Quaternionic Darmon points and arithmetic applications

M. Longo, joint work with V. Rotger and S. Vigni

November 4, 2011

Aim of the talk

1. Explain a Darmon-style construction of local points on Jacobians of compact Shimura curves (over $\mathbb{Q}$).

Aim of the talk

1. Explain a Darmon-style construction of local points on Jacobians of compact Shimura curves (over $\mathbb{Q}$).

2. Give some results on the rationality of these points, and some applications to the Birch and Swinnerton-Dyer conjecture

§1. Constructions.
Notations

Fix:

- $D > 1$ an integer which is a product of an even number of distinct primes;

§1. Constructions.
Notations

Fix:

- $D > 1$ an integer which is a product of an even number of distinct primes;
- M a square free integer, prime to D;

§1. Constructions.
Notations

Fix:

- $D > 1$ an integer which is a product of an even number of distinct primes;
- M a square free integer, prime to D;
- $p \nmid MD$ a prime number;

§1. Constructions.
Notations

Fix:

- $D > 1$ an integer which is a product of an even number of distinct primes;
- M a square free integer, prime to D;
- $p \nmid MD$ a prime number;
- $B/\mathbb{Q}$ quaternion algebra of discriminant D and an isomorphism $i_\infty : B \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R})$;

§1. Constructions.
Notations

Fix:

- $D > 1$ an integer which is a product of an even number of distinct primes;
- M a square free integer, prime to D;
- $p \nmid MD$ a prime number;
- $B/\mathbb{Q}$ quaternion algebra of discriminant D and an isomorphism $i_\infty : B \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R})$;
- $R_{Mp} \subseteq R_M$ Eichler orders in B of level Mp and M, respectively.

§1. Constructions.
Notations

Fix:

- $D > 1$ an integer which is a product of an even number of distinct primes;
- M a square free integer, prime to D;
- $p \nmid MD$ a prime number;
- $B/\mathbb{Q}$ quaternion algebra of discriminant D and an isomorphism $i_\infty : B \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R})$;
- $R_{Mp} \subseteq R_M$ Eichler orders in B of level Mp and M, respectively.
- $\Gamma_{Mp} \subseteq \Gamma_M$ units of norm one in R_{Mp} and R_M, respectively.

Homology of Shimura curves

Define

$$X_{Mp} := \Gamma_{Mp} \backslash \mathcal{H}$$

a compact Riemann surface, where the elements of positive norm in $B^\times$ act on the upper half plane $\mathcal{H}$ via i_∞.

Homology of Shimura curves

Define

$$X_{Mp} := \Gamma_{Mp} \backslash \mathcal{H}$$

a compact Riemann surface, where the elements of positive norm in $B^\times$ act on the upper half plane $\mathcal{H}$ via i_∞.

Let

$$H := H_1\left(X_{Mp}, \mathbb{Z}\right)^{p\text{-new}} / \text{torsion}$$

where the upper index p-new denotes the submodule obtained by taking quotient of $H_1\left(X_{Mp}, \mathbb{Z}\right)$ by the image of the homology of the Riemann surface $X_M := \Gamma_M \backslash \mathcal{H}$ via the two canonical degeneracy maps.

First step to the construction of points:

Define

$$T := \mathbb{G}_m \otimes_{\mathbb{Z}} H.$$

First step to the construction of points:

Define

$$T := \mathbb{G}_m \otimes_{\mathbb{Z}} H.$$

$$J := \mathrm{Jac}(X_{Mp})^{p\text{-new}}.$$

First step to the construction of points:

Define

$$T := \mathbb{G}_m \otimes_{\mathbb{Z}} H.$$

$$J := \mathrm{Jac}\left(X_{Mp}\right)^{p\text{-new}}.$$

Denote by K_p the unramified quadratic extension of $\mathbb{Q}_p$.

First step to the construction of points:

Define

$$T := \mathbb{G}_m \otimes_{\mathbb{Z}} H.$$

$$J := \mathrm{Jac}\left(X_{Mp}\right)^{p\text{-new}}.$$

Denote by K_p the unramified quadratic extension of $\mathbb{Q}_p$.

Following works by S. Dasgupta and M. Greenberg, we will explicitly describe a lattice $L \subseteq T(K_p)$ such that there is an isogeny

$$T(K_p)/L \to J^2(K_p)$$

defined over K_p and Hecke-equivariant.

Measure-valued cohomology

We begin by constricting lattices in $T(K_p)$ which are the candidates for our uniformization result.

Measure-valued cohomology

We begin by constricting lattices in $T(K_p)$ which are the candidates for our uniformization result.

Define the Ihara's group:

$$\Gamma := \left(R_M[1/p]\right)_{\text{norm}=1}.$$

Measure-valued cohomology

We begin by constricting lattices in $T(K_p)$ which are the candidates for our uniformization result.

Define the Ihara's group:

$$\Gamma := \left(R_M[1/p]\right)_{\text{norm}=1}.$$

Let

$$\mathcal{M} := \mathrm{Meas}^0(\mathbb{P}^1(\mathbb{Q}_p), H)$$

denote the group of measures on $\mathbb{P}^1(\mathbb{Q}_p)$ with values in H and total mass equal to zero.

