Computing equations of elliptic curves over number fields via *p*-adic methods

Xevi Guitart[1] Marc Masdeu[2] Haluk Sengun[3]

[1]Institut für Experimentelle Mathematik, Essen

[2]University of Warwick

[3]University of Sheffield

Conference for young researchers in arithmetic and algebraic geometry, Bonn Oct 2014

Computing equations of elliptic curves

- K a number field

$$E/K\colon\ y^2 = x^3 + c_4x + c_6, \quad \text{with } c_i \in K$$

- Conductor $\mathcal{N} \subset \mathcal{O}_K$ (supported on the primes of bad reduction)
- There are finitely many curves with a given conductor

Problem

Compute equations of "the first" elliptic curves over K
(ordered by the norm of the conductor)

- For $K = \mathbb{Q}$ we have the ANTWERP or Cremona tables
- Other number fields: not many systematic tables yet
- Naive enumeration algorithm:
  - list tuples $[c_4, c_6]$
  - compute the conductor (Tate's algorithm)
  - keep those of small conductor
- Curves of small conductor might have c_i's of large height
- How do we know if the list is complete?
- Modularity: elliptic curves (should) correspond to modular forms

Modularity over number fields

- K number field. Let us assume that $h_K^+ = 1$.
- K of signature (n, s): $K \hookrightarrow \mathbb{R}^n \times \mathbb{C}^s$
- Given an ideal $\mathcal{N} \subset \mathcal{O}_K$

$$\Gamma_0(\mathcal{N}) = \{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathcal{O}_K) \colon \mathcal{N} \mid c\} \subset \mathrm{SL}_2(\mathbb{R})^n \times \mathrm{SL}_2(\mathbb{C})^s$$

- $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathcal{H} = \{z = x + iy \colon y > 0\}$ (upper half plane)
- $\mathrm{SL}_2(\mathbb{C})$ acts on $\mathcal{H}_3 = \mathbb{C} \times \mathbb{R}_{>0}$ (hyperbolic 3-space)
- $Y_0(\mathcal{N}) = \Gamma_0(\mathcal{N}) \backslash \mathcal{H}^n \times \mathcal{H}_3^s$
  - e.g. $K = \mathbb{Q}$: it is the (open) modular curve
- $H^{n+s}(Y_0(\mathcal{N}), \mathbb{C})$ finite dimensional vector space
  - Admits a description in terms of modular forms for $\Gamma_0(\mathcal{N})$
  - Hecke operators $T_\mathfrak{l}$ for primes $\mathfrak{l} \nmid \mathcal{N}$
- Rational eigenclass $f \in H^{n+s}(Y_0(\mathcal{N}), \mathbb{C})$ such that

$$T_\mathfrak{l} f = a_\mathfrak{l} f \text{ with } a_\mathfrak{l} \in \mathbb{Z} \text{ for all } \mathfrak{l}$$

- Conjecture: $f \rightsquigarrow E_f/K$

Modularity over number fields

- $f \in H^{n+s}(Y_0(\mathcal{N}), \mathbb{C})$ a (non-trivial) rational eigenclass

Conjecture

There is an elliptic curve $^{(*)}$ E_f/K of conductor $\mathcal{N}$ corresponding to f:

$$\#E_f(\mathcal{O}_K/\mathfrak{l}) = |\mathfrak{l}| + 1 - a_{\mathfrak{l}} \text{ for all } \mathfrak{l} \nmid \mathcal{N}$$

Conversely: any (non-CM) curve E/K is isogenous to E_f for some f.

$(*)$: If K is totally imaginary, E_f may be an abelian surface

- It's known for $K = \mathbb{Q}$ (Eichler–Shimura + Modularity Theorem) and in many cases for K totally real.
- Much less is known if K has a complex place
- $H^{n+s}(Y_0(\mathcal{N}), \mathbb{C})$: very concrete and (let's say) can be computed

Problem

Given a rational eigenclass $f \in H^{n+s}(Y_0(\mathcal{N}), \mathbb{C})$, construct E_f.

- For $K = \mathbb{Q}$ this is the classical Eichler–Shimura construction

The Eichler-Shimura construction

- If $K = \mathbb{Q}$ then $H^1(Y_0(N), \mathbb{C}) \longleftrightarrow$ classical modular forms
- $f(z) = \sum_{j\geq 1} a_j e^{2\pi ijz}$ with $a_j \in \mathbb{Z}$
- Lattice $\Lambda_f = \{\int_\tau^{\gamma\tau} 2\pi i f(z)dz \colon \gamma \in \Gamma_0(N)\} \subset \mathbb{C}$

Theorem (Manin)

Λ_f is the period lattice of E_f. That is, $\mathbb{C}/\Lambda_f \sim E_f(\mathbb{C})$

- Explicit formulas for $c_4(\Lambda_f)$ and $c_6(\Lambda_f)$, hence an equation of E_f
  - Cremona's tables: curves up to $N = 350,000$ (and increasing)
- Why does this work?
  - There is some geometry behind: $\mathrm{Jac}(X_0(N)) \longrightarrow E_f$
- K totally real $\rightsquigarrow$ f Hilbert modular form
  - Eichler–Shimura generalizes, at least in some cases (e.g. $[K \colon \mathbb{Q}]$ odd or there exists a prime $\mathfrak{p} \,||\, \mathcal{N}$)
  - Some computations (Voight–Willis, Nelson)

What if K has a complex place?

