Numerical Computation of Stark–Hegner points in higher level

Xevi Guitart[1] Marc Masdeu[2]

[1]Max Planck Institute/U. Politècnica de Catalunya

[2]Columbia University

Rational points on curves:
A *p*-adic and computational perspective
Mathematical College, Oxford 2012

Stark–Heegner points in higher level

- $E/\mathbb{Q}$ elliptic curve of conductor $N = pM$, with $p \nmid M$.
- $K/\mathbb{Q}$ real quadratic field in which
  - p is inert
  - all primes dividing M are split
- Darmon's construction of Stark–Heegner points

$$\begin{array}{rccc} \mathbb{P}^1(K_p) \setminus \mathbb{P}^1(\mathbb{Q}_p) = & \mathcal{H}_p & \longrightarrow & E(K_p) \\ & \tau & \longmapsto & P_\tau \end{array}$$

- P_τ is defined in terms of certain p-adic periods of $f = f_E \in S_2(N)$

Conjecture (Darmon, 2001)

P_τ is a global point: $P_\tau \in E(H_\tau)$ where H_τ is a Ring Class Field of K

- Explicit computations and numerical evidence:
  - Darmon–Green (2002): algorithm for computing P_τ
  - Darmon–Pollack (2006): more efficient calculations with OMS
    The algorithm needs to assume $M = 1$
    (P_τ's only computed on curves of conductor p)
- In this talk: remove the requirement $M = 1$ in this algorithm, so that P_τ in curves of composite conductor can be computed.

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

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

- Definition
  - $\Gamma_0(M) = \left\{\gamma \in \mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])\colon \gamma \equiv \left(\begin{smallmatrix}\star & \star\\ 0 & \star\end{smallmatrix}\right) \pmod{M}\right\} \subset \mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])$
  - $\int_{\tau_1}^{\tau_2}\int_{x}^{y} \omega_f := \int_{\mathbb{P}^1(\mathbb{Q}_p)} \log\left(\frac{t-\tau_2}{t-\tau_1}\right) d\mu_f\{x\to y\}(t) \in K_p$
  - $\mu_f\{x\to y\}$ measure in $\mathbb{P}^1(\mathbb{Q}_p)$
    - ★ $\mu_f\{x\to y\}(\gamma\mathbb{Z}_p) = \frac{1}{\Omega^+}\int_{\gamma^{-1}x}^{\gamma^{-1}y} \mathrm{Re}(2\pi i f(z)dz) \in \mathbb{Z}$ *for* $\gamma \in \Gamma_0(M)$
- Double multiplicative integral:

$$\oint_{\tau_1}^{\tau_2}\int_{x}^{y} \omega_f := \oint_{\mathbb{P}^1(\mathbb{Q}_p)} \left(\frac{t-\tau_2}{t-\tau_1}\right) d\mu_f\{x\to y\}(t) \in K_p^\times$$

  - $\int_{\tau_1}^{\tau_2}\int_{x}^{y} \omega_f = \log\left(\oint_{\tau_1}^{\tau_2}\int_{x}^{y} \omega_f\right)$
- Effective computation:
  - They can be very efficiently computed (up to a prescribed p-adic precision) using overconvergent modular symbols

Semi-indefinite integrals

$$\not\int_x^{\tau}\int_x^{y}\omega_f \in K_p^{\times}/q^{\mathbb{Z}},\ \ \tau\in\mathcal{H}_p,\ x,y\in\mathbb{P}^1(\mathbb{Q}),\ x=\gamma y \text{ some } \gamma\in\Gamma_0(M)$$

