Computation of quaternionic p-adic Darmon points

Xevi Guitart[1] Marc Masdeu[2]

[1]Institut für Experimentelle Mathematik, Essen

[2]Columbia University

Algebra and Number Theory Seminar, Heidelberg

Outline

Outline

Computing algebraic points

- E elliptic curve with rational coefficients

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

Computing algebraic points

- E elliptic curve with rational coefficients

$$E\colon\ y^2 + b_1xy + b_3y = x^3 + b_2x^2 + b_4x + b_6, \quad b_i \in \mathbb{Z}$$

- K a number field. $E(K) = \{\text{solutions } (x, y) \in K^2\}$

Computing algebraic points

- E elliptic curve with rational coefficients

$$E\colon\ y^2 + b_1xy + b_3y = x^3 + b_2x^2 + b_4x + b_6, \quad b_i \in \mathbb{Z}$$

- K a number field. $E(K) = \{\text{solutions } (x, y) \in K^2\}$

Question

Does there exist any algorithm for computing $E(K)$?

Computing algebraic points

- E elliptic curve with rational coefficients

$$E\colon\; y^2 + b_1xy + b_3y = x^3 + b_2x^2 + b_4x + b_6, \quad b_i \in \mathbb{Z}$$

- K a number field. $E(K) = \{\text{solutions } (x, y) \in K^2\}$

Question

Does there exist any algorithm for computing $E(K)$?

- Answer: Not known

Computing algebraic points

- E elliptic curve with rational coefficients

$$E\colon\ y^2 + b_1xy + b_3y = x^3 + b_2x^2 + b_4x + b_6, \quad b_i \in \mathbb{Z}$$

- K a number field. $E(K) = \{\text{solutions } (x,y) \in K^2\}$

Question

Does there exist any algorithm for computing $E(K)$?

- Answer: Not known

Mordell–Weil Theorem

$E(K)$ has a group structure and $E(K) \simeq E(K)_{\mathrm{tor}} \oplus \mathbb{Z}^r$

Computing algebraic points

- E elliptic curve with rational coefficients

$$E\colon\ y^2 + b_1xy + b_3y = x^3 + b_2x^2 + b_4x + b_6, \quad b_i \in \mathbb{Z}$$

- K a number field. $E(K) = \{\text{solutions } (x, y) \in K^2\}$

Question

Does there exist any algorithm for computing $E(K)$?

- Answer: Not known

Mordell–Weil Theorem

$E(K)$ has a group structure and $E(K) \simeq E(K)_{\mathrm{tor}} \oplus \mathbb{Z}^r$

- $E(K)_{\mathrm{tor}}$: there DO exist algorithms

Computing algebraic points

- E elliptic curve with rational coefficients

$$E\colon\ y^2 + b_1xy + b_3y = x^3 + b_2x^2 + b_4x + b_6, \quad b_i \in \mathbb{Z}$$

- K a number field. $E(K) = \{\text{solutions } (x, y) \in K^2\}$

Question

Does there exist any algorithm for computing $E(K)$?

- Answer: Not known

Mordell–Weil Theorem

$E(K)$ has a group structure and $E(K) \simeq E(K)_{\mathrm{tor}} \oplus \mathbb{Z}^r$

- $E(K)_{\mathrm{tor}}$: there DO exist algorithms
- Compute r linearly independent points of infinite order?

Computing algebraic points

- E elliptic curve with rational coefficients

$$E\colon\ y^2 + b_1xy + b_3y = x^3 + b_2x^2 + b_4x + b_6, \quad b_i \in \mathbb{Z}$$

- K a number field. $E(K) = \{\text{solutions } (x,y) \in K^2\}$

Question

Does there exist any algorithm for computing $E(K)$?

- Answer: Not known

Mordell–Weil Theorem

$E(K)$ has a group structure and $E(K) \simeq E(K)_{\mathrm{tor}} \oplus \mathbb{Z}^r$

- $E(K)_{\mathrm{tor}}$: there DO exist algorithms
- Compute r linearly independent points of infinite order?
- Compute the rank r?
  - Related to the Birch and Swinnerton–Dyer Conjecture

The Birch and Swinnerton–Dyer Conjecture (BSD)

Hasse–Weil L-function

$$L(E/K,s) = \sum_{\mathfrak{n}\subseteq\mathcal{O}_K} a_{\mathfrak{n}} n^{-s}, \quad a_{\mathfrak{p}} = |\mathfrak{p}| + 1 - \#E(\mathcal{O}_K/\mathfrak{p})$$

The Birch and Swinnerton–Dyer Conjecture (BSD)

Hasse–Weil *L*-function

$$L(E/K,s) = \sum_{\mathfrak{n}\subseteq\mathcal{O}_K} a_{\mathfrak{n}} n^{-s}, \quad a_{\mathfrak{p}} = |\mathfrak{p}| + 1 - \#E(\mathcal{O}_K/\mathfrak{p})$$

Birch–Swinnerton-Dyer Conjecture (BSD)

$$r(E/K) = \mathrm{ord}_{s=1} L(E/K,s)$$

The Birch and Swinnerton–Dyer Conjecture (BSD)

Hasse–Weil L-function

$$L(E/K,s)=\sum_{\mathfrak{n}\subseteq\mathcal{O}_K} a_{\mathfrak{n}} n^{-s},\quad a_{\mathfrak{p}}=|\mathfrak{p}|+1-\#E(\mathcal{O}_K/\mathfrak{p})$$

Birch–Swinnerton-Dyer Conjecture (BSD)

$$r(E/K)=\operatorname{ord}_{s=1}L(E/K,s)$$

Theorem (Gross–Zagier 1986, Kolyvagin 1989)

If $K=\mathbb{Q}$ or $K=$ quadratic imaginary and $\operatorname{ord}_{s=1}L(E/K,s)\leq 1$ then BSD holds

The Birch and Swinnerton–Dyer Conjecture (BSD)

Hasse–Weil *L*-function

$$L(E/K,s)=\sum_{\mathfrak{n}\subseteq\mathcal{O}_K} a_{\mathfrak{n}} n^{-s},\qquad a_{\mathfrak{p}}=|\mathfrak{p}|+1-\#E(\mathcal{O}_K/\mathfrak{p})$$

Birch–Swinnerton-Dyer Conjecture (BSD)

$$r(E/K)=\mathrm{ord}_{s=1}L(E/K,s)$$

Theorem (Gross–Zagier 1986, Kolyvagin 1989)

If $K=\mathbb{Q}$ or $K=$ quadratic imaginary and $\mathrm{ord}_{s=1}L(E/K,s)\leq 1$ then BSD holds

Question

If $K=$ quadratic imaginary and $\mathrm{ord}_{s=1}L(E/K,s)=1$, does there exist an efficient algorithm for computing a point of infinite order?

The Birch and Swinnerton–Dyer Conjecture (BSD)

Hasse–Weil L-function

$$L(E/K,s) = \sum_{\mathfrak{n}\subseteq\mathcal{O}_K} a_{\mathfrak{n}} n^{-s}, \quad a_{\mathfrak{p}} = |\mathfrak{p}| + 1 - \#E(\mathcal{O}_K/\mathfrak{p})$$

Birch–Swinnerton-Dyer Conjecture (BSD)

$$r(E/K) = \mathrm{ord}_{s=1} L(E/K,s)$$

Theorem (Gross–Zagier 1986, Kolyvagin 1989)

If $K = \mathbb{Q}$ or $K =$ quadratic imaginary and $\mathrm{ord}_{s=1} L(E/K,s) \leq 1$ then BSD holds

Question

If $K =$ quadratic imaginary and $\mathrm{ord}_{s=1} L(E/K,s) = 1$, does there exist an efficient algorithm for computing a point of infinite order?

- Answer: yes, the Heegner points method
  - Fundamental ingredient in the Gross–Zagier–Kolyvagin theorem

Outline

Heegner points

$K = \mathbb{Q}(\sqrt{-D})$ cuadratic imaginary field

Method for computing points on $E(K^{\mathrm{ab}})$

Heegner points

$K = \mathbb{Q}(\sqrt{-D})$ cuadratic imaginary field

Method for computing points on $E(K^{\mathrm{ab}})$

- Geometric construction

Heegner points

$K = \mathbb{Q}(\sqrt{-D})$ cuadratic imaginary field

Method for computing points on $E(K^{\mathrm{ab}})$

- Geometric construction
  - Modular uniformization (Wiles et. al): $X_0(N) \longrightarrow E$

Heegner points

$K = \mathbb{Q}(\sqrt{-D})$ cuadratic imaginary field

Method for computing points on $E(K^{\mathrm{ab}})$

- Geometric construction
  - Modular uniformization (Wiles et. al): $X_0(N) \longrightarrow E$
  - Points on $X_0(N)$ parametrize elliptic curves

Heegner points

$K = \mathbb{Q}(\sqrt{-D})$ cuadratic imaginary field

Method for computing points on $E(K^{\mathrm{ab}})$

- Geometric construction
  - Modular uniformization (Wiles et. al): $X_0(N) \longrightarrow E$
  - Points on $X_0(N)$ parametrize elliptic curves
  - CM points on $X_0(N)$ (correspond to curves with CM by K)

Heegner points

$K = \mathbb{Q}(\sqrt{-D})$ cuadratic imaginary field

Method for computing points on $E(K^{\mathrm{ab}})$

- Geometric construction
  - Modular uniformization (Wiles et. al): $X_0(N) \longrightarrow E$
  - Points on $X_0(N)$ parametrize elliptic curves
  - CM points on $X_0(N)$ (correspond to curves with CM by K)
  - Theory of Complex Multiplication: CM points $\in X_0(N)(K^{\mathrm{ab}})$

Heegner points

$K = \mathbb{Q}(\sqrt{-D})$ cuadratic imaginary field

Method for computing points on $E(K^{\mathrm{ab}})$

- Geometric construction
  - Modular uniformization (Wiles et. al): $X_0(N) \longrightarrow E$
  - Points on $X_0(N)$ parametrize elliptic curves
  - CM points on $X_0(N)$ (correspond to curves with CM by K)
  - Theory of Complex Multiplication: CM points $\in X_0(N)(K^{\mathrm{ab}})$
  - Their image in E give rise to Heegner points

