A *p*-adic Construction of Points on Elliptic Curves over Imaginary Quadratic fields

Mak Trifković

Appetizer

The elliptic curve over $F = \mathbb{Q}(\sqrt{-3})$ given by $E: y^2 + xy = x^3 + \frac{3 + \sqrt{-3}}{2}x^2 + \frac{1 + \sqrt{-3}}{2}x$ has a $K = F(\sqrt{22 + \sqrt{-3}})$ -valued point (x, y) with

$$\begin{aligned} x &= \frac{125460788 - 629994\sqrt{-3}}{127165927} \\ y &= \frac{12488668253575 + 1451573987512\sqrt{-3}}{31646131095439} \sqrt{22 + \sqrt{-3}} \\ &- \frac{62730394 - 314997\sqrt{-3}}{127165927}. \end{aligned}$$

Modularity of Elliptic Curves over IQ Fields

Let $F = \mathbb{Q}(\sqrt{d})$ be a Euclidean imaginary quadratic field (so $d \in \{-1, -2, -3, -7, -11\}$).

Langlands predicts:

Elliptic curve
$$E_{/F}$$
 (with $\operatorname{End}(E) \otimes \mathbb{Q} \neq F$)
 \uparrow (conjectured)
A \mathbb{C}^3 -valued harmonic 1-form on the upper half-space
 $\mathcal{H}^{(3)} = \mathbb{C} \times \mathbb{R}_{>0}$

Such differentials on $\mathcal{H}^{(3)}$ allow for an elementary description of modularity in this case – amenable to computations.

The Geometry of the Upper Half-Space

Think of $(z,t) \in \mathcal{H}^{(3)}$ as the quaternion $z + tj \in \mathbb{H}$.

This allows us to define an action of $GL_2(\mathbb{C})$ on $\mathcal{H}^{(3)}$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : h \mapsto (ah+b)(ch+d)^{-1},$$

A basis of 1-forms is given by the triple

$$\vec{\beta} = \left(\frac{-dz}{t}, \frac{dt}{t}, \frac{d\bar{z}}{t}\right).$$

Congruence subgroup: for $\mathcal{N} \subset \mathcal{O}_K$ an ideal, set

$$\Gamma_0(\mathcal{N}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathcal{O}_F) | c \in \mathcal{N} \right\}$$

(Note we're working with GL_2 rather than SL_2).

Definition 1. A cusp form of weight 2 on $\Gamma_0(\mathcal{N})$ is a vector-valued function $\vec{f}: \mathcal{H}^{(3)} \to \mathbb{C}^3$ (row vectors) satisfying

- (Invariance) The harmonic 1-form $\vec{f} \cdot \vec{\beta}$ is
- invariant under $\gamma \in \Gamma_0(\mathcal{N})$; (Cuspidality) $\int_{\mathbb{C}/\mathcal{O}_F} (\gamma^*) (\vec{f} \cdot \vec{\beta}) = 0$ for all $\gamma \in PSL_2(\mathcal{O}_F)$ (i.e. the constant term of the Fourier-Bessel expansion of \vec{f} - see below – at the cusp $\gamma^{-1}\infty$ is zero).

The space of all plus-cusp forms of weight 2 and level \mathcal{N} is denoted by $S_2^+(\mathcal{N})$.

Hecke theory entirely analogous to \mathbb{Q} .

FOURIER-BESSEL EXPANSION

A cusp form has a Fourier-Bessel expansion:

$$\vec{f}(z,t) = \sum_{(\alpha)\neq 0} c(\alpha) t^2 \vec{K} \left(\frac{4\pi |\alpha| t}{\sqrt{|D|}} \right) \sum_{\epsilon \in \mathcal{O}_F^{\times}} \psi \left(\frac{\epsilon \alpha z}{\sqrt{D}} \right).$$

where

$$\psi(z) = e^{4\pi i \operatorname{Re} z}, \vec{K}(t) = \left(-\frac{i}{2}K_1(t), K_0(t), \frac{i}{2}K_1(t)\right).$$

The hyperbolic Bessel functions $K_i(t)$ are rapidly decreasing as $t \to \infty$, and $\psi(z)$ is a character of the additive group, so $\vec{K}\psi$ is analogous to $e^{-2\pi y}e^{2\pi i x} = e^{2\pi i z}$.

