# Problema del subgrup de congruència efectiu i càlcul de punts de Stark–Heegner.

Xevi Guitart[1] Marc Masdeu[2]

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

[2]Columbia University

Tercera trobada de joves investigadors de la SCM

# Càlcul de punts de Stark–Heegner

- $E/\mathbb{Q}$ corba el·líptica de conductor $N = pM$, amb $p \nmid M$.
- $K/\mathbb{Q}$ cos quadràtic real en el qual
  - $p$ és inert (per tant $[K_p : \mathbb{Q}_p] = 2$)
  - tots els primers dividint $M$ descomponen
- Construcció de Darmon de punts de Stark–Heegner

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

- $P_\tau$ es defineix en termes de períodes $p$-àdics de $f = f_E \in S_2(N)$

**Conjectura (Darmon, 2001)**

$P_\tau$ és un punt global: $P_\tau \in E(H_\tau)$ on $H_\tau$ és un Ring Class Field de $K$

- Càlculs explícits i evidència numèrica:
  - Darmon–Green (2002): algoritme per a calcular $P_\tau$
  - Darmon–Pollack (2006): càlculs més eficients utilitzant OMS
    Aquest algoritme funciona només si $M = 1$
    (permet calcular $P_\tau$ en corbes de conductor $p$)
- En aquesta xerrada: eliminar el requeriment $M = 1$ en aquest algoritme, i poder calcular els $P_\tau$ en corbes de conductor compost.

# Integració en $\mathcal{H}_p \times \mathcal{H}$

Integrals dobles $\int\!\!\!\!\!\!\diagup_{\tau_1}^{\tau_2} \int_x^y \omega_f \in K_p^\times, \quad \tau_1, \tau_2 \in \mathcal{H}_p,\ x, y \in \mathbb{P}^1(\mathbb{Q})$

- Definició
  - $\Gamma_0(M) = \left\{\gamma \in \mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}]) \colon \gamma \equiv \left(\begin{smallmatrix} \star & \star \\ 0 & \star \end{smallmatrix}\right) \pmod{M}\right\} \subset \mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])$
  - $\int\!\!\!\!\!\!\diagup_{\tau_1}^{\tau_2} \int_x^y \omega_f := \int\!\!\!\!\!\!\diagup_{\mathbb{P}^1(\mathbb{Q}_p)} \left(\frac{t-\tau_2}{t-\tau_1}\right) d\mu_f\{x \to y\}(t) \in K_p^\times$
  - $\mu_f\{x \to y\}$ mesura en $\mathbb{P}^1(\mathbb{Q}_p)$

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

  - Integral multiplicativa: productes de Riemann en comptes de sumes de Riemann
- Càlcul efectiu:
  - Es poden calcular de manera molt eficient (fins a qualsevol precisió $p$-àdica prefixada) gràcies als simbols modulars sobreconvergents de Pollack–Stevens.

# Integrals semi-indefinides

$$\oint_{}^{\tau} \int_{x}^{y} \omega_f \in K_p^{\times}, \quad \tau \in \mathcal{H}_p, \; x, y \in \mathbb{P}^1(\mathbb{Q})$$

- Definició
  - Cohomologia de simbols modulars amb valors en mesures
- Propietats (que de fet la caracteritzen)
  1. $\oint^{\tau} \int_x^y \omega_f \times \oint^{\tau} \int_y^z \omega_f = \oint^{\tau} \int_x^z \omega_f$ (multiplicativa en els límits)
  2. $\oint^{\gamma\tau} \int_{\gamma x}^{\gamma y} \omega_f = \oint^{\tau} \int_x^y \omega_f$ for all $\gamma \in \Gamma_0(M)$ (invariància per $\Gamma_0(M)$)
  3. $\oint^{\tau_2} \int_x^y \omega_f \div \oint^{\tau_1} \int_x^y \omega_f = \oint_{\tau_1}^{\tau_2} \int_x^y \omega_f$ (Relació amb integrals dobles)
- Punts de Stark–Heegner $\quad P_\tau = \Phi_{\mathrm{Tate}}\left(\oint^{\tau} \int_{\infty}^{\gamma_\tau \infty} \omega_f\right)$

$$\Phi_{\mathrm{Tate}} \colon K_p^{\times}/q_E^{\mathbb{Z}} \longrightarrow E(K_p), \quad \langle \gamma_\tau \rangle = \mathrm{Stab}_{\Gamma_0(M)}(\tau)$$

- Calcular $P_\tau$ és equivalent a calcular integrals semi-indefinides
  - El càlcul directe (via la definició) és complicat
  - Darmon-Green-Pollack: utilitzen 1, 2 and 3 per a transformar integrals semi-indefinides en definides
  - Aquest és l'únic pas en què necessiten $M = 1$.
  - Ens cal un mètode alternatiu, que funcioni per a $M > 1$