Measure-valued cohomology

We begin by constricting lattices in $T(K_p)$ which are the candidates for our uniformization result.

Define the Ihara's group:

$$\Gamma := \left(R_M[1/p]\right)_{\mathrm{norm}=1}.$$

Let

$$\mathcal{M} := \mathrm{Meas}^0(\mathbb{P}^1(\mathbb{Q}_p), H)$$

denote the group of measures on $\mathbb{P}^1(\mathbb{Q}_p)$ with values in H and total mass equal to zero.
The group $\mathcal{M}$ is endowed with an action of Γ as follows: fix an isomorphism

$$i_p : B \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq \mathrm{M}_2(\mathbb{Q}_p)$$

and let Γ act on $\mathbb{P}^1(\mathbb{Q}_p)$ by fractional linear transformations via i_p. Then define

$$(\gamma\nu)(U) := \nu(\gamma^{-1}(U)).$$

Construction of lattices/1

We know a procedure to construct lattices L_ν in $T(K_p)$ using classes

$$\nu \in H^1(\Gamma, \mathcal{M})$$

which we now describe.

Construction of lattices/1

We know a procedure to construct lattices L_ν in $T(K_p)$ using classes

$$\nu \in H^1(\Gamma, \mathcal{M})$$

which we now describe.

Define:

$$\mathcal{H}_p := K_p - \mathbb{Q}_p.$$

The group $B^\times$ acts on $\mathcal{H}_p$ by fractional linear transformations via $i_p : B \otimes \mathbb{Q}_p \simeq \mathrm{M}_2(\mathbb{Q}_p)$.

Construction of lattices/1

We know a procedure to construct lattices L_ν in $T(K_p)$ using classes

$$\nu \in H^1(\Gamma, \mathcal{M})$$

which we now describe.

Define:

$$\mathcal{H}_p := K_p - \mathbb{Q}_p.$$

The group $B^\times$ acts on $\mathcal{H}_p$ by fractional linear transformations via $i_p : B \otimes \mathbb{Q}_p \simeq \mathrm{M}_2(\mathbb{Q}_p)$.

There is a map (which depends on the choice of $\nu \in H^1(\Gamma, \mathcal{M})$):

$$\phi_\nu : H_2(\Gamma, \mathbb{Z}) \xrightarrow{(1)} H_1(\Gamma, \mathrm{Div}^0 \mathcal{H}_p) \xrightarrow{(2)} T(K_p)$$

where (1) and (2) are as follows:

Construction of lattices/2

$$H_2(\Gamma, \mathbb{Z}) \xrightarrow{(1)} H_1(\Gamma, \mathrm{Div}^0 \mathcal{H}_p)$$

arises taking the Γ-homology of the exact sequence:

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

Construction of lattices/3

$$H_1(\Gamma, \mathrm{Div}^0 \mathcal{H}_p) \xrightarrow{(2)} T(K_p)$$

can be described as follows:

Construction of lattices/3

$$H_1(\Gamma, \mathrm{Div}^0 \mathcal{H}_p) \xrightarrow{(2)} T(K_p)$$

can be described as follows:

First we note that there is a pairing:

$$\langle , \rangle : \mathrm{Div}^0 \mathcal{H}_p \times \mathcal{M} \longrightarrow T(K_p)$$

defined by the integration formula:

$$\langle d, \nu \rangle := \times\!\!\!\!\!\!\int_{\mathbb{P}^1(\mathbb{Q}_p)} f_d d\nu$$

where f_d is any rational function on $\mathbb{P}^1(K_p)$ with $\mathrm{div}(f_d) = d$.

Construction of lattices/4

We get a pairing:

$$H_1(\Gamma, \mathrm{Div}^0 \mathcal{H}_p) \times H^1(\Gamma, \mathcal{M}) \longrightarrow T(K_p).$$

Fixing ν in the second variable gives the map (2):

$$H_1(\Gamma, \mathrm{Div}^0 \mathcal{H}_p) \xrightarrow{(2)} T(K_p).$$

.

Uniformization result

We thus have, for any $\nu \in H^1(\Gamma, \mathcal{M})$:

$$\phi_\nu : H_2(\Gamma, \mathbb{Z}) \xrightarrow{(1)} H_1(\Gamma, \mathrm{Div}^0 \mathcal{H}_p) \xrightarrow{(2)} T(K_p).$$

Uniformization result

We thus have, for any $\nu \in H^1(\Gamma, \mathcal{M})$:

$$\phi_\nu : H_2(\Gamma, \mathbb{Z}) \xrightarrow{(1)} H_1(\Gamma, \operatorname{Div}^0 \mathcal{H}_p) \xrightarrow{(2)} T(K_p).$$

We can explicitly construct an element

$$\mu_H \in H^1(\Gamma, \mathcal{M})$$

such that the following theorem is true.

Uniformization result

We thus have, for any $\nu \in H^1(\Gamma, \mathcal{M})$:

$$\phi_\nu : H_2(\Gamma, \mathbb{Z}) \xrightarrow{(1)} H_1(\Gamma, \mathrm{Div}^0 \mathcal{H}_p) \xrightarrow{(2)} T(K_p).$$

We can explicitly construct an element

$$\mu_H \in H^1(\Gamma, \mathcal{M})$$

such that the following theorem is true.

