Darmon points: algorithms and numerical evidence

Xevi Guitart

Max-Planck-Institute for Mathematics

Number Theory Lunch Seminar,
14 November 2012

The Birch and Swinnerton-Dyer conjecture

F totally real field, E/F elliptic curve of conductor $\mathcal{N} \subseteq F$.

Modularity conjecture

There exists a Hilbert modular form f over F with $L(E/F, s) = L(f, s)$

- Modularity of E is known in many cases: we will just assume it.
  - $L(E/F, s)$ 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

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

Theorem (Gross–Zagier, Kolyvagin, Zhang)

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

- (JL) either $[F : \mathbb{Q}]$ is odd or $\mathcal{N}$ is not a square

then BSD holds true: $r_{an}(E/F) = r(E/F)$.

Key ingredient: Heegner points

- Points coming from Shimura curve parametrizations.
- Condition (JL) is needed to ensure geometric modularity

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

- Shimura curves are endowed with a plentiful of algebraic points: the so-called CM points
  - They are associated to elements in quadratic CM extensions K/F
  - $\tau \in K \setminus F \rightsquigarrow$ CM point $J_\tau \in \mathrm{Jac}(X)(K^{\mathrm{ab}})$
- Heegner points: CM points satisfying certain additional conditions (e.g., that sign $L(E/K,s) = 1$)
- By means of π_E one obtains Heegner points on E

$$P_\tau \in E(K^{\mathrm{ab}})$$

- The arithmetic of P_τ is related to $L(E/K,s)$ thanks to formulas of Gross–Zagier and Zhang

Particular case: $F = \mathbb{Q}$ and $X = X_0(N)$

- E defined over $\mathbb{Q}$ of conductor N, and K quadratic imaginary field
- $\pi_E \colon X_0(N) = \Gamma_0(N) \setminus \mathcal{H}^* \longrightarrow E$
- Let $f \in S_2(\Gamma_0(N))$ be the newform such that $L(E/\mathbb{Q}; s) = L(f; s)$
- $\omega_f = 2\pi i f(z) dz$ a differential on $X_0(N)$
- For $\tau \in K \cap \mathcal{H}$ let $J_\tau = \int_\infty^\tau \omega_f \in \mathbb{C}/\Lambda_f \sim \mathbb{C}/\Lambda_E$

$$\Lambda_f = \{ \int_\gamma \omega_f \mid \gamma \in H_1(X_0(N), \mathbb{Z}) \}$$

- $P_\tau = \Phi_{\mathrm{W}}(J_\tau) \in E(\mathbb{C}),$ where $\Phi_{\mathrm{W}} : \mathbb{C}/\Lambda \rightarrow E(\mathbb{C})$
- This is computable: $f(z) = \sum a_n e^{2\pi i n z}$ with $a_p = p + 1 - \#E(F_p)$
  - it gives a good algorithm for doing explicit calculations
- Structure of the construction:
  - $E \rightsquigarrow$ differential form ω_f
  - $\tau \rightsquigarrow$ chain $\Delta_\tau = \{\tau \rightarrow \infty\}$

  $\Big\} \longrightarrow J_\tau = \int_{\Delta_\tau} \omega_f$
- This is a local construction
  - In principle $P_\tau \in E(\mathbb{C})$ (but in fact $P_\tau \in E(K^{\mathrm{ab}})$)

A natural question

- K/F arbitrary quadratic extension (not necessarily CM) with sign $L(E/K, s) = -1$

Question

Is there an analytical construction of points in $E(K^{\mathrm{ab}})$?

- To the best of my knowledge, nothing about this question 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, Pollack, Rotger, Longo, Vigni, Gartner, Trifkovic...)
  - Construction of local points in $E(K_v)$, where v is a place of K ($K_v = \mathbb{C}$ or a p-adic field, depending on v)
  - They are conjectured to be global points, namely to lie in $E(K^{\mathrm{ab}})$
  - The constructions are different, depending on K/F and v.
- All these constructions are known under the generic name of Darmon points (a.k.a. Stark–Heegner points).

