Algoritmos para puntos de Darmon

Xevi Guitart[1] Marc Masdeu[2]

[1]Universitat Politècnica de Catalunya

[2]Columbia University

Quintas Jornadas de Teoría de Números

Índex

Índex

Curvas elípticas sobre $\mathbb{Q}$

- E curva elíptica con coeficientes racionales

$$E\colon y^2 + b_1 xy + b_3 y = x^3 + b_2 x^2 + b_4 x + b_6, \quad b_i \in \mathbb{Z}$$

Curvas elípticas sobre $\mathbb{Q}$

- E curva elíptica con coeficientes racionales

$$E\colon y^2 + b_1 xy + b_3 y = x^3 + b_2 x^2 + b_4 x + b_6, \quad b_i \in \mathbb{Z}$$

- $E(\mathbb{Q}) = \{\text{soluciones } (x, y) \in \mathbb{Q}^2\}$

Curvas elípticas sobre $\mathbb{Q}$

- E curva elíptica con coeficientes racionales

$$E\colon\ y^2 + b_1 xy + b_3 y = x^3 + b_2 x^2 + b_4 x + b_6, \quad b_i \in \mathbb{Z}$$

- $E(\mathbb{Q}) = \{\text{soluciones } (x, y) \in \mathbb{Q}^2\}$

Problema

Existe algun algoritmo para calcular $E(\mathbb{Q})$?

Curvas elípticas sobre $\mathbb{Q}$

- E curva elíptica con coeficientes racionales

$$E\colon\ y^2 + b_1 xy + b_3 y = x^3 + b_2 x^2 + b_4 x + b_6, \quad b_i \in \mathbb{Z}$$

- $E(\mathbb{Q}) = \{\text{soluciones } (x, y) \in \mathbb{Q}^2\}$

Problema

Existe algun algoritmo para calcular $E(\mathbb{Q})$?

Teorema de Mordell–Weil

$E(\mathbb{Q})$ tiene estructura de grupo y $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tor}} \oplus \mathbb{Z}^r$

Curvas elípticas sobre $\mathbb{Q}$

- E curva elíptica con coeficientes racionales

$$E\colon\ y^2 + b_1 xy + b_3 y = x^3 + b_2 x^2 + b_4 x + b_6, \quad b_i \in \mathbb{Z}$$

- $E(\mathbb{Q}) = \{\text{soluciones } (x, y) \in \mathbb{Q}^2\}$

Problema

Existe algun algoritmo para calcular $E(\mathbb{Q})$?

Teorema de Mordell–Weil

$E(\mathbb{Q})$ tiene estructura de grupo y $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tor}} \oplus \mathbb{Z}^r$

- $E(\mathbb{Q})_{\text{tor}}$: sí que hay algoritmos para calcularlos

Curvas elípticas sobre $\mathbb{Q}$

- E curva elíptica con coeficientes racionales

$$E\colon y^2 + b_1 xy + b_3 y = x^3 + b_2 x^2 + b_4 x + b_6, \quad b_i \in \mathbb{Z}$$

- $E(\mathbb{Q}) = \{\text{soluciones } (x, y) \in \mathbb{Q}^2\}$

Problema

Existe algun algoritmo para calcular $E(\mathbb{Q})$?

Teorema de Mordell–Weil

$E(\mathbb{Q})$ tiene estructura de grupo y $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tor}} \oplus \mathbb{Z}^r$

- $E(\mathbb{Q})_{\text{tor}}$: sí que hay algoritmos para calcularlos
- Calcular r puntos de orden infinito independientes?

Curvas elípticas sobre $\mathbb{Q}$

- E curva elíptica con coeficientes racionales

$$E\colon\ y^2 + b_1 xy + b_3 y = x^3 + b_2 x^2 + b_4 x + b_6, \quad b_i \in \mathbb{Z}$$

- $E(\mathbb{Q}) = \{\text{soluciones } (x, y) \in \mathbb{Q}^2\}$

Problema

Existe algun algoritmo para calcular $E(\mathbb{Q})$?

Teorema de Mordell–Weil

$E(\mathbb{Q})$ tiene estructura de grupo y $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tor}} \oplus \mathbb{Z}^r$

- $E(\mathbb{Q})_{\text{tor}}$: sí que hay algoritmos para calcularlos
- Calcular r puntos de orden infinito independientes?
- Calcular el rango r?

Curvas elípticas sobre $\mathbb{Q}$

- E curva elíptica con coeficientes racionales

$$E\colon\ y^2 + b_1 xy + b_3 y = x^3 + b_2 x^2 + b_4 x + b_6, \quad b_i \in \mathbb{Z}$$

- $E(\mathbb{Q}) = \{\text{soluciones } (x, y) \in \mathbb{Q}^2\}$

Problema

Existe algun algoritmo para calcular $E(\mathbb{Q})$?

Teorema de Mordell–Weil

$E(\mathbb{Q})$ tiene estructura de grupo y $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tor}} \oplus \mathbb{Z}^r$

- $E(\mathbb{Q})_{\text{tor}}$: sí que hay algoritmos para calcularlos
- Calcular r puntos de orden infinito independientes?
- Calcular el rango r?
  - Està relacionado con la Conjetura de Birch y Swinnerton–Dyer

La conjetura de Birch y Swinnerton–Dyer (BSD)

Figura: Birch y Swinnerton–Dyer

La conjetura de Birch y Swinnerton–Dyer (BSD)

Función L de Hasse–Weil

Es una función analítica asociada a E:

$$L(E/\mathbb{Q}, s) = \sum_{n=1}^{\infty} a_n n^{-s}, \qquad a_p = p - \#\text{soluciones de } E \pmod{p}$$

La conjetura de Birch y Swinnerton–Dyer (BSD)

Función L de Hasse–Weil

Es una función analítica asociada a E:

$$L(E/\mathbb{Q}, s) = \sum_{n=1}^{\infty} a_n n^{-s}, \qquad a_p = p - \#\text{soluciones de } E \pmod{p}$$

Conjetura Birch–Swinnerton-Dyer (1965)

$$r(E/\mathbb{Q}) = \operatorname{ord}_{s=1} L(E/\mathbb{Q}, s) = r_{\text{an}}(E/\mathbb{Q})$$

La conjetura de Birch y Swinnerton–Dyer (BSD)

Función L de Hasse–Weil

Es una función analítica asociada a E:

$$L(E/\mathbb{Q}, s) = \sum_{n=1}^{\infty} a_n n^{-s}, \quad a_p = p - \#\text{soluciones de } E \pmod{p}$$

Conjetura Birch–Swinnerton-Dyer (1965)

$$r(E/\mathbb{Q}) = \operatorname{ord}_{s=1} L(E/\mathbb{Q}, s) = r_{\text{an}}(E/\mathbb{Q})$$

Teorema (Gross–Zagier 1986, Kolyvagin 1989)

Si $\operatorname{ord}_{s=1} L(E/\mathbb{Q}, s) \leq 1$ entonces $r(E/\mathbb{Q}) = \operatorname{ord}_{s=1} L(E/\mathbb{Q}, s)$

La conjetura de Birch y Swinnerton–Dyer (BSD)

Función L de Hasse–Weil

Es una función analítica asociada a E:

$$L(E/\mathbb{Q}, s) = \sum_{n=1}^{\infty} a_n n^{-s}, \quad a_p = p - \#\text{soluciones de } E \pmod{p}$$

Conjetura Birch–Swinnerton-Dyer (1965)

$$r(E/\mathbb{Q}) = \operatorname{ord}_{s=1} L(E/\mathbb{Q}, s) = r_{\text{an}}(E/\mathbb{Q})$$

Teorema (Gross–Zagier 1986, Kolyvagin 1989)

Si $\operatorname{ord}_{s=1} L(E/\mathbb{Q}, s) \leq 1$ entonces $r(E/\mathbb{Q}) = \operatorname{ord}_{s=1} L(E/\mathbb{Q}, s)$

Problema

Si E tiene rango analítico 1, existe algun algoritmo eficiente para calcular un punto de orde infinito?