Theorem (L.-Rotger-Vigni)

Define

$$L := \phi_{\mu_H}(H_2(\Gamma, \mathbb{Z})).$$

Then there exists an Hecke-equivariant isogeny defined over K_p*:*

$$\phi : T(K_p)/L \longrightarrow J^2(K_p).$$

Darmon points

We now apply the above uniformization result to define Darmon (or Stark-Heegner) points on $J^2(K_p)$.

Splitting 2-cocycles

Fix a representative $\gamma \mapsto \mu_{H,\gamma}$ of μ_H and a point $\tau \in \mathcal{H}_p$.

Splitting 2-cocycles

Fix a representative $\gamma \mapsto \mu_{H,\gamma}$ of μ_H and a point $\tau \in \mathcal{H}_p$.

Define the 2-cocycle $d_\tau : \Gamma \times \Gamma \to T(K_p)$ by:

$$(\gamma_1, \gamma_2) \longmapsto \times\!\!\!\!\!\!\int_{\mathbb{P}^1(\mathbb{Q}_p)} \frac{t - \gamma_1^{-1}(\tau)}{t - \tau} d\mu_{H,\gamma_2}.$$

Splitting 2-cocycles

Fix a representative $\gamma \mapsto \mu_{H,\gamma}$ of μ_H and a point $\tau \in \mathcal{H}_p$.

Define the 2-cocycle $d_\tau : \Gamma \times \Gamma \to T(K_p)$ by:

$$(\gamma_1, \gamma_2) \longmapsto \times\!\!\!\!\!\!\int_{\mathbb{P}^1(\mathbb{Q}_p)} \frac{t - \gamma_1^{-1}(\tau)}{t - \tau} d\mu_{H,\gamma_2}.$$

d_τ splits on $T(K_p)/L$.

Splitting 2-cocycles

Fix a representative $\gamma \mapsto \mu_{H,\gamma}$ of μ_H and a point $\tau \in \mathcal{H}_p$.

Define the 2-cocycle $d_\tau : \Gamma \times \Gamma \to T(K_p)$ by:

$$(\gamma_1, \gamma_2) \longmapsto \times\!\!\!\!\!\!\int_{\mathbb{P}^1(\mathbb{Q}_p)} \frac{t - \gamma_1^{-1}(\tau)}{t - \tau} d\mu_{H,\gamma_2}.$$

d_τ splits on $T(K_p)/L$.

Fix $\beta_\tau : \Gamma \to T(K_p)/L$ splitting d_τ.

Splitting 2-cocycles

Fix a representative $\gamma \mapsto \mu_{H,\gamma}$ of μ_H and a point $\tau \in \mathcal{H}_p$.

Define the 2-cocycle $d_\tau : \Gamma \times \Gamma \to T(K_p)$ by:

$$(\gamma_1, \gamma_2) \longmapsto \times\!\!\!\!\!\!\int_{\mathbb{P}^1(\mathbb{Q}_p)} \frac{t - \gamma_1^{-1}(\tau)}{t - \tau} d\mu_{H,\gamma_2}.$$

d_τ splits on $T(K_p)/L$.

Fix $\beta_\tau : \Gamma \to T(K_p)/L$ splitting d_τ.

Let $t := |\Gamma^{\mathrm{ab}}|$. Then $t\beta_\tau$ does not depend on the choice of β_τ.

Global data

Let K be a real quadratic field such that:

Global data

Let K be a real quadratic field such that:

- all primes $\ell \mid M$ are split in K;

Global data

Let K be a real quadratic field such that:

- all primes $\ell \mid M$ are split in K;
- all primes $\ell \mid Dp$ are inert in K.

Global data

Let K be a real quadratic field such that:

- all primes $\ell \mid M$ are split in K;
- all primes $\ell \mid Dp$ are inert in K.

Let $\mathcal{O}_c$ be the order of K of conductor c with $c > 1$ an integer such that $(c, \mathrm{disc}(K)MDp) = 1$.

Global data

Let K be a real quadratic field such that:

- all primes $\ell \mid M$ are split in K;
- all primes $\ell \mid Dp$ are inert in K.

Let $\mathcal{O}_c$ be the order of K of conductor c with $c > 1$ an integer such that $(c, \mathrm{disc}(K)MDp) = 1$.

Fix an optimal embedding $\psi : K \hookrightarrow B$ of $\mathcal{O}_c$ into R_M. So we have:

$$\psi(\mathcal{O}_c) = \psi(K) \cap R_M.$$

Global data

Let K be a real quadratic field such that:

- all primes $\ell \mid M$ are split in K;
- all primes $\ell \mid Dp$ are inert in K.

Let $\mathcal{O}_c$ be the order of K of conductor c with $c > 1$ an integer such that $(c, \mathrm{disc}(K)MDp) = 1$.

Fix an optimal embedding $\psi : K \hookrightarrow B$ of $\mathcal{O}_c$ into R_M. So we have:

$$\psi(\mathcal{O}_c) = \psi(K) \cap R_M.$$

Denote by ϵ_c a positive (w.r.t. a chosen $K \hookrightarrow \mathbb{R}$) generator of $\mathcal{O}_c^\times$.