Numerical calculation of Darmon points

- The constructions resemble some formal similarities, and are inspired by, the Heegner point construction:
  - $E \rightsquigarrow \omega_f$
  - $\tau \in K \rightsquigarrow \Delta_\tau$

  $$\left.\begin{array}{l} E \rightsquigarrow \omega_f \\ \tau \in K \rightsquigarrow \Delta_\tau \end{array}\right\} \longrightarrow P_\tau = \int_{\Delta_\tau} \omega_f$$
- But no "moduli interpretation" for this points is known: they do not correspond to projecting points from any Shimura variety.
  - They are available even when E is not geometrically modular
- Evidence for the rationality: mainly from numerical computations
  - The computed points are really close to global points!
  - Actually, in some cases they turn out to be amazingly efficient algorithms for computing rational points
- But the computational and algorithmic picture is still not complete
  - For some instances of Darmon points, there are no algorithms at all
  - For the instances in which there are, sometimes the algorithm is still very restrictive and applies under some additional hypothesis
- In this talk: explain two instances of Darmon points
  - There was an algorithm, but quite restrictive
  - Provide some extensions that lead to a more general algorithm (joint work with Marc Masdeu)

Outline

ATR points (in a simplified setting)

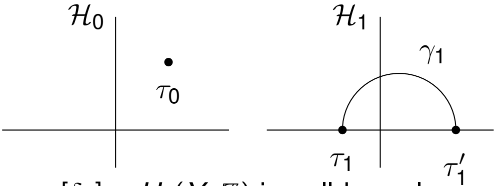
- F real quadratic with $h^+(F) = 1$
- E/F elliptic curve of conductor (1)
- K/F an almost totally real (ATR) quadratic extension (K has 1 complex place and 2 real places)
- This is a situation already presents interesting difficulties
  - E does not satisfy (JL), so it is not geometrically modular in general (excepcion: if f_E is a base change, then it is geom. modular)
  - The method of Heegner points is not available for these curves
  - The simplest example is this curve over $\mathbb{Q}(\sqrt{509})$:

$$E_{509}\colon y^2 - xy - \omega y = x^3 + (2+2\omega)x^2 + (162+3\omega)x + (71+34\omega),\ \omega = \frac{1+\sqrt{509}}{2}$$

- The differential form attached to E:
  - Modularity: f Hilbert modular form$/F$ with $L(E/F, s) = L(f, s)$
  - $f\colon \mathcal{H}\times\mathcal{H}\to\mathbb{C}$ invariance property w.r.t. the action of $\mathrm{SL}_2(\mathcal{O}_F)$
  - $f(z_0, z_1)dz_0dz_1$ descends to a holomorphic differential on $Y = \mathrm{SL}_2(\mathcal{O}_F)\backslash(\mathcal{H}\times\mathcal{H})$, the (open) principal Hilbert modular surface
  - We let $\omega_f = f(z_0, z_1)dz_0dz_1 - f(\epsilon_0 z_0, \epsilon_1\overline{z}_1)dz_0d\overline{z}_1$ (ϵ = fundamental unit of F)

ATR points II

- The ATR cycle attached to $\tau \in K \setminus F$:



$$\delta_\tau = \{\tau_0\} \times \gamma_1 \subseteq \mathcal{H} \times \mathcal{H}$$

- $[\delta_\tau] \in H_1(Y, \mathbb{Z})$ is null-homologous: $\delta_\tau = \partial \Delta_\tau$ with $\Delta_\tau \in C_2(Y, \mathbb{Z})$.
- ATR point: $J_\tau = \int_{\Delta_\tau} \omega_f \in \mathbb{C}/\Lambda_f$
- Oda's conjecture: $\mathbb{C}/\Lambda_f \overset{\iota}{\sim} \mathbb{C}/\Lambda_E$

Conjecture (Darmon)