- $Y_0(\mathcal{N}) = \Gamma_0(\mathcal{N})\backslash\mathcal{H}^n \times \mathcal{H}_3^s$ is not an algebraic variety anymore
- Simplest case: K imaginary quadratic
  - $f \rightsquigarrow$ Bianchi modular form
  - $\{\int_\gamma \omega_f \colon \gamma \in H_1(\Gamma_0(\mathcal{N})\backslash\mathcal{H}_3, \mathbb{Z})\}$ is a lattice in $\mathbb{R}$: doesn't give E_f
- Apparently: no geometric construction of E_f for non-totally real K

Our goal

- Propose a conjectural analytic construction of E_f, under the additional assumption that there exists a prime $\mathfrak{p} \mid\mid \mathcal{N}$
- Provide numerical evidence for the conjecture

- The construction is a (rather straightforward) generalization of the p-adic uniformizations arising in the theory of Stark–Heegner points (Bertolini–Darmon, Dasgupta, M. Greenberg, Trifkovic,...)
- Compute the $\mathfrak{p}$-adic lattice: replace $\mathbb{C}$ by $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}}_p}$
  - Tate's uniformization: $E(\mathbb{C}_p) \simeq \mathbb{C}_p^\times/\Lambda_E$ for some $\Lambda_E \subset \mathbb{C}_\mathfrak{p}^\times$

The $\mathfrak{p}$-adic integration pairing

- Recall the integration pairing in the Eichler–Shimura construction

$$\begin{array}{ccc} H^0(\Gamma_0(N), \Omega^1_{\mathcal{H}}) \times H_0(\Gamma_0(N), \mathrm{Div}^0(\mathcal{H})) & \longrightarrow & \mathbb{C} \\ (f(z)dz, \tau_2 - \tau_1) & \longmapsto & \int_{\tau_1}^{\tau_2} f(z)dz \end{array}$$

- In fact: $f(z)dz \in H^0(\Gamma_0(N), \Omega^1_{\mathcal{H}})$ and $\tau_2 - \tau_1 \in H_0(\Gamma_0(N), \mathrm{Div}^0(\mathcal{H}))$
- Replace $\mathcal{H}$ by the $\mathfrak{p}$-adic upper half plane $\mathcal{H}_\mathfrak{p} = \mathbb{C}_p \setminus K_\mathfrak{p}$
    - $\Omega^1_{\mathcal{H}_\mathfrak{p}}$ = rigid analytic differentials on $\mathcal{H}_\mathfrak{p}$
    - Coleman integral: $\omega \in \Omega^1_{\mathcal{H}_\mathfrak{p}},\ \tau_1, \tau_2 \in \mathcal{H}_\mathfrak{p} \rightsquigarrow \int_{\tau_2}^{\tau_1} \omega \in \mathbb{C}_p$
    - Multiplicative integral: $\omega \in \Omega^1_{\mathcal{H}_\mathfrak{p}}(\mathbb{Z}) \rightsquigarrow \times\!\!\!\!\int_{\tau_2}^{\tau_1} \omega \in \mathbb{C}_p^\times$
    - $\times\!\!\!\!\int \colon \Omega^1_{\mathcal{H}_\mathfrak{p}}(\mathbb{Z}) \times \mathrm{Div}^0(\mathcal{H}_\mathfrak{p}) \longrightarrow \mathbb{C}_\mathfrak{p}^\times$
- Multiplicative integration pairing:

$$\times\!\!\!\!\int \colon H^{n+s}(\Gamma, \Omega^1_{\mathcal{H}_\mathfrak{p}}(\mathbb{Z})) \times H_{n+s}(\Gamma, \mathrm{Div}^0(\mathcal{H}_\mathfrak{p})) \longrightarrow \mathbb{C}_p^\times$$

- S-arithmetic group: $\Gamma = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathcal{O}_K[\frac{1}{\mathfrak{p}}]) \colon \mathcal{N} \mid c\}$
- More generally: $\Gamma \subset B^\times$ non-split quaternion algebras
    - $n + s \rightsquigarrow$ number of infinite places of K at which B splits