Global data

Let K be a real quadratic field such that:

- all primes $\ell \mid M$ are split in K;
- all primes $\ell \mid Dp$ are inert in K.

Let $\mathcal{O}_c$ be the order of K of conductor c with $c > 1$ an integer such that $(c, \mathrm{disc}(K)MDp) = 1$.

Fix an optimal embedding $\psi : K \hookrightarrow B$ of $\mathcal{O}_c$ into R_M. So we have:

$$\psi(\mathcal{O}_c) = \psi(K) \cap R_M.$$

Denote by ϵ_c a positive (w.r.t. a chosen $K \hookrightarrow \mathbb{R}$) generator of $\mathcal{O}_c^\times$.

Define $\gamma_\psi := \psi(\epsilon_c) \in \Gamma$.

Global data

Let K be a real quadratic field such that:

- all primes $\ell \mid M$ are split in K;
- all primes $\ell \mid Dp$ are inert in K.

Let $\mathcal{O}_c$ be the order of K of conductor c with $c > 1$ an integer such that $(c, \mathrm{disc}(K)MDp) = 1$.

Fix an optimal embedding $\psi : K \hookrightarrow B$ of $\mathcal{O}_c$ into R_M. So we have:

$$\psi(\mathcal{O}_c) = \psi(K) \cap R_M.$$

Denote by ϵ_c a positive (w.r.t. a chosen $K \hookrightarrow \mathbb{R}$) generator of $\mathcal{O}_c^\times$.

Define $\gamma_\psi := \psi(\epsilon_c) \in \Gamma$.

Let z_ψ denote one of the two fixed points of $\psi(K^\times)$ acting on $\mathbb{P}^1(\mathbb{Q}_p)$ via i_p (a suitable normalization specifies the choice).

Definition of Darmon points

Recall the data:

Definition of Darmon points

Recall the data:

1. The optimal embedding $\psi : K \hookrightarrow B$ of $\mathcal{O}_c$ in R_M, the global unit ϵ_c and its image $\gamma_\psi := \psi(\epsilon_c) \in \Gamma$.

Definition of Darmon points

Recall the data:

1. The optimal embedding $\psi : K \hookrightarrow B$ of $\mathcal{O}_c$ in R_M, the global unit ϵ_c and its image $\gamma_\psi := \psi(\epsilon_c) \in \Gamma$.
2. The fixed point $z_\psi \in K_p - \mathbb{Q}_p$, so that we can consider the function $\beta_{z_\psi} : \Gamma \to T(K_p)/L$ splitting the 2-cocycle d_{z_ψ}.

Definition of Darmon points

Recall the data:

1. The optimal embedding $\psi : K \hookrightarrow B$ of $\mathcal{O}_c$ in R_M, the global unit ϵ_c and its image $\gamma_\psi := \psi(\epsilon_c) \in \Gamma$.
2. The fixed point $z_\psi \in K_p - \mathbb{Q}_p$, so that we can consider the function $\beta_{z_\psi} : \Gamma \to T(K_p)/L$ splitting the 2-cocycle d_{z_ψ}.

Definition

Darmon points $P_{J,\psi}$ on $J^2(K_p)$ are

$$\begin{array}{ccc} T(K_p)/L & \xrightarrow{\phi_{L_\mu}} & J^2(K_p) \\ t\beta_{z_\psi}(\gamma_\psi) & \longmapsto & P_{J,\psi}. \end{array}$$

Definition of Darmon points

Recall the data:

1. The optimal embedding $\psi : K \hookrightarrow B$ of $\mathcal{O}_c$ in R_M, the global unit ϵ_c and its image $\gamma_\psi := \psi(\epsilon_c) \in \Gamma$.
2. The fixed point $z_\psi \in K_p - \mathbb{Q}_p$, so that we can consider the function $\beta_{z_\psi} : \Gamma \to T(K_p)/L$ splitting the 2-cocycle d_{z_ψ}.

Definition

Darmon points $P_{J,\psi}$ on $J^2(K_p)$ are

$$\begin{array}{ccc} T(K_p)/L & \xrightarrow{\phi_{L_\mu}} & J^2(K_p) \\ t\beta_{z_\psi}(\gamma_\psi) & \longmapsto & P_{J,\psi}. \end{array}$$

Conjecture

$P_{J,\psi} \in J^2(H_c^+)$, where H_c^+ is the narrow ring class field of conductor c of K, so that $G_c^+ := \mathrm{Gal}(H_c^+/K) \simeq \mathrm{Pic}^+(\mathcal{O}_c)$.

Modular forms

Let now f be a weight 2 newform of level $\Gamma_0(MDp)$. We may choose one component of J^2 and compose with the projection to the abelian variety A_f associated with f.

$$J^2 \longrightarrow J \longrightarrow A_f.$$

In this way we also get points $P_{f,\psi} \in A_f(K_p)$.

Modular forms

Let now f be a weight 2 newform of level $\Gamma_0(MDp)$. We may choose one component of J^2 and compose with the projection to the abelian variety A_f associated with f.

$$J^2 \longrightarrow J \longrightarrow A_f.$$

In this way we also get points $P_{f,\psi} \in A_f(K_p)$.