La conjetura de Birch y Swinnerton–Dyer (BSD)

Función L de Hasse–Weil

Es una función analítica asociada a E:

$$L(E/\mathbb{Q}, s) = \sum_{n=1}^{\infty} a_n n^{-s}, \quad a_p = p - \#\text{soluciones de } E \pmod{p}$$

Conjetura Birch–Swinnerton-Dyer (1965)

$$r(E/\mathbb{Q}) = \operatorname{ord}_{s=1} L(E/\mathbb{Q}, s) = r_{\text{an}}(E/\mathbb{Q})$$

Teorema (Gross–Zagier 1986, Kolyvagin 1989)

Si $\operatorname{ord}_{s=1} L(E/\mathbb{Q}, s) \leq 1$ entonces $r(E/\mathbb{Q}) = \operatorname{ord}_{s=1} L(E/\mathbb{Q}, s)$

Problema

Si E tiene rango analítico 1, existe algun algoritmo eficiente para calcular un punto de orde infinito?

- Respuesta: sí, el método de los puntos de Heegner
  - ingrediente fundamental del teorema de Gross–Zagier y Kolyvagin

Índex

Puntos de Heegner

Figura: Kurt Heegner

Puntos de Heegner

$K = \mathbb{Q}(\sqrt{-D})$ cuerpo cuadrático imaginario ($h(K) = 1$)

Método para construir puntos en $E(K)$

Puntos de Heegner

$K = \mathbb{Q}(\sqrt{-D})$ cuerpo cuadrático imaginario ($h(K) = 1$)

Método para construir puntos en $E(K)$

- Construcción geométrica

Puntos de Heegner

$K = \mathbb{Q}(\sqrt{-D})$ cuerpo cuadrático imaginario ($h(K) = 1$)

Método para construir puntos en $E(K)$

- Construcción geométrica
  - Uniformización modular (Wiles et. al): $X_0(N) \longrightarrow E$

Puntos de Heegner

$K = \mathbb{Q}(\sqrt{-D})$ cuerpo cuadrático imaginario ($h(K) = 1$)

Método para construir puntos en $E(K)$

- Construcción geométrica
  - Uniformización modular (Wiles et. al): $X_0(N) \longrightarrow E$
  - Los puntos $X_0(N)$ parametrizan curvas elípticas

Puntos de Heegner

$K = \mathbb{Q}(\sqrt{-D})$ cuerpo cuadrático imaginario ($h(K) = 1$)

Método para construir puntos en $E(K)$

- Construcción geométrica
  - Uniformización modular (Wiles et. al): $X_0(N) \longrightarrow E$
  - Los puntos $X_0(N)$ parametrizan curvas elípticas
  - Puntos CM en $X_0(N)$ (corresponden a curvas con CM por K)

Puntos de Heegner

$K = \mathbb{Q}(\sqrt{-D})$ cuerpo cuadrático imaginario ($h(K) = 1$)

Método para construir puntos en $E(K)$

- Construcción geométrica
  - Uniformización modular (Wiles et. al): $X_0(N) \longrightarrow E$
  - Los puntos $X_0(N)$ parametrizan curvas elípticas
  - Puntos CM en $X_0(N)$ (corresponden a curvas con CM por K)
  - Teoría de la multiplicación compleja: los puntos CM $\in X_0(N)(K)$

Puntos de Heegner

$K = \mathbb{Q}(\sqrt{-D})$ cuerpo cuadrático imaginario ($h(K) = 1$)

Método para construir puntos en $E(K)$

- Construcción geométrica
  - Uniformización modular (Wiles et. al): $X_0(N) \longrightarrow E$
  - Los puntos $X_0(N)$ parametrizan curvas elípticas
  - Puntos CM en $X_0(N)$ (corresponden a curvas con CM por K)
  - Teoría de la multiplicación compleja: los puntos CM $\in X_0(N)(K)$
  - Su imagen en E son los puntos de Heegner

Puntos de Heegner

$K = \mathbb{Q}(\sqrt{-D})$ cuerpo cuadrático imaginario ($h(K) = 1$)

Método para construir puntos en $E(K)$

- Construcción geométrica
  - Uniformización modular (Wiles et. al): $X_0(N) \longrightarrow E$
  - Los puntos $X_0(N)$ parametrizan curvas elípticas
  - Puntos CM en $X_0(N)$ (corresponden a curvas con CM por K)
  - Teoría de la multiplicación compleja: los puntos CM $\in X_0(N)(K)$
  - Su imagen en E son los puntos de Heegner
- Fórmula explícita

Puntos de Heegner

$K = \mathbb{Q}(\sqrt{-D})$ cuerpo cuadrático imaginario ($h(K) = 1$)

Método para construir puntos en $E(K)$

- Construcción geométrica
  - Uniformización modular (Wiles et. al): $X_0(N) \longrightarrow E$
  - Los puntos $X_0(N)$ parametrizan curvas elípticas
  - Puntos CM en $X_0(N)$ (corresponden a curvas con CM por K)
  - Teoría de la multiplicación compleja: los puntos CM $\in X_0(N)(K)$
  - Su imagen en E son los puntos de Heegner
- Fórmula explícita
  - $X_0(N)(\mathbb{C}) = \Gamma_0(N)\backslash\mathcal{H} \longrightarrow E(\mathbb{C}) \simeq \mathbb{C}/\Lambda_E$

Puntos de Heegner

$K = \mathbb{Q}(\sqrt{-D})$ cuerpo cuadrático imaginario ($h(K) = 1$)

Método para construir puntos en $E(K)$

- Construcción geométrica
  - Uniformización modular (Wiles et. al): $X_0(N) \longrightarrow E$
  - Los puntos $X_0(N)$ parametrizan curvas elípticas
  - Puntos CM en $X_0(N)$ (corresponden a curvas con CM por K)
  - Teoría de la multiplicación compleja: los puntos CM $\in X_0(N)(K)$
  - Su imagen en E son los puntos de Heegner
- Fórmula explícita
  - $X_0(N)(\mathbb{C}) = \Gamma_0(N)\backslash\mathcal{H} \longrightarrow E(\mathbb{C}) \simeq \mathbb{C}/\Lambda_E$
  - Puntos CM: $\tau \in \mathcal{H} \cap K$