The $\mathfrak{p}$-adic lattice

- $\times\!\!\!\!\!\!\int : H^{n+s}(\Gamma, \Omega^1_{\mathcal{H}_\mathfrak{p}}(\mathbb{Z})) \times H_{n+s}(\Gamma, \mathrm{Div}^0(\mathcal{H}_\mathfrak{p})) \longrightarrow \mathbb{C}_p^\times$
- Our data: $f \in H^{n+s}(\Gamma_0(\mathcal{N}), \mathbb{Q})$ rational eigenclass
- $H^{n+s}(\Gamma, \Omega^1_{\mathcal{H}_\mathfrak{p}}(\mathbb{Z}))$ is a Hecke module
  - There exists $\omega_f \in H^{n+s}(\Gamma, \Omega^1_{\mathcal{H}_\mathfrak{p}}(\mathbb{Z}))$ with the same eigenvalues as f
- $0 \longrightarrow \mathrm{Div}^0\mathcal{H}_\mathfrak{p} \longrightarrow \mathrm{Div}\mathcal{H}_\mathfrak{p} \longrightarrow \mathbb{Z} \longrightarrow 0$
  - induces a connecting map $H_{n+s+1}(\Gamma, \mathbb{Z}) \xrightarrow{\delta} H_{n+s}(\Gamma, \mathrm{Div}^0\mathcal{H}_\mathfrak{p})$
- Define $\Lambda_f = \{\times\!\!\!\!\!\!\int_{\delta\Delta} \omega_f : \Delta \in H_{n+s+1}(\Gamma, \mathbb{Z})\} \subset \mathbb{C}_p^\times$

Conjecture

$\mathbb{C}_p^\times/\Lambda_f$ is isogenous to $E_f/\mathbb{C}_p$

- For $K = \mathbb{Q}$ this is proven (Darmon, [DG], [LRV])
- For $K \neq \mathbb{Q}$ it is open
  - Λ_f is explicitly computable in some cases
  - extensive numerical evidence for the conjecture
  - in practice, this can be used to compute E_f

Algorithms and computations

- Computational restriction: only work with H_1 and H^1
  - This translates into: K must have at most one complex place
- Homology and cohomology computations:
  - Compute $\Gamma_0(\mathcal{N})$ and Γ (algorithms of J. Voight and A. Page)
  - Compute the Hecke action, diagonalize and find rational lines
- Integration
  - Teitelbaum: $\Omega^1_{\mathcal{H}_\mathfrak{p}}(\mathbb{Z}) \simeq \mathrm{Meas}_0(\mathbb{P}^1(K_\mathfrak{p}), \mathbb{Z})$
  - Need integrals of the form $\times\!\!\!\!\!\!\int_{\mathbb{P}^1(K_\mathfrak{p})} \left(\frac{t-\tau_1}{t-\tau_2}\right) d\mu_f(t)$
  - Riemann products $\rightsquigarrow$ exponential algorithm
  - use overconvergent cohomology instead $\rightsquigarrow$ polynomial algorithm (generalization of Steven's overconvergent modular symbols)

An explicit example

- $K = \mathbb{Q}(r)$ with $r^4 - r^2 - 4r - 1 = 0$. Has signature $(2,1)$
- $\mathcal{N} = (r^3 - 4)\mathcal{O}_K$, an ideal of norm 17
- $\Gamma_0(\mathcal{N}) \subset B^\times$ ($\mathrm{disc}(B/K) = (1)$ and ramifies at the real places)
- There is a rational eigenclass in $f \in H^1(\Gamma_0(\mathcal{N}), \mathbb{Q})$
  - $\omega_f \in H^1(\Gamma, \mathrm{Meas}_0(\mathbb{P}^1(\mathbb{Q}_{17}, \mathbb{Z})))$ and $\gamma \in H_2(\Gamma_0(\mathcal{N}), \mathbb{Z})$

$$q_E = \times\!\!\!\!\!\!\int_{\delta\gamma} \omega_f = 10 \cdot 17^{-1} + 11 + 13 \cdot 17 + 7 \cdot 17^2 + 7 \cdot 17^3 + 13 \cdot 17^4 + 9 \cdot 17^5 + \cdots + O(17^{100})$$

- We get 17-adic approximations to $c_4, c_6 \in \mathbb{Q}_{17}$
- They are close to these elements in K:

$$c_4 = -1325859270120180r^3 - 2460982567523193r^2 - 3242072888399232r - 714309328055430$$

$$c_6 = 78543185680947745285236r^3 + 145787275553784015951756r^2 + 192058643480032231752528r + 42315298049698090866126$$

- Check that the curve $y^2 = x^3 + c_4 x + c_6$ has indeed conductor $\mathcal{N}$
- Similarly: over 300 curves over fields of degree 2, 3, 4, 5.

Computing equations of elliptic curves over number fields via *p*-adic methods

Xevi Guitart[1] Marc Masdeu[2] Haluk Sengun[3]

[1]Institut für Experimentelle Mathematik, Essen

[2]University of Warwick

[3]University of Sheffield

Conference for young researchers in arithmetic and algebraic geometry, Bonn Oct 2014