Conjecture

(1) $P_{f,\psi} \in A_f(H_c^+)$.
(2) For any $\chi : G_c^+ \to \mathbb{C}^\times$, *define the point*

$$P_{f,\chi} := \sum_{\sigma \in G_c^+} P_{f,\psi}^{\sigma} \otimes \chi^{-1}(\sigma) \in (A_f(H_c^+) \otimes_{\mathbb{Z}} \mathbb{C})^{\chi}.$$

Then $P_{f,\chi} \neq 0$ *if and only if* $L_K'(f,\chi,1) \neq 0$.

§2 Results and applications
§2.1 Applications to BSD conjecture.

Fix an elliptic curve E of conductor MD and $K/\mathbb{Q}$ a real quadratic extension such that

§2 Results and applications
§2.1 Applications to BSD conjecture.

Fix an elliptic curve E of conductor MD and $K/\mathbb{Q}$ a real quadratic extension such that

- all primes dividing M are split in K;

§2 Results and applications
§2.1 Applications to BSD conjecture.

Fix an elliptic curve E of conductor MD and $K/\mathbb{Q}$ a real quadratic extension such that

- all primes dividing M are split in K;
- all primes dividing D are inert in K.

§2 Results and applications
§2.1 Applications to BSD conjecture.

Fix an elliptic curve E of conductor MD and $K/\mathbb{Q}$ a real quadratic extension such that

- all primes dividing M are split in K;
- all primes dividing D are inert in K.

Parity arguments show that the order of vanishing of $L_K(E, \chi, 1)$ is even, for characters $\chi : G_c^+ \to \mathbb{C}^\times$ with $(c, \mathrm{disc}(K)MD) = 1$.

§2 Results and applications
§2.1 Applications to BSD conjecture.

Fix an elliptic curve E of conductor MD and $K/\mathbb{Q}$ a real quadratic extension such that

- all primes dividing M are split in K;
- all primes dividing D are inert in K.

Parity arguments show that the order of vanishing of $L_K(E,\chi,1)$ is even, for characters $\chi : G_c^+ \to \mathbb{C}^\times$ with $(c, \mathrm{disc}(K)MD) = 1$.

Theorem (L.-Rotger-Vigni)

Assume the first conjecture ($P_{J,\psi} \in J^2(H_c^+)$). If $L_K(E,\chi,1) \neq 0$ then $(E(H_c^+) \otimes_{\mathbb{Z}} \mathbb{C})^\chi = 0$.

§2 Results and applications
§2.1 Applications to BSD conjecture.

Fix an elliptic curve E of conductor MD and $K/\mathbb{Q}$ a real quadratic extension such that

- all primes dividing M are split in K;
- all primes dividing D are inert in K.

Parity arguments show that the order of vanishing of $L_K(E,\chi,1)$ is even, for characters $\chi : G_c^+ \to \mathbb{C}^\times$ with $(c, \mathrm{disc}(K)MD) = 1$.

Theorem (L.-Rotger-Vigni)

Assume the first conjecture ($P_{J,\psi} \in J^2(H_c^+)$). If $L_K(E,\chi,1) \neq 0$ then $(E(H_c^+) \otimes_{\mathbb{Z}} \mathbb{C})^\chi = 0$.

As you may notice, the prime p inert in K does not appear in the statement of this result. To explain the connection with Darmon points, let us consider the simplest case when $c = 1$ and $H_1^+ = K$.

Proof: Selmer group and auxiliary primes p

Fix a prime $\ell \nmid MD$ and consider the Selmer group

$$\mathrm{Sel}_\ell(E/K) \subseteq H^1(K, E[\ell]).$$

Proof: Selmer group and auxiliary primes p

Fix a prime $\ell \nmid MD$ and consider the Selmer group

$$\mathrm{Sel}_\ell(E/K) \subseteq H^1(K, E[\ell]).$$

Our aim is to show that this group is trivial, for at least one prime ℓ as above if $L_K(E, 1) \neq 0$ (in fact, we can show this statement for all ℓ except a finite number, as predicted by the BSD conjecture).

Proof: Selmer group and auxiliary primes p

Fix a prime $\ell \nmid MD$ and consider the Selmer group

$$\mathrm{Sel}_\ell(E/K) \subseteq H^1(K, E[\ell]).$$

Our aim is to show that this group is trivial, for at least one prime ℓ as above if $L_K(E, 1) \neq 0$ (in fact, we can show this statement for all ℓ except a finite number, as predicted by the BSD conjecture).