Puntos de Heegner

$K = \mathbb{Q}(\sqrt{-D})$ cuerpo cuadrático imaginario ($h(K) = 1$)

Método para construir puntos en $E(K)$

- Construcción geométrica
  - Uniformización modular (Wiles et. al): $X_0(N) \longrightarrow E$
  - Los puntos $X_0(N)$ parametrizan curvas elípticas
  - Puntos CM en $X_0(N)$ (corresponden a curvas con CM por K)
  - Teoría de la multiplicación compleja: los puntos CM $\in X_0(N)(K)$
  - Su imagen en E son los puntos de Heegner
- Fórmula explícita
  - $X_0(N)(\mathbb{C}) = \Gamma_0(N)\backslash\mathcal{H} \longrightarrow E(\mathbb{C}) \simeq \mathbb{C}/\Lambda_E$
  - Puntos CM: $\tau \in \mathcal{H} \cap K$
  - $f(z) = \sum_{n\geq 1} a_n e^{2\pi i n z} \rightsquigarrow f(z)dz$ diferencial en $\Gamma_0(N)\backslash\mathcal{H}$

Puntos de Heegner

$K = \mathbb{Q}(\sqrt{-D})$ cuerpo cuadrático imaginario ($h(K) = 1$)

Método para construir puntos en $E(K)$

- Construcción geométrica
  - Uniformización modular (Wiles et. al): $X_0(N) \longrightarrow E$
  - Los puntos $X_0(N)$ parametrizan curvas elípticas
  - Puntos CM en $X_0(N)$ (corresponden a curvas con CM por K)
  - Teoría de la multiplicación compleja: los puntos CM $\in X_0(N)(K)$
  - Su imagen en E son los puntos de Heegner
- Fórmula explícita
  - $X_0(N)(\mathbb{C}) = \Gamma_0(N)\backslash\mathcal{H} \longrightarrow E(\mathbb{C}) \simeq \mathbb{C}/\Lambda_E$
  - Puntos CM: $\tau \in \mathcal{H} \cap K$
  - $f(z) = \sum_{n\geq 1} a_n e^{2\pi i n z} \rightsquigarrow f(z)dz$ diferencial en $\Gamma_0(N)\backslash\mathcal{H}$

Punto de Heegner

$J_\tau = \int_\tau^\infty 2\pi i f(z)dz \in \mathbb{C}/\Lambda_f$

Puntos de Heegner

$K = \mathbb{Q}(\sqrt{-D})$ cuerpo cuadrático imaginario ($h(K) = 1$)

Método para construir puntos en $E(K)$

- Construcción geométrica
  - Uniformización modular (Wiles et. al): $X_0(N) \longrightarrow E$
  - Los puntos $X_0(N)$ parametrizan curvas elípticas
  - Puntos CM en $X_0(N)$ (corresponden a curvas con CM por K)
  - Teoría de la multiplicación compleja: los puntos CM $\in X_0(N)(K)$
  - Su imagen en E son los puntos de Heegner
- Fórmula explícita
  - $X_0(N)(\mathbb{C}) = \Gamma_0(N)\backslash\mathcal{H} \longrightarrow E(\mathbb{C}) \simeq \mathbb{C}/\Lambda_E$
  - Puntos CM: $\tau \in \mathcal{H} \cap K$
  - $f(z) = \sum_{n\geq 1} a_n e^{2\pi i n z} \rightsquigarrow f(z)dz$ diferencial en $\Gamma_0(N)\backslash\mathcal{H}$

Punto de Heegner

$J_\tau = \int_\tau^\infty 2\pi i f(z)dz \in \mathbb{C}/\Lambda_f \simeq \mathbb{C}/\Lambda_E$

Puntos de Heegner

$K = \mathbb{Q}(\sqrt{-D})$ cuerpo cuadrático imaginario ($h(K) = 1$)

Método para construir puntos en $E(K)$

- Construcción geométrica
  - Uniformización modular (Wiles et. al): $X_0(N) \longrightarrow E$
  - Los puntos $X_0(N)$ parametrizan curvas elípticas
  - Puntos CM en $X_0(N)$ (corresponden a curvas con CM por K)
  - Teoría de la multiplicación compleja: los puntos CM $\in X_0(N)(K)$
  - Su imagen en E son los puntos de Heegner
- Fórmula explícita
  - $X_0(N)(\mathbb{C}) = \Gamma_0(N)\backslash\mathcal{H} \longrightarrow E(\mathbb{C}) \simeq \mathbb{C}/\Lambda_E$
  - Puntos CM: $\tau \in \mathcal{H} \cap K$
  - $f(z) = \sum_{n\geq 1} a_n e^{2\pi i n z} \rightsquigarrow f(z)dz$ diferencial en $\Gamma_0(N)\backslash\mathcal{H}$

Punto de Heegner

$J_\tau = \int_\tau^\infty 2\pi i f(z)dz \in \mathbb{C}/\Lambda_f \simeq \mathbb{C}/\Lambda_E \rightsquigarrow J_\tau \in E(K)$

Un ejemplo extremo (M. Watkins)

$$y^2 + y = x^3 - 5115523309x - 140826120488927 \quad (N = 66157667)$$

Un ejemplo extremo (M. Watkins)

$$y^2 + y = x^3 - 5115523309x - 140826120488927 \quad (N = 66157667)$$

el numerador de la coordenada x del punto es:

Un ejemplo extremo (M. Watkins)

$$y^2 + y = x^3 - 5115523309x - 140826120488927 \quad (N = 66157667)$$

el numerador de la coordenada x del punto es:

600 million terms of the L-series. This takes less than a day. We list the x-coordinate of the point on the original elliptic curve. It has numerator