Heegner points

$K = \mathbb{Q}(\sqrt{-D})$ cuadratic imaginary field

Method for computing points on $E(K^{\mathrm{ab}})$

- Geometric construction
  - Modular uniformization (Wiles et. al): $X_0(N) \longrightarrow E$
  - Points on $X_0(N)$ parametrize elliptic curves
  - CM points on $X_0(N)$ (correspond to curves with CM by K)
  - Theory of Complex Multiplication: CM points $\in X_0(N)(K^{\mathrm{ab}})$
  - Their image in E give rise to Heegner points
- Explicit formula

Heegner points

$K = \mathbb{Q}(\sqrt{-D})$ cuadratic imaginary field

Method for computing points on $E(K^{\mathrm{ab}})$

- Geometric construction
  - Modular uniformization (Wiles et. al): $X_0(N) \longrightarrow E$
  - Points on $X_0(N)$ parametrize elliptic curves
  - CM points on $X_0(N)$ (correspond to curves with CM by K)
  - Theory of Complex Multiplication: CM points $\in X_0(N)(K^{\mathrm{ab}})$
  - Their image in E give rise to Heegner points
- Explicit formula
  - $X_0(N)(\mathbb{C}) = \Gamma_0(N)\backslash\mathcal{H} \longrightarrow E(\mathbb{C}) \simeq \mathbb{C}/\Lambda_E$

Heegner points

$K = \mathbb{Q}(\sqrt{-D})$ cuadratic imaginary field

Method for computing points on $E(K^{\mathrm{ab}})$

- Geometric construction
  - Modular uniformization (Wiles et. al): $X_0(N) \longrightarrow E$
  - Points on $X_0(N)$ parametrize elliptic curves
  - CM points on $X_0(N)$ (correspond to curves with CM by K)
  - Theory of Complex Multiplication: CM points $\in X_0(N)(K^{\mathrm{ab}})$
  - Their image in E give rise to Heegner points
- Explicit formula
  - $X_0(N)(\mathbb{C}) = \Gamma_0(N)\backslash\mathcal{H} \longrightarrow E(\mathbb{C}) \simeq \mathbb{C}/\Lambda_E$
  - CM Points: $\tau \in \mathcal{H} \cap K$

Heegner points

$K = \mathbb{Q}(\sqrt{-D})$ cuadratic imaginary field

Method for computing points on $E(K^{\mathrm{ab}})$

- Geometric construction
  - Modular uniformization (Wiles et. al): $X_0(N) \longrightarrow E$
  - Points on $X_0(N)$ parametrize elliptic curves
  - CM points on $X_0(N)$ (correspond to curves with CM by K)
  - Theory of Complex Multiplication: CM points $\in X_0(N)(K^{\mathrm{ab}})$
  - Their image in E give rise to Heegner points
- Explicit formula
  - $X_0(N)(\mathbb{C}) = \Gamma_0(N)\backslash\mathcal{H} \longrightarrow E(\mathbb{C}) \simeq \mathbb{C}/\Lambda_E$
  - CM Points: $\tau \in \mathcal{H} \cap K$
  - $f(z) = \sum_{n\geq 1} a_n e^{2\pi i n z} \rightsquigarrow f(z)dz$ differential on $\Gamma_0(N)\backslash\mathcal{H}$

Heegner points

$K = \mathbb{Q}(\sqrt{-D})$ cuadratic imaginary field

Method for computing points on $E(K^{\mathrm{ab}})$

- Geometric construction
  - Modular uniformization (Wiles et. al): $X_0(N) \longrightarrow E$
  - Points on $X_0(N)$ parametrize elliptic curves
  - CM points on $X_0(N)$ (correspond to curves with CM by K)
  - Theory of Complex Multiplication: CM points $\in X_0(N)(K^{\mathrm{ab}})$
  - Their image in E give rise to Heegner points
- Explicit formula
  - $X_0(N)(\mathbb{C}) = \Gamma_0(N)\backslash\mathcal{H} \longrightarrow E(\mathbb{C}) \simeq \mathbb{C}/\Lambda_E$
  - CM Points: $\tau \in \mathcal{H} \cap K$
  - $f(z) = \sum_{n\geq 1} a_n e^{2\pi i n z} \rightsquigarrow f(z)dz$ differential on $\Gamma_0(N)\backslash\mathcal{H}$

Heegner Point

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

Heegner points

$K = \mathbb{Q}(\sqrt{-D})$ cuadratic imaginary field

Method for computing points on $E(K^{\mathrm{ab}})$

- Geometric construction
  - Modular uniformization (Wiles et. al): $X_0(N) \longrightarrow E$
  - Points on $X_0(N)$ parametrize elliptic curves
  - CM points on $X_0(N)$ (correspond to curves with CM by K)
  - Theory of Complex Multiplication: CM points $\in X_0(N)(K^{\mathrm{ab}})$
  - Their image in E give rise to Heegner points
- Explicit formula
  - $X_0(N)(\mathbb{C}) = \Gamma_0(N)\backslash\mathcal{H} \longrightarrow E(\mathbb{C}) \simeq \mathbb{C}/\Lambda_E$
  - CM Points: $\tau \in \mathcal{H} \cap K$
  - $f(z) = \sum_{n\geq 1} a_n e^{2\pi i n z} \rightsquigarrow f(z)dz$ differential on $\Gamma_0(N)\backslash\mathcal{H}$

Heegner Point

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

Heegner points

$K = \mathbb{Q}(\sqrt{-D})$ cuadratic imaginary field

Method for computing points on $E(K^{\mathrm{ab}})$

- Geometric construction
  - Modular uniformization (Wiles et. al): $X_0(N) \longrightarrow E$
  - Points on $X_0(N)$ parametrize elliptic curves
  - CM points on $X_0(N)$ (correspond to curves with CM by K)
  - Theory of Complex Multiplication: CM points $\in X_0(N)(K^{\mathrm{ab}})$
  - Their image in E give rise to Heegner points
- Explicit formula
  - $X_0(N)(\mathbb{C}) = \Gamma_0(N)\backslash\mathcal{H} \longrightarrow E(\mathbb{C}) \simeq \mathbb{C}/\Lambda_E$
  - CM Points: $\tau \in \mathcal{H} \cap K$
  - $f(z) = \sum_{n\geq 1} a_n e^{2\pi i n z} \rightsquigarrow f(z)dz$ differential on $\Gamma_0(N)\backslash\mathcal{H}$

Heegner Point

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

An extreme example (M. Watkins)

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

An extreme example (M. Watkins)

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

the numerator of the x-coordinate is:

An extreme example (M. Watkins)

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

the numerator of the x-coordinate is:

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

367770537186677506614005642341827170087932269492285584726218770061653546349271015805365134370326743061141306464500052886704651998399766478840791915307861741150
72739338026281573250924797082687602171017553858718167805487654785022844156276828471927526818990949626599378706300367603592935770218062374839710749312284163465
07852381696883227650072039964481597215995993299744934117106289850389364006552497835877740257534533113775202882210048356163645919345794812074571029660897173224
37033770105616573500859064029709029870912150626669726646199320182539736999955086814229431275632217741073053282806475960497536924235099356803072693704991160726
41097827468479512837941192989412144907943309029865829912295694015235199387427463761071907702040105138183490127866378892547110594555551738109049119276198990318
55149292325338589831979737026402711049742594116000380601480839982975557506035851728035645241044229165029649347049289119188596869401159325131363345962579503132
33984727542244009455382470518922565367745951286311791172183855293430912450813449336643740809392436203974991190741697350414232211175705858420072502263211616472
01649986417295226774605259994990779421258204288795260637356926859910185168629387960475973239865371541712483169437963732171919939969937146546295368843960579247
90938647656663281596178145722116098216500930333824321806726937018190136190556573208807048355335567078793126656928657859036779350593274598717379730880724034301
86773944374984180945671588419372032890146155265988262840584220975675716781666213994508186464210853359598997571625925924015283405094065447961714768592250085694
44498220453860921224090969785448172188478976405134778065983291776042463808123777390491844755507773416209859765703930378802827649670195524084007307548226764414
81715385344001979832232652414888335865567377214360456003296961668177481944809066257442596772347829664126972931904101685281128944780074646796760942430959617022
25747987408940356496503888537981786692004892981452026849367750705907376590267163808736648849670283632626857459312324510742034887810176312389334765702027559124
88242478005942708620520821859733932900091898676772594580806760650987034535395255769756395437005076256407298723407894063143944684005844559206833619762001218344
30751233901473228497490561998078486251074993528871318797403348087370426900997556442577081254910572185107856605139877331015042842121106080690743578173268489400
49905689831262195394796701235841454775289708109709179574420369768404606625566320124229276012675987126600451637743296191727204021714708356339998761242059527579
20338556769918233682548621595584500438080514815332972700352873822470382792932239463850701180823069589872686033969240544031038574440588486055874154005176700326
31121206127732481340391088277796488544415738156553014768406246154666005139690428085145098272500791416214774673484501826722500527091164944262537169595848931680
75409677471286049057274622409403118704320452610723920107960346829752289510659856743701508334879787536416279769396881980413954888575128268715223707826035870523
02844262030644936842506142828799181077337962070672500038239594129356776240932360470386373655773263995890088045077860119731559277310730347065365574614438066227
07622411087809371872157210456836892493613836792026761820382217165481998924123604782787923229739171920575447007099501678380795077013113325989801385729993920818
30165442425133956460687682012192837224621339985921328279251116804395344383979390113997419447930029756609766453919938465190843618873242881837330238304638885942
79378938418880142666851776166056447837041357949318307502656863359340665652409440494482130055919971289855607602603992142786359126343515867623548693540215307461
89992899582554597632108309638569296964800046983072736238483149014714600896056552029642747991419063454749142059564274298254654925893866404955146903330024475746
16354371499624965242017117105423172633649354158697143177894405148105963373839941141857432381177094972972684361267292500063135565983416420055444131545100343345
24662047071238116636236628372968629480617587599286317636619851856158018862057707210320063041448677873470583163922956715800916558720872094859132869301288586404
42589125454268580397484571921012318872311624898317615607628176460097441336323549031828235965636277950827328087547939511112374216436584203379248450122647406094
03517113074066372354767593988595936388113589303510201838944421274614625032834824261067352402237899497839202009881472197450206269281573668922975906582209394279
53187053452755989894263352359355056053114113015603211922694308617337435444029085864973053536009094312149332025225287171092144929593300160658102876231441792884
66664888540622702346704213752456372574449563979215782406566937885352945871994541770838871930542220307771671498466518108722622109421676741544945695403509866953
16727762828023246483921500347404889696803754466002975574006558127013908324990321257223041794224979546710070039394431032500967717918210997094334680733501444683
96122825088243240736795841228512083604591663154848919522994493400258965092989359393577217235439331087432419973874470183959253201676376403284079570698454395013
81234605867495003402016724626400855369636521155009147176245904149069225438646928549072337653348704931901764847439772432025275648964681387210234070849306330191
79038041239611544624083258348136637213230084906083526213683231531105290336750385743792050893130528314337942393060136915457253067727886206663888425022179164712
3563828956462530983567929499493346622977494903591722345188975062941907415400740881

A natural question: what if K is real quadratic?

