Rational points on elliptic curves over almost totally complex quadratic extensions

Xevi Guitart[1] Víctor Rotger[2] Yu Zhao[3]

[1]Universitat Politècnica de Catalunya

[2]Universitat Politècnica de Catalunya

[3]McGill University

Adam Mickiewicz University, Poznan
9 November 2011

Outline

1. BSD conjecture over totally real number fields and Heegner points
2. Darmon's ATR points and Gartner's generalization
3. ATC points

BSD over totally real fields

- F totally real field, E/F elliptic curve of conductor $\mathcal{N} \subseteq F$.
- We assume that E/F is modular:
  - $L(E/F, s) = L(f, s)$ for some Hilbert modular form f over F.
  - $L(E/F, s)$ extends to an entire function.
  - Let $r_{an}(E/F) = \mathrm{ord}_{s=1} L(E/F, s)$.

Conjecture (BSD)

Let $r(E/F)$ denote the rank of $E(F)$. Then

$$r(E/F) = r_{an}(F).$$

Theorem (Gross-Zagier, Kolyvagin, Zhang)

If $r_{an}(E/F) \leq 1$ and E satisfies the Jacquet–Langlands condition:

- (JL) either $[F\colon \mathbb{Q}]$ is odd or $v_{\mathfrak{p}}(\mathcal{N}) = 1$ for some $\mathfrak{p} \subseteq F$

then

$$r_{an}(E/F) = r(E/F).$$

Heegner points

- Condition (JL) is needed to ensure geometric modularity:

$$\pi_E\colon\ Jac(X) \longrightarrow E, \quad X/F \text{ Shimura curve.}$$

- Heegner points: for a quadratic CM extension K/F they belong to $Jac(X)(K^{ab})$ and can be projected to $E(K^{ab})$
- They are defined over certain ring class fields H/K; if $\mathrm{sign}(E/K) = -1$ they are non-torsion if and only if $L'(E/H,1) \neq 0$.

- When $F = \mathbb{Q}$ they can be explicitly computed:
  - Let f be the newform such that $L(E/\mathbb{Q};s) = L(f;s)$.
  - Let $\omega_f = 2\pi i f(z)dz$, a differential on $X = X_0(N)$.
  - $\Lambda_f = \{\int_\gamma \omega_f \mid \gamma \in H_1(X,\mathbb{Z})\} \subseteq \mathbb{C}$
  - $\mathbb{C}/\Lambda_f \sim E$
  - $K = \mathbb{Q}(\tau)$ then the CM point is

$$J_\tau = \int_{\Delta_\tau} \omega_f \in \mathbb{C}/\Lambda_f \sim E,$$

where $\Delta_\tau = \{\tau \rightarrow \infty\} \in C_1(X,\mathbb{Z})$.

Some questions

1. When $F \neq \mathbb{Q}$, what if (JL) is not satisfied?
2. What about quadratic extensions which are not CM?
   If M/F is a quadratic extension (with $\mathrm{sign}\, L(E/M, s) = -1$):
   is there a way of analytically constructing points on $E(M^{ab})$?

- Up to now, nothing about these questions has been proved beyond the result of Gross–Zagier and Zhang.
- However, a collection of conjectural constructions of points have been proposed by several authors (Darmon, Dasgupta, Greenberg, Rotger, Longo, Vigni, Gartner,...). These points are the so-called Stark–Heegner points (or also Darmon points).
  - They belong to $E(H_v)$, where H is a class field of M and v is a place of H (either archimedean of finite).
  - It is conjectured that they actually belong to $E(H)$ and that they are non-torsion if and only if $L'(E/H, 1) \neq 0$.
- Darmon's ATR points:
  - Defined when M/F is a quadratic Almost Totally Real extension (ATR) (i.e. M has exactly one complex archimedean place).
  - Defined as integrals of the Hilbert modular form attached to E.