To this end, we consider a suitable infinite set of primes p, which are inert in K, and such that

$$\ell \mid a_p^2 - (p+1)^2.$$

For this primes, we have a raising the level result which allows to view the Galois module $E[\ell]$ as a quotient of $J_p[\ell]$, where

$$J_p := \mathrm{Jac}\left(X_{Mp}\right)^{p\text{-new}}.$$

Proof: Darmon points

Kummer maps and the above observation can be used to associate $P_{J,\psi} \in J_p(K)$ with a cohomology class $\kappa_p \in H^1(K, E[p])$:

$$J_p(K) \longrightarrow H^1(K, J_p[\ell]) \longrightarrow H^1(K, E[\ell]).$$

Proof: Darmon points

Kummer maps and the above observation can be used to associate $P_{J,\psi} \in J_p(K)$ with a cohomology class $\kappa_p \in H^1(K, E[p])$:

$$J_p(K) \longrightarrow H^1(K, J_p[\ell]) \longrightarrow H^1(K, E[\ell]).$$

The collection $\{\kappa_p\}_p$ can be used, in combination with the global Tate pairing, to deduce the triviality of $\mathrm{Sel}_\ell(E/K)$ under the condition $L_K(E, 1) \neq 0$.

Proof: Darmon points

Kummer maps and the above observation can be used to associate $P_{J,\psi} \in J_p(K)$ with a cohomology class $\kappa_p \in H^1(K, E[p])$:

$$J_p(K) \longrightarrow H^1(K, J_p[\ell]) \longrightarrow H^1(K, E[\ell]).$$

The collection $\{\kappa_p\}_p$ can be used, in combination with the global Tate pairing, to deduce the triviality of $\mathrm{Sel}_\ell(E/K)$ under the condition $L_K(E, 1) \neq 0$.

For this, we need a reciprocity law relating the restriction at ℓ of the classes κ_p with the algebraic part of the special value of $L_K(E, 1)$.

§2.2 Results for genus characters

A genus character is a quadratic unramified character of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. Let H_χ denote the field cut out by χ (biquadratic, unless χ is trivial).

§2.2 Results for genus characters

A genus character is a quadratic unramified character of $\mathrm{Gal}\,(K^{\mathrm{ab}}/K)$. Let H_χ denote the field cut out by χ (biquadratic, unless χ is trivial).
Genus characters are described by unordered pairs (χ_1, χ_2) of Dirichlet characters of discriminants d_1 and d_2 with $d_1 d_2 = d_K$.

§2.2 Results for genus characters

A genus character is a quadratic unramified character of $\mathrm{Gal}\,(K^{\mathrm{ab}}/K)$. Let H_χ denote the field cut out by χ (biquadratic, unless χ is trivial).
Genus characters are described by unordered pairs (χ_1, χ_2) of Dirichlet characters of discriminants d_1 and d_2 with $d_1 d_2 = d_K$.

Theorem (L.-Vigni)

Suppose that $A_f = E$ is an elliptic curve and χ is a genus character of K with $\chi_1(-MD) = \chi_2(-MD) = -w_{MD}$. Then there exists an integer $n \geq 1$ such that:

- $nP_{f,\chi} \in E(H_\chi)$
- $nP_{f,\chi} \neq 0$ *in* $(E(H_\chi) \otimes \mathbb{C})^\chi$ *if and only if* $L'_K(E, \chi, 1) \neq 0$.

§2.2 Results for genus characters

A genus character is a quadratic unramified character of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. Let H_χ denote the field cut out by χ (biquadratic, unless χ is trivial).
Genus characters are described by unordered pairs (χ_1, χ_2) of Dirichlet characters of discriminants d_1 and d_2 with $d_1 d_2 = d_K$.

Theorem (L.-Vigni)

Suppose that $A_f = E$ is an elliptic curve and χ is a genus character of K with $\chi_1(-MD) = \chi_2(-MD) = -w_{MD}$. Then there exists an integer $n \geq 1$ such that:

- $nP_{f,\chi} \in E(H_\chi)$
- $nP_{f,\chi} \neq 0$ *in* $(E(H_\chi) \otimes \mathbb{C})^\chi$ *if and only if* $L'_K(E, \chi, 1) \neq 0$.

The proof generalizes arguments by Bertolini-Darmon for the split quaternion algebra $\mathrm{M}_2(\mathbb{Q})$.

Step I. Lift of measure-valued cohomology/1

Choose a sign $\pm$ (depending on χ) and let

$$\mu_f \in H^1(\Gamma, \mathrm{Meas}^0(\mathbb{P}^1(\mathbb{Q}_p), H_E^{\pm}))$$

denote the projection of μ_H to

$$H_E^{\pm} := H_1(E(\mathbb{C}), \mathbb{Z})^{\pm}$$

(=$\pm$-eigenmodule for the complex conjugation).

Step I. Lift of measure-valued cohomology/1

Choose a sign $\pm$ (depending on χ) and let

$$\mu_f \in H^1(\Gamma, \mathrm{Meas}^0(\mathbb{P}^1(\mathbb{Q}_p), H_E^\pm))$$

denote the projection of μ_H to

$$H_E^\pm := H_1(E(\mathbb{C}), \mathbb{Z})^\pm$$

(=$\pm$-eigenmodule for the complex conjugation).

- $f \Longrightarrow f_\infty$: Hida family passing through f.

Step I. Lift of measure-valued cohomology/1

Choose a sign $\pm$ (depending on χ) and let

$$\mu_f \in H^1(\Gamma, \mathrm{Meas}^0(\mathbb{P}^1(\mathbb{Q}_p), H_E^\pm))$$

denote the projection of μ_H to

$$H_E^\pm := H_1(E(\mathbb{C}), \mathbb{Z})^\pm$$

(=$\pm$-eigenmodule for the complex conjugation).