A natural question: what if K is real quadratic?

Question

- $E/\mathbb{Q}$ elliptic curve
- K real cuadratic such that $\operatorname{ord}_{s=1} L(E/K, s) = 1$
  - algorithm for computing points of infinite order in $E(K^{\text{ab}})$?

A natural question: what if K is real quadratic?

Question

- $E/\mathbb{Q}$ elliptic curve
- K real cuadratic such that $\mathrm{ord}_{s=1} L(E/K, s) = 1$
  - algorithm for computing points of infinite order in $E(K^{\mathrm{ab}})$?

- Idea: look for a construction analogous to that of Heegner points

A natural question: what if K is real quadratic?

Question

- $E/\mathbb{Q}$ elliptic curve
- K real cuadratic such that $\mathrm{ord}_{s=1} L(E/K,s) = 1$
  - algorithm for computing points of infinite order in $E(K^{\mathrm{ab}})$?

- Idea: look for a construction analogous to that of Heegner points
- Darmon Points

A natural question: what if K is real quadratic?

Question

- $E/\mathbb{Q}$ elliptic curve
- K real cuadratic such that $\mathrm{ord}_{s=1} L(E/K, s) = 1$
  - algorithm for computing points of infinite order in $E(K^{\mathrm{ab}})$?

- Idea: look for a construction analogous to that of Heegner points
- Darmon Points (a.k.a. Stark–Heegner Points)


Heegner points

K cuadratic imaginary

Method for constructing points of infinite order in $E(K^{\mathrm{ab}})$

- Geometric construction (proves algebraicity)
  - Modular uniformization $X_0(N) \longrightarrow E$
  - complex multiplication
- Explicit formula (good for computations)
  - $J_\tau = \int_\tau^\infty 2\pi i f(z)dz \in \mathbb{C}/\Lambda = E(\mathbb{C})$

~~Heegner points~~ Darmon points

K cuadratic imaginary

Method for constructing points of infinite order in $E(K^{\mathrm{ab}})$

- Geometric construction (proves algebraicity)
  - Modular uniformization $X_0(N) \longrightarrow E$
  - complex multiplication
- Explicit formula (good for computations)
  - $J_\tau = \int_\tau^\infty 2\pi i f(z)dz \in \mathbb{C}/\Lambda = E(\mathbb{C})$

~~Heegner points~~ Darmon points

K ~~cuadratic imaginary~~ real cuadratic

Method for constructing points of infinite order in $E(K^{\text{ab}})$

- Geometric construction (proves algebraicity)
  - Modular uniformization $X_0(N) \longrightarrow E$
  - complex multiplication
- Explicit formula (good for computations)
  - $J_\tau = \int_\tau^\infty 2\pi i f(z) dz \in \mathbb{C}/\Lambda = E(\mathbb{C})$

~~Heegner points~~ Darmon points

K ~~cuadratic imaginary~~ real cuadratic

Method for constructing points of infinite order in $E(K^{\text{ab}})$

- Geometric construction (proves algebraicity)
  - Modular uniformization $X_0(N) \longrightarrow E$
  - ~~complex multiplication~~ real multiplication
- Explicit formula (good for computations)
  - $J_\tau = \int_\tau^\infty 2\pi i f(z)dz \in \mathbb{C}/\Lambda = E(\mathbb{C})$

~~Heegner points~~ Darmon points

K ~~cuadratic imaginary~~ real cuadratic

Method for constructing points of infinite order in $E(K^{\mathrm{ab}})$

- Geometric construction (proves algebraicity)
  - Modular uniformization $X_0(N) \longrightarrow E$
  - ~~complex multiplication~~ real multiplication $\rightsquigarrow$ Doesn't exist!
- Explicit formula (good for computations)
  - $J_\tau = \int_\tau^\infty 2\pi i f(z) dz \in \mathbb{C}/\Lambda = E(\mathbb{C})$

~~Heegner points~~ Darmon points

K ~~cuadratic imaginary~~ real cuadratic

Method for constructing points of infinite order in $E(K^{\mathrm{ab}})$

- ~~Geometric construction (proves algebraicity)~~
  - Modular uniformization $X_0(N) \longrightarrow E$
  - ~~complex multiplication~~ real multiplication $\rightsquigarrow$ Doesn't exist!
- Explicit formula (good for computations)
  - $J_\tau = \int_\tau^\infty 2\pi i f(z)dz \in \mathbb{C}/\Lambda = E(\mathbb{C})$

~~Heegner points~~ Darmon points

K ~~cuadratic imaginary~~ real cuadratic

Method for constructing points of infinite order in $E(K^{ab})$

- ~~Geometric construction (proves algebraicity)~~
  - Modular uniformization $X_0(N) \longrightarrow E$
  - ~~complex multiplication~~ real multiplication $\rightsquigarrow$ Doesn't exist!
- Explicit formula (good for computations)
  - $J_\tau = \int_\tau^\infty 2\pi i f(z)dz \in \mathbb{C}/\Lambda = E(\mathbb{C})$

~~Heegner points~~ Darmon points

K ~~cuadratic imaginary~~ real cuadratic

Method for constructing points of infinite order in $E(K^{\mathrm{ab}})$

- ~~Geometric construction (proves algebraicity)~~
  - Modular uniformization $X_0(N) \longrightarrow E$
  - ~~complex multiplication~~ real multiplication $\rightsquigarrow$ Doesn't exist!
- Explicit formula (good for computations)
  - $J_\tau = \int_\tau^\infty 2\pi i f(z)dz \in \mathbb{C}/\Lambda = E(\mathbb{C})$
  - Ingredients

$$\left.\begin{array}{r} E \rightsquigarrow \omega_E \in \Omega^1_{\mathcal{H}} \\ \tau \in K \cap \mathcal{H} \rightsquigarrow \Delta_\tau \in \mathrm{Div}^0 \mathcal{H} \end{array}\right\} \longrightarrow J_\tau = \int_{\Delta_\tau} \omega_E \in \mathbb{C}/\Lambda_E$$

~~Heegner points~~ Darmon points

K ~~cuadratic imaginary~~ real cuadratic

Method for constructing points of infinite order in $E(K^{\mathrm{ab}})$

- ~~Geometric construction (proves algebraicity)~~
  - Modular uniformization $X_0(N) \longrightarrow E$
  - ~~complex multiplication~~ real multiplication $\rightsquigarrow$ Doesn't exist!
- Explicit formula (good for computations)
  - $J_\tau = \int_\tau^\infty 2\pi i f(z)dz \in \mathbb{C}/\Lambda = E(\mathbb{C})$
  - Ingredients

$$\left.\begin{aligned} E \rightsquigarrow \omega_E \in \Omega^1_{\mathcal{H}} \\ \tau \in K \cap \mathcal{H} \rightsquigarrow \Delta_\tau \in \mathrm{Div}^0 \mathcal{H} \end{aligned}\right\} \longrightarrow J_\tau = \int_{\Delta_\tau} \omega_E \in \mathbb{C}/\Lambda_E$$

  - Filosophy: look for analogues of ω_E and Δ_τ

~~Heegner points~~ Darmon points

K ~~cuadratic imaginary~~ real cuadratic

Method for constructing points of infinite order in $E(K^{\mathrm{ab}})$

- ~~Geometric construction (proves algebraicity)~~
  - Modular uniformization $X_0(N) \longrightarrow E$
  - ~~complex multiplication~~ real multiplication $\rightsquigarrow$ Doesn't exist!
- Explicit formula (good for computations)
  - $J_\tau = \int_\tau^\infty 2\pi i f(z) dz \in \mathbb{C}/\Lambda = E(\mathbb{C})$
  - Ingredients

$$\left.\begin{array}{r} E \rightsquigarrow \omega_E \in \Omega^1_{\mathcal{H}} \\ \tau \in K \cap \mathcal{H} \rightsquigarrow \Delta_\tau \in \mathrm{Div}^0 \mathcal{H} \end{array}\right\} \longrightarrow J_\tau = \int_{\Delta_\tau} \omega_E \in \mathbb{C}/\Lambda_E$$

  - Filosophy: look for analogues of ω_E and Δ_τ
  - In fact: $\omega_E \in H^0(\Gamma_0(N), \Omega^1_{\mathcal{H}})$ and $\Delta_\tau \in H_0(\Gamma_0(N), \mathrm{Div}^0 \mathcal{H})$

~~Heegner points~~ Darmon points

K ~~cuadratic imaginary~~ real cuadratic

Method for constructing points of infinite order in $E(K^{\mathrm{ab}})$

- ~~Geometric construction (proves algebraicity)~~
  - Modular uniformization $X_0(N) \longrightarrow E$
  - ~~complex multiplication~~ real multiplication $\rightsquigarrow$ Doesn't exist!
- Explicit formula (good for computations)
  - $J_\tau = \int_\tau^\infty 2\pi i f(z) dz \in \mathbb{C}/\Lambda = E(\mathbb{C})$
  - Ingredients

$$\left.\begin{array}{r} E \rightsquigarrow \omega_E \in \Omega^1_{\mathcal{H}} \\ \tau \in K \cap \mathcal{H} \rightsquigarrow \Delta_\tau \in \mathrm{Div}^0 \mathcal{H} \end{array}\right\} \longrightarrow J_\tau = \int_{\Delta_\tau} \omega_E \in \mathbb{C}/\Lambda_E$$

  - Filosophy: look for analogues of ω_E and Δ_τ
  - In fact: $\omega_E \in H^0(\Gamma_0(N), \Omega^1_{\mathcal{H}})$ and $\Delta_\tau \in H_0(\Gamma_0(N), \mathrm{Div}^0 \mathcal{H})$
- Obstruction: K real $\Rightarrow K \cap \mathcal{H} = \emptyset$!