- Definition
  - Cohomology of measured valued modular symbols
- Properties
  1. $\not\int^{\tau}\int_x^{y}\omega_f \times \not\int^{\tau}\int_y^{z}\omega_f = \not\int^{\tau}\int_x^{z}\omega_f$ (multiplicative in the limits)
  2. $\not\int^{\gamma\tau}\int_{\gamma x}^{\gamma y}\omega_f = \not\int^{\tau}\int_x^{y}\omega_f$ for all $\gamma\in\Gamma_0(M)$ (invariance under $\Gamma_0(M)$)
  3. $\not\int^{\tau_2}\int_x^{y}\omega_f \div \not\int^{\tau_1}\int_x^{y}\omega_f = \not\int_{\tau_1}^{\tau_2}\int_x^{y}\omega_f$ (Relation with double integrals)
- Definition of Stark–Heegner points

$$P_\tau = \Phi_{\mathrm{Tate}}\left(\not\int^{\tau}\int_{\infty}^{\gamma_\tau\infty}\omega_f\right), \mathrm{Stab}_{\Gamma_0(M)}(\tau)=\langle\gamma_\tau\rangle$$

- Computing P_τ boils down to compute semi-indefinite integrals
  - Direct computation (using the very definition) seems to be difficult
  - Darmon-Green-Pollack: use 1, 2 and 3 to transform semi-indefinite integrals into definite double integrals.
  - This is the only stage where the assumption $M=1$ is needed.
  - We give a different method, that works with $M>1$

Reduction to $\Gamma_1(M)$

$$\Gamma_1(M) = \{\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}[1/p]) \colon \gamma \equiv \left(\begin{smallmatrix} 1 & \star \\ 0 & 1 \end{smallmatrix}\right) \pmod{M}\} \subset \Gamma_0(M)$$

- $\gamma_\tau \in \Gamma_0(M)$, but we can reduce to the case where $\gamma_\tau \in \Gamma_1(M)$
  - If $m = [\Gamma_0(M) \colon \Gamma_1(M)]$, computing $mP_\tau = \Phi_{\mathrm{Tate}}\left(\oint^\tau \int_\infty^{\gamma_\tau^m \infty}\right)$
  - if $a \equiv p^n \pmod{M}$ we let $\alpha = \left(\begin{smallmatrix} p^{-n} & 0 \\ 0 & p^n \end{smallmatrix}\right)$ and

$$P_\tau = \oint^\tau \int_\infty^{\gamma_\tau \infty} = \oint^{\alpha\tau} \int_\infty^{\alpha\gamma_\tau \infty}$$

with $\alpha\gamma_\tau \in \Gamma_1(M)$

- We are reduced to compute $\not\int^{\tau} \int_{\infty}^{\gamma\infty}$ with $\gamma \in \Gamma_1(M)$
- $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])$ has the congruence subgroup property

$$\gamma = \begin{pmatrix} 1 & 0 \\ Mx_1 & 1 \end{pmatrix} \begin{pmatrix} 1 & x_2 \\ 0 & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & 0 \\ Mx_{r-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & x_r \\ 0 & 1 \end{pmatrix}, \quad \gamma \in \Gamma_1(M)$$

$$\not\int^{\tau} \int_{\infty}^{\gamma\infty} \omega_f = \not\int^{\tau} \int_{\infty}^{0} \omega_f \times \not\int^{\tau} \int_{0}^{\gamma\infty} \omega_f = \not\int^{\tau} \int_{\infty}^{0} \omega_f \times \not\int^{E_1^{-1}\cdot\tau} \int_{0}^{E_1^{-1}\gamma\cdot\infty} \omega_f$$

$$= \not\int^{\tau} \int_{\infty}^{0} \omega_f \times \not\int^{E_1^{-1}\cdot\tau} \int_{0}^{\infty} \omega_f \times \not\int^{E_1^{-1}\cdot\tau} \int_{\infty}^{E_1^{-1}\gamma\cdot\infty} \omega_f = \not\int_{\tau}^{E_1^{-1}\cdot\tau} \int_{0}^{\infty} \omega_f \times \not\int^{E_1^{-1}\cdot\tau} \int_{\infty}^{E_1^{-1}\gamma\cdot\infty} \omega_f$$

- Small problem: 0 and ∞ are not $\Gamma_0(M)$-equivalent if $M > 1$
- But $W_d \cdot 0 = \infty$, $\quad W_d = \begin{pmatrix} 0 & -1 \\ d & 0 \end{pmatrix}$

Assumption

There exists $d \mid M$ such that $W_d(f) = f$

  - For instance, if M has at least two factors this is always true

- Then semi-indefinite integrals are also defined on W_d-equivalent cusps.