The point $\Phi_{\mathrm{W}}(\iota(J_\tau)) \in E(\mathbb{C})$ belongs to $E(K^{\mathrm{ab}})$

- Question: how to compute $\int_{\Delta_\tau} \omega_f$ in practice?
  - ω_f is a 2-form: we can compute are double integrals $\int_x^y \int_z^t \omega_f$
  - It seems that the ATR cycle only gives 3-limits: $\int^{\tau_0} \int_{\tau_1}^{\tau_1'} \omega_f$

Darmon–Logan algorithm

- Idea: to give a precise meaning to semi-indefinite integrals
- There is a unique map

$$\begin{array}{ccc} \mathcal{H} \times \mathbb{P}^1(F) \times \mathbb{P}^1(F) & \longrightarrow & \mathbb{C}/\Lambda_f \\ (z,x,y) & \longmapsto & \int^z \int_x^y \omega_f \end{array}$$

  satisfying certain natural conditions conditions

  (i) $\int^{\gamma z} \int_{\gamma x}^{\gamma y} \omega_f = \int^z \int_x^y \omega_f$ for all $\gamma \in \mathrm{SL}_2(\mathcal{O}_F)$,

  (ii) $\int^z \int_x^y \omega_f + \int^z \int_y^t \omega_f = \int^z \int_x^t \omega_f$,

  (iii) $\int^{z_2} \int_x^y \omega_f - \int^{z_1} \int_x^y \omega_f = \int_{z_1}^{z_2} \int_x^y \omega_f$.

- Then $\displaystyle\int_{\Delta_\tau} \omega_f = \int^{\tau_0} \int_{\infty}^{\gamma_\tau \infty} \omega_f$, where $\langle \gamma_\tau \rangle = \mathrm{Stab}_{\mathrm{SL}_2(\mathcal{O}_F)}(\tau_0)$
- Darmon–Logan algorithm: use $(i), (ii), (iii)$ to transform semi-indefinite integrals into sums of double integrals $\int_x^y \int_z^t \omega_f$, which can be computed summing the Fourier series
  - Restriction: algorithm needs to assume F is norm-euclidean
  - only 16 real quadratic fields are euclidean ($\mathbb{Q}(\sqrt{73})$ the last one)

Extending Darmon–Logan: continued fractions

- A key step for transforming semi-indefinite integrals into double integrals is a sort of “Manin Trick”.
- Involves computing the continued fraction expansion of $c \in F$:

$$c = q_1 + \cfrac{1}{q_2 + \frac{1}{q_3 + \cdots + \frac{1}{q_n}}}, \quad q_1, \ldots, q_n \in \mathcal{O}_F$$

- If F is norm-euclidean: euclidean algorithm computes the q_i
- Cooke: all fields $\mathbb{Q}(\sqrt{d})$ with class number 1 are conjectured to be 2-stage euclidean: for all $a, b \in \mathcal{O}_F$ there exist q_1, q_2, r_1, r_2

$$\begin{aligned} a &= bq_1 + r_1; \\ b &= q_2 r_1 + r_2; \ \mathrm{Nm}_{F/\mathbb{Q}}(r_2) < \mathrm{Nm}_{F/\mathbb{Q}}(b) \end{aligned}$$

Teorema (G.-Masdeu)

There exists an algorithm for verifying if $\mathbb{Q}(\sqrt{d})$ is 2-stage euclidean, and if it is so, for computing continued fractions of elements in F.
All $\mathbb{Q}(\sqrt{d})$ with class number 1 and $d \leq 8000$ are 2-stage euclidean.

