\iota}\mathrm{Div}\,\mathcal{H}_p\xrightarrow{\deg}\mathbb{Z}\to 0.$$

- Taking Γ-homology, get a long exact sequence

$$\cdots\to H_2(\Gamma,\mathbb{Z})\xrightarrow{\delta}H_1(\Gamma,\mathrm{Div}^0\mathcal{H}_p)\xrightarrow{\iota_*}H_1(\Gamma,\mathrm{Div}\,\mathcal{H}_p)\xrightarrow{\deg_*}H_1(\Gamma,\mathbb{Z})\to\cdots$$

- **Fact:** $H_1(\Gamma,\mathbb{Z})=\Gamma^{\mathrm{ab}}$ is a finite abelian group, say of size e_Γ.
- So $\Theta\in H_1(\Gamma,\mathrm{Div}\,\mathcal{H}_p)\rightsquigarrow\Theta_0\in H_1(\Gamma,\mathrm{Div}^0\mathcal{H}_p)$ such that $\iota_*(\Theta_0)=e_\Gamma\Theta$.
- Define $\langle\mu_f,\Theta\rangle:=\frac{1}{e_\Gamma}\langle\mu_f,\Theta_0\rangle$, which is an "indefinite integral"

$$\langle\cdot,\cdot\rangle\colon H^1(\Gamma,\mathrm{Meas}^0(\mathbb{P}^1(\mathbb{Q}_p)))\times H_1(\Gamma,\mathrm{Div}\,\mathcal{H}_p)\to\mathbb{C}_p.$$

Darmon points

- Recall $K/\mathbb{Q}$ our real quadratic field, of discriminant D.
- $\mathrm{Cl}^+(K)$ the narrow class group of K.
- Consider optimal embeddings

$$\psi\colon \mathcal{O}_K \hookrightarrow M_0(M) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z}) \ : \ M \mid c\}.$$

- Similar to Carlos' talk, have action:

$$\mathrm{Cl}^+(K) \curvearrowright \mathrm{Emb}(\mathcal{O}_K) = \{ \text{ conjugacy classes of optimal embeddings}\}.$$

  - If $\sigma \in \mathrm{Cl}^+(K)$ and $\psi \in \mathrm{Emb}(\mathcal{O}_K)$, write ψ^σ for the translate.
- Global class-field theory gives

$$\mathrm{rec}\colon \ \mathrm{Cl}^+(K) \xrightarrow{\simeq} \mathrm{Gal}(H_K^+/K), \quad H_K^+ = \text{ narrow Hilbert class field of K.}$$

- $\psi \in \mathrm{Emb}(\mathcal{O}_K) \rightsquigarrow \Theta_K = [\gamma_\psi \otimes \tau_\psi] \in H_1(\Gamma, \mathrm{Div}\,\mathcal{H}_p)$:
  - $\gamma_\psi = \psi(u_K) \in \Gamma_0(M) \subset \Gamma$, where $\mathcal{O}_{K,1}^\times/\mathrm{tors} = \langle u_K \rangle$.
  - τ_ψ is fixed by γ_ψ (one can consistently choose one of two options).
- Define $J_\psi = \langle \mu_f, \Theta_\psi \rangle \in \mathbb{C}_p$.

Conjecture (Darmon, 2001)

1. For each $\psi \in \mathrm{Emb}(\mathcal{O}_K)$, there exists $\mathbb{P}_\psi \in E(H_K^+)$ and $t \in \mathbb{Q}^\times$ s.t.:

$$J_\psi = t \log_E(\mathbb{P}_\psi).$$

2. For each $\sigma \in \mathrm{Cl}^+(K)$, the points $\mathbb{P}_\psi$ satisfy

$$\mathbb{P}_{\psi^\sigma} = \mathrm{rec}(\sigma)^{-1}(\mathbb{P}_\psi).$$

- Using “multiplicative integrals” $\rightsquigarrow P_\psi$ satisfying $J_\psi = \log_E(P_\psi)$.
  - Part 1 of conjecture then says that $P_\psi \in E(H_K^+) \otimes \mathbb{Q}$.
- Darmon–Green and Darmon–Pollack: numerical evidence.
- The construction has been generalized to many different settings (Greenberg, Gartner, Trifkovic, Guitart–M.–Sengun, Longo–Vigni, Rotger–Seveso,. . .).
- Guitart–M.: more numerical evidence supporting these conjectures.