Review of Hilbert modular forms

- F totally real number field of degree r and $h^+(F) = 1$.
- $v_1, \ldots, v_r \colon F \hookrightarrow \mathbb{R}$ which give $v_1, \ldots, v_r \colon \mathrm{SL}_2(\mathcal{O}_F) \hookrightarrow SL_2(\mathbb{R})$.
- $\Gamma = \mathrm{SL}_2(\mathcal{O}_F)$ acts discretely on $\mathcal{H}^r$ via $v_1 \times \cdots \times v_r$.
- The analytical variety $X = \mathcal{H}^r/\Gamma$ is the Hilbert modular variety attached to Γ.
- A Hilbert modular form of parallel weight 2 on Γ is:

$$f \colon \mathcal{H}^r \longrightarrow \mathbb{C} \quad \text{homomorphic}$$

  such that $f(z_1, \ldots, z_r)dz_1 \ldots dz_r$ descends to a holomorphic r-form on X.
- It admits a Fourier expansion at ∞:

$$f(z_1, \ldots, z_r) = \sum_{n \in \mathcal{O}_F^+} a_{(n)} e^{2\pi i \left(\frac{n_1}{d_1} z_1 + \cdots + \frac{n_r}{d_r} z_r \right)},$$

  $x_i = v_i(x)$, $n \in \mathcal{O}_F$, $(d) =$ different ideal of F.

Definition of the ATR points

- E/F an elliptic curve of conductor 1.
- M/F quadratic Almost Totally Real extension (ATR): M has exactly one complex archimedean place.
- Let $v_1 : F \hookrightarrow \mathbb{R}$ the one that extends to a complex place of M and think $M \subseteq \mathbb{C}$ via v_1.
- Let $f \in S_2(\Gamma)$ be the Hilbert modular form attached to E.

$$f(z_0, \ldots, z_r) = \sum_{n>>0} a_{(n)} e^{2\pi i \left(\frac{n_0}{d_0} z_0 + \cdots + \frac{n_r}{d_r} z_r\right)},$$

where $a_{\mathfrak{p}} = \mathrm{N}\mathfrak{p} + 1 - \#E(\mathcal{O}_F/\mathfrak{p})$ and

$$\prod_{\mathfrak{p}} (1 - a_{\mathfrak{p}} \mathrm{N}\mathfrak{p}^{-s} + \mathrm{N}\mathfrak{p}^{1-2s}) = \sum_{\mathfrak{n}} a_{\mathfrak{n}} \mathrm{N}\mathfrak{n}^{-s}$$

(observe that $a_{(n)} \in \mathbb{Z}$)

The period lattice and Oda's conjecture

- On $X = \mathcal{H}^r/\Gamma$ we have the holomorphic r-form ω_f^{hol}

$$\omega_f^{hol} = (2\pi i)^r f(z_1, \dots, z_r) dz_1 \cdots dz_r,$$

  but one has to consider a certain non-holomorphic r-form ω_f.

- For instance, if F is quadratic and $u \in \mathcal{O}_F^\times$ with $u_1 > 0,\ u_2 < 0$ then

$$\omega_f = (2\pi i)^2 f(z_1, z_2) dz_1 dz_2 + (2\pi i)^2 f(u_1 z_1, u_2 \bar{z}_2) d(u_1 z_1) d(u_2 \bar{z}_2)$$

- In general ω_f is defined similarly summing over $u \in \mathcal{O}_F^\times/(\mathcal{O}_F^+)^\times$ with $u_1 > 0$.
- Let $\Lambda_f = \left\{ \int_\gamma \omega_f,\ \ \gamma \in H_r(X(\mathbb{C}), \mathbb{Z}) \right\} \subseteq \mathbb{C}$.

Conjecture (Oda)

$\mathbb{C}/\Lambda_f$ is isogenous to E.

