Darmon Points: an overview

Explicit Methods for Darmon Points, Benasque

Marc Masdeu

Columbia University

August 25, 2013

(part of joint project with X.Guitart and M.H.Sengun)

Basic Setup

- $E =$ (semistable) elliptic curve defined over a number field F.
- Let $\mathfrak{N} = \mathrm{conductor}(E)$.
- **Assume** (for simplicity) that $\mathfrak{N}$ is square-free.
- Let K/F a quadratic extension.
- **Assume** (for simplicity) that $\mathrm{disc}(K/F)$ is coprime to $\mathfrak{N}$.
- For each prime $\mathfrak{p}$ of K, $a_{\mathfrak{p}}(E) = 1 + |\mathfrak{p}| - \#E(\mathbb{F}_{\mathfrak{p}})$.

$$L(E/K,s) = \prod_{\mathfrak{p}|\mathfrak{N}} \left(1 - a_{|\mathfrak{p}|}|\mathfrak{p}|^{-s}\right)^{-1} \times \prod_{\mathfrak{p}\nmid\mathfrak{N}} \left(1 - a_{|\mathfrak{p}|}|\mathfrak{p}|^{-s} + |\mathfrak{p}|^{1-2s}\right)^{-1}$$

- Modularity conjecture $\implies$
  - Analytic continuation of $L(E/K,s)$ to $\mathbb{C}$.
  - Functional equation relating $s \leftrightarrow 2-s$.

Birch and Swinnerton-Dyer

Conjecture (BSD, rough version)

$$\operatorname{ord}_{s=1} L(E/K, s) = \operatorname{rk}_{\mathbb{Z}} E(K).$$

- So $L(E/K,1) = 0 \implies \exists P_K \in E(K)$ of infinite order.
- The sign of the functional equation of $L(E/K,s)$ should be:

$$\operatorname{sign}(E,K) = (-1)^{\#\{v \mid \mathfrak{N}\infty_F : v \text{ not split in } K\}}.$$

- So $\operatorname{sign}(E,K) = -1$ + BSD " $\implies$ " $E(K)$ has points of infinite order.
- From here on, **assume** that $\operatorname{sign}(E,K) = -1$.

Classical Example: Heegner Points

- $\exists$ when F is totally real and K/F is totally complex (CM extension).
- Suppose $F = \mathbb{Q}$ and $E/\mathbb{Q}$.
- $X_0(N)/\mathbb{Q}$ modular curve with a morphism $\mathrm{Jac}(X_0(N)) \to E$.
- $X_0(N)(\mathbb{C}) = \Gamma_0(N)\backslash\mathfrak{H}$.
- $\exists$ cycles on $\mathrm{Jac}(X_0(N))$ attached to K, giving points on $E(K^{\mathrm{ab}})$.
- $E \rightsquigarrow \omega_E \in H^0(\Gamma_0(N), \Omega^1_{\mathfrak{H}})$.
- For each $\tau \in K \cap \mathfrak{H}$, set:

$$J_\tau = \int_\infty^\tau \omega_E \in \mathbb{C}.$$

  - Well-defined up to $\Lambda_E = \{\int_\gamma \omega_E \mid \gamma \in H_1(X_0(N), \mathbb{Z})\}$.
- Set $P_\tau = \Phi_{\text{Weierstrass}}(J_\tau) \in E(\mathbb{C})$.

Theorem (Shimura)

$P_\tau \in E(H_\tau)$, where H_τ/K is a class field attached to τ.

- Gross-Zagier: $\mathrm{Tr}_{H_\tau/K}(P_\tau) \in E(K)$ nontorsion $\iff r_{\text{an}}(E,K) = 1$.

Darmon's Dream

- Drop hypothesis of K/F being CM.
  - Simplest case: $F = \mathbb{Q}$, K real quadratic.
- However:
  - There are **no** points on $X_0(N)$ attached to K.
  - For F **not totally real**, even the curve $X_0(N)$ is missing.
- Nevertheless, Darmon points exist!
  - (We just can't prove it, so far.)