Experimental evidence of the ATR conjecture

- We used this method to compute an ATR point on the non-geometrically modular curve

$$E_{509}\colon\ y^2 - xy - \omega y = x^3 + (2+2\omega)x^2 + (162+3\omega)x + (71+34\omega),\ \omega = \frac{1+\sqrt{509}}{2}$$

- We computed a point over the ATR field given by
  - $K = F(\sqrt{\alpha})$, $\alpha = 9144\omega + 98577$.
  - the ATR point coincides with a global point of infinite order (up to the computed numerical accuracy)
  - $P_\tau \simeq 4 \cdot (\omega + 17, \frac{\sqrt{\alpha}+\sqrt{509}+18}{2}) \in E(K)$
- This gives experimental evidence supporting Darmon's conjecture
  - but this is not an efficient method for computing rational points
  - it took about 2 days in the 32-processor machine of the MPIM to compute it to 12-digits of accuracy!
- *p*-adic methods turn out to be much more efficient!

p-adic Darmon points

- $E/\mathbb{Q}$ elliptic curve of conductor $N = pM$, with $p \nmid M$.
- $K/\mathbb{Q}$ real quadratic field in which
  - p is inert and all primes dividing M are split
- Recall the modular parametrization $\Gamma_0(N) \setminus \mathcal{H} \longrightarrow E(\mathbb{C})$
- Naive obstruction to Heegner points: $K \cap \mathcal{H} = \emptyset$
- Idea: replace $\mathcal{H}$ by the p-adic upper half plane $\mathcal{H}_p := \mathbb{C}_p \setminus \mathbb{Q}_p$
  - Here $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}_p}}$ (p-adic analogous to $\mathbb{C} \setminus \mathbb{R} = \mathcal{H} \cup \mathcal{H}^-$)
  - Key property: $K \cap \mathcal{H}_p \neq \emptyset$ (because $K_p \setminus \mathbb{Q}_p \neq \emptyset$)
- In this case the Stark–Heegner point construction is

$$\begin{array}{ccc} K \cap \mathcal{H}_p & \longrightarrow & E(\mathbb{C}_p) \\ \tau & \longmapsto & P_\tau \end{array}$$

- P_τ is defined via certain p-adic periods of the modular form $f = f_E$

Conjecture (Darmon, 2001)

P_τ a global point, and it is defined over K^{ab}

- Effective computation: Darmon–Green–Pollack algorithm
  - under the restriction that $M = 1$ (i.e., on curves of prime conductor)

Integration in $\mathcal{H}_p \times \mathcal{H}$

Double integrals $\times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2} \int_x^y \omega_f \in K_p^\times, \quad \tau_1, \tau_2 \in \mathcal{H}_p,\ x, y \in \mathbb{P}^1(\mathbb{Q})$

- Definition
  - $\Gamma_0(M) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}]) \colon \gamma \equiv \left(\begin{smallmatrix} \star & \star \\ 0 & \star \end{smallmatrix}\right) \pmod{M} \right\} \subset \mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])$
  - $x, y \in \mathbb{P}^1(\mathbb{Q}) \rightsquigarrow$ measure in $\mathbb{P}^1(\mathbb{Q}_p)$: $\mu_f\{x \to y\}$

$$\mu_f\{x \to y\}(\gamma \mathbb{Z}_p) = \frac{1}{\Omega^+} \int_{\gamma^{-1}x}^{\gamma^{-1}y} \mathrm{Re}(2\pi i f(z) dz) \in \mathbb{Z} \ \text{ for } \gamma \in \Gamma_0(M)$$

  - $\times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2} \int_x^y \omega_f := \times\!\!\!\!\!\!\int_{\mathbb{P}^1(\mathbb{Q}_p)} \left(\frac{t - \tau_2}{t - \tau_1} \right) d\mu_f\{x \to y\}(t) \in K_p^\times$
  - They are multiplicative integrals (Riemann products)
  - They can be very efficiently computed using the theory of overconvergent modular symbols of Pollack–Stevens

Semi-indefinite integrals $\times\!\!\!\!\!\!\int^{\tau} \int_x^y \omega_f \in K_p^\times, \ \tau \in \mathcal{H}_p,\ x, y \in \mathbb{P}^1(\mathbb{Q})$

- $\times\!\!\!\!\!\!\int^{\tau_2} \int_x^y \omega_f \div \times\!\!\!\!\!\!\int^{\tau_1} \int_x^y \omega_f = \times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2} \int_x^y \omega_f$

p-adic Darmon points

Definition (Darmon)