THE SHIMURA-TANIYAMA CONJECTURE

Conjecture 1 (Shimura-Taniyama). To every isogeny class of elliptic curves $E_{/F}$ of conductor ideal \mathcal{N} with $End(E) \otimes \mathbb{Q} \neq F$ there corresponds a newform $\vec{f} \in S_2^+(\mathcal{N})$ characterized by $c(\mathfrak{p}) = N\mathfrak{p} + 1 - \#E(\mathbb{F}_{\mathfrak{p}}).$

for all prime ideals $\mathfrak{p} \neq 0$.

This is a much weaker claim than Shimura-Taniyama over \mathbb{Q} :

1. Manin: there exists a single positive real period Ω for which

$$\left\{\int_{P}^{\gamma P} \vec{f} \cdot \vec{\beta} | \gamma \in \Gamma_0(\mathcal{N})\right\} = \Omega \mathbb{Z}$$

Can't reconstruct the Weierstrass lattice of $E(\mathbb{C})$.

2. $\mathcal{H}^{(3)}$ is a 3D real manifold, so there can't be a holomorphic modular parametrization $\mathcal{H}^{(3)} \to E$ – bad news for modular constructions of points.

A Comparison With Modular Forms on $GL_2(\mathbb{A}_{\mathbb{Q}})$

Let E be an elliptic curve over \mathbb{Q} . Two views of the modular parametrization of E:

Algebraic Geometry. There is a morphism of algebraic curves $\psi : X_0(N) \to E$ defined over \mathbb{Q} .

Heegner points: $\mathcal{O} \subset K$ an order in an imaginary quadratic field N factors as $N = \mathcal{N} \cdot \overline{\mathcal{N}}$.

 $x_c = (\mathbb{C}/\mathcal{O} \to \mathbb{C}/\mathcal{N}^{-1}) \in X_0(N)(H_c)$, where H_c is the ring class field of K of conductor c.

Applying ϕ yields essentially the only known systematic construction of rational points on E.

Analysis. The composed map

$$\psi: \mathcal{H} \to \mathcal{H}/\Gamma_0(N) \hookrightarrow X_0(N)(\mathbb{C}) \to E(\mathbb{C})$$

can be computed as follows:

$$\psi(\tau) = c \int_{i\infty}^{\tau} f_E(z) dz = \sum_{n=1}^{\infty} \frac{a_n}{n} e^{2\pi i n \tau} \pmod{\Lambda_E},$$

Heegner points: If $\mathcal{O} = \mathbb{Z}[\tau]$, the Heegner point is given by $\psi(\tau)$.

THE DICTIONARY

Over F, no algebraic geometry, but the analytic construction still makes sense, provided we work at a finite prime $\pi | \mathcal{N}$ instead of ∞ .

Complex	$p ext{-adic}$
1. Archimedean place ∞	1. Non-Archimedean place $\pi \ \mathcal{N} \ $
2. K/\mathbb{Q} imaginary quadratic	2. K/F quadratic, inert at π
(local degree 2 at ∞)	(local degree 2 at π)
3. Poincaré upper half-plane \mathcal{H}	3. Hyperbolic upper half-space $\mathcal{H}^{(3)}$
(domain of $f(z)dz$)	(domain of $\omega_{\vec{f}}$)
4. Poincaré upper half plane \mathcal{H} (\supset quadratic irrationalities $K \cap \mathcal{H} \neq \emptyset$)	4. <i>p</i> -adic upper half-plane $\mathcal{H}_{\pi} = \mathbb{P}^{1}(\mathbb{C}_{p}) - \mathbb{P}^{1}(F_{\pi})$ $(\supset K \cap \mathcal{H}_{\pi} \neq \emptyset)$
5. Weierstrass parametrization	5. Tate parametrization
$\Phi_{Wei} : \mathbb{C}/\Lambda_E \to E(\mathbb{C})$	$\Phi_{Tate}: \mathbb{C}_p^{\times}/q_E^{\mathbb{Z}} \to E(\mathbb{C}_p)$
6. Complex line integral	6. 'Mixed multiplicative integral'
$\int_{\tau_1}^{\tau_2} f(z) dz \in \mathbb{C}, \tau_1, \tau_2 \in \mathcal{H}^*$	$ \oint_{\tau_1}^{\tau_2} \int_r^s \omega_{\vec{f}} \in \mathbb{C}_p^{\times}, \tau_1, \tau_2 \in \mathcal{H}_{\pi}, \\ r, s \in \mathbb{P}^1(F) $