3677705371866775066140056423418271700879322694922855847262187700616535463492710158053651343703267430611411306464500052886704651998399766478840791915307861741507273933802628157325092479708268760217101755385871816780548765478502284415627682847192752681899094962659937870630036760359293577021806237483971074931228416346507852381696883227650072039964481597215995993299744934117106289850389364006552497835877740257534533113775202882210048356163645919345794812074571029660897173224370337701056165735008590640297090298709121506266697266461993201825397369999550868142294312756322177410730532828064759604975369242350993568030726937049911607264109782746847951283794119298941214490794330902986582991229569401523519938742746376107190770204010513818349012786637889254711059455555173810904911927619899031855149292325338589831979737026402711049742594116000380601480839982975557506035851728035645241044229165029649347049289119188596869401159325131363345962579503132339847275422440094553824705189225653677459512863117911721838552934309124508134493366437408093924362039749911907416973504142322111757058584200725022632116164720164998641729522677460525999499077942125820428879526063735692685991018516862938796047597323986537154171248316943796373217191993996993714654629536884396057924790938647656663281596178145722116098216500930333824321806726937018190136190556573208807048355335567078793126656928657859036779350593274598717397308807240343018677394437498418094567158841937203289014615526598826284058422097567571678166621399450818646421085335959899757162592592401528340509406544796171476859225008569444498220453860921224090969785448172188478976405134778065983291776042463808123777390491844755507773416209859765703930378802827649670195524084007307548226764414817153853440019798322326524148883358655673772143604560032969616681774819448090662574425967723478296641269729319041016852811289447800746467967609424309596170222574798740894035649650388853798178669200489298145202684936775070590737659026716380873664884967028363262685745931232451074203488781017631238933476570202755912488242478005942708620520821859733932900091898676772594580806760650987034535395255769756395437005076256407298723407894063143944684005844559206833619762001218344307512339014732284974905619980784862510749935288713187974033480873704269009975564425770812549105721851078566051398773310150428421211060806907435781732684894009956898312621953947967012358414547752897081097091795744203697684046066255663201242292760126759871266004516377432961917272040217147083563399987612420595275792033855676991823368254862159558450043808051481533297270035287382247038279293223946385070118082306958987268603396924054403103857444058848605587415400517670032631121206127732481340391088277796488544415738156553014768406246154666005139690428085145098272500791416214774673484501826722500527091164944262537169595848931680754096774712860490572746224094031187043204526107239201079603468297522895106598567437015083348797875364162797693968819804139548885751282687152237078260358705230284426203064493684250614282879918107733796207067250003823959412935677624093236047038637365577326399589008804507786011973155927731073034706536557461443806622707622411087809371872157210456836892493613836792026761820382217165481998924123604782787923229739171920575447007099501678380795077013113325989801385729993920818301654424251339564606876820121928372246213399859213282792511168043953443839793901139974194479300297566097664539199384651908436188732428818373302383043868859427937893841888014266685177616605644783704135794931830750265686335934066565240944044948213005591997128985560760260399214278635912634351586762354869354021530746199899289958255459763210830963856929696480004698307273623848314901471460089605655202964274799141906345474914205956427429825465492589386640495514690333002447574616354371499624965242017117105423172633649354158697143177894405148105963373839941141857432381177094972972684361267292500063135565983416420055444131545100343345246620470712381166362366283729686294806175875992863176366198518561580188620577072103200630414486778734705831639229567158009165587208720948591328693012885864044258912545426858039748457192101231887231162489831761560762817646009744133632354903182823596563627795082732808754793951111237421643658420337924845012264740609403517113074066372354767593988595936388113589303510201838944421274614625032834824261067352402237899497839202008881472197450206269281573668922975906582209394279531870534527559898942633523593550560531141130156032119226943086173374354440290858649730535360909431214933202522528717109214492959330016065810287623144179288466644062270234670421375245637257444956397921578240656693788532945871994541770838871930542220307771671498466518108722622109421676741544945695403509866953167277628280232464839215003474048896968037544660029755740065581270139083249903212572230417942249795467100700393944310325009677179182109970943346807330144468396122825088243240736795841228512083604591663154848919522994493400258965092989359393577217235439331087432419973874470183959253201676376403284079570698454395013812346058674950034020167246264008553696365211550091471762459041490692254386469285490723376533487049319017648474397724320252756489646813872102340708493063301919079380412396115446240832583481366372132300849060835262136832315110529033675038574379205089313052831433794239306013691545725306772788620666388842502217916471256382895646253098356792949949334662297749490359172234518897506294190741540074088 1

Una pregunta natural: y si K es cuadrático real?

Una pregunta natural: y si K es cuadrático real?

Problema

- $E/\mathbb{Q}$ curva elíptica
- Si K es un cuadrático real tal que $\mathrm{ord}_{s=1} L(E/K, s) = 1$
  - algoritmo para calcular puntos de orden infinito en $E(K)$?

Una pregunta natural: y si K es cuadrático real?

Problema

- $E/\mathbb{Q}$ curva elíptica
- Si K es un cuadrático real tal que $\mathrm{ord}_{s=1} L(E/K, s) = 1$
  - algoritmo para calcular puntos de orden infinito en $E(K)$?

- Idea: buscar un análogo del método de puntos de Heegner

Una pregunta natural: y si K es cuadrático real?

Problema

- $E/\mathbb{Q}$ curva elíptica
- Si K es un cuadrático real tal que $\mathrm{ord}_{s=1} L(E/K, s) = 1$
  - algoritmo para calcular puntos de orden infinito en $E(K)$?

- Idea: buscar un análogo del método de puntos de Heegner
- Puntos de Darmon

Una pregunta natural: y si K es cuadrático real?

Problema

- $E/\mathbb{Q}$ curva elíptica
- Si K es un cuadrático real tal que $\mathrm{ord}_{s=1} L(E/K, s) = 1$
  - algoritmo para calcular puntos de orden infinito en $E(K)$?

- Idea: buscar un análogo del método de puntos de Heegner
- Puntos de Darmon (a.k.a. Puntos de Stark–Heegner)

Puntos de Heegner

K cuerpo cuadrático imaginario

Método para construir puntos de orden infinito en $E(K)$

- Construcción geométrica (demuestra algebraicidad)
  - Uniformización modular $X_0(N) \longrightarrow E$
  - Teoría de la multiplicación compleja
- Fórmula explícita (sirve para calcularlos)
  - $J_\tau = \int_\tau^\infty 2\pi i f(z) dz \in \mathbb{C}/\Lambda = E(\mathbb{C})$

Puntos de ~~Heegner~~ Darmon

K cuerpo cuadrático imaginario

Método para construir puntos de orden infinito en $E(K)$

- Construcción geométrica (demuestra algebraicidad)
  - Uniformización modular $X_0(N) \longrightarrow E$
  - Teoría de la multiplicación compleja
- Fórmula explícita (sirve para calcularlos)
  - $J_\tau = \int_\tau^\infty 2\pi i f(z) dz \in \mathbb{C}/\Lambda = E(\mathbb{C})$

Puntos de ~~Heegner~~ Darmon

K cuerpo cuadrático ~~imaginario~~ real

Método para construir puntos de orden infinito en $E(K)$

- Construcción geométrica (demuestra algebraicidad)
  - Uniformización modular $X_0(N) \longrightarrow E$
  - Teoría de la multiplicación compleja
- Fórmula explícita (sirve para calcularlos)
  - $J_\tau = \int_\tau^\infty 2\pi i f(z) dz \in \mathbb{C}/\Lambda = E(\mathbb{C})$

Puntos de ~~Heegner~~ Darmon

K cuerpo cuadrático ~~imaginario~~ real

Método para construir puntos de orden infinito en $E(K)$

- Construcción geométrica (demuestra algebraicidad)
  - Uniformización modular $X_0(N) \longrightarrow E$
  - Teoría de la multiplicación ~~compleja~~ real
- Fórmula explícita (sirve para calcularlos)
  - $J_\tau = \int_\tau^\infty 2\pi i f(z) dz \in \mathbb{C}/\Lambda = E(\mathbb{C})$