Goals

In this talk we will:

1. Explain what **Darmon Points** are,
2. Give hints on how we **calculate them**, and

> “The **fun** of the subject seems to me to be in the **examples**.”
>
> B. Gross, in a letter to B. Birch, 1982

3. Show some **fun examples**!

More Notation

$$S(K,\mathfrak{N}\infty_F) = \{v \mid \mathfrak{N}\infty_F : v \text{ not split in } K\}.$$

- Recall that we assume that $\#S(K,\mathfrak{N}\infty_F)$ is **odd.**
- Fix a place $w \in S(K,\mathfrak{N}\infty_F)$.
- Let B be a quaternion algebra over F with

$$\mathrm{Ram}(B) = S(K,\mathfrak{N}\infty_F) \setminus \{w\}.$$

  - Let $\mathfrak{D}$ be the discriminant of B.
- $\mathfrak{m} =$ product of the primes in F diving $\mathfrak{N}$ and which are split in K.
- Let $R_0^{\mathfrak{D}}(\mathfrak{m})$ be an Eichler order of level $\mathfrak{m}$ inside B.
- Fix an embedding

$$\iota_w \colon R_0^{\mathfrak{D}}(\mathfrak{m}) \hookrightarrow M_2(\mathcal{O}_{F,w})$$

- Set $\Gamma = \iota_w\left(R_0^{\mathfrak{D}}(\mathfrak{m})[1/w]_1^\times\right) \subset \mathrm{SL}_2(F_w)$.
- $n := \#\{v \mid \infty_F \colon K \otimes_F F_v \cong F_v \times F_v\}$.
  - K/F is CM $\iff n = 0$.

Non-archimedean History

Definition

$$s = \#S(K, \mathfrak{N}\infty_F) = \{v \mid \mathfrak{N}\infty_F : v \text{ not split in } K\}$$
$$n = \#\infty_F \setminus S(K, \infty_F) = \{v \mid \infty_F : v \text{ split in } K\}$$

- H. Darmon (1999): $F = \mathbb{Q}$, $n = 1$ and $s = 1$.
  - Darmon-Green (2001): $\mathfrak{m}$ trivial, Riemann products.
  - Darmon-Pollack (2002): $\mathfrak{m}$ trivial, overconvergent.
  - Guitart-M. (2012): Allowed for $\mathfrak{m}$ arbitrary.
- M. Trifkovic (2006): F imag. quadratic ($n = 1$) and $s = 1$.
  - Trifkovic (2006): F euclidean, $\mathfrak{m}$ trivial.
  - Guitart-M. (2013): F arbitrary, $\mathfrak{m}$ arbitrary.
- M. Greenberg (2008):F totally real, $n \geq 1$ and $s \geq 1$.
  - Guitart-M. (2013): $n = 1$.

Archimedean History

Definition

$$s = \#S(K, \mathfrak{N}\infty_F) = \{v \mid \mathfrak{N}\infty_F \colon v \text{ not split in } K\}$$
$$n = \#\infty_F \setminus S(K, \infty_F) = \{v \mid \infty_F \colon v \text{ split in } K\}$$

- H. Darmon (2000): F totally real and $s = 1$.
  - Darmon-Logan (2007): F real quadratic and norm-euclidean, $n = 1$, $\mathfrak{m}$ trivial.
  - Guitart-M. (2011): F real quadratic and arbitrary, $n = 1$, $\mathfrak{m}$ trivial.
  - Guitart-M. (2012): F real quadratic and arbitrary, $n = 1$, $\mathfrak{m}$ arbitrary.
- J. Gartner (2010): F totally real, $s \geq 1$.

Integration Pairing

- Let $w \in S(K, \mathfrak{N}\infty_F)$.
- Let $\mathfrak{H}_w =$ the w-adic upper half plane. That is:
  - The Poincaré upper half plane if w is infinite,
  - The $\mathfrak{p}$-adic upper-half plane if $w = \mathfrak{p}$ is finite.
- $\mathfrak{H}_w$ comes equipped with an analytic structure (complex- or rigid-).
- If w is infinite, there is a natural pairing

$$\Omega^1_{\mathfrak{H}_w} \times \operatorname{Div}^0 \mathfrak{H}_w \to \mathbb{C} = K_w,$$

  which sends

$$(\omega, (\tau_2) - (\tau_2)) \mapsto \int_{\tau_1}^{\tau_2} \omega \in \mathbb{C} = K_w.$$

- Analogously, Coleman integration gives a natural pairing

$$\Omega^1_{\mathfrak{H}_w} \times \operatorname{Div}^0 \mathfrak{H}_w \to K_w.$$

Rigid one-forms and measures

The assignment

$$\mu \mapsto \omega = \int_{\mathbb{P}^1(\mathbb{Q}_p)} \frac{dz}{z-t} d\mu(t)$$

induces an isomorphism $\mathrm{Meas}_0(\mathbb{P}^1(\mathbb{Q}_p), \mathbb{Z}) \cong \Omega^1_{\mathfrak{H}_w, \mathbb{Z}}$.