Given $\tau \in K \cap \mathcal{H}_p$ then

$$P_\tau = \Phi_{\mathrm{Tate}}\left(\int^{\tau}\int_{\infty}^{\gamma_\tau\infty}\omega_f\right), \quad \langle\gamma_\tau\rangle = \mathrm{Stab}_{\Gamma_0(M)}(\tau)$$

- Tate's uniformization map: $\Phi_{\mathrm{Tate}}\colon K_p^\times/q_E^{\mathbb{Z}} \longrightarrow E(K_p)$
- Darmon-Green-Pollack algorithm
  - Transform semi-indefinite integral into a product of double integrals
  - Compute the double integrals using OMS
- This is the only stage where the assumption $M = 1$ is needed.
- We give a different method, that works with $M > 1$.
  - This extends the algorithm to curves of arbitrary conductor.
- Key step: we can assume that $\gamma_\tau \in \Gamma_1(M)$

$$\Gamma_1(M) = \left\{\gamma \in \mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])\colon \gamma \equiv \left(\begin{smallmatrix}1 & \star\\ 0 & 1\end{smallmatrix}\right) \pmod{M}\right\} \subset \mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])$$

Extending the Darmon–Green–Pollack algorithm

- In this context there is also a “Manin Trick” involved
- Need to express $\gamma_\tau\infty \in \mathbb{P}^1(\mathbb{Q})$ as a “continued fraction” of the form

$$\gamma_\tau\infty = q_1 + \cfrac{1}{Mq_2 + \cfrac{1}{q_3 + \cfrac{1}{Mq_4 + \cdots}}}, \quad q_1, \ldots, q_n \in \mathbb{Z}[\frac{1}{p}]$$

- This is equivalent to a decomposition into elementary matrices

$$\gamma_\tau = \begin{pmatrix} 1 & q_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ Mq_2 & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & q_{r-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ Mq_r & 1 \end{pmatrix}$$

- If $M = 1$, this is again the euclidean algorithm!

Theorem (G.–Masdeu)

Assume GRH. There is an algorithm that, given $\gamma \in \Gamma_1(M)$ computes a decomposition of the form

$$\gamma_\tau = \begin{pmatrix} 1 & q_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ Mq_2 & 1 \end{pmatrix} \begin{pmatrix} 1 & q_3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ Mq_4 & 1 \end{pmatrix} \begin{pmatrix} 1 & q_5 \\ 0 & 1 \end{pmatrix}, \; q_i \in \mathbb{Z}[\frac{1}{p}]$$

Implementation

- We implemented the algorithm in SAGE
  - We used some code by Pollack for computing with overconvergent modular symbols.
  - We have programed the routines for computing the elementary matrix decomposition and for expressing semi-indefinite integrals as products of definite integrals.
- Given an elliptic curve E and $K = \mathbb{Q}(\sqrt{D})$ a real quadratic field:
  - choose $\tau \in K_p$ such that P_τ is conjecturally defined over H_K
  - $\Phi_{\mathrm{Tate}}(⨍^{\tau} \int_{\infty}^{\gamma_\tau \infty} \omega_f) = (x, y)$, in principle $x, y \in K_p$
  - We can recognize x, y as elements of H_K

Curve 21A1 (p=7, M=3, prec=7^{80}, $K = \mathbb{Q}(\sqrt{D})$)

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

Curve 33A1 ($p = 11$, $M = 3$, prec=3^{80}, $K = \mathbb{Q}(\sqrt{D})$)

D	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	$\left(-\frac{51842}{21025}, \frac{2065147}{3048625}\sqrt{43} + \frac{25921}{21025}\right)$
193	1	$\left(\frac{94663533349261}{678412148664608}\sqrt{193} + \frac{1048806825770477}{678412148664608}, \frac{147778957920931299317}{1249468831181355374184}\sqrt{193} + \frac{308629344930924160355541}{1249468831181355374184}\right)$