Puntos de ~~Heegner~~ Darmon

K cuerpo cuadrático ~~imaginario~~ real

Método para construir puntos de orden infinito en $E(K)$

- Construcción geométrica (demuestra algebraicidad)
  - Uniformización modular $X_0(N) \longrightarrow E$
  - Teoría de la multiplicación ~~compleja~~ real $\rightsquigarrow$ No existe!
- Fórmula explícita (sirve para calcularlos)
  - $J_\tau = \int_\tau^\infty 2\pi i f(z) dz \in \mathbb{C}/\Lambda = E(\mathbb{C})$

Puntos de ~~Heegner~~ Darmon

K cuerpo cuadrático ~~imaginario~~ real

Método para construir puntos de orden infinito en $E(K)$

- ~~Construcción geométrica (demuestra algebraicidad)~~
  - Uniformización modular $X_0(N) \longrightarrow E$
  - Teoría de la multiplicación ~~compleja~~ real $\rightsquigarrow$ No existe!
- Fórmula explícita (sirve para calcularlos)
  - $J_\tau = \int_\tau^\infty 2\pi i f(z) dz \in \mathbb{C}/\Lambda = E(\mathbb{C})$

Puntos de ~~Heegner~~ Darmon

K cuerpo cuadrático ~~imaginario~~ real

Método para construir puntos de orden infinito en $E(K)$

- ~~Construcción geométrica (demuestra algebraicidad)~~
  - Uniformización modular $X_0(N) \longrightarrow E$
  - Teoría de la multiplicación ~~compleja~~ real $\rightsquigarrow$ No existe!
- Fórmula explícita (sirve para calcularlos)
  - $J_\tau = \int_\tau^\infty 2\pi i f(z) dz \in \mathbb{C}/\Lambda = E(\mathbb{C})$

Puntos de ~~Heegner~~ Darmon

K cuerpo cuadrático ~~imaginario~~ real

Método para construir puntos de orden infinito en $E(K)$

- ~~Construcción geométrica (demuestra algebraicidad)~~
  - Uniformización modular $X_0(N) \longrightarrow E$
  - Teoría de la multiplicación ~~compleja~~ real $\rightsquigarrow$ No existe!
- Fórmula explícita (sirve para calcularlos)
  - $J_\tau = \int_\tau^\infty 2\pi i f(z) dz \in \mathbb{C}/\Lambda = E(\mathbb{C})$
  - Ingredientes

$$\left.\begin{array}{r} E \rightsquigarrow \omega_E \text{ 1-forma} \\ \tau \in K \cap \mathcal{H} \rightsquigarrow \Delta_\tau \text{ 1-cadena} \end{array}\right\} \longrightarrow J_\tau = \int_{\Delta_\tau} \omega_E \in \mathbb{C}/\Lambda_E$$

Puntos de ~~Heegner~~ Darmon

K cuerpo cuadrático ~~imaginario~~ real

Método para construir puntos de orden infinito en $E(K)$

- ~~Construcción geométrica (demuestra algebraicidad)~~
  - Uniformización modular $X_0(N) \longrightarrow E$
  - Teoría de la multiplicación ~~compleja~~ real $\rightsquigarrow$ No existe!
- Fórmula explícita (sirve para calcularlos)
  - $J_\tau = \int_\tau^\infty 2\pi i f(z) dz \in \mathbb{C}/\Lambda = E(\mathbb{C})$
  - Ingredientes

$$\left.\begin{array}{r} E \rightsquigarrow \omega_E \text{ 1-forma} \\ \tau \in K \cap \mathcal{H} \rightsquigarrow \Delta_\tau \text{ 1-cadena} \end{array}\right\} \longrightarrow J_\tau = \int_{\Delta_\tau} \omega_E \in \mathbb{C}/\Lambda_E$$

  - Filosofía: Buscar análogos de ω_E y Δ_τ

Puntos de ~~Heegner~~ Darmon

K cuerpo cuadrático ~~imaginario~~ real

Método para construir puntos de orden infinito en $E(K)$

- ~~Construcción geométrica (demuestra algebraicidad)~~
  - Uniformización modular $X_0(N) \longrightarrow E$
  - Teoría de la multiplicación ~~compleja~~ real $\rightsquigarrow$ No existe!
- Fórmula explícita (sirve para calcularlos)
  - $J_\tau = \int_\tau^\infty 2\pi i f(z) dz \in \mathbb{C}/\Lambda = E(\mathbb{C})$
  - Ingredientes

$$\left.\begin{array}{r} E \rightsquigarrow \omega_E \text{ 1-forma} \\ \tau \in K \cap \mathcal{H} \rightsquigarrow \Delta_\tau \text{ 1-cadena} \end{array}\right\} \longrightarrow J_\tau = \int_{\Delta_\tau} \omega_E \in \mathbb{C}/\Lambda_E$$

  - Filosofía: Buscar análogos de ω_E y Δ_τ
- Obstrucción: K real $\Rightarrow K \cap \mathcal{H} = \emptyset$!

Índex

Puntos de Darmon

- Idea: sustituir $\mathcal{H}$ por $\mathcal{H}_p$ (el semiplano p-adico)

Puntos de Darmon

- Idea: sustituir $\mathcal{H}$ por $\mathcal{H}_p$ (el semiplano p-adico)
  - $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}_p}}$ (análogo de $\mathbb{C}$)

Puntos de Darmon

- Idea: sustituir $\mathcal{H}$ por $\mathcal{H}_p$ (el semiplano p-adico)
  - $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}_p}}$ (análogo de $\mathbb{C}$)
  - $\mathcal{H}_p = \mathbb{C}_p \setminus \mathbb{Q}_p$ (análogo de $\mathbb{C} \setminus \mathbb{R} = \mathcal{H}^{\pm}$)

Puntos de Darmon

- Idea: sustituir $\mathcal{H}$ por $\mathcal{H}_p$ (el semiplano p-adico)
  - $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}_p}}$ (análogo de $\mathbb{C}$)
  - $\mathcal{H}_p = \mathbb{C}_p \setminus \mathbb{Q}_p$ (análogo de $\mathbb{C} \setminus \mathbb{R} = \mathcal{H}^{\pm}$)
  - p es inerte en $K \Rightarrow K \cap \mathcal{H}_p \neq \emptyset$

Puntos de Darmon

- Idea: sustituir $\mathcal{H}$ por $\mathcal{H}_p$ (el semiplano p-adico)
  - $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}_p}}$ (análogo de $\mathbb{C}$)
  - $\mathcal{H}_p = \mathbb{C}_p \setminus \mathbb{Q}_p$ (análogo de $\mathbb{C} \setminus \mathbb{R} = \mathcal{H}^{\pm}$)
  - p es inerte en $K \Rightarrow K \cap \mathcal{H}_p \neq \emptyset$
  - $\Omega^1_{\mathcal{H}_p} =$ diferenciales rígidas analíticas en $\mathcal{H}_p$