- Inverse given by $\omega \mapsto \left[U \mapsto \mu(U) = \mathrm{res}_{A(U)}\, \omega\right]$.

Theorem (Teitelbaum)

$$\int_{\tau_1}^{\tau_2} \omega = \int_{\mathbb{P}^1(\mathbb{Q}_p)} \log\left(\frac{t-\tau_1}{t-\tau_2}\right) d\mu(t).$$

Proof sketch.

$$\int_{\tau_1}^{\tau_2} \omega = \int_{\tau_1}^{\tau_2} \int_{\mathbb{P}^1(\mathbb{Q}_p)} \frac{dz}{z-t} d\mu(t) = \int_{\mathbb{P}^1(\mathbb{Q}_p)} \log\left(\frac{t-\tau_2}{t-\tau_1}\right) d\mu(t).$$

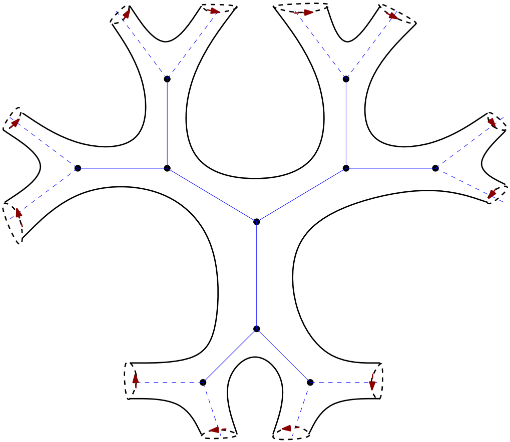
□

The p-adic upper half plane

If the residues of ω are all integers, have a multiplicative refinement:

$$\times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2} \omega = \lim_{\overrightarrow{\mathcal{U}}} \prod_{U \in \mathcal{U}} \left(\frac{t_U - \tau_2}{t_U - \tau_1} \right)^{\mu(U)} \in K_w^\times \quad \text{where } \mu(U) = \operatorname{res}_{A(U)} \omega.$$

- Bruhat-Tits tree of $\mathrm{GL}_2(\mathbb{Q}_p)$ with $p = 2$.
- $\mathfrak{H}_p$ having the Bruhat-Tits as retract.
- Annuli $A(U)$ for $\mathcal{U}$ a covering of size p^{-3}.
- t_U is any point in $U \subset \mathbb{P}^1(\mathbb{Q}_p)$.



(Co)homology

- $S(K, \mathfrak{N}\infty)$ and w determine an S-arithmetic group Γ.
  - e.g. $S(K, \mathfrak{N}\infty) = \{p\}$ gives $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])$.
- Attach to E a unique class (up to sign):

$$[\Phi_E] \in H^n\left(\Gamma, \Omega^1_{\mathfrak{H}_\mathfrak{p},\mathbb{Z}}\right).$$

  - $\Omega^1_{\mathfrak{H}_\mathfrak{p},\mathbb{Z}} =$ rigid-analytic differentials having integral residues.
  - Uses Hecke action and Shapiro's lemma.
- Attach to each embedding $\psi\colon \mathcal{O}_K \hookrightarrow R_0^D(\mathfrak{m})$ a homology class:

$$[\Theta_\psi] \in H_n\left(\Gamma, \mathrm{Div}^0 \mathfrak{H}_p\right).$$

- Integration yields an element

$$J_\psi = \times\!\!\!\!\!\!\int \langle \Phi_E, \Theta_\psi \rangle \in K_w^\times.$$

Uniformization

$$J_\psi = \times\!\!\!\!\!\!\int \langle \Phi_E, \Theta_\psi \rangle \in K_w^\times.$$

- J_ψ is well-defined up to a lattice $L \subset K_v^\times$.
- It is conjectured (and in some cases proven) that this lattice is commensurable to the (Weierstrass or Tate) lattice $\langle q_E \rangle$ of E.
  - $\exists$ isogeny $\beta\colon K_w^\times/L \to K_w^\times/q_E^{\mathbb{Z}}$.
- When w is **infinite**, there is a complex-analytic map

$$\Phi = \Phi_{\text{Weierstrass}}\colon \mathbb{C} \to E(\mathbb{C}).$$

- When w is **finite**, Tate uniformization provides a rigid-analytic map

$$\Phi = \Phi_{\text{Tate}}\colon K_w^\times \to E(K_w).$$

Conjecture

- Define $P_\psi = \Phi(\beta(J_\psi)) \in E(K_w)$.