- The problem is reduced to finding an algorithm for computing

$$\gamma = \begin{pmatrix} 1 & 0 \\ Mx_1 & 1 \end{pmatrix} \begin{pmatrix} 1 & x_2 \\ 0 & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & 0 \\ Mx_{r-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & x_r \\ 0 & 1 \end{pmatrix}, \quad \gamma \in \Gamma_1(M).$$

- Remark: if $M = 1$ then the x_i's are the quotients of the contineued fraction of a/c, if $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$.
- For $M > 1$ we need another algorithm.

A more general setting

- F: number field with at least a real place
- S a set of places of F containing the archimedean ones
- $\mathcal{O}_S$ ring of S-integers, $\mathfrak{M} \subset \mathcal{O}_S$ an ideal
- $\Gamma_1(\mathfrak{M}) = \{\gamma \in \mathrm{SL}_2(\mathcal{O}_S) \colon \gamma \equiv \left(\begin{smallmatrix} 1 & \star \\ 0 & 1 \end{smallmatrix}\right) \pmod{\mathfrak{M}}\}$
  (p-adic Stark–Heegner points $F = \mathbb{Q}$, $S = \{p, \infty\}$, $\mathfrak{M} = M \cdot \mathbb{Z}[\frac{1}{p}]$)
- Theorem (Serre, Vaserstein): If $\mathcal{O}_S^\times$ is infinite (i.e. if $\#S > 1$) then $\Gamma_1(\mathfrak{M})$ is generated by the matrices

$$\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) \text{ with } x \in \mathcal{O}_S, \quad \left(\begin{smallmatrix} 1 & 0 \\ x & 1 \end{smallmatrix}\right) \text{ with } x \in \mathfrak{M},$$

- Problem: given $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(\mathfrak{M})$, write it as a product of elementary matrices
- Simple case: if $c = u + ta$ with $u \in \mathcal{O}_S^\times$ and $t \in \mathcal{O}_S$ then

$$\gamma = \left(\begin{smallmatrix} 1 & 0 \\ c+t(1-a) & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & -u^{-1} \\ 0 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 0 \\ u(1-a) & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right). \tag{1}$$

- We can replace $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ by $\left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right) \gamma = \left(\begin{smallmatrix} a+\lambda c & b+\lambda d \\ c & d \end{smallmatrix}\right)$

Effective Congruence Subgroup Problem

Theorem (Cooke–Weinberger)

Assume GRH. Then the set of prime ideals in $\mathcal{O}_S$ of the form $a + \lambda c$ such that $\mathcal{O}_S^\times \longrightarrow (\mathcal{O}_S/(a+\lambda c)\mathcal{O}_S)^\times$ is onto has positive density.

Algorithm for elmentary matrix decomposition

Given $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(\mathfrak{M})$

1. Find $\lambda \in \mathcal{O}_S$ such that $\mathcal{O}_S^\times \longrightarrow (\mathcal{O}_S/(a+\lambda c)\mathcal{O}_S)^\times$ is onto
2. Set $\gamma' = \left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right)\gamma = \left(\begin{smallmatrix} a+\lambda c & b+\lambda d \\ c & d \end{smallmatrix}\right)$
3. Find $u \in \mathcal{O}_S^\times$ representing the class of c modulo $a + \lambda c$
4. Compute the explicit decomposition (1) to γ'.

Corollary

Assuming GRH, every matrix in $\Gamma_1(\mathfrak{M})$ can be expressed as a product of 5 elementary matrices.