Main Theorem of [BD09]

Define:

$$J_K = \sum_{\psi \in \mathrm{Emb}(\mathcal{O}_K)} J_\psi \quad \in \mathbb{C}_p.$$

Theorem (Bertolini–Darmon, 2009)

Suppose that:

- *E has **split** multiplicative reduction at p (i.e. $a_p(E) = 1$).*
- *$\exists$ prime $q \neq p$ of multiplicative reduction.*

Then:

1. *There exists a point $\mathbb{P}_K \in E(K)$ and $t \in \mathbb{Q}^\times$ such that $J_K = t \log_E(\mathbb{P})$.*
2. *The point $\mathbb{P}_K$ is of infinite order if and only if $L'(E/K, 1) \neq 0$.*

- In [BD09] they prove the "rationality" not only of J_K, but also of "twisted traces" of the points J_ψ by genus characters.
- Analogues of this result:
  - For "quaternionic Darmon points" (Longo–Vigni).
  - For "Darmon cycles" (Seveso).
- Strategy of proof "inspired by" a **very famous** proof from 1863...

Proof Strategy

1. Construct a p-adic L-function $\mathcal{L}_p(f_\infty/K,k)$ attached to f_∞ and K.
2. Relate J_K to $\mathcal{L}_p(f_\infty/K,k)$:

$$J_K = \mathcal{L}_p'(f_\infty/K,k).$$

3. Factor $\mathcal{L}_p(f_\infty/K,k)^2$ in terms of Mazur–Kitagawa p-adic L-functions:

$$\mathcal{L}_p(f_\infty/K,k)^2 = D^{\frac{k-2}{2}} L_p(f_\infty,k,k/2) L_p(f_\infty^K,k,k/2).$$

4. Deduce the theorem from the results in Carlos' talk on the Mazur–Kitagawa p-adic L-functions appearing in the RHS.

□

A p-adic L-function attached to f_∞ and K

- $E \rightsquigarrow f \in S_2^{\text{new}}(\Gamma_0(N)) \rightsquigarrow I_f = I_f^+ \in H^1(\Gamma_0(N), \mathbb{Z})^{w_\infty = 1}$.
- I_f lives in a family: there exists $\boldsymbol{\mu} \in H^1(\Gamma_0(M), \mathbb{D}_*^\dagger)^{\text{ord}}$ such that
  1. $\rho_2(\boldsymbol{\mu}) = I_f$, and
  2. For all $k \in U \cap \mathbb{Z}_{\geqslant 2}$, $\exists \lambda(k) \in \mathbb{C}_p^\times$ such that $\rho_k(\boldsymbol{\mu}) = \lambda(k) I_{f_k}$.
- For each $\psi \in \mathrm{Emb}(\mathcal{O}_K)$, consider γ_ψ as before, and $\tau_\psi, \bar{\tau}_\psi$ the fixed points by $\psi(K^\times)$ acting on $\mathcal{H}_p$.
- **Very Important Fact:** $J_\tau = \int_{(\mathbb{Z}_p^2)'} \log(x - \tau_\psi y) d\boldsymbol{\mu}_{\gamma_\tau}(x, y)$.
- Define $\mathcal{L}_p(f_\infty, \psi, k)$ as

$$\mathcal{L}_p(f_\infty, \psi, k) = \int_{(\mathbb{Z}_p^2)'} \left((x - \tau_\psi)(x - \bar{\tau}_\psi)\right)^{\frac{k-2}{2}} d\boldsymbol{\mu}_{\gamma_\psi}(x, y).$$

Definition

The "square-root p-adic L-function" is:

$$\mathcal{L}_p(f_\infty/K, k) = \sum_{\psi \in \mathrm{Emb}(\mathcal{O}_K)} \mathcal{L}_p(f_\infty, \psi, k).$$

$$\mathcal{L}_p(f_\infty, \psi, k) = \int_{(\mathbb{Z}_p^2)'} ((x-\tau_\psi)(x-\bar{\tau}_\psi))^{\frac{k-2}{2}} \, d\boldsymbol{\mu}_{\gamma_\psi}(x,y),$$

$$\mathcal{L}_p(f_\infty/K, k) = \sum_\psi \mathcal{L}_p(f_\infty, \psi, k).$$

Theorem A - p-adic Gross–Zagier

We have $\mathcal{L}_p(f_\infty/K, 2) = 0$ and $\mathcal{L}'_p(f_\infty/K, 2) = J_K$.