Conjecture (Darmon, ...)

The local point P_ψ belongs to $E(K^{ab})$.
Moreover P_ψ is torsion if and only if $L'(E/K,1) = 0$.

- The conjecture predicts the exact number field over which P_ψ is defined.
- It also includes a Shimura reciprocity law, mimicking the behavior of Heegner points.

A special case

- We will restrict to the **non-archimedean** setting, $w = \mathfrak{p}$.
- Suppose also that $F_{\mathfrak{p}} \cong \mathbb{Q}_p$, i.e. $\mathfrak{p}$ is split in F.
  - But recall the running assumption: $\mathfrak{p}$ is inert in K.
- Suppose also that $n = 1$. This includes the cases:
  1. F totally real and K/F **almost totally complex.**
     - ⋆ e.g. $F = \mathbb{Q}$ and K real quadratic. (Darmon)
  2. F **almost totally real** and K/F totally imaginary.
     - ⋆ e.g. F quadratic imaginary. (Trifkovic)

Cohomology

- Jacquet-Langlands correspondence gives:

$$\dim_{\mathbb{Q}}\left(H^1\left(\Gamma_0^D(\mathfrak{pm}),\mathbb{Q}\right)_{\mathfrak{p}\text{-new}}^{\lambda_E}\right)=1$$

- Let $\varphi_E \in \left(H^1(\Gamma_0^D(\mathfrak{pm}),\mathbb{Z})_{\mathfrak{p}\text{-new}}\right)^{\lambda_E}$
  - Well-defined up to sign.
- Shapiro's isomorphism gives $\Phi'_E \in H^1(\Gamma, \operatorname{coind}_{\Gamma_0^D(\mathfrak{pm})}^{\Gamma}\mathbb{Z})$.
- Choose an "harmonic" system of representatives, to pull back to

$$\Phi_E \in H^1(\Gamma, \mathrm{HC}(\mathbb{Z})),$$

  - Here $\mathrm{HC}(\mathbb{Z}) = \ker\left(\operatorname{coind}_{\Gamma_0^D(\mathfrak{pm})}^{\Gamma}\mathbb{Z} \to \left(\operatorname{coind}_{\Gamma_0^D(\mathfrak{m})}^{\Gamma}\mathbb{Z}\right)^2\right)$.
- Finally, use isomorphisms

$$\mathrm{HC}(\mathbb{Z}) \cong \mathrm{Meas}_0(\mathbb{P}^1(\mathbb{Q}_p),\mathbb{Z}) \cong \Omega^1_{\mathfrak{H}_p,\mathbb{Z}}.$$

- Obtain $\Phi_E \in H^1(\Gamma, \Omega^1_{\mathfrak{H}_p,\mathbb{Z}})$.

Homology

- Let $\psi\colon \mathcal{O} \hookrightarrow R_0(\mathfrak{m})$ be an embedding of an order $\mathcal{O}$ of K.
  - ...which is optimal: $\psi(\mathcal{O}) = R_0(\mathfrak{m}) \cap \psi(K)$.
- Consider the group

$$\mathcal{O}_1^\times = \{u \in \mathcal{O}^\times \colon \operatorname{Nm}_{K/F}(u) = 1\}.$$

  - $\operatorname{rank}(\mathcal{O}_1^\times) = \operatorname{rank}(\mathcal{O}^\times) - \operatorname{rank}(\mathcal{O}_F) = 1$.
- Let $u \in \mathcal{O}_1^\times$ be a non-torsion unit, and let $\gamma_\psi = \psi(u)$.
- u acts on $\mathfrak{H}_p$ via $K^\times \hookrightarrow B_1^\times \hookrightarrow B_{1,\mathfrak{p}}^\times \cong \mathrm{SL}_2(\mathbb{Q}_p)$ with fixed points $\tau_\psi, \overline{\tau}_\psi$.
- Consider $\tilde{\Theta}_\psi = [\gamma_\psi \otimes \tau_\psi]$ in $H_1(\Gamma, \operatorname{Div}\mathfrak{H}_p)$.
- Have the exact sequence

$$\begin{array}{ccccc} H_1(\Gamma, \operatorname{Div}^0\mathfrak{H}_p) & \longrightarrow & H_1(\Gamma, \operatorname{Div}\mathfrak{H}_p) & \xrightarrow{\deg} & H_1(\Gamma, \mathbb{Z}) \\ \Theta_\psi & \overset{?}{\mapsto} & \tilde{\Theta}_\psi & \longmapsto & \deg\tilde{\Theta}_\psi \end{array}$$