The Conjecture

Conjecture 2. Let $\tau_1, \tau_2 \in \mathcal{O}_K[1/\pi]$ such that $\mathcal{O}_F[1/\pi][\tau_1] = \mathcal{O}_F[1/\pi][\tau_1] = \mathcal{O}$. There is an explicit matrix $\gamma_{\mathcal{O}}$ with the same characteristic polynomial as a fundamental unit of $\mathcal{O}_K[1/\pi]^{\times}$, and an integer $t \in \mathbb{Z}$, such that the point

$$J_{\tau_1,\tau_2} = \Phi_{Tate}\left(\left[\oint_{\tau_1}^{\tau_2} \int_r^{\gamma_{\mathcal{O}}r} \omega_{\vec{f}} \right]^t \right) \in \mathbb{C}_p^{\times}/q_E^{\mathbb{Z}} \cong E(\mathbb{C}_p).$$

(a 'Stark-Heegner point') is in fact in $E(K^{ab})$.

A more precise version of the conjecture, stated in terms of a conjectural 'indefinite mixed multiplicative integral', allows a precise description of the action of $Gal(K^{ab}/K)$ on (a variant of) J_{τ_1,τ_2} .

This gives a conjectural answer to a special case (K totally complex quartic field) of

Hilbert's 12th Problem For an arbitrary field K, is it possible to generate K^{ab} by special values of analytic functions?

So far, only known answers are for \mathbb{Q} and K imaginary quadratic.

For more general fields, we may have to allow p-adic as well as complex analysis.

Analogy with Darmon's Stark-Heegner Points

A) Darmon's setting: $E_{/\mathbb{Q}},$ auxiliary K real quadratic

 \Downarrow Conjecture

- Stark-Heegner points defined over ring class fields of K
- Hilbert's 12th problem for real quadratic K.

B) Our setting: $E_{/F}$, auxiliary quadratic K/F

\Downarrow Conjecture

- Stark-Heegner points defined over ring class fields of K
- Hilbert's 12th problem for totally complex quartic K.

In both cases, the main ingredients:

(1) Modular symbols (2) rk $\mathcal{O}_K^{\times} = 1$

In the imaginary quadratic case, no modular parametrization.

THE COMPUTATION

Proposition 1 (Manin-Drinfeld). There exists a $d \in \mathbb{Z}$ such that for any two cusps $r, s \in \mathbb{P}^1(F)$, $\int_r^s \vec{f} \cdot \vec{\beta} \in \frac{\Omega}{d}\mathbb{Z}$.

The \mathbb{Z} -valued modular symbol

$$\phi\{r \to s\} = \frac{d}{\Omega} \int_{r}^{s} \vec{f} \cdot \vec{\beta}, \qquad r, s \in \mathbb{P}^{1}(F)$$

is an eigensymbol for U_{π} :

$$U_{\pi}\phi_{\{}r \to s\} = \sum_{\alpha \in \mathcal{O}_{F}/\pi} \phi_{\{}\frac{r+\alpha}{\pi} \to \frac{s+\alpha}{\pi}\} = c(\pi)\phi_{\{}r \to s\}.$$

We can compute the mixed multiplicative integrals if we can lift this to a U_{π} eigensymbol with values in measures on \mathcal{O}_{π} . Pollack-Stevens/Pollack-Darmon polynomial-time algorithm for computing the mixed multiplicative integral:

(1) Lift ϕ to *some* modular symbol Φ_0 with values in measures on \mathcal{O}_{π} (need not be a U_{π} eigensymbol):

$$\phi\{r \to s\} = \int_{\mathcal{O}_{\pi}} d\Phi_0\{r \to s\}$$

(2) Iterate U_{π} :

$$\Phi = \lim_{n \to \infty} U_{\pi}^n \Phi_0$$

is a U_{π} -eigensymbol.

(3) Compute the integrals from Φ by simple algebra.

Q: How do you find the initial lift Φ_0 ?