Outline

Darmon points

- Idea: instad of $\mathcal{H}$ look at $\mathcal{H}_p$ (p-adic upper half plane)

Darmon points

- Idea: instad of $\mathcal{H}$ look at $\mathcal{H}_p$ (p-adic upper half plane)
  - $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}_p}}$ (analogous to $\mathbb{C}$)

Darmon points

- Idea: instad of $\mathcal{H}$ look at $\mathcal{H}_p$ (p-adic upper half plane)
  - $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}_p}}$ (analogous to $\mathbb{C}$)
  - $\mathcal{H}_p = \mathbb{C}_p \setminus \mathbb{Q}_p$ (analogous to $\mathbb{C} \setminus \mathbb{R} = \mathcal{H}^{\pm}$)

Darmon points

- Idea: instad of $\mathcal{H}$ look at $\mathcal{H}_p$ (p-adic upper half plane)
  - $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}_p}}$ (analogous to $\mathbb{C}$)
  - $\mathcal{H}_p = \mathbb{C}_p \setminus \mathbb{Q}_p$ (analogous to $\mathbb{C} \setminus \mathbb{R} = \mathcal{H}^{\pm}$)
  - p is inert in $K \Rightarrow K \cap \mathcal{H}_p \neq \emptyset$

Darmon points

- Idea: instad of $\mathcal{H}$ look at $\mathcal{H}_p$ (p-adic upper half plane)
  - $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}_p}}$ (analogous to $\mathbb{C}$)
  - $\mathcal{H}_p = \mathbb{C}_p \setminus \mathbb{Q}_p$ (analogous to $\mathbb{C} \setminus \mathbb{R} = \mathcal{H}^{\pm}$)
  - p is inert in $K \Rightarrow K \cap \mathcal{H}_p \neq \emptyset$
  - $\Omega^1_{\mathcal{H}_p}$ = rigid analytic differentials on $\mathcal{H}_p$

Darmon points

- Idea: instad of $\mathcal{H}$ look at $\mathcal{H}_p$ (p-adic upper half plane)
  - $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}_p}}$ (analogous to $\mathbb{C}$)
  - $\mathcal{H}_p = \mathbb{C}_p \setminus \mathbb{Q}_p$ (analogous to $\mathbb{C} \setminus \mathbb{R} = \mathcal{H}^\pm$)
  - p is inert in $K \Rightarrow K \cap \mathcal{H}_p \neq \emptyset$
  - $\Omega^1_{\mathcal{H}_p}$ = rigid analytic differentials on $\mathcal{H}_p$
  - Coleman Integral (analogous to the line integral)

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

Darmon points

- Idea: instad of $\mathcal{H}$ look at $\mathcal{H}_p$ (p-adic upper half plane)
  - $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}_p}}$ (analogous to $\mathbb{C}$)
  - $\mathcal{H}_p = \mathbb{C}_p \setminus \mathbb{Q}_p$ (analogous to $\mathbb{C} \setminus \mathbb{R} = \mathcal{H}^{\pm}$)
  - p is inert in $K \Rightarrow K \cap \mathcal{H}_p \neq \emptyset$
  - $\Omega^1_{\mathcal{H}_p}$ = rigid analytic differentials on $\mathcal{H}_p$
  - Coleman Integral (analogous to the line integral)

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

- Local description of E:
  - If $p \mid N$: Tate uniformization

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

Darmon points

- Idea: instad of $\mathcal{H}$ look at $\mathcal{H}_p$ (p-adic upper half plane)
  - $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}_p}}$ (analogous to $\mathbb{C}$)
  - $\mathcal{H}_p = \mathbb{C}_p \setminus \mathbb{Q}_p$ (analogous to $\mathbb{C} \setminus \mathbb{R} = \mathcal{H}^{\pm}$)
  - p is inert in $K \Rightarrow K \cap \mathcal{H}_p \neq \emptyset$
  - $\Omega^1_{\mathcal{H}_p}$ = rigid analytic differentials on $\mathcal{H}_p$
  - Coleman Integral (analogous to the line integral)

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

  - Multiplicative Coleman integral: if ω has integral residues

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

- Local description of E:
  - If $p \mid N$: Tate uniformization

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

Darmon points, à la Greenberg

Darmon points, à la Greenberg

- $E/\mathbb{Q}$ of conductor N. If $\operatorname{sign} L(E/K,s) = -1$ then $N = pDM$
  - M product of primes that split or ramify in K
  - D product of an even number of primes which are inert in K

Darmon points, à la Greenberg

- $E/\mathbb{Q}$ of conductor N. If sign$L(E/K,s) = -1$ then $N = pDM$
  - M product of primes that split or ramify in K
  - D product of an even number of primes which are inert in K
- $B/\mathbb{Q}$ quaternion algebra of discriminant D ($= \mathrm{M}_2(\mathbb{Q})$ if $D = 1$)

Darmon points, à la Greenberg

- $E/\mathbb{Q}$ of conductor N. If $\text{sign}L(E/K,s) = -1$ then $N = pDM$
  - M product of primes that split or ramify in K
  - D product of an even number of primes which are inert in K
- $B/\mathbb{Q}$ quaternion algebra of discriminant D ($= \mathrm{M}_2(\mathbb{Q})$ if $D = 1$)
- $R(pM) \subset B$ Eichler order of level pM and $\Gamma_0(pM) = R_0(pM)_1^\times$

Darmon points, à la Greenberg

- $E/\mathbb{Q}$ of conductor N. If sign$L(E/K,s) = -1$ then $N = pDM$
  - M product of primes that split or ramify in K
  - D product of an even number of primes which are inert in K
- $B/\mathbb{Q}$ quaternion algebra of discriminant D ($= \mathrm{M}_2(\mathbb{Q})$ if $D = 1$)
- $R(pM) \subset B$ Eichler order of level pM and $\Gamma_0(pM) = R_0(pM)_1^\times$
- $\Gamma = \left(R_0(M) \otimes \mathbb{Z}[\frac{1}{p}]\right)_1^\times; \quad \Gamma \simeq \Gamma_0(M) \star_{\Gamma_0(pM)} \Gamma_0(M)$

Darmon points, à la Greenberg

- $E/\mathbb{Q}$ of conductor N. If $\operatorname{sign} L(E/K,s) = -1$ then $N = pDM$
  - M product of primes that split or ramify in K
  - D product of an even number of primes which are inert in K
- $B/\mathbb{Q}$ quaternion algebra of discriminant D ($= \mathrm{M}_2(\mathbb{Q})$ if $D = 1$)
- $R(pM) \subset B$ Eichler order of level pM and $\Gamma_0(pM) = R_0(pM)_1^\times$
- $\Gamma = \left(R_0(M) \otimes \mathbb{Z}[\frac{1}{p}]\right)_1^\times; \quad \Gamma \simeq \Gamma_0(M) \star_{\Gamma_0(pM)} \Gamma_0(M)$

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

$$\left.\begin{aligned} E \rightsquigarrow \omega_E \in H^1(\Gamma, \Omega^1_{\mathcal{H}_p}) \\ \tau \in K \cap \mathcal{H}_p \rightsquigarrow \Delta_\tau \in H_1(\Gamma, \mathrm{Div}^0 \mathcal{H}_p) \end{aligned}\right\}$$

Darmon points, à la Greenberg

- $E/\mathbb{Q}$ of conductor N. If $\operatorname{sign} L(E/K,s) = -1$ then $N = pDM$
  - M product of primes that split or ramify in K
  - D product of an even number of primes which are inert in K
- $B/\mathbb{Q}$ quaternion algebra of discriminant D ($= \mathrm{M}_2(\mathbb{Q})$ if $D = 1$)
- $R(pM) \subset B$ Eichler order of level pM and $\Gamma_0(pM) = R_0(pM)_1^\times$
- $\Gamma = \left(R_0(M) \otimes \mathbb{Z}[\tfrac{1}{p}]\right)_1^\times$; $\quad \Gamma \simeq \Gamma_0(M) \star_{\Gamma_0(pM)} \Gamma_0(M)$

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

$$\left.\begin{array}{r} E \rightsquigarrow \omega_E \in H^1(\Gamma, \Omega^1_{\mathcal{H}_p}) \\ \tau \in K \cap \mathcal{H}_p \rightsquigarrow \Delta_\tau \in H_1(\Gamma, \mathrm{Div}^0 \mathcal{H}_p) \end{array}\right\} \to J_\tau = \times\!\!\!\!\!\!\int_{\Delta_\tau} \omega_E \in \mathbb{C}_p^\times / \langle q \rangle$$

Darmon points, à la Greenberg

- $E/\mathbb{Q}$ of conductor N. If $\mathrm{sign}L(E/K,s)=-1$ then $N=pDM$
  - M product of primes that split or ramify in K
  - D product of an even number of primes which are inert in K
- $B/\mathbb{Q}$ quaternion algebra of discriminant D ($=\mathrm{M}_2(\mathbb{Q})$ if $D=1$)
- $R(pM)\subset B$ Eichler order of level pM and $\Gamma_0(pM)=R_0(pM)_1^\times$
- $\Gamma=\left(R_0(M)\otimes\mathbb{Z}[\tfrac{1}{p}]\right)_1^\times;\quad \Gamma\simeq\Gamma_0(M)\star_{\Gamma_0(pM)}\Gamma_0(M)$