- $f \Longrightarrow f_\infty$: Hida family passing through f.
- Want: $\mu_f \Longrightarrow \tilde{\mu}_f$.

Step I. Lift of measure-valued cohomology/2

Write $\mathbb{D}$ for the module of $\mathbb{Z}_p$-valued measures on $\mathbb{Y} := \mathbb{Z}_p^2$ which are supported on the subset $\mathbb{X}$ of primitive elements (i.e., those vectors in $\mathbb{Y}$ which are not divisible by p).

Step I. Lift of measure-valued cohomology/2

Write $\mathbb{D}$ for the module of $\mathbb{Z}_p$-valued measures on $\mathbb{Y} := \mathbb{Z}_p^2$ which are supported on the subset $\mathbb{X}$ of primitive elements (i.e., those vectors in $\mathbb{Y}$ which are not divisible by p).

There is a map

$$\pi : \mathbb{X} \longrightarrow \mathbb{P}^1(\mathbb{Q}_p)$$

taking (x, y) to x/y

Step I. Lift of measure-valued cohomology/2

Write $\mathbb{D}$ for the module of $\mathbb{Z}_p$-valued measures on $\mathbb{Y} := \mathbb{Z}_p^2$ which are supported on the subset $\mathbb{X}$ of primitive elements (i.e., those vectors in $\mathbb{Y}$ which are not divisible by p).

There is a map

$$\pi : \mathbb{X} \longrightarrow \mathbb{P}^1(\mathbb{Q}_p)$$

taking (x, y) to x/y

If f_k is the weight k-specialization, trivial character, of f_∞, combining Jacquet-Langlands and Matsushima-Shimura we get an element

$$\phi_k \in H^1(\Gamma_{Mp}, \mathrm{Sym}^{k-2}(\mathbb{C}^2)).$$

Step I. Lift of measure-valued cohomology/3

We can construct an element $\tilde{\mu}_f \in H^1(\Gamma_M, \mathbb{D}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ such that:

Step I. Lift of measure-valued cohomology/3

We can construct an element $\tilde{\mu}_f \in H^1(\Gamma_M, \mathbb{D}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ such that:

- $\pi_*(\tilde{\mu}_f) = \mu_f$ (recall $\pi : \mathbb{X} \to \mathbb{P}^1(\mathbb{Q}_p)$).

Step I. Lift of measure-valued cohomology/3

We can construct an element $\tilde{\mu}_f \in H^1(\Gamma_M, \mathbb{D}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ such that:

- $\pi_*(\tilde{\mu}_f) = \mu_f$ (recall $\pi : \mathbb{X} \to \mathbb{P}^1(\mathbb{Q}_p)$).
- There are *specialization maps* ρ_k such that

$$\rho_k(\tilde{\mu}_f) = (\text{multiple of })\phi_k \in H^1(\Gamma_{Mp}, \mathrm{Sym}^{k-2}(\mathbb{C}^2)).$$

Step II: Esplicit expression for Darmon points

Now let

$$\Phi_{\mathrm{Tate}} : \bar{K}_p^\times / q^{\mathbb{Z}} \longrightarrow E(\bar{K}_p)$$

denote Tate's p-adic uniformization.

Step II: Esplicit expression for Darmon points

Now let

$$\Phi_{\mathrm{Tate}} : \bar{K}_p^{\times}/q^{\mathbb{Z}} \longrightarrow E(\bar{K}_p)$$

denote Tate's p-adic uniformization.

Let $\log_q$ be the branch of the p-adic logarithm satisfying $\log_q(q) = 0$ and define

$$\log_E(P) := \log_q\left(\Phi_{\mathrm{Tate}}^{-1}(P)\right)$$

for all $P \in E(K_p)$.

Step II: Esplicit expression for Darmon points

Now let

$$\Phi_{\mathrm{Tate}} : \bar{K}_p^{\times}/q^{\mathbb{Z}} \longrightarrow E(\bar{K}_p)$$

denote Tate's p-adic uniformization.

Let $\log_q$ be the branch of the p-adic logarithm satisfying $\log_q(q) = 0$ and define

$$\log_E(P) := \log_q\left(\Phi_{\mathrm{Tate}}^{-1}(P)\right)$$

for all $P \in E(K_p)$.

The first auxiliary result is the following

Theorem (Explicit expression of Darmon points)

$$\log_E(P_{f,\psi}) = (-t) \cdot \int_{\mathbb{X}} \log_q(x - z_\psi y) d\tilde{\mu}_{f,\gamma_\psi}.$$

Step III. p-adic L-functions

Associate to $\tilde{\mu}_f$ a p-adic L-function $L_p(f_\infty/K, \chi, k)$ attached to f_∞, a genus character χ of K, and a p-adic variable k.

Step III. p-adic L-functions

Associate to $\tilde{\mu}_f$ a p-adic L-function $L_p(f_\infty/K, \chi, k)$ attached to f_∞, a genus character χ of K, and a p-adic variable k.