Puntos de Darmon

- Idea: sustituir $\mathcal{H}$ por $\mathcal{H}_p$ (el semiplano p-adico)
  - $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}_p}}$ (análogo de $\mathbb{C}$)
  - $\mathcal{H}_p = \mathbb{C}_p \setminus \mathbb{Q}_p$ (análogo de $\mathbb{C} \setminus \mathbb{R} = \mathcal{H}^{\pm}$)
  - p es inerte en $K \Rightarrow K \cap \mathcal{H}_p \neq \emptyset$
  - $\Omega^1_{\mathcal{H}_p}$ = diferenciales rígidas analíticas en $\mathcal{H}_p$
  - Integral de Coleman (análogo de la integral de línea)

$$\omega \in \Omega_{\mathcal{H}_p},\ \tau_1, \tau_2 \in \mathcal{H}_p,\ \rightsquigarrow\ \int_{\tau_1}^{\tau_2} \omega \in \mathbb{C}_p$$

Puntos de Darmon

- Idea: sustituir $\mathcal{H}$ por $\mathcal{H}_p$ (el semiplano p-adico)
  - $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}_p}}$ (análogo de $\mathbb{C}$)
  - $\mathcal{H}_p = \mathbb{C}_p \setminus \mathbb{Q}_p$ (análogo de $\mathbb{C} \setminus \mathbb{R} = \mathcal{H}^{\pm}$)
  - p es inerte en $K \Rightarrow K \cap \mathcal{H}_p \neq \emptyset$
  - $\Omega^1_{\mathcal{H}_p}$ = diferenciales rígidas analíticas en $\mathcal{H}_p$
  - Integral de Coleman (análogo de la integral de línea)

$$\omega \in \Omega_{\mathcal{H}_p},\ \tau_1, \tau_2 \in \mathcal{H}_p,\ \rightsquigarrow\ \int_{\tau_1}^{\tau_2} \omega \in \mathbb{C}_p$$

- Descripción local de E:
  - Si $p \mid N$: uniformización de Tate

$$E(\mathbb{C}_p) \simeq \mathbb{C}_p^{\times} / < q_E >$$

Puntos de Darmon

- Idea: sustituir $\mathcal{H}$ por $\mathcal{H}_p$ (el semiplano p-adico)
  - $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}_p}}$ (análogo de $\mathbb{C}$)
  - $\mathcal{H}_p = \mathbb{C}_p \setminus \mathbb{Q}_p$ (análogo de $\mathbb{C} \setminus \mathbb{R} = \mathcal{H}^{\pm}$)
  - p es inerte en $K \Rightarrow K \cap \mathcal{H}_p \neq \emptyset$
  - $\Omega^1_{\mathcal{H}_p}$ = diferenciales rígidas analíticas en $\mathcal{H}_p$
  - Integral de Coleman (análogo de la integral de línea)

$$\omega \in \Omega_{\mathcal{H}_p},\ \tau_1, \tau_2 \in \mathcal{H}_p,\ \rightsquigarrow\ \int_{\tau_1}^{\tau_2} \omega \in \mathbb{C}_p$$

  - Integral de Coleman multiplicativa: si ω tiene residuos en $\mathbb{Z}$

$$\oint_{\tau_1}^{\tau_2} \omega \in \mathbb{C}_p^{\times}$$

- Descripción local de E:
  - Si $p \mid N$: uniformización de Tate

$$E(\mathbb{C}_p) \simeq \mathbb{C}_p^{\times} / < q_E >$$

Puntos de Darmon, à la Greenberg

Puntos de Darmon, à la Greenberg

- $E/\mathbb{Q}$ curva de conductor $\square \nmid N$. Supongamos que $N = pMD$
  - D es producto de un número par de primos inertes en K
  - M es producto de primos que descomponen o ramifican en K
  - (siempre se cumple si $\mathrm{ord}_{s=1} L(E/K, 1) = 1$)

Puntos de Darmon, à la Greenberg

- $E/\mathbb{Q}$ curva de conductor $\square \nmid N$. Supongamos que $N = pMD$
  - D es producto de un número par de primos inertes en K
  - M es producto de primos que descomponen o ramifican en K
  - (siempre se cumple si $\mathrm{ord}_{s=1} L(E/K, 1) = 1$)
- $B/\mathbb{Q}$ algebra de cuaterniones discriminante D ($= \mathrm{M}_2(\mathbb{Q})$ si $D = 1$)
- B actua en $\mathcal{H}_p$ via $B \otimes \mathbb{Q}_p \simeq \mathrm{M}_2(\mathbb{Q}_p)$
- $\Gamma \subset B^\times$ subgrupo de congruencia de nivel M

Puntos de Darmon, à la Greenberg

- $E/\mathbb{Q}$ curva de conductor $\square \nmid N$. Supongamos que $N = pMD$
  - D es producto de un número par de primos inertes en K
  - M es producto de primos que descomponen o ramifican en K
  - (siempre se cumple si $\mathrm{ord}_{s=1} L(E/K, 1) = 1$)
- $B/\mathbb{Q}$ algebra de cuaterniones discriminante D ($= \mathrm{M}_2(\mathbb{Q})$ si $D = 1$)
- B actua en $\mathcal{H}_p$ via $B \otimes \mathbb{Q}_p \simeq \mathrm{M}_2(\mathbb{Q}_p)$
- $\Gamma \subset B^\times$ subgrupo de congruencia de nivel M

Construcción (Darmon $D = 1$ (2001), Greenberg $D > 1$ (2011))

$$\left.\begin{aligned} E &\rightsquigarrow \omega_E \in H^1(\Gamma, \Omega^1_{\mathcal{H}_p}) \\ \tau \in K \cap \mathcal{H}_p &\rightsquigarrow \Delta_\tau \in C_1(\Gamma, \mathrm{Div}^0 \mathcal{H}_p) \end{aligned}\right\}$$

Puntos de Darmon, à la Greenberg

- $E/\mathbb{Q}$ curva de conductor $\square \nmid N$. Supongamos que $N = pMD$
  - D es producto de un número par de primos inertes en K
  - M es producto de primos que descomponen o ramifican en K
  - (siempre se cumple si $\mathrm{ord}_{s=1} L(E/K, 1) = 1$)
- $B/\mathbb{Q}$ algebra de cuaterniones discriminante D ($= \mathrm{M}_2(\mathbb{Q})$ si $D = 1$)
- B actua en $\mathcal{H}_p$ via $B \otimes \mathbb{Q}_p \simeq \mathrm{M}_2(\mathbb{Q}_p)$
- $\Gamma \subset B^\times$ subgrupo de congruencia de nivel M

Construcción (Darmon $D = 1$ (2001), Greenberg $D > 1$ (2011))

$$\left.\begin{array}{r} E \rightsquigarrow \omega_E \in H^1(\Gamma, \Omega^1_{\mathcal{H}_p}) \\ \tau \in K \cap \mathcal{H}_p \rightsquigarrow \Delta_\tau \in C_1(\Gamma, \mathrm{Div}^0 \mathcal{H}_p) \end{array}\right\} \to J_\tau = \int\!\!\!\!\!\!\diagup_{\Delta_\tau} \omega_E \in \mathbb{C}_p^\times / \langle q \rangle$$