- **Lemma:** $\deg\tilde{\Theta}_\psi$ is torsion.
  - Can pull back (a multiple of) $\tilde{\Theta}_\psi$ to $\Theta_\psi \in H_1(\Gamma, \operatorname{Div}^0\mathfrak{H}_p)$.

Overconvergent Integration (I)

- $\mathbb{D} = \{$ locally-analytic $\mathbb{Z}_p$-valued distributions on $\mathbb{Z}_p$ $\}$.
- $\Sigma_0(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_p) \mid p \mid c, d \in \mathbb{Z}_p^\times, ad - bc \neq 0 \right\}$.
- $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \in \Sigma_0(p)$ acts on $\nu \in \mathbb{D}$ by:

$$\int_{\mathbb{Z}_p} h(t) d(\gamma\nu) = \int_{\mathbb{Z}_p} h\left(\frac{at+b}{ct+d}\right) d\nu.$$

- Can define U_p operator on $H^1(\Gamma_0^D(\mathfrak{p}\mathfrak{m}), \mathbb{D})$.

Theorem (Pollack-Pollack)

Let $\varphi \in H^1(\Gamma_0^{\mathfrak{D}}(\mathfrak{p}\mathfrak{m}), \mathbb{Z}_p)$ be such that $U_p\varphi = \alpha\varphi$ with $\alpha \in \mathbb{Z}_p^\times$. Then there is a unique lift $\Phi \in H^1(\Gamma_0^{\mathfrak{D}}(\mathfrak{p}\mathfrak{m}), \mathbb{D})$ such that $U_p\Phi = \alpha\Phi$.

Overconvergent Integration (II)

Theorem (Pollack-Pollack)

Let $\varphi \in H^1(\Gamma_0^{\mathfrak{D}}(\mathfrak{p}\mathfrak{m}), \mathbb{Z}_p)$ be such that $U_p\varphi = \alpha\varphi$ with $\alpha \in \mathbb{Z}_p^\times$. Then there is a unique lift $\Phi \in H^1(\Gamma_0^{\mathfrak{D}}(\mathfrak{p}\mathfrak{m}), \mathbb{D})$ such that $U_p\Phi = \alpha\Phi$.

- Recall we have $\varphi_E \in H^1(\Gamma, \mathrm{Meas}_0(\mathbb{P}^1(\mathbb{Q}_p), ZZ))$.
- The cocycle Φ' given by:

$$(\Phi'_\gamma)(h(t)) = \int_{\mathbb{Z}_p} h(t) d\varphi_{E,\gamma}(t), \quad \gamma \in \Gamma_0^D(pM).$$

  is a lift of φ_E which is also an U_p-eigenclass.
- So $\Phi' = \Phi$, and obtain a way to integrate.
- We can extend this in order to:
  1. Evaluate at $\gamma \in \Gamma$ (not just $\Gamma_0^{\mathfrak{D}}(\mathfrak{p}\mathfrak{m})$).
  2. Integrate over all of $\mathbb{P}^1(\mathbb{Q}_p)$ (not just $\mathbb{Z}_p$).
  3. Compute **multiplicative** integrals.

Implementation

- We have written SAGE code to compute non-archimedean Darmon points when $n = 1$.
- Depend on:
  1. Overconvergent method for $F = \mathbb{Q}$ and $\mathfrak{D} = 1$ (R.Pollack).
  2. Finding a presentation for units of orders in B (J.Voight, A.Page).
     - ★ Currently depends on MAGMA.
- Overconvergent methods (adapted to $\mathfrak{D} \neq 1$).
  - Efficient (polynomial time) integration algorithm.
  - Apart from checking the conjecture, can use the method to actually **finding** the points.
- Need more geometric ideas to treat $n > 1$.

Examples

Please show them the **examples** !