Computing the double integrals

- We need to compute integrals of the form $\oint_{\tau_1}^{\tau_2} \int_0^\infty \omega_f$
- The hard part is $\int_{\mathbb{P}^1(\mathbb{Q}_p)} \log\left(\frac{t-\tau_1}{t-\tau_2}\right) d\mu_f(t)$
- Darmon–Pollack: $\mathbb{P}^1(\mathbb{Q}_p) = \bigcup_{i=1}^{L} g_i \mathbb{Z}_p$, $g_i \in \mathrm{GL}_2(\mathbb{Q})$

$$\int_{g_i\mathbb{Z}_p} \log\left(\frac{t-\tau_1}{t-\tau_2}\right) d\mu_f(t) = \cdots = \sum_{n\geq 1} \alpha_n \int_{g_i\mathbb{Z}_p} (g_i^{-1}t)^n d\mu_f(t)$$

  - $\int_{g_i\mathbb{Z}_p} (g_i^{-1}t)^n d\mu_f(t)$: the moments can be efficiently computed via overconvergent modular symbols
  - Number of g_i's depends on the affinoid $\mathcal{H}_p^n$ containing τ_1, τ_2
    $\mathcal{H}_p^0 = \{\tau \in \mathbb{P}^1(K_p) \colon \mathrm{red}(\tau) \notin \mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})\}$
    $\mathcal{H}_p^n = \{\tau \in \mathbb{P}^1(K_p) \colon \mathrm{red}(\tau) \notin \mathbb{P}^1(\mathbb{Z}/p^{n+1}\mathbb{Z})\} \setminus \mathcal{H}_p^{n-1}$
  - We can take a covering of size $(p+1)+n(p-1)$
  - This increases the running time with respect to the $M=1$ case (when $M=1$, then $\tau_1, \tau_2 \in \mathcal{H}_p^0$ so $p+1$ evaluations is enough), but it is not critical in the range of values we tested.

Implementation

- We have written a SAGE implementation of the method
  - we use Robert Pollack's implementation in SAGE for computing the moments with overconvergent modular symbols
  - we adapt part of the code written by Darmon and Pollack in Magma for the $M = 1$ case
  - we added the routines for the elementary matrix decomposition, for transforming semi-indefinite into definite integrals, and for integrating over the appropriate open covers.
- $(x, y) = \Phi_{\mathrm{Tate}}(J_\tau)$ and we can actually recognize $x, y \in K_p$ as elements of the expected number field H_τ (usually we choose τ so that H_τ is the Hilbert class field of 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	$\left(\frac{94663533349261}{678412148664608}\sqrt{193}+\frac{1048806825770477}{678412148664608}, \frac{1477789579209312993 17}{12494688311813553741184}\sqrt{193}+\frac{3086293449309241603 5541}{12494688311813553741184}\right)$

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

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	$\left(-\frac{656788148124048}{108395925566683225}\sqrt{101} + \frac{108663526315570777}{108395925566683225}, \frac{43274260598510467034409 6}{35687772118459783422252125}\sqrt{101} - \frac{71551860216079551941383354}{35687772118459783422252125}\right)$
137	1	$\left(\frac{83}{81}, \frac{193}{1458}\sqrt{137} - \frac{1}{2}\right)$
149	1	$\left(-\frac{41662615293}{110013332450}\sqrt{149} + \frac{802189306199}{110013332450}, \frac{39791672228037249}{2580197692616075 0}\sqrt{149} - \frac{635290450369692907}{2580197692616075 0}\right)$
152	1	$\left(-\frac{1915814571}{20670100441}\sqrt{38} + \frac{24731592007}{20670100441}, \frac{577303899566856}{297176101050301 1}\sqrt{38} - \frac{7167395643538198}{297176101050301 1}\right)$
161	1	$\left(\frac{62146167667}{49710362300}, \frac{8395974419456303}{53153799096521000}\sqrt{161} - \frac{1}{2}\right)$
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	$\left(\frac{41297}{48050}\sqrt{149} + \frac{554429}{48050}, \frac{28371039}{7447750}\sqrt{149} + \frac{340434623}{7447750} \right)$

Numerical Computation of Stark–Hegner points in higher level

Xevi Guitart[1] Marc Masdeu[2]

[1]Max Planck Institute/U. Politècnica de Catalunya

[2]Columbia University

Rational points on curves:
A *p*-adic and computational perspective
Mathematical College, Oxford 2012