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	$x^4 + \left(\frac{169016003453}{83168215321}\sqrt{145} - \frac{1621540207320}{83168215321}\right)x^3 + \left(-\frac{1534717557538}{83168215321}\sqrt{145} + \frac{18972823294799}{83168215321}\right)x^2 + \left(\frac{5533405190489}{83168215321}\sqrt{145} - \frac{66553066916820}{83168215321}\right) + -\frac{6414913389456}{83168215321}\sqrt{145} + \frac{77248348177561}{83168215321}$

Curve 51A1 (p=3, M=17, prec=3^{80}, $K = \mathbb{Q}(\sqrt{D})$)

D	h	P^+
8	1	$\left(\frac{1}{2}, \frac{1}{4}\sqrt{2} - \frac{1}{2}\right)$
53	1	$\left(\frac{3}{2}\sqrt{53} + \frac{23}{2}, \frac{15}{2}\sqrt{53} + \frac{107}{2}\right)$
77	1	$\left(\frac{5559}{55778}\sqrt{77} + \frac{78911}{55778}, \frac{2040153}{9314926}\sqrt{77} + \frac{17804737}{9314926}\right)$
89	1	$\left(\frac{793511}{2401}, \frac{150079871}{235298}\sqrt{89} - \frac{1}{2}\right)$
101	1	$\left(-\frac{656788148124048}{1083959255666683225}\sqrt{101} + \frac{1086635263155707777}{1083959255666683225}, \frac{43274260598510467034409 6}{3568777211845978342225212 5}\sqrt{101} - \frac{715518602160795519413833 54}{356877721184597834222521 25}\right)$
137	1	$\left(\frac{83}{81}, \frac{193}{1458}\sqrt{137} - \frac{1}{2}\right)$
149	1	$\left(-\frac{41662615293}{110013332450}\sqrt{149} + \frac{802189306199}{110013332450}, \frac{3979167222803724 9}{2580197692616075 0}\sqrt{149} - \frac{6352904503696929 07}{2580197692616075 0}\right)$
152	1	$\left(-\frac{1915814571}{20670100441}\sqrt{38} + \frac{24731592007}{20670100441}, \frac{577303899566856}{297176101050301 1}\sqrt{38} - \frac{7167395643538198}{2971761010503011}\right)$
161	1	$\left(\frac{62146167667}{49710362300}, \frac{8395974419456303}{5315379909652100 0}\sqrt{161} - \frac{1}{2}\right)$
104	2	$x^2 + \left(-\frac{992302702743}{1960400420449}\sqrt{26} - \frac{57132410901980}{1960400420449}\right)x - \frac{4968445297101}{1960400420449}\sqrt{26} + \frac{61480175149213}{1960400420449}$
140	2	$x^2 - \frac{7073157}{13924}x + \frac{398237221}{55696}$
185	2	$x^2 + \left(-\frac{908505900}{7532677681}\sqrt{185} - \frac{54207252962}{7532677681}\right)x - \frac{787814100}{7532677681}\sqrt{185} + \frac{45005684581}{7532677681}$

Curve 105A1 ($p = 3$, $M = 5 \cdot 7$, prec=3^{80}, $K = \mathbb{Q}(\sqrt{D})$)

D	h	P^+
29	1	$2 \cdot \left(\frac{5}{2}\sqrt{29} + \frac{29}{2}, \frac{25}{2}\sqrt{29} + \frac{133}{2}\right)$
44	1	$\left(\frac{47}{36}, \frac{13}{54}\sqrt{11} - \frac{83}{72}\right)$
149	1	$\left(\frac{41297}{48050}\sqrt{149} + \frac{554429}{48050}, \frac{28371039}{7447750}\sqrt{149} + \frac{340434623}{7447750}\right)$

Darmon points: algorithms and numerical evidence

Xevi Guitart

Max-Planck-Institute for Mathematics

Number Theory Lunch Seminar,
14 November 2012