$p = 5$, Curve 15A1

$$E : \quad y^2 + xy + y = x^3 + x^2 - 10x - 10$$

d_K	h	P
13	1	$(-\sqrt{13}+1, 2\sqrt{13}-4)$
28	1	$(-15\sqrt{7}+43, 150\sqrt{7}-402)$
37	1	$(-\frac{5}{9}\sqrt{37}+\frac{5}{9}, \frac{25}{27}\sqrt{37}-\frac{70}{27})$
73	1	$(-\frac{17}{32}\sqrt{73}+\frac{77}{32}, \frac{187}{128}\sqrt{73}-\frac{1199}{128})$
88	1	$(-\frac{17}{9}, \frac{14}{27}\sqrt{22}+\frac{4}{9})$
97	1	$(-\frac{25}{121}\sqrt{97}+\frac{123}{121}, \frac{375}{2662}\sqrt{97}-\frac{4749}{2662})$
133	1	$(\frac{103}{9}, \frac{92}{27}\sqrt{133}-\frac{56}{9})$
172	1	$(-\frac{1923}{1681}, \frac{11781}{68921}\sqrt{43}+\frac{121}{1681})$
193	1	$(\frac{1885}{288}\sqrt{193}+\frac{25885}{288}, \frac{292175}{3456}\sqrt{193}+\frac{4056815}{3456})$

$p = 3$, Curve 21A1

$$E: \quad y^2 + xy = x^3 - 4x - 1$$

d_K	h	P
8	1	$\left(-9\sqrt{2}+11, 45\sqrt{2}-64\right)$
29	1	$\left(-\frac{9}{25}\sqrt{29}+\frac{32}{25}, \frac{63}{125}\sqrt{29}-\frac{449}{125}\right)$
44	1	$\left(-\frac{9}{49}\sqrt{11}-\frac{52}{49}, \frac{54}{343}\sqrt{11}+\frac{557}{343}\right)$
53	1	$\left(-\frac{37}{169}\sqrt{53}+\frac{184}{169}, \frac{555}{2197}\sqrt{53}-\frac{5633}{2197}\right)$
92	1	$\left(\frac{533}{46}, \frac{17325}{2116}\sqrt{23}-\frac{533}{92}\right)$
137	1	$\left(-\frac{1959}{11449}\sqrt{137}+\frac{242}{11449}, \frac{295809}{2450086}\sqrt{137}-\frac{162481}{2450086}\right)$
149	1	$\left(-\frac{261}{2809}\sqrt{149}+\frac{2468}{2809}, \frac{8091}{148877}\sqrt{149}-\frac{101789}{148877}\right)$
197	1	$\left(-\frac{79135143}{209961032}\sqrt{197}+\frac{977125081}{209961032}, \frac{1439547386313}{1075630366936}\sqrt{197}-\frac{9297639417941}{537815183468}\right)$

D	h	$h_D(x)$
65	2	$x^2+\left(\frac{61851}{6241}\sqrt{65}-\frac{491926}{6241}\right)x-\frac{403782}{6241}\sqrt{65}+\frac{3256777}{6241}$

$p = 11$, Curve 33A1

$$E: \quad y^2 + xy = x^3 + x^2 - 11x$$

d_K	h	P
13	1	$\left(-\frac{1}{2}\sqrt{13}+\frac{3}{2}, \frac{1}{2}\sqrt{13}-\frac{7}{2}\right)$
28	1	$\left(\frac{22}{7}, \frac{55}{49}\sqrt{7}-\frac{11}{7}\right)$
61	1	$\left(-\frac{1}{2}\sqrt{61}+\frac{5}{2}, \sqrt{61}-11\right)$
73	1	$\left(-\frac{53339}{49928}\sqrt{73}+\frac{324687}{49928}, \frac{31203315}{7888624}\sqrt{73}-\frac{290996167}{7888624}\right)$
76	1	$\left(-2, \sqrt{19}+1\right)$
109	1	$\left(-\frac{143}{2}\sqrt{109}+\frac{1485}{2}, \frac{5577}{2}\sqrt{109}-\frac{58223}{2}\right)$
172	1	$\left(-\frac{51842}{21025}, \frac{2065147}{3048625}\sqrt{43}+\frac{25921}{21025}\right)$
184	1	$\left(\frac{59488}{21609}, \frac{109252}{3176523}\sqrt{46}-\frac{29744}{21609}\right)$
193	1	$\left(\frac{94663533349261}{678412148664608}\sqrt{193}+\frac{1048806825770477}{678412148664608}, \frac{14777895792093129931 7}{1249468831181355374118 4}\sqrt{193}+\frac{30862934493092416035541}{12494688311813553741184}\right)$