Puntos de Darmon, à la Greenberg

- $E/\mathbb{Q}$ curva de conductor $\square \nmid N$. Supongamos que $N = pMD$
  - D es producto de un número par de primos inertes en K
  - M es producto de primos que descomponen o ramifican en K
  - (siempre se cumple si $\mathrm{ord}_{s=1} L(E/K, 1) = 1$)
- $B/\mathbb{Q}$ algebra de cuaterniones discriminante D ($= \mathrm{M}_2(\mathbb{Q})$ si $D = 1$)
- B actua en $\mathcal{H}_p$ via $B \otimes \mathbb{Q}_p \simeq \mathrm{M}_2(\mathbb{Q}_p)$
- $\Gamma \subset B^\times$ subgrupo de congruencia de nivel M

Construcción (Darmon $D = 1$ (2001), Greenberg $D > 1$ (2011))

$$\left.\begin{array}{r} E \rightsquigarrow \omega_E \in H^1(\Gamma, \Omega^1_{\mathcal{H}_p}) \\ \tau \in K \cap \mathcal{H}_p \rightsquigarrow \Delta_\tau \in C_1(\Gamma, \mathrm{Div}^0 \mathcal{H}_p) \end{array}\right\} \to J_\tau = \int\!\!\!\!\!\!\diagup_{\Delta_\tau} \omega_E \in \mathbb{C}_p^\times / \langle q \rangle$$

- $\mathbb{C}_p^\times / \langle q \rangle \simeq \mathbb{C}_p^\times / \langle q_E \rangle$ (Greenberg–Dasgupta, Longo–Rotger–Vigni)

Puntos de Darmon, à la Greenberg

- $E/\mathbb{Q}$ curva de conductor $\square \nmid N$. Supongamos que $N = pMD$
  - D es producto de un número par de primos inertes en K
  - M es producto de primos que descomponen o ramifican en K
  - (siempre se cumple si $\mathrm{ord}_{s=1} L(E/K, 1) = 1$)
- $B/\mathbb{Q}$ algebra de cuaterniones discriminante D ($= \mathrm{M}_2(\mathbb{Q})$ si $D = 1$)
- B actua en $\mathcal{H}_p$ via $B \otimes \mathbb{Q}_p \simeq \mathrm{M}_2(\mathbb{Q}_p)$
- $\Gamma \subset B^\times$ subgrupo de congruencia de nivel M

Construcción (Darmon $D = 1$ (2001), Greenberg $D > 1$ (2011))

$$\left.\begin{array}{r} E \rightsquigarrow \omega_E \in H^1(\Gamma, \Omega^1_{\mathcal{H}_p}) \\ \tau \in K \cap \mathcal{H}_p \rightsquigarrow \Delta_\tau \in C_1(\Gamma, \mathrm{Div}^0 \mathcal{H}_p) \end{array}\right\} \to J_\tau = \int\!\!\!\!\!\!\diagup_{\Delta_\tau} \omega_E \in \mathbb{C}_p^\times / \langle q \rangle \simeq E(\mathbb{C}_p)$$

- $\mathbb{C}_p^\times / \langle q \rangle \simeq \mathbb{C}_p^\times / \langle q_E \rangle$ (Greenberg–Dasgupta, Longo–Rotger–Vigni)

Puntos de Darmon, à la Greenberg

- $E/\mathbb{Q}$ curva de conductor $\square \nmid N$. Supongamos que $N = pMD$
  - D es producto de un número par de primos inertes en K
  - M es producto de primos que descomponen o ramifican en K
  - (siempre se cumple si $\mathrm{ord}_{s=1} L(E/K, 1) = 1$)
- $B/\mathbb{Q}$ algebra de cuaterniones discriminante D ($= \mathrm{M}_2(\mathbb{Q})$ si $D = 1$)
- B actua en $\mathcal{H}_p$ via $B \otimes \mathbb{Q}_p \simeq \mathrm{M}_2(\mathbb{Q}_p)$
- $\Gamma \subset B^\times$ subgrupo de congruencia de nivel M

Construcción (Darmon $D = 1$ (2001), Greenberg $D > 1$ (2011))

$$\left.\begin{array}{r} E \rightsquigarrow \omega_E \in H^1(\Gamma, \Omega^1_{\mathcal{H}_p}) \\ \tau \in K \cap \mathcal{H}_p \rightsquigarrow \Delta_\tau \in C_1(\Gamma, \mathrm{Div}^0 \mathcal{H}_p) \end{array}\right\} \to J_\tau = \int\!\!\!\!\!\!\diagup_{\Delta_\tau} \omega_E \in \mathbb{C}_p^\times / \langle q \rangle \simeq E(\mathbb{C}_p)$$

- $\mathbb{C}_p^\times / \langle q \rangle \simeq \mathbb{C}_p^\times / \langle q_E \rangle$ (Greenberg–Dasgupta, Longo–Rotger–Vigni)

Conjetura (racionalidad de puntos de Darmon)

$J_\tau \in E(\mathbb{C}_p)$ de hecho pertenece a $E(K^{\mathrm{ab}})$

Calculando en homologia y cohomologia

- La clase de cohomología $\omega_E \in H^1(\Gamma, \Omega_{\mathcal{H}_p,\mathbb{Z}})$
  - $T_\ell \colon H^1(\Gamma, \Omega_{\mathcal{H}_p,\mathbb{Z}}) \longrightarrow H^1(\Gamma, \Omega_{\mathcal{H}_p,\mathbb{Z}})$ operadores de Hecke
  - ω_E es la “unica” forma tal que

$$T_\ell \omega_E = a_\ell \omega_E$$

Calculando en homologia y cohomologia

- La clase de cohomología $\omega_E \in H^1(\Gamma, \Omega_{\mathcal{H}_p,\mathbb{Z}})$
  - $T_\ell \colon H^1(\Gamma, \Omega_{\mathcal{H}_p,\mathbb{Z}}) \longrightarrow H^1(\Gamma, \Omega_{\mathcal{H}_p,\mathbb{Z}})$ operadores de Hecke
  - ω_E es la "unica" forma tal que

$$T_\ell \omega_E = a_\ell \omega_E$$

- La cadena $\Delta_\tau \in C_1(\Gamma, \mathrm{Div}^0(\mathcal{H}_p))$
  - $D = 1$, $B = \mathrm{M}_2(\mathbb{Q})$
    - ★ Fracciones contínuas si $M = 1$ (Darmon–Green)
    - ★ Versión efectiva del problema del subgrupo de congruencia si $M > 1$ (G.-Masdeu)
  - $D > 1$, B algebra de división
    - ★ Algoritmos de Voight para calcular generadores y relaciones en Γ

Calculando con diferenciales rígidas analíticas

- En el caso clasico $\omega \in \Omega^1_{\mathcal{H}}$: tiene serie de Fourier

Calculando con diferenciales rígidas analíticas

- En el caso clasico $\omega \in \Omega^1_{\mathcal{H}}$: tiene serie de Fourier

Realización concreta de las diferenciales p-adicas

$\{$ Medidas de $\mathbb{P}^1(\mathbb{Q}_p)$ con valores en $\mathbb{Z}\} \xrightarrow{\simeq} \Omega^1_{\mathcal{H}_p,\mathbb{Z}}$