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

$$\left.\begin{array}{r} E\rightsquigarrow\omega_E\in H^1(\Gamma,\Omega^1_{\mathcal{H}_p}) \\ \tau\in K\cap\mathcal{H}_p\rightsquigarrow\Delta_\tau\in H_1(\Gamma,\mathrm{Div}^0\mathcal{H}_p)\end{array}\right\}\to J_\tau=⨍_{\Delta_\tau}\omega_E\in\mathbb{C}_p^\times/\langle q\rangle$$

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

Darmon points, à la Greenberg

- $E/\mathbb{Q}$ of conductor N. If $\operatorname{sign} L(E/K,s) = -1$ then $N = pDM$
  - M product of primes that split or ramify in K
  - D product of an even number of primes which are inert in K
- $B/\mathbb{Q}$ quaternion algebra of discriminant D ($= \mathrm{M}_2(\mathbb{Q})$ if $D = 1$)
- $R(pM) \subset B$ Eichler order of level pM and $\Gamma_0(pM) = R_0(pM)_1^\times$
- $\Gamma = \left(R_0(M) \otimes \mathbb{Z}[\frac{1}{p}]\right)_1^\times$; $\quad \Gamma \simeq \Gamma_0(M) \star_{\Gamma_0(pM)} \Gamma_0(M)$

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

$$\left.\begin{array}{r} E \rightsquigarrow \omega_E \in H^1(\Gamma, \Omega^1_{\mathcal{H}_p}) \\ \tau \in K \cap \mathcal{H}_p \rightsquigarrow \Delta_\tau \in H_1(\Gamma, \mathrm{Div}^0 \mathcal{H}_p) \end{array}\right\} \to J_\tau = \times\!\!\!\!\!\!\int_{\Delta_\tau} \omega_E \in \mathbb{C}_p^\times/\langle q\rangle \sim E(\mathbb{C}_p)$$

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

Darmon points, à la Greenberg

- $E/\mathbb{Q}$ of conductor N. If $\operatorname{sign} L(E/K,s) = -1$ then $N = pDM$
  - M product of primes that split or ramify in K
  - D product of an even number of primes which are inert in K
- $B/\mathbb{Q}$ quaternion algebra of discriminant D ($= \mathrm{M}_2(\mathbb{Q})$ if $D = 1$)
- $R(pM) \subset B$ Eichler order of level pM and $\Gamma_0(pM) = R_0(pM)_1^\times$
- $\Gamma = \left(R_0(M) \otimes \mathbb{Z}[\frac{1}{p}]\right)_1^\times; \quad \Gamma \simeq \Gamma_0(M) \star_{\Gamma_0(pM)} \Gamma_0(M)$

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

$$\left.\begin{array}{r} E \rightsquigarrow \omega_E \in H^1(\Gamma, \Omega^1_{\mathcal{H}_p}) \\ \tau \in K \cap \mathcal{H}_p \rightsquigarrow \Delta_\tau \in H_1(\Gamma, \mathrm{Div}^0 \mathcal{H}_p) \end{array}\right\} \to J_\tau = \times\!\!\!\!\!\!\int_{\Delta_\tau} \omega_E \in \mathbb{C}_p^\times/\langle q\rangle \sim E(\mathbb{C}_p)$$

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

Conjecture (rationality)

$J_\tau \in E(K^{\mathrm{ab}})$ and $\operatorname{Tr}(J_\tau)$ of infinite order if $\operatorname{ord}_{s=1} L(E/K,s) = 1$

Where does the evidence come from?

- Theoretical evidence: certain linear combinations are rational over genus fields
  - Bertolini–Darmon ($D = 1$) and Longo–Vigni ($D > 1$)

Where does the evidence come from?

- Theoretical evidence: certain linear combinations are rational over genus fields
  - Bertolini–Darmon ($D = 1$) and Longo–Vigni ($D > 1$)
- Numerical evidence: computed points appear to be algebraic

Algorithms and numerical evidence

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

Where does the evidence come from?

- Theoretical evidence: certain linear combinations are rational over genus fields
  - Bertolini–Darmon ($D = 1$) and Longo–Vigni ($D > 1$)
- Numerical evidence: computed points appear to be algebraic

Algorithms and numerical evidence

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

Where does the evidence come from?

- Theoretical evidence: certain linear combinations are rational over genus fields
  - Bertolini–Darmon ($D = 1$) and Longo–Vigni ($D > 1$)
- Numerical evidence: computed points appear to be algebraic

Algorithms and numerical evidence

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

- Rest of the talk: explain the algorithm for $D > 1$
  - the homology class attached to $\tau \in K \cap \mathcal{H}_p$
  - the cohomology class attached to E
  - the integration pairing

  present some numerical evidence for the conjecture with $D > 1$

The homology class in $H_1(\Gamma, \mathrm{Div}^0\mathcal{H}_p)$

- $B \otimes \mathbb{Q}_p \simeq \mathrm{M}_2(\mathbb{Q}_p)$ so $\Gamma \subset B$ acts on $\mathcal{H}_p$ via linear fractional transf.

The homology class in $H_1(\Gamma, \mathrm{Div}^0\mathcal{H}_p)$

- $B \otimes \mathbb{Q}_p \simeq \mathrm{M}_2(\mathbb{Q}_p)$ so $\Gamma \subset B$ acts on $\mathcal{H}_p$ via linear fractional transf.
- We have our $\tau \in \mathcal{H}_p \cap K$.

The homology class in $H_1(\Gamma, \mathrm{Div}^0\mathcal{H}_p)$

- $B \otimes \mathbb{Q}_p \simeq \mathrm{M}_2(\mathbb{Q}_p)$ so $\Gamma \subset B$ acts on $\mathcal{H}_p$ via linear fractional transf.
- We have our $\tau \in \mathcal{H}_p \cap K$.
- It turns out that $\mathrm{Stab}_\Gamma(\tau)$ is cyclic, say generated by $\gamma_\tau \in \Gamma$.

The homology class in $H_1(\Gamma, \mathrm{Div}^0\mathcal{H}_p)$

- $B \otimes \mathbb{Q}_p \simeq \mathrm{M}_2(\mathbb{Q}_p)$ so $\Gamma \subset B$ acts on $\mathcal{H}_p$ via linear fractional transf.
- We have our $\tau \in \mathcal{H}_p \cap K$.
- It turns out that $\mathrm{Stab}_\Gamma(\tau)$ is cyclic, say generated by $\gamma_\tau \in \Gamma$.
- We can consider $\gamma_\tau \otimes \tau \in H_1(\Gamma, \mathrm{Div}\mathcal{H}_p)$.

The homology class in $H_1(\Gamma, \mathrm{Div}^0\mathcal{H}_p)$

- $B \otimes \mathbb{Q}_p \simeq \mathrm{M}_2(\mathbb{Q}_p)$ so $\Gamma \subset B$ acts on $\mathcal{H}_p$ via linear fractional transf.
- We have our $\tau \in \mathcal{H}_p \cap K$.
- It turns out that $\mathrm{Stab}_\Gamma(\tau)$ is cyclic, say generated by $\gamma_\tau \in \Gamma$.
- We can consider $\gamma_\tau \otimes \tau \in H_1(\Gamma, \mathrm{Div}\mathcal{H}_p)$.
- It would be nice if $\gamma_\tau \otimes \tau$ was homologous to a cycle like

$$\sum \gamma_i \otimes (x_i - y_i), \quad \text{for some } \gamma_i \in \Gamma,\ x_i, y_i \in \mathcal{H}_p \tag{1}$$

The homology class in $H_1(\Gamma, \mathrm{Div}^0\mathcal{H}_p)$

- $B \otimes \mathbb{Q}_p \simeq \mathrm{M}_2(\mathbb{Q}_p)$ so $\Gamma \subset B$ acts on $\mathcal{H}_p$ via linear fractional transf.
- We have our $\tau \in \mathcal{H}_p \cap K$.
- It turns out that $\mathrm{Stab}_\Gamma(\tau)$ is cyclic, say generated by $\gamma_\tau \in \Gamma$.
- We can consider $\gamma_\tau \otimes \tau \in H_1(\Gamma, \mathrm{Div}\mathcal{H}_p)$.
- It would be nice if $\gamma_\tau \otimes \tau$ was homologous to a cycle like

$$\sum \gamma_i \otimes (x_i - y_i), \quad \text{for some } \gamma_i \in \Gamma,\ x_i, y_i \in \mathcal{H}_p \tag{1}$$

- Theorem (Ihara): Γ_{ab} is finite
  - γ_τ^e is a product of commutators
  - $\gamma_\tau^e \otimes \tau \equiv \sum \gamma_i \otimes (x_i - y_i) \in H_1(\Gamma, \mathrm{Div}^0\mathcal{H}_p)$ by an explicit formula

The homology class in $H_1(\Gamma, \mathrm{Div}^0 \mathcal{H}_p)$

- $B \otimes \mathbb{Q}_p \simeq \mathrm{M}_2(\mathbb{Q}_p)$ so $\Gamma \subset B$ acts on $\mathcal{H}_p$ via linear fractional transf.
- We have our $\tau \in \mathcal{H}_p \cap K$.
- It turns out that $\mathrm{Stab}_\Gamma(\tau)$ is cyclic, say generated by $\gamma_\tau \in \Gamma$.
- We can consider $\gamma_\tau \otimes \tau \in H_1(\Gamma, \mathrm{Div}\mathcal{H}_p)$.
- It would be nice if $\gamma_\tau \otimes \tau$ was homologous to a cycle like

$$\sum \gamma_i \otimes (x_i - y_i), \quad \text{for some } \gamma_i \in \Gamma,\ x_i, y_i \in \mathcal{H}_p \tag{1}$$

- Theorem (Ihara): Γ_{ab} is finite
  - γ_τ^e is a product of commutators
  - $\gamma_\tau^e \otimes \tau \equiv \sum \gamma_i \otimes (x_i - y_i) \in H_1(\Gamma, \mathrm{Div}^0 \mathcal{H}_p)$ by an explicit formula
- Computing this explicitly boils down to compute Γ_{ab}
  - Computing generators
  - Given $\gamma \in [\Gamma, \Gamma]$ write it explicitly as a product of commutators