A result by Popa + the interpolation property $\rho_k(\tilde{\mu}_f) = \phi_k$ in $H^1(\Gamma_{Mp}, \mathrm{Sym}^{k-2}(\mathbb{C}^2))$ imply: for $k \geq 4$ an even integer

$$L_p(f_\infty/K, \chi, k) = (\text{non-zero constant})\; L(f_k^\sharp/K, \chi, k/2)$$

where the form f_k is the p-stabilization of $f_k^\sharp \in S_k(\Gamma_0(MD))$.

Step III. p-adic L-functions

Associate to $\tilde{\mu}_f$ a p-adic L-function $L_p(f_\infty/K, \chi, k)$ attached to f_∞, a genus character χ of K, and a p-adic variable k.

A result by Popa + the interpolation property $\rho_k(\tilde{\mu}_f) = \phi_k$ in $H^1(\Gamma_{Mp}, \mathrm{Sym}^{k-2}(\mathbb{C}^2))$ imply: for $k \geq 4$ an even integer

$$L_p(f_\infty/K, \chi, k) = (\text{non-zero constant})\ L(f_k^\sharp/K, \chi, k/2)$$

where the form f_k is the p-stabilization of $f_k^\sharp \in S_k(\Gamma_0(MD))$.

Theorem (Factorization of p-adic L-functions)

$$L_p(f_\infty/K, \chi, k) = \eta(k) L_p(f_\infty, \chi_1, k, k/2) L_p(f_\infty, \chi_2, k, k/2)$$

Step III. p-adic L-functions

Associate to $\tilde{\mu}_f$ a p-adic L-function $L_p(f_\infty/K, \chi, k)$ attached to f_∞, a genus character χ of K, and a p-adic variable k.

A result by Popa + the interpolation property $\rho_k(\tilde{\mu}_f) = \phi_k$ in $H^1(\Gamma_{Mp}, \mathrm{Sym}^{k-2}(\mathbb{C}^2))$ imply: for $k \geq 4$ an even integer

$$L_p(f_\infty/K, \chi, k) = (\text{non-zero constant})\ L(f_k^\sharp/K, \chi, k/2)$$

where the form f_k is the p-stabilization of $f_k^\sharp \in S_k(\Gamma_0(MD))$.

Theorem (Factorization of p-adic L-functions)

$$L_p(f_\infty/K, \chi, k) = \eta(k) L_p(f_\infty, \chi_1, k, k/2) L_p(f_\infty, \chi_2, k, k/2)$$

- *$L(f_\infty, \chi_i, k, s)$ is the Mazur-Kitagawa p-adic L-function*

Step III. p-adic L-functions

Associate to $\tilde{\mu}_f$ a p-adic L-function $L_p(f_\infty/K, \chi, k)$ attached to f_∞, a genus character χ of K, and a p-adic variable k.

A result by Popa + the interpolation property $\rho_k(\tilde{\mu}_f) = \phi_k$ in $H^1(\Gamma_{Mp}, \mathrm{Sym}^{k-2}(\mathbb{C}^2))$ imply: for $k \geq 4$ an even integer

$$L_p(f_\infty/K, \chi, k) = (\text{non-zero constant})\ L(f_k^\sharp/K, \chi, k/2)$$

where the form f_k is the p-stabilization of $f_k^\sharp \in S_k(\Gamma_0(MD))$.

Theorem (Factorization of p-adic L-functions)

$$L_p(f_\infty/K, \chi, k) = \eta(k) L_p(f_\infty, \chi_1, k, k/2) L_p(f_\infty, \chi_2, k, k/2)$$

- *$L(f_\infty, \chi_i, k, s)$ is the Mazur-Kitagawa p-adic L-function*
- *$k \mapsto \eta(k) \neq 0$ is a p-adic analytic function.*

Proof of the main result

Proof of the main result

1. Step II (explicit expressions for Darmon points):

$$\mathrm{P}_{f,\chi} \longleftrightarrow \frac{d}{d^2k} L_p(f_\infty/K, \chi, k)_{|k=2}$$

Proof of the main result

1. Step II (explicit expressions for Darmon points):

$$\mathrm{P}_{f,\chi} \longleftrightarrow \frac{d}{d^2k} L_p(f_\infty/K, \chi, k)_{|k=2}$$

2. Step III (factorization of L-functions)

$$\frac{d}{d^2k} L_p(f_\infty/K, \chi, k)_{|k=2} \longleftrightarrow \frac{d}{d^2k} L_p(f_\infty, \chi_1, k, k/2)_{|k=2}$$

(for a suitable ordering of (χ_1, χ_2)).

Proof of the main result

1. Step II (explicit expressions for Darmon points):

$$\mathrm{P}_{f,\chi} \longleftrightarrow \frac{d}{d^2k} L_p(f_\infty/K, \chi, k)_{|k=2}$$

2. Step III (factorization of L-functions)

$$\frac{d}{d^2k} L_p(f_\infty/K, \chi, k)_{|k=2} \longleftrightarrow \frac{d}{d^2k} L_p(f_\infty, \chi_1, k, k/2)_{|k=2}$$

   (for a suitable ordering of (χ_1, χ_2)).
3. Bertolini and Darmon:

$$\frac{d}{d^2k} L_p(f_\infty, \chi_1, k, k/2)_{|k=2} \longleftrightarrow \text{Heegner divisors}$$