# Reducció a $\Gamma_1(M)$

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

- Volem calcular $\displaystyle\int^{\tau}\int_{\infty}^{\gamma_\tau \infty} \omega_f$ on $\gamma_\tau \in \Gamma_0(M)$
- De fet, ens podem reduir al cas en què $\gamma_\tau \in \Gamma_1(M)$
  - Per exemple calculant un múltiple de $P_\tau$: Si $m = [\Gamma_0(M) \colon \Gamma_1(M)]$

$$mP_\tau = \Phi_{\mathrm{Tate}}\left(\int^{\tau}\int_{\infty}^{\gamma_\tau^m \infty}\right), \quad \gamma_\tau^m \in \Gamma_1(M)$$

- Ens hem reduït a calcular $\not\int^{\tau} \int_{\infty}^{\gamma\infty}$ amb $\gamma \in \Gamma_1(M)$
- $\mathrm{SL}_2(\mathbb{Z}[\frac{1}{p}])$ té la propietat del subgrup de congruència

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

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

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

- Hem reduït el problema a trobar un algoritme per a calcular descomposicions

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

- Observació: si $M = 1$ aleshores els $x_i$'s són els quocients de la fracció contínua de $a/c$, on $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$.
- Per $M > 1$ necessitem un algoritme alternatiu.

# Un escenari més general

- $F$: cos de nombres amb almenys una plaça real
- $S$ conjunt de places de $F$ que conté les arquimedianes
- $\mathcal{O}_S$ anell de $S$-enters, $\mathfrak{M} \subset \mathcal{O}_S$ un ideal
- $\Gamma_1(\mathfrak{M}) = \{\gamma \in \mathrm{SL}_2(\mathcal{O}_S) \colon \gamma \equiv \left(\begin{smallmatrix} 1 & \star \\ 0 & 1 \end{smallmatrix}\right) \pmod{\mathfrak{M}}\}$
  (punts de Stark–Heegner: $F = \mathbb{Q}$, $S = \{p, \infty\}$, $\mathfrak{M} = M \cdot \mathbb{Z}[\frac{1}{p}]$)
- **Teorema** (Serre, Vaserstein): Si $\mathcal{O}_S^\times$ és infinit (i.e. si $\#S > 1$) aleshores $\Gamma_1(\mathfrak{M})$ és generat per les matrius

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

- Problema: donada $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(\mathfrak{M})$, escriure-la com a producte de matrius elementals
- Cas fàcil: si $c = u + ta$ with $u \in \mathcal{O}_S^\times$ i $t \in \mathcal{O}_S$ aleshores

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

- Podem canviar $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ per $\left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right) \gamma = \left(\begin{smallmatrix} a+\lambda c & b+\lambda d \\ c & d \end{smallmatrix}\right)$

# Problema del subgrup de congruència efectiu

## Teorema (Cooke–Weinberger)

Si assumim GRH, el conjunt d'ideals $\mathcal{O}_S$ de la forma $a+\lambda c$ tals que $\mathcal{O}_S^\times \longrightarrow (\mathcal{O}_S/(a+\lambda c)\mathcal{O}_S)^\times$ és exhaustiva té densitat positiva.

## Algoritme per a la descomposició en matrius elementals

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

1. Trobar $\lambda \in \mathcal{O}_S$ tal que $\mathcal{O}_S^\times \longrightarrow (\mathcal{O}_S/(a+\lambda c)\mathcal{O}_S)^\times$ és exhaustiva
2. Posem $\gamma' = \left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right)\gamma = \left(\begin{smallmatrix} a+\lambda c & b+\lambda d \\ c & d \end{smallmatrix}\right)$
3. Trobar $u \in \mathcal{O}_S^\times$ que representi la classe de $c$ mòdul $a+\lambda c$
4. Calcular la descomposició explícita (1) de $\gamma'$.

## Corol·lari

Si assumim GRH, tota matriu de $\Gamma_1(\mathfrak{M})$ es pot expressar com a producte de 5 matrius elementals.

# Implementació

- Hem realitzat una implementació en SAGE
  - Per a calcular els moments via simbols modulars sobreconvergents hem utilitzat les rutines implementades per en Robert Pollack.
  - Hem afegit les rutines per a la descomposició en matrius elementals i per a transformar integrals semi-indefinides en definides.
- Donada una corba el·líptica $E$ i $K = \mathbb{Q}(\sqrt{D})$ un quadràtic real:
  - escollim $\tau \in K_p$ tal que $H_\tau = H_K$
  - $\Phi_{\mathrm{Tate}}(\oint^{\tau} \int_{\infty}^{\gamma_\tau \infty} \omega_f) = (x, y)$, on en principi $x, y \in K_p$
  - Podem reconèixer $x, y$ com a elements de $H_K$

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

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

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

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

# Corba 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 | $x^2 + \left(-\frac{908505900}{7532677681}\sqrt{185} - \frac{54207252962}{7532677681}\right)x - \frac{787814100}{7532677681}\sqrt{185} + \frac{45005684581}{7532677681}$ |

# Corba 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 | $\left( \frac{41297}{48050}\sqrt{149} + \frac{554429}{48050}, \frac{28371039}{7447750}\sqrt{149} + \frac{340434623}{7447750} \right)$ |

# Problema del subgrup de congruència efectiu i càlcul de punts de Stark–Heegner.

Xevi Guitart[1] Marc Masdeu[2]

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

[2]Columbia University

Tercera trobada de joves investigadors de la SCM