The homology class in $H_1(\Gamma, \mathrm{Div}^0\mathcal{H}_p)$

- $B \otimes \mathbb{Q}_p \simeq \mathrm{M}_2(\mathbb{Q}_p)$ so $\Gamma \subset B$ acts on $\mathcal{H}_p$ via linear fractional transf.
- We have our $\tau \in \mathcal{H}_p \cap K$.
- It turns out that $\mathrm{Stab}_\Gamma(\tau)$ is cyclic, say generated by $\gamma_\tau \in \Gamma$.
- We can consider $\gamma_\tau \otimes \tau \in H_1(\Gamma, \mathrm{Div}\mathcal{H}_p)$.
- It would be nice if $\gamma_\tau \otimes \tau$ was homologous to a cycle like

$$\sum \gamma_i \otimes (x_i - y_i), \quad \text{for some } \gamma_i \in \Gamma,\ x_i, y_i \in \mathcal{H}_p \tag{1}$$

- Theorem (Ihara): Γ_{ab} is finite
  - γ_τ^e is a product of commutators
  - $\gamma_\tau^e \otimes \tau \equiv \sum \gamma_i \otimes (x_i - y_i) \in H_1(\Gamma, \mathrm{Div}^0\mathcal{H}_p)$ by an explicit formula
- Computing this explicitly boils down to compute Γ_{ab}
  - Computing generators
  - Given $\gamma \in [\Gamma, \Gamma]$ write it explicitly as a product of commutators
- John Voight's algorithms: generators and word problem for Γ

The homology class in $H_1(\Gamma, \mathrm{Div}^0\mathcal{H}_p)$

- $B \otimes \mathbb{Q}_p \simeq \mathrm{M}_2(\mathbb{Q}_p)$ so $\Gamma \subset B$ acts on $\mathcal{H}_p$ via linear fractional transf.
- We have our $\tau \in \mathcal{H}_p \cap K$.
- It turns out that $\mathrm{Stab}_\Gamma(\tau)$ is cyclic, say generated by $\gamma_\tau \in \Gamma$.
- We can consider $\gamma_\tau \otimes \tau \in H_1(\Gamma, \mathrm{Div}\mathcal{H}_p)$.
- It would be nice if $\gamma_\tau \otimes \tau$ was homologous to a cycle like

$$\sum \gamma_i \otimes (x_i - y_i), \quad \text{for some } \gamma_i \in \Gamma,\ x_i, y_i \in \mathcal{H}_p \tag{1}$$

- Theorem (Ihara): Γ_{ab} is finite
  - γ_τ^e is a product of commutators
  - $\gamma_\tau^e \otimes \tau \equiv \sum \gamma_i \otimes (x_i - y_i) \in H_1(\Gamma, \mathrm{Div}^0\mathcal{H}_p)$ by an explicit formula
- Computing this explicitly boils down to compute Γ_{ab}
  - Computing generators
  - Given $\gamma \in [\Gamma, \Gamma]$ write it explicitly as a product of commutators
- John Voight's algorithms: generators and word problem for Γ
- It is not difficult to use this in order to express any element in $[\Gamma, \Gamma]$ as a product of commutators.

The homology class in $H_1(\Gamma, \mathrm{Div}^0\mathcal{H}_p)$

- $B \otimes \mathbb{Q}_p \simeq \mathrm{M}_2(\mathbb{Q}_p)$ so $\Gamma \subset B$ acts on $\mathcal{H}_p$ via linear fractional transf.
- We have our $\tau \in \mathcal{H}_p \cap K$.
- It turns out that $\mathrm{Stab}_\Gamma(\tau)$ is cyclic, say generated by $\gamma_\tau \in \Gamma$.
- We can consider $\gamma_\tau \otimes \tau \in H_1(\Gamma, \mathrm{Div}\mathcal{H}_p)$.
- It would be nice if $\gamma_\tau \otimes \tau$ was homologous to a cycle like

$$\sum \gamma_i \otimes (x_i - y_i), \quad \text{for some } \gamma_i \in \Gamma,\ x_i, y_i \in \mathcal{H}_p \tag{1}$$

- Theorem (Ihara): Γ_{ab} is finite
  - γ_τ^e is a product of commutators
  - $\gamma_\tau^e \otimes \tau \equiv \sum \gamma_i \otimes (x_i - y_i) \in H_1(\Gamma, \mathrm{Div}^0\mathcal{H}_p)$ by an explicit formula
- Computing this explicitly boils down to compute Γ_{ab}
  - Computing generators
  - Given $\gamma \in [\Gamma, \Gamma]$ write it explicitly as a product of commutators
- John Voight's algorithms: generators and word problem for Γ
- It is not difficult to use this in order to express any element in $[\Gamma, \Gamma]$ as a product of commutators.
- Key to assume that B is a division algebra.

The cohomology class

- $E \rightsquigarrow \omega_E \in H^1(\Gamma, \Omega^1_{\mathcal{H}_p})$

The cohomology class

- $E \rightsquigarrow \omega_E \in H^1(\Gamma, \Omega^1_{H_p})$
- Hecke operators act on this cohomology group:

$$T_\ell \colon H^1(\Gamma, \Omega^1_{\mathcal{H}_p}) \longrightarrow H^1(\Gamma, \Omega^1_{\mathcal{H}_p})$$

The cohomology class

- $E \rightsquigarrow \omega_E \in H^1(\Gamma, \Omega^1_{H_p})$
- Hecke operators act on this cohomology group:

$$T_\ell \colon H^1(\Gamma, \Omega^1_{\mathcal{H}_p}) \longrightarrow H^1(\Gamma, \Omega^1_{\mathcal{H}_p})$$

Theorem (M. Greenberg)

The isotypical component $H^1(\Gamma, \Omega^1_{\mathcal{H}_p})^{\lambda_E}$ is 1-dimensional.

- ω_E the "single" cohomology class such that

$$T_\ell \omega_E = a_\ell \omega_E, \quad \text{where } a_\ell = \ell + 1 - \#E(\mathbb{F}_\ell)$$

The cohomology class

- $E \rightsquigarrow \omega_E \in H^1(\Gamma, \Omega^1_{H_p})$
- Hecke operators act on this cohomology group:

$$T_\ell \colon H^1(\Gamma, \Omega^1_{\mathcal{H}_p}) \longrightarrow H^1(\Gamma, \Omega^1_{\mathcal{H}_p})$$

Theorem (M. Greenberg)

The isotypical component $H^1(\Gamma, \Omega^1_{\mathcal{H}_p})^{\lambda_E}$ is 1-dimensional.

- ω_E the "single" cohomology class such that

$$T_\ell \omega_E = a_\ell \omega_E, \quad \text{where } a_\ell = \ell + 1 - \#E(\mathbb{F}_\ell)$$

- How to compute effectively with rigid analytic differentials?
- How to compute $\int_{\tau_1}^{\tau_2} \omega$?

Rigid analytic differentials and measures

Concrete realization of p-adic differentials (Schneider)

$$\Omega^1_{\mathcal{H}_p,\mathbb{Z}} \xrightarrow{\simeq} \{\text{Measures on } \mathbb{P}^1(\mathbb{Q}_p) \text{ with values in } \mathbb{Z}\}$$

Rigid analytic differentials and measures

Concrete realization of p-adic differentials (Schneider)

$$\Omega^1_{\mathcal{H}_p,\mathbb{Z}} \xrightarrow{\simeq} \{\text{Measures on } \mathbb{P}^1(\mathbb{Q}_p) \text{ with values in } \mathbb{Z}\}$$

- We can view $\omega_E = \mu_E \in H^1(\Gamma, \mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p, \mathbb{Z})))$

Rigid analytic differentials and measures

Concrete realization of p-adic differentials (Schneider)

$$\Omega^1_{\mathcal{H}_p,\mathbb{Z}} \xrightarrow{\simeq} \{\text{Measures on } \mathbb{P}^1(\mathbb{Q}_p) \text{ with values in } \mathbb{Z}\}$$

- We can view $\omega_E = \mu_E \in H^1(\Gamma, \text{Meas}(\mathbb{P}^1(\mathbb{Q}_p, \mathbb{Z})))$
- $\text{Meas}(\mathbb{P}^1(\mathbb{Q}_p, \mathbb{Z})) \to \mathbb{Z}\colon \nu \mapsto \nu(\mathbb{Z}_p)$

Rigid analytic differentials and measures

Concrete realization of p-adic differentials (Schneider)

$$\Omega^1_{\mathcal{H}_p,\mathbb{Z}} \xrightarrow{\simeq} \{\text{Measures on } \mathbb{P}^1(\mathbb{Q}_p) \text{ with values in } \mathbb{Z}\}$$

- We can view $\omega_E = \mu_E \in H^1(\Gamma, \mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p, \mathbb{Z})))$
- $\mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p, \mathbb{Z})) \to \mathbb{Z} \colon \nu \mapsto \nu(\mathbb{Z}_p)$
- $H^1(\Gamma, \mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p), \mathbb{Z}))^{\lambda_E} \longrightarrow H^1(\Gamma, \mathbb{Z})^{\lambda_E}$

Rigid analytic differentials and measures

Concrete realization of p-adic differentials (Schneider)

$$\Omega^1_{\mathcal{H}_p,\mathbb{Z}} \xrightarrow{\simeq} \{\text{Measures on } \mathbb{P}^1(\mathbb{Q}_p) \text{ with values in } \mathbb{Z}\}$$

- We can view $\omega_E = \mu_E \in H^1(\Gamma, \mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p, \mathbb{Z})))$
- $\mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p, \mathbb{Z})) \to \mathbb{Z}\colon \nu \mapsto \nu(\mathbb{Z}_p)$
- $H^1(\Gamma, \mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p), \mathbb{Z}))^{\lambda_E} \longrightarrow H^1(\Gamma, \mathbb{Z})^{\lambda_E} \xrightarrow{\text{res}} H^1(\Gamma_0(pM), \mathbb{Z})^{\lambda_E}$

Rigid analytic differentials and measures

Concrete realization of p-adic differentials (Schneider)

$$\Omega^1_{\mathcal{H}_p,\mathbb{Z}} \xrightarrow{\simeq} \{\text{Measures on } \mathbb{P}^1(\mathbb{Q}_p) \text{ with values in } \mathbb{Z}\}$$

- We can view $\omega_E = \mu_E \in H^1(\Gamma, \mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p, \mathbb{Z})))$
- $\mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p, \mathbb{Z})) \to \mathbb{Z} \colon \nu \mapsto \nu(\mathbb{Z}_p)$
- $H^1(\Gamma, \mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p), \mathbb{Z}))^{\lambda_E} \longrightarrow H^1(\Gamma, \mathbb{Z})^{\lambda_E} \xrightarrow{\text{res}} H^1(\Gamma_0(pM), \mathbb{Z})^{\lambda_E}$
- Greenberg's theorem: the above map is an isomorphism.