Proof

- $\mathcal{L}_p(f_\infty/K, \psi, 2) = \int_{(\mathbb{Z}_p)'} d\boldsymbol{\mu}_{\gamma_\tau}(x,y) = \boldsymbol{\mu}_{\gamma_\tau}(\mathbb{P}^1(\mathbb{Q}_p)) = 0$.
- $\mathcal{L}'_p(f_\infty/K, \psi, 2) = \frac{1}{2}\int_{(\mathbb{Z}_p^2)'} (\log(x-\tau_\psi y) + \log(x-\bar{\tau}_\psi y)) \, d\boldsymbol{\mu}_{\gamma_\tau}(x,y)$
  $= \frac{1}{2}(J_\tau + \mathrm{Frob}_p(J_\tau))$
  $= \frac{1}{2}(J_\tau - w_M J_{\tau^\sigma})$ (for some σ depending only on τ).
  $= \frac{1}{2}(J_\tau + J_{\tau^\sigma})$ (since $w_M = -a_p = -1$).
- Summing over all embeddings we get

$$\mathcal{L}'_p(f_\infty/K, 2) = \frac{1}{2}(1-w_M) \sum_{\sigma\in \mathrm{Cl}^+(K)} J_{\tau^\sigma} = \sum_\psi J_\psi.$$

Factorization

Theorem B - Factorization

For all $k \in U$,

$$\mathcal{L}_p(f_\infty/K,k)^2 = D^{\frac{k-2}{2}} L_p(f_\infty,k,k/2) L_p(f_\infty^K,k,k/2).$$

Proof

1. Interpolation property for $\mathcal{L}_p(f_\infty/K,k)^2$ (Popa 2006):

For all $k \in U \cap \mathbb{Z}_{\geqslant 2}$,

$$\mathcal{L}_p(f_\infty/K,k)^2 = \lambda(k)^2(1-a_p(k)^{-2}p^{k-2})^2 D^{\frac{k-2}{2}} L^*(f_k^\sharp/K,k/2).$$

$$= \lambda(k)^2(1-a_p(k)^{-2}p^{k-2})^2 D^{\frac{k-2}{2}} L^*(f_k^\sharp,k/2) L^*(f_k^{K,\sharp},k/2)$$

2. Use the interpolation property of the MK p-adic L-functions (RHS) to show that the factorization occurs for all $k \in U \cap \mathbb{Z}_{\geqslant 2}$.
3. Conclude using that $U \cap \mathbb{Z}_{\geqslant 2}$ is dense in U.

□

End of proof

$$J_K = \mathcal{L}_p'(f_\infty/K, 2) \qquad \text{(A - } p\text{-adic GZ)}$$

$$\mathcal{L}_p(f_\infty/K, k)^2 = D^{\frac{k-2}{2}} L_p(f_\infty, k, k/2) L_p(f_\infty^K, k, k/2) \qquad \text{(B - Factorization)}$$

- Easy observations:
  1. $D^{\frac{k-2}{2}} = 1 + O(k-2)$,
  2. $L_p(f_\infty, k, k/2) = O((k-2)^2)$ (exceptional zero case)
- Deduce that

$$J_K^2 = \frac{1}{2}\left(\frac{d^2}{dk^2}\Big|_{k=2} L_p(f_\infty, k, k/2)\right) L_p(f_\infty^K, 2, 1).$$

- Need to understand the two terms in the RHS.

End of proof (continued)

$$A + B \implies J_K^2 = \frac{1}{2}\left(\frac{d^2}{dk^2}\Big|_{k=2} L_p(f_\infty, k, k/2)\right) L_p(f_\infty^K, 2, 1).$$

Theorem C - Bertolini–Darmon 2007

1. There exists $\mathbb{P} \in E(\mathbb{Q})$, and $\ell_1 \in \mathbb{Q}^\times$, such that

$$\frac{d^2}{dk^2}\Big|_{k=2} L_p(f_\infty, k, k/2) = \ell_1 \log_E^2(\mathbb{P}).$$

2. $\mathbb{P}$ is nontorsion if and only if $L'(E, 1) \neq 0$.

- $a_p(E^K) = -1 \implies L_p(f_\infty^K, 2, 1) = 2L^*(E^K, 1) = 2\ell_2 \in \mathbb{Q}^\times$.
- Get $\log_E^2(P_K) = \ell_1\ell_2 \log_E^2(\mathbb{P})$, and one sees that $\ell_1\ell_2 = t^2$ is a square.
- Taking square roots yields the theorem:

$$J_K = t\log_E^2(\mathbb{P}), \text{ and } \mathbb{P} \text{ is nontorsion iff } L'(E/K, 1) \neq 0.$$

Thank you !

Bibliography, code and slides at:

`http://www.warwick.ac.uk/mmasdeu/`