D	h	$h_D(x)$
40	2	$x^2+\left(\frac{2849}{1681}\sqrt{10}-\frac{6347}{1681}\right)x-\frac{5082}{1681}\sqrt{10}+\frac{16819}{1681}$
85	2	$x^2+\left(\frac{119}{361}\sqrt{85}-\frac{1022}{361}\right)x-\frac{168}{361}\sqrt{85}+\frac{1549}{361}$
145	4	$x^4+\left(\frac{169016003453}{83168215321}\sqrt{145}-\frac{1621540207320}{83168215321}\right)x^3 + \left(-\frac{1534717557538}{83168215321}\sqrt{145}+\frac{18972823294799}{83168215321}\right)x^2+\left(\frac{5533405190489}{83168215321}\sqrt{145}-\frac{66553066916820}{83168215321}\right)x + -\frac{6414913389456}{83168215321}\sqrt{145}+\frac{77248348177561}{83168215321}$

$p = 13$, Curve 78A1

- $78 = 2 \cdot 3 \cdot 13$, we take $p = 13$ and $D = 6$.

$$E: \quad y^2 + xy = x^3 + x^2 - 19x + 685$$

d_K	P
5	$1 \cdot 48 \cdot \left(-2, 12\sqrt{5} + 1\right)$
149	$1 \cdot 48 \cdot \left(1558, -5040\sqrt{149} - 779\right)$
197	$1 \cdot 48 \cdot \left(\frac{310}{49}, \frac{720}{343}\sqrt{197} - \frac{155}{49}\right)$
293	$1 \cdot 48 \cdot \left(40, -15\sqrt{293} - 20\right)$
317	$1 \cdot 48 \cdot \left(382, -420\sqrt{317} - 191\right)$
437	$1 \cdot 48 \cdot \left(\frac{986}{23}, \frac{7200}{529}\sqrt{437} - \frac{493}{23}\right)$
461	$1 \cdot 48 \cdot \left(232, -165\sqrt{461} - 116\right)$
509	$1 \cdot 48 \cdot \left(-\frac{2}{289}, -\frac{5700}{4913}\sqrt{509} + \frac{1}{289}\right)$
557	$1 \cdot 48 \cdot \left(\frac{75622}{121}, \frac{882000}{1331}\sqrt{557} - \frac{37811}{121}\right)$

$p = 11$, Curve 110A1

- $110 = 2 \cdot 5 \cdot 11$, we take $p = 11$ and $D = 10$.

$$E: \quad y^2 + xy + y = x^3 + x^2 + 10x - 45.$$

d_K	P
13	$2 \cdot 30 \cdot \left(\frac{1103}{81} - \frac{250}{81}\sqrt{13}, -\frac{52403}{729} + \frac{13750}{729}\sqrt{13}\right)$
173	$2 \cdot 30 \cdot \left(\frac{1532132}{9025}, -\frac{1541157}{18050} - \frac{289481483}{1714750}\sqrt{173}\right)$
237	$2 \cdot 30 \cdot \left(\frac{190966548837842073867}{4016648659658412649} - \frac{10722443619184119320}{4016648659658412649}\sqrt{237},\right.$
	$\left.-\frac{3505590193011437142853233857149}{8049997913829845411423756107} + \frac{235448460130564520991320372200}{8049997913829845411423756107}\sqrt{237}\right)$
277	$2 \cdot 30 \left(\frac{46317716623881}{12553387541776}, -\frac{58871104165657}{25106775083552} - \frac{20912769335239055243}{44477606117965542976}\sqrt{277}\right)$
293	$2 \cdot 30 \cdot \left(\frac{7088486530742}{2971834657801}, -\frac{10060321188543}{5943669315602} - \frac{591566427769149607}{10246297476835603402}\sqrt{293}\right)$
373	$2 \cdot 30 \cdot \left(\frac{298780258398}{62087183929}, -\frac{360867442327}{124174367858} - \frac{19368919551426449}{30940899762281434}\sqrt{373}\right)$

$p = 5$, Curve 110A1

- $110 = 2 \cdot 5 \cdot 11$, we take $p = 5$ and $D = 22$.