Rigid analytic differentials and measures

Concrete realization of p-adic differentials (Schneider)

$$\Omega^1_{\mathcal{H}_p,\mathbb{Z}} \xrightarrow{\simeq} \{\text{Measures on } \mathbb{P}^1(\mathbb{Q}_p) \text{ with values in } \mathbb{Z}\}$$

- We can view $\omega_E = \mu_E \in H^1(\Gamma, \mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p, \mathbb{Z})))$
- $\mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p, \mathbb{Z}))\to\mathbb{Z}$: $\nu \mapsto \nu(\mathbb{Z}_p)$
- $H^1(\Gamma, \mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p), \mathbb{Z}))^{\lambda_E} \longrightarrow H^1(\Gamma, \mathbb{Z})^{\lambda_E} \xrightarrow{\text{res}} H^1(\Gamma_0(pM), \mathbb{Z})^{\lambda_E}$
- Greenberg's theorem: the above map is an isomorphism.
- Let $\varphi_E \in H^1(\Gamma_0(pM), \mathbb{Z})$ corresponding to μ_E

Rigid analytic differentials and measures

Concrete realization of p-adic differentials (Schneider)

$$\Omega^1_{\mathcal{H}_p,\mathbb{Z}} \xrightarrow{\simeq} \{\text{Measures on } \mathbb{P}^1(\mathbb{Q}_p) \text{ with values in } \mathbb{Z}\}$$

- We can view $\omega_E = \mu_E \in H^1(\Gamma, \mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p, \mathbb{Z})))$
- $\mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p, \mathbb{Z})) \to \mathbb{Z} \colon \nu \mapsto \nu(\mathbb{Z}_p)$
- $H^1(\Gamma, \mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p), \mathbb{Z}))^{\lambda_E} \longrightarrow H^1(\Gamma, \mathbb{Z})^{\lambda_E} \xrightarrow{\text{res}} H^1(\Gamma_0(pM), \mathbb{Z})^{\lambda_E}$
- Greenberg's theorem: the above map is an isomorphism.
- Let $\varphi_E \in H^1(\Gamma_0(pM), \mathbb{Z})$ corresponding to μ_E
- φ_E is easy to compute:
  - compute the Hecke action on $\Gamma_0(pM)_{\mathrm{ab}} = H^1(\Gamma_0(pM), \mathbb{Z})$ (again using Voight's algorithms)
  - Diagonalize and take φ_E be the element in the isotypical component of E.

Rigid analytic differentials and measures

Concrete realization of p-adic differentials (Schneider)

$$\Omega^1_{\mathcal{H}_p,\mathbb{Z}} \xrightarrow{\simeq} \{\text{Measures on } \mathbb{P}^1(\mathbb{Q}_p) \text{ with values in } \mathbb{Z}\}$$

- We can view $\omega_E = \mu_E \in H^1(\Gamma, \mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p, \mathbb{Z})))$
- $\mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p, \mathbb{Z})) \to \mathbb{Z} \colon \nu \mapsto \nu(\mathbb{Z}_p)$
- $H^1(\Gamma, \mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p), \mathbb{Z}))^{\lambda_E} \longrightarrow H^1(\Gamma, \mathbb{Z})^{\lambda_E} \xrightarrow{\text{res}} H^1(\Gamma_0(pM), \mathbb{Z})^{\lambda_E}$
- Greenberg's theorem: the above map is an isomorphism.
- Let $\varphi_E \in H^1(\Gamma_0(pM), \mathbb{Z})$ corresponding to μ_E
- φ_E is easy to compute:
  - compute the Hecke action on $\Gamma_0(pM)_{\mathrm{ab}} = H^1(\Gamma_0(pM), \mathbb{Z})$ (again using Voight's algorithms)
  - Diagonalize and take φ_E be the element in the isotypical component of E.
- The isomorphism is explicit (it is essentially Shapiro's Lemma). So we can recover μ_E from φ_E.

The integration pairing

Theorem (Teitelbaum)

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

The integration pairing

Theorem (Teitelbaum)

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

- Given the cycle $\sum \gamma_i \otimes (\tau_2^i - \tau_1^i)$ for computing the Darmon point we need to evaluate the integrals

$$\sum_i \int_{\mathbb{P}^1(\mathbb{Q}_p)} \log\left(\frac{t-\tau_2^i}{t-\tau_1^i}\right) d\mu_{E,\gamma_i}(t)$$

The integration pairing

Theorem (Teitelbaum)

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

- Given the cycle $\sum \gamma_i \otimes (\tau_2^i - \tau_1^i)$ for computing the Darmon point we need to evaluate the integrals

$$\sum_i \int_{\mathbb{P}^1(\mathbb{Q}_p)} \log\left(\frac{t-\tau_2^i}{t-\tau_1^i}\right) d\mu_{E,\gamma_i}(t)$$

- Computing the integrals by Riemann sums is too inefficient

The integration pairing

Theorem (Teitelbaum)

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

- Given the cycle $\sum \gamma_i \otimes (\tau_2^i - \tau_1^i)$ for computing the Darmon point we need to evaluate the integrals

$$\sum_i \int_{\mathbb{P}^1(\mathbb{Q}_p)} \log\left(\frac{t-\tau_2^i}{t-\tau_1^i}\right) d\mu_{E,\gamma_i}(t)$$

- Computing the integrals by Riemann sums is too inefficient
- We use instead an overconvergent method

The integration pairing

Theorem (Teitelbaum)

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

- Given the cycle $\sum \gamma_i \otimes (\tau_2^i - \tau_1^i)$ for computing the Darmon point we need to evaluate the integrals

$$\sum_i \int_{\mathbb{P}^1(\mathbb{Q}_p)} \log\left(\frac{t-\tau_2^i}{t-\tau_1^i}\right) d\mu_{E,\gamma_i}(t)$$

- Computing the integrals by Riemann sums is too inefficient
- We use instead an overconvergent method
    - Darmon–Pollack used overconvergent modular symbols for $D = 1$

The integration pairing

Theorem (Teitelbaum)

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

- Given the cycle $\sum \gamma_i \otimes (\tau_2^i - \tau_1^i)$ for computing the Darmon point we need to evaluate the integrals

$$\sum_i \int_{\mathbb{P}^1(\mathbb{Q}_p)} \log\left(\frac{t-\tau_2^i}{t-\tau_1^i}\right) d\mu_{E,\gamma_i}(t)$$

- Computing the integrals by Riemann sums is too inefficient
- We use instead an overconvergent method
  - Darmon–Pollack used overconvergent modular symbols for $D = 1$
  - We need overconvergent cohomology

Integrals and overconvergent cohomology (I)

- We want to compute

$$\int_{\mathbb{P}^1(\mathbb{Q}_p)} \log\left(\frac{t-\tau_2}{t-\tau_1}\right) d\mu_{E,\gamma}(t)$$

Integrals and overconvergent cohomology (I)

- We want to compute

$$\int_{\mathbb{P}^1(\mathbb{Q}_p)} \log\left(\frac{t-\tau_2}{t-\tau_1}\right) d\mu_{E,\gamma}(t)$$

- Expanding in power series the integrand and using change of variables everything boils down to compute the moments

$$\int_{\mathbb{Z}_p} t^i d\mu_{E,\gamma}(t), \text{ for } \gamma \in \Gamma.$$

Integrals and overconvergent cohomology (I)

- We want to compute

$$\int_{\mathbb{P}^1(\mathbb{Q}_p)} \log\left(\frac{t-\tau_2}{t-\tau_1}\right) d\mu_{E,\gamma}(t)$$

- Expanding in power series the integrand and using change of variables everything boils down to compute the moments

$$\int_{\mathbb{Z}_p} t^i d\mu_{E,\gamma}(t), \text{ for } \gamma \in \Gamma.$$

Key technical Lemma

It is enough to compute the above integrals for $\gamma \in \Gamma_0(pM)$.

Integrals and overconvergent cohomology (I)

- We want to compute

$$\int_{\mathbb{P}^1(\mathbb{Q}_p)} \log\left(\frac{t-\tau_2}{t-\tau_1}\right) d\mu_{E,\gamma}(t)$$

- Expanding in power series the integrand and using change of variables everything boils down to compute the moments

$$\int_{\mathbb{Z}_p} t^i d\mu_{E,\gamma}(t), \text{ for } \gamma \in \Gamma.$$

Key technical Lemma

It is enough to compute the above integrals for $\gamma \in \Gamma_0(pM)$.

- This is what we can compute using overconvergent cohomology.