Calculando con diferenciales rígidas analíticas

- En el caso clasico $\omega \in \Omega^1_{\mathcal{H}}$: tiene serie de Fourier

Realización concreta de las diferenciales p-adicas

$\{$ Medidas de $\mathbb{P}^1(\mathbb{Q}_p)$ con valores en $\mathbb{Z}\} \xrightarrow{\simeq} \Omega^1_{\mathcal{H}_p,\mathbb{Z}}$

- f : $\{$Bolas en $\mathbb{P}(\mathbb{Q}_p)\} \longrightarrow \mathbb{Z}$ tal que $f(B) = \sum_{i=0}^{p} f(B_i)$

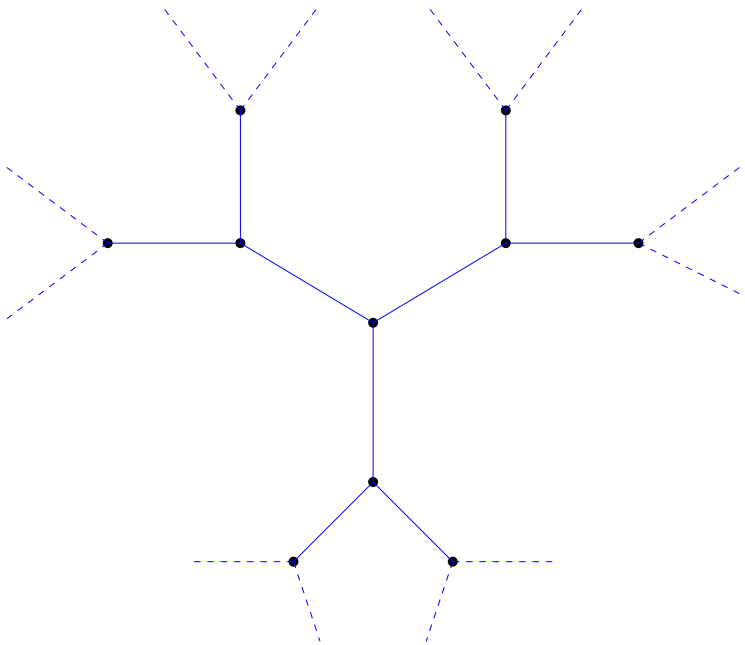
Calculando con diferenciales rígidas analíticas

- En el caso clasico $\omega \in \Omega^1_{\mathcal{H}}$: tiene serie de Fourier

Realización concreta de las diferenciales p-adicas

$\{$ Medidas de $\mathbb{P}^1(\mathbb{Q}_p)$ con valores en $\mathbb{Z}\} \xrightarrow{\simeq} \Omega^1_{\mathcal{H}_p,\mathbb{Z}}$

- f: $\{$Bolas en $\mathbb{P}(\mathbb{Q}_p)\} \longrightarrow \mathbb{Z}$ tal que $f(B) = \sum_{i=0}^{p} f(B_i)$
- $\{$Bolas en $\mathbb{P}(\mathbb{Q}_p)\} \longleftrightarrow$ árbol de Bruhat–Tits



Índex

Motivación

- Evidencia numérica para las conjeturas de Darmon–Greenberg
- A la práctica: método eficiente para calcular puntos en $E(K^{\mathrm{ab}})$

Algoritmos y evidencia numérica

	$M = 1$	$M > 1$
$D = 1$, $B = \mathrm{M}_2(\mathbb{Q})$	Darmon–Green (2002) Darmon–Pollack (2006)	G.-Masdeu (2012)
$D > 1$, B alg. div	G.-Masdeu	(2013)

Cálculos explícitos $p = 13$, $D = 1$, $M = 5$, $\mathrm{prec} = 13^{60}$

$$E_{51} : y^2 + y = x^3 + x^2 + x - 1$$

d_K	h	P^+
101	1	$\left(-\frac{656788148124048}{108395925566683225}\sqrt{101} + \frac{108663526315570777}{108395925566683225}, \frac{43274260598510467034409 6}{35687772118459783422252125}\sqrt{101} - \frac{7155186021607955194138335 4}{35687772118459783422252125} \right)$
149	1	$\left(-\frac{41662615293}{110013332450}\sqrt{149} + \frac{802189306199}{110013332450}, \frac{39791672228037249}{2580197692616075 0}\sqrt{149} - \frac{635290450369692907}{2580197692616075 0} \right)$
152	1	$\left(-\frac{1915814571}{20670100441}\sqrt{38} + \frac{24731592007}{20670100441}, \frac{577303899566856}{2971761010503011}\sqrt{38} - \frac{7167395643538198}{2971761010503011} \right)$
161	1	$\left(\frac{62146167667}{49710362300}, \frac{8395974419456303}{53153799096521000}\sqrt{161} - \frac{1}{2} \right)$
188	1	$\left(\frac{3178296211866}{1135825194001}\sqrt{47} + \frac{22525829850817}{1135825194001}, \frac{218641162308913160 04}{12105068363317597 51}\sqrt{47} + \frac{148356498531472446055}{12105068363317597 51} \right)$

d_K	h	$h_D(x)$
104	2	$x^2 + \left(-\frac{992302702743}{1960400420449}\sqrt{26} - \frac{57132410901980}{1960400420449} \right) x - \frac{4968445297101}{1960400420449}\sqrt{26} + \frac{61480175149213}{1960400420449}$
185	2	$x^2 + \left(-\frac{908505900}{7532677681}\sqrt{185} - \frac{54207252962}{7532677681} \right) x - \frac{787814100}{7532677681}\sqrt{185} + \frac{45005684581}{7532677681}$

Cálculos explícitos $p = 11$, $D = 10$, $M = 1$, $\mathrm{prec} = 11^{60}$

$$E_{110}: \quad y^2 + xy + y = x^3 + x^2 + 10x - 45.$$

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	$2 \cdot 30 \cdot \left(\frac{190966548837842073867}{4016648659658412649} - \frac{10722443619184119320}{4016648659658412649}\sqrt{237}, -\frac{3505590193011437142853233857149}{804999791382984541142375 6107} + \frac{2354484601305645209913203722 00}{804999791382984541142375 6107}\sqrt{237} \right)$
277	$2 \cdot 30 \left(\frac{46317716623881}{12553387541776}, -\frac{58871104165657}{25106775083552} - \frac{20912769335239055243}{44477606117965542976}\sqrt{277} \right)$
293	$2 \cdot 30 \cdot \left(\frac{7088486530742}{2971834657801}, -\frac{10060321188543}{5943669315602} - \frac{591566427769149607}{102462974768356034 02}\sqrt{293} \right)$
373	$2 \cdot 30 \cdot \left(\frac{298780258398}{62087183929}, -\frac{360867442327}{124174367858} - \frac{19368919551426449}{30940899762281434}\sqrt{373} \right)$

Algoritmos para puntos de Darmon

Xevi Guitart[1] Marc Masdeu[2]

[1]Universitat Politècnica de Catalunya

[2]Columbia University

Quintas Jornadas de Teoría de Números