Definition of the ATR points

- Let $M = F(\tau)$.
- Darmon defines r-dimensional chain $\Delta_\tau \in C_r(X, \mathbb{Z})$ so that the ATR point is defined as

$$J_\tau = \int_{\Delta_\tau} \omega_f \in \mathbb{C}/\Lambda_f \overset{\iota}{\sim} E$$

- Analogous to Heegner points, and it is explicitly computable.
- Definition of the ATR chain Δ_τ:
  - τ goes to $\tau_1 \in \mathcal{H}_1$ under the extension of v_1, and to $\tau_i, \tau_i' \in \partial\mathcal{H}_i = \mathbb{R}$ under the extensions of v_i for $i > 1$.
  - Let γ_i be the geodesic joining τ_i and τ_i'.
  - Let $\tilde{\Delta}_\tau$ be the image in X of the region $\{\tau_1\} \times \gamma_2 \cdots \times \gamma_r$.
  - $\tilde{\Delta}_\tau$ belongs to $H_{r-1}(X(\mathbb{C}), \mathbb{Z})$.
  - $\tilde{\Delta}_\tau$ actually belongs to $H_{r-1}(X(\mathbb{C}), \mathbb{Z})_{\mathrm{tors}}$.
  - There exists $\Delta_\tau \in C_r(X(\mathbb{C}), \mathbb{Z})$ with $\partial\Delta_\tau = m\tilde{\Delta}_\tau$ for some m.

$$J_\tau = \int_{\Delta_\tau} \omega_f \in \mathbb{C}/\Lambda_f \overset{\iota}{\sim} E$$

- $\mathcal{O}_\tau = \{\gamma \in \mathrm{M}_2(\mathcal{O}_F) \colon v_1(\gamma) \cdot \tau = \tau\}$
- $\mathcal{O}_\tau$ is an order in $\mathcal{O}_K$:

$$v_1(\gamma) \begin{pmatrix} \tau \\ 1 \end{pmatrix} = \lambda_\gamma \begin{pmatrix} \tau \\ 1 \end{pmatrix} \text{ with } \lambda_\gamma \in K.$$

- Let H_τ be the ring class field attached to $\mathcal{O}_\tau$ (in particular $\mathrm{Gal}(H_\tau/K) \simeq \mathrm{Pic}(\mathcal{O}_\tau)$).

Conjecture (Darmon)

The isogeny ι can be chosen such that $\iota(J_\tau)$ belongs $E(H_\tau)$.

- It does not assume (JL): it also applies to elliptic curves which are not expected to be geometrically modular in general.

Gartner's generalization

- Recently J. Gartner has generalized this construction to M/F an arbitrary quadratic extension.
  - This points are defined also with a formula of the type

$$J_\tau = \int_{\Delta_\tau} \omega_f \in \mathbb{C}/\Lambda_f \overset{\iota}{\sim} E$$

    where now f is a modular form on a Shimura variety attached to a quaternion division algebra.
  - This construction has the advantage that it is very general.
  - However, it is hard to compute in any specific example because of the lack of Fourier expansion for the modular forms used.

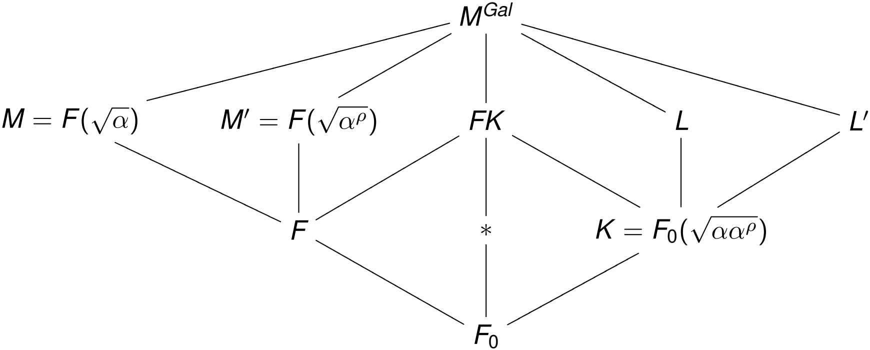
Our Goal

To analytically construct points on $E(M^{ab})$, for a class of fields M which are not ATR. We want the construction to be explicitly computable. In particular, we want to be able to verify the construction in examples.