Integrals and overconvergent cohomology (II)

- Let $\mathcal{D}$ be the module of locally analytic distributions on $\mathbb{Z}_p$
  - If $h(t)$ locally analytic function on $\mathbb{Z}_p$ and $\psi \in \mathcal{D}$ then $\psi(h(t)) \in \mathbb{Z}_p$

Integrals and overconvergent cohomology (II)

- Let $\mathcal{D}$ be the module of locally analytic distributions on $\mathbb{Z}_p$
  - If $h(t)$ locally analytic function on $\mathbb{Z}_p$ and $\psi \in \mathcal{D}$ then $\psi(h(t)) \in \mathbb{Z}_p$
- Overconvergent cohomology classes: $H^1(\Gamma_0(pM), \mathcal{D})$

Integrals and overconvergent cohomology (II)

- Let $\mathcal{D}$ be the module of locally analytic distributions on $\mathbb{Z}_p$
  - If $h(t)$ locally analytic function on $\mathbb{Z}_p$ and $\psi \in \mathcal{D}$ then $\psi(h(t)) \in \mathbb{Z}_p$
- Overconvergent cohomology classes: $H^1(\Gamma_0(pM), \mathcal{D})$
- The map $\mathcal{D} \to \mathbb{Z}_p \colon \psi \mapsto \psi(1)$ induces

$$H^1(\Gamma_0(pM), \mathcal{D}) \longrightarrow H^1(\Gamma_0(pM), \mathbb{Z}_p)$$

Integrals and overconvergent cohomology (II)

- Let $\mathcal{D}$ be the module of locally analytic distributions on $\mathbb{Z}_p$
  - If $h(t)$ locally analytic function on $\mathbb{Z}_p$ and $\psi \in \mathcal{D}$ then $\psi(h(t)) \in \mathbb{Z}_p$
- Overconvergent cohomology classes: $H^1(\Gamma_0(pM), \mathcal{D})$
- The map $\mathcal{D} \to \mathbb{Z}_p \colon \psi \mapsto \psi(1)$ induces

$$H^1(\Gamma_0(pM), \mathcal{D}) \longrightarrow H^1(\Gamma_0(pM), \mathbb{Z}_p)$$

- Recall our cocyle $\varphi_E \in H^1(\Gamma_0(pM), \mathbb{Z})$.
  - It satisfies that $U_p \varphi_E = a_p \varphi_E$ ($a_p = \pm 1$).

Integrals and overconvergent cohomology (II)

- Let $\mathcal{D}$ be the module of locally analytic distributions on $\mathbb{Z}_p$
  - If $h(t)$ locally analytic function on $\mathbb{Z}_p$ and $\psi \in \mathcal{D}$ then $\psi(h(t)) \in \mathbb{Z}_p$
- Overconvergent cohomology classes: $H^1(\Gamma_0(pM), \mathcal{D})$
- The map $\mathcal{D} \to \mathbb{Z}_p$: $\psi \mapsto \psi(1)$ induces

$$H^1(\Gamma_0(pM), \mathcal{D}) \longrightarrow H^1(\Gamma_0(pM), \mathbb{Z}_p)$$

- Recall our cocyle $\varphi_E \in H^1(\Gamma_0(pM), \mathbb{Z})$.
  - It satisfies that $U_p\varphi_E = a_p\varphi_E$ ($a_p = \pm 1$).

Theorem (Pollack–Pollack)

There exists unique $\Phi_E \in H^1(\Gamma_0(pM), \mathcal{D})$ lifting φ_E s.t. $U_p\Phi_E = a_p\Phi_E$.

Integrals and overconvergent cohomology (II)

- Let $\mathcal{D}$ be the module of locally analytic distributions on $\mathbb{Z}_p$
  - If $h(t)$ locally analytic function on $\mathbb{Z}_p$ and $\psi \in \mathcal{D}$ then $\psi(h(t)) \in \mathbb{Z}_p$
- Overconvergent cohomology classes: $H^1(\Gamma_0(pM), \mathcal{D})$
- The map $\mathcal{D} \to \mathbb{Z}_p$: $\psi \mapsto \psi(1)$ induces

$$H^1(\Gamma_0(pM), \mathcal{D}) \longrightarrow H^1(\Gamma_0(pM), \mathbb{Z}_p)$$

- Recall our cocyle $\varphi_E \in H^1(\Gamma_0(pM), \mathbb{Z})$.
  - It satisfies that $U_p \varphi_E = a_p \varphi_E$ ($a_p = \pm 1$).

Theorem (Pollack–Pollack)

There exists unique $\Phi_E \in H^1(\Gamma_0(pM), \mathcal{D})$ lifting φ_E s.t. $U_p \Phi_E = a_p \Phi_E$.

- Moreover, it can be explicitly computed:
  - Take $\tilde{\varphi} \in \text{Maps}(\Gamma_0(pM), \mathcal{D})$ any lift
  - Iterate U_p: compute $\frac{1}{a_p^n} U_p^n(\tilde{\varphi})$
  - The limit when $n \to \infty$ converges to $\Phi_E \in H_1(\Gamma_0(pM), \mathcal{D})$

Integrals and overconvergent cohomology (III)

- How does this help us to compute the moments $\int_{\mathbb{Z}_p} t^i d\mu_\gamma(t)$?

Integrals and overconvergent cohomology (III)

- How does this help us to compute the moments $\int_{\mathbb{Z}_p} t^i d\mu_\gamma(t)$?
- The map

$$\gamma \mapsto \left(h(t) \mapsto \int_{\mathbb{Z}_p} h(t) d\mu_{E,\gamma}(t) \right)$$

belongs to $H^1(\Gamma_0(pM), \mathcal{D})$, lifts φ_E and has eigenvalue ± 1 by U_p.

Integrals and overconvergent cohomology (III)

- How does this help us to compute the moments $\int_{\mathbb{Z}_p} t^i d\mu_\gamma(t)$?
- The map
$$\gamma \mapsto \left(h(t) \mapsto \int_{\mathbb{Z}_p} h(t) d\mu_{E,\gamma}(t) \right)$$
belongs to $H^1(\Gamma_0(pM), \mathcal{D})$, lifts φ_E and has eigenvalue ± 1 by U_p.
- By the uniqueness property of the above theorem, this must coincide with the cocycle obtained by lifting φ_E and iterating U_p.

Integrals and overconvergent cohomology (III)

- How does this help us to compute the moments $\int_{\mathbb{Z}_p} t^i d\mu_\gamma(t)$?
- The map

$$\gamma \mapsto \left(h(t) \mapsto \int_{\mathbb{Z}_p} h(t) d\mu_{E,\gamma}(t) \right)$$

  belongs to $H^1(\Gamma_0(pM), \mathcal{D})$, lifts φ_E and has eigenvalue ± 1 by U_p.
- By the uniqueness property of the above theorem, this must coincide with the cocycle obtained by lifting φ_E and iterating U_p.
- So we can compute the integrals by lifting φ_E and integrating U_p

Integrals and overconvergent cohomology (III)

- How does this help us to compute the moments $\int_{\mathbb{Z}_p} t^i d\mu_\gamma(t)$?
- The map

$$\gamma \mapsto \left(h(t) \mapsto \int_{\mathbb{Z}_p} h(t) d\mu_{E,\gamma}(t) \right)$$

  belongs to $H^1(\Gamma_0(pM), \mathcal{D})$, lifts φ_E and has eigenvalue ± 1 by U_p.
- By the uniqueness property of the above theorem, this must coincide with the cocycle obtained by lifting φ_E and iterating U_p.
- So we can compute the integrals by lifting φ_E and integrating U_p
- Each iteration of U_p increases the accuracy of the computation in one p-adic digit

Outline

$p = 13$, $D = 6$, $\text{prec} = 13^{60}$

$$E_{78}: \quad y^2 + xy = x^3 + x^2 - 19x + 685$$

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

$p = 11$, $D = 10$, $\mathrm{prec} = 11^{60}$

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

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	$2 \cdot 30 \cdot (\frac{1909665488378420738 67}{4016648659658412649} - \frac{1072244361918411932 0}{4016648659658412649}\sqrt{237}, -\frac{3505590193011437142853233857149}{8049997913829845411423756107} + \frac{2354484601305645209913 20372200}{8049997913829845411423756107}\sqrt{237})$
277	$2 \cdot 30 \left(\frac{46317716623881}{12553387541776}, -\frac{58871104165657}{25106775083552} - \frac{2091276933523905 5243}{4447760611796554 2976}\sqrt{277}\right)$
293	$2 \cdot 30 \cdot \left(\frac{7088486530742}{2971834657801}, -\frac{10060321188543}{5943669315602} - \frac{591566427769149607}{1024629747683560 3402}\sqrt{293}\right)$
373	$2 \cdot 30 \cdot \left(\frac{298780258398}{62087183929}, -\frac{360867442327}{124174367858} - \frac{19368919551426449}{3094089976228143 4}\sqrt{373}\right)$

$p = 19$, $D = 6$, $\mathrm{prec} = 19^{60}$

$$E_{110}: \quad y^2 + xy = x^3 - 8x$$

d_K	P
29	$1 \cdot 72 \cdot \left(-\frac{6}{25}\sqrt{29} - \frac{38}{25}, -\frac{18}{125}\sqrt{29} + \frac{86}{125}\right)$
53	$1 \cdot 72 \cdot \left(-\frac{1}{9}, \frac{7}{54}\sqrt{53} + \frac{1}{18}\right)$
173	$1 \cdot 72 \cdot \left(-\frac{3481}{13689}, \frac{347333}{3203226}\sqrt{173} + \frac{3481}{27378}\right)$
269	$1 \cdot 72 \cdot \left(\frac{1647149414400}{23887470525361}\sqrt{269} - \frac{43248475603556}{23887470525361}, \frac{2359447648611379200}{116749558330761905641}\sqrt{269} + \frac{268177497417024307564}{116749558330761905641}\right)$
293	$1 \cdot 72 \cdot \left(\frac{21289143620808}{4902225525409}, \frac{4567039561444642548}{10854002829131490673}\sqrt{293} - \frac{10644571810404}{4902225525409}\right)$
317	$1 \cdot 72 \cdot \left(-\frac{25}{9}, -\frac{5}{54}\sqrt{317} + \frac{25}{18}\right)$
341	$1 \cdot 72 \cdot \left(\frac{3449809443179}{499880896975}, \frac{3600393040902501011}{3935597293546963250}\sqrt{341} - \frac{3449809443179}{999761793950}\right)$
413	$1 \cdot 72 \cdot \left(\frac{59}{7}, \frac{113}{98}\sqrt{413} - \frac{59}{14}\right)$

Computation of quaternionic p-adic Darmon points

Xevi Guitart[1] Marc Masdeu[2]

[1]Institut für Experimentelle Mathematik, Essen

[2]Columbia University

Algebra and Number Theory Seminar, Heidelberg