$$E: \quad y^2 + xy + y = x^3 + x^2 + 10x - 45.$$

d_K	P
13	$2 \cdot 12 \cdot \left(4, \frac{5}{2}\sqrt{13} - \frac{5}{2}\right)$
173	$2 \cdot 12 \cdot \left(\frac{1532132}{9025}, -\frac{289481483}{1714750}\sqrt{173} - \frac{1541157}{18050}\right)$
237	$2 \cdot 12 \cdot \left(\frac{5585462179}{1193768112}, -\frac{53751973226309}{71439858894528}\sqrt{237} - \frac{6779230291}{2387536224}\right)$
277	—
293	$2 \cdot 12 \cdot \left(\frac{7088486530742}{2971834657801}, -\frac{591566427769149607}{10246297476835603402}\sqrt{293} - \frac{10060321188543}{5943669315602}\right)$
373	$2 \cdot 12 \cdot \left(\frac{298780258398}{62087183929}, \frac{193689195514264449}{309408997622814 34}\sqrt{373} - \frac{360867442327}{124174367858}\right)$

$p = 19$, Curve 114A1

- $114 = 2 \cdot 3 \cdot 19$, we take $p = 19$ and $D = 6$.

$$E: \quad y^2 + xy = x^3 - 8x.$$

d_K	P
29	$1 \cdot 72 \cdot \left(-\frac{6}{25}\sqrt{29} - \frac{38}{25}, -\frac{18}{125}\sqrt{29} + \frac{86}{125}\right)$
53	$1 \cdot 72 \cdot \left(-\frac{1}{9}, \frac{7}{54}\sqrt{53} + \frac{1}{18}\right)$
173	$1 \cdot 72 \cdot \left(-\frac{3481}{13689}, \frac{347333}{3203226}\sqrt{173} + \frac{3481}{27378}\right)$
269	$1 \cdot 72 \cdot \left(\frac{1647149414400}{23887470525361}\sqrt{269} - \frac{43248475603556}{23887470525361}, \frac{2359447648611379200}{116749558330761905641}\sqrt{269} + \frac{26817749741702430756 4}{116749558330761905641}\right)$
293	$1 \cdot 72 \cdot \left(\frac{21289143620808}{4902225525409}, \frac{4567039561444642548}{1085400282913149067 3}\sqrt{293} - \frac{10644571810404}{4902225525409}\right)$
317	$1 \cdot 72 \cdot \left(-\frac{25}{9}, -\frac{5}{54}\sqrt{317} + \frac{25}{18}\right)$
341	$1 \cdot 72 \cdot \left(\frac{3449809443179}{499880896975}, \frac{3600393040902501011}{3935597293546963250}\sqrt{341} - \frac{3449809443179}{999761793950}\right)$
413	$1 \cdot 72 \cdot \left(\frac{59}{7}, \frac{113}{98}\sqrt{413} - \frac{59}{14}\right)$

Thank you !

Bibliography and slides at:

`http://www.math.columbia.edu/~masdeu/`

Bibliography

Henri Darmon and Adam Logan, *Periods of Hilbert modular forms and rational points on elliptic curves*, Int. Math. Res. Not. (2003), no. 40, 2153–2180.

Henri Darmon and Peter Green.
Elliptic curves and class fields of real quadratic fields: Algorithms and evidence.
Exp. Math., 11, No. 1, 37-55, 2002.

Henri Darmon and Robert Pollack.
Efficient calculation of Stark-Heegner points via overconvergent modular symbols.
Israel J. Math., 153:319–354, 2006.

Jérôme Gärtner, *Darmon's points and quaternionic Shimura varieties*
arXiv.org, 1104.3338, 2011.

Xavier Guitart and Marc Masdeu.
Elementary matrix Decomposition and the computation of Darmon points with higher conductor.
arXiv.org, 1209.4614, 2012.

Xavier Guitart and Marc Masdeu.
Computation of ATR Darmon points on non-geometrically modular elliptic curves.
Experimental Mathematics, 2012.

Xavier Guitart and Marc Masdeu.
Computation of quaternionic p-adic Darmon points.
arXiv.org, ?, 2013.

Matthew Greenberg.
Stark-Heegner points and the cohomology of quaternionic Shimura varieties.
Duke Math. J., 147(3):541–575, 2009.

David Pollack and Robert Pollack.
A construction of rigid analytic cohomology classes for congruence subgroups of $\mathrm{SL}_3(\mathbb{Z})$.
Canad. J. Math., 61(3):674–690, 2009.