- We want to define our points in terms of Hilbert modular forms instead of modular forms over quaternion division algebras.
- The price we pay for this is that our construction is not as general as Gartner's. We restrict to the following situation:
  - M/F a quadratic Almost Totally Complex extension (ATC) All archimedean places of M are complex except a pair of real places.
  - There exists $F_0 \subseteq F$ with $[F : F_0] = 2$ such that E is an F_0-curve (i.e. E is F-isogenous to its $\mathrm{Gal}(F/F_0)$-conjugate)

Idea behind the construction

- E/F an F_0-curve and $M = F(\sqrt{\alpha})$ an ATC extension



- Since M is ATC, K is an ATR extension of F_0
- We consider $A = \mathrm{Res}_{F/F_0} E$, an abelian surface defined over F_0
- Extending Darmon's construction we define ATR points on $A(K^{ab})$.
- We then consider the parametrization $A(K^{ab}) \longrightarrow E(FK^{ab})$
- We take as model the case $F_0 = \mathbb{Q}$ (Darmon–Rotger–Zhao).
- $F_0 = \mathbb{Q}$ is classical: K is CM so they really use Heegner points.

- Let $A = \mathrm{Res}_{F/F_0} E$ be the surface obtained by restriction of scalars.

Proposition

If E is a F_0-curve then A/F_0 is a GL_2-type variety: $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_{F_0}(A)$ is isomorphic to a quadratic number field.

- The generalization of the Shimura–Taniyama conjecture for HMF implies that A is modular. That is, there exists a HMF f over F_0 such that
    - Its field of Fourier coefficients $\mathbb{Q}_f$ is isomorphic to $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_{F_0}(A)$
    - $L(A/F_0; s) = L(f; s) \cdot L(^{\sigma} f; s)$
- We also restrict to the case where $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_{F_0}(A)$ is imaginary. Then f is a HMF over F_0 of level N and character ψ where
    - $N \subseteq F_0$ can be explicitly computed from the conductor of E
    - $\psi \colon \mathbb{A}_{F_0}^{\times} \longrightarrow \{\pm 1\}$ is the quadratic character of F/F_0.
- If $[F_0 : \mathbb{Q}] = r$, then f is a r-differential form on the variety $X_{\psi}(N) = \mathcal{H}^r / \Gamma_{\psi}(N)$

$$\Gamma_{\psi}(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_{F_0}) \, : \, N \mid c, \; \psi(a) = 1 \right\}$$

ATR points for abelian varieties

- Let K/F_0 be a quadratic ATR extension (think $K \subseteq \mathbb{C}$ via the unique complex place)
- The differential forms $\omega_f^{hol}, \sigma(\omega_f^{hol})$ generate the f-isotypical component of $H^0(X_\psi(N), \Omega^r)$
- We can consider, as before the non-holomorphic forms $\omega_f, \sigma(\omega_f)$ and the lattice

$$\Lambda_f = \left\{ \left(\int_\gamma \omega_f, \int_\gamma \sigma(\omega_f) \right) \ : \gamma \in H_r(X_\psi(N)_{\mathbb{C}}, \mathbb{Z}) \right\} \subseteq \mathbb{C}^2$$

Oda's conjecture

$\mathbb{C}^2/\Lambda_f$ is isogenous to A

ATR points for abelian varieties

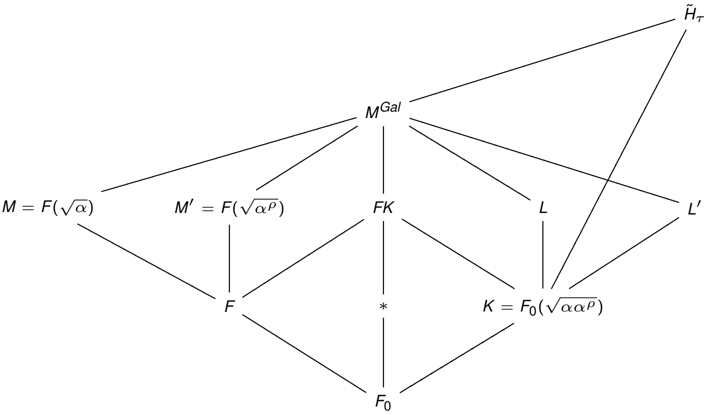
- If $K = F_0(\tau)$, then we can define a point J_τ as

$$J_\tau = \left(\int_{\Delta_\tau} \omega_f, \int_{\Delta_\tau} \sigma(\omega_f) \right) \in \mathbb{C}^2/\Lambda_f \overset{\iota}{\sim} A$$

- Let $\mathcal{O}_\tau = \{\gamma \in M_0(N) \colon v_1(\gamma) \cdot \tau = \tau\} \subseteq \mathcal{O}_K$
- Let H_τ be the ring class field of $\mathcal{O}_\tau$.
- J_τ is not defined over H_τ, but over a biquadratic extension $\tilde{H}_\tau$. (because of the caracter ψ)

Extension of Darmon's ATR Conjecture

The isogeny ι can be chosen such that $\iota(J_\tau)$ belongs to $A(\tilde{H}_\tau)$.



- E/F an F_0-curve and $M = F(\sqrt{\alpha})$ an ATC extension
- We can construct points on $A(\tilde{H}_\tau)$, but are $\tilde{H}_\tau$ and M^{Gal} related?
- Not always, but at least for some τ they are:

Proposition

$d(L/K) = \mathcal{N}c$ with $\mathrm{Nm}_{K/F_0}(\mathcal{N}) = N$ and $c \subseteq F_0$. If $\mathcal{O}_\tau$ is the order of conductor c then $M^{\mathrm{Gal}} \subseteq \tilde{H}_\tau$.

- The projection $A \longrightarrow E$ is given by the Atkin–Lehner involution.
- $(1 + W_N)A \sim_F E$, which means that we can compute this projection using the formula

$$J_\tau^E = \int_{\Delta_\tau} \omega_f + W_N(\omega_f) \in \mathbb{C}/\left\langle \int_\gamma \omega_f + W_N(\omega_f) \right\rangle \overset{\iota}{\sim} E$$

Conjecture

The isogeny ι can be chosen such that $\iota(J_\tau^E) \in E(\tilde{H}_\tau)$. Moreover, the point $\mathrm{Tr}_{\tilde{H}_\tau/M}(\iota(J_\tau))$ is non torsion if and only if $L'(E/M, 1) \neq 0$.

Main Theorem

If we assume the extension of Darmon's conjecture on ATR points then the above conjecture holds true.

Concrete example

- $F_0 = \mathbb{Q}(\sqrt{2})$, $F = \mathbb{Q}(\sqrt{2}, \sqrt{5})$.
- $E\colon y^2 = x^3 - 54(63 + 46\sqrt{2} + 27\sqrt{5} + 18\sqrt{10})x - 116(409 + 287\sqrt{2} + 189\sqrt{5} + 135\sqrt{10})$
- E is an F_0-curve, but it is also a $\mathbb{Q}$-curve (computed by J. Quer).
- The HMF f is base change to F_0 of a modular form $f_{\mathbb{Q}} \in S_2(40, \varepsilon_{10})$
- $M = F(\sqrt{\sqrt{10} + \sqrt{5} + \sqrt{2}})$ is ATC and $E(M) \simeq \mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$.
- We take τ such that $\mathcal{O}_\tau = \mathcal{O}_K$. In this case $\tilde{H}_\tau = M^{\mathrm{Gal}}$
- We computed the ATC point $J_\tau^E = \int_{\Delta_\tau} \omega_f + W_N(\omega_f) \in \mathbb{C}/\Lambda_f$
- We (Magma) computed $z_{nt} \in \mathbb{C}/\Lambda_E$, a non-torsion point in $E(M)$.
- We numerically find the relation

$$7 \cdot \iota(J_\tau^E) - 14 \cdot z_{nt} = 0 \mod \Lambda_E$$

(checked up to 30 digits of precision), which gives evidence that J_τ^E belongs to $E(M)$ and it has infinite order.

Rational points on elliptic curves over almost totally complex quadratic extensions

Xevi Guitart[1] Víctor Rotger[2] Yu Zhao[3]

[1]Universitat Politècnica de Catalunya

[2]Universitat Politècnica de Catalunya

[3]McGill University

Adam Mickiewicz University, Poznan
9 November 2011