Biggest problem computationally: need to specify Φ_0 values on edge of the fundamental domain for $\Gamma_0(\mathcal{N})$, with each of the (many) faces imposing a $\mathbb{Z}[\Gamma_0(\mathcal{N})]$ -linear relation.

A: You don't!

For any pair of cusps r, s, choose $\Phi_0\{r \to s\}$ to be an arbitrary measure with total integral $\phi\{r \to s\}$ (not necessarily satisfying face relations). Then

$$\lim_{n \to \infty} U_{\pi}^n \Phi_0$$

turns out to be an honest modular symbol, i.e. satisfies the face relations even thought Φ_0 didn't.

p-ADIC APPROXIMATION

$$x_{p-\text{adic}} = 56 \cdot 73^{-2} + 43 \cdot 73^{-1} + 35 + 68 \cdot 73 + 36 \cdot 73^{2} + 61 \cdot 73^{3} + 27 \cdot 73^{4} + 36 \cdot 73^{5} + 69 \cdot 73^{6} + 58 \cdot 73^{7} \dots$$

Find the shortest element of F which agrees with $x_{p-\text{adic}}$ to given precision

$$x_{\rm global} = \frac{125460788 - 629994\sqrt{-3}}{127165927}$$

The point is:

1. The *p*-adic values of x_{p-adic} and y_{p-adic} satisfy the cubic equation to the given precision.

2. The global values x_{global} and y_{global} are obtained by *independently* approximating their *p*-adic counterparts.

3. x_{global} and y_{global} satisfy the cubic equation *exactly*.

More Examples

Consider the curve over $F = \mathbb{Q}(\sqrt{-11})$ given by $E: y^2 + y = x^3 + \frac{1 - \sqrt{-11}}{2}x^2 - x,$ with prime conductor $\pi = 6 + \sqrt{-11}$ of norm p = 47.

Take $K = F(\sqrt{13})$, whose Hilbert class field H is of degree 5.

A refinement of the Conjecture produces five 47adic Stark-Heegner points $\{J_1, \ldots, J_5\}$ which conjecturally form an orbit under the action of $Gal(H/K) \cong$ Cl(K). We find that, to 20 digits of 47-adic accuracy, the x and the y-coordinates of the J_i 's seem to be the roots of global polynomials

$$\begin{aligned} f_x(T) &= T^5 + (1 - \sqrt{-11})T^4 - \frac{13 + 5\sqrt{-11}}{2}T^3 - 9T^2 - \frac{1 + \sqrt{-11}}{2}T + \frac{3 - \sqrt{-11}}{2}\\ f_y(T) &= T^5 - \frac{3 + \sqrt{-11}}{2}T^4 + \frac{25 - \sqrt{-11}}{2}T^3 + (30 - 2\sqrt{-11})T^2 + \frac{23 + \sqrt{-11}}{2}T + \\ &+ \frac{15 + 5\sqrt{-11}}{2} \end{aligned}$$

respectively, both of which do generate the Hilbert class field of K.

Let $\alpha = \frac{1+\sqrt{-11}}{2}$.

Let $K = F(\sqrt{-31\alpha + 13})$ of class number 11. As in the previous example, we get a conjectural orbit $\{J_1, \ldots, J_{11}\}$ whose x and y coordinates satisfy respectively the polynomials

$$\begin{split} f_x(T) &= T^{11} + \left(-\frac{1001}{81}\alpha + \frac{17}{27}\right) T^{10} + \left(\frac{323272}{6561}\alpha - \frac{424678}{2187}\right) T^9 + \left(\frac{1089383}{2187}\alpha + \frac{171223}{729}\right) T^8 + \\ &+ \left(-\frac{6204140}{6561}\alpha + \frac{6960362}{2187}\right) T^7 + \left(-\frac{23838260}{6561}\alpha - \frac{2734360}{2187}\right) T^6 + \\ &+ \left(\frac{14741863}{6561}\alpha - \frac{21734605}{2187}\right) T^5 + \left(\frac{31785055}{6561}\alpha + \frac{945548}{2187}\right) T^4 + \\ &+ \left(-\frac{187616}{243}\alpha + \frac{345851}{81}\right) T^3 + \left(-\frac{1233710}{6561}\alpha + \frac{39776}{2187}\right) T^2 + \\ &+ \left(-\frac{418849}{2187}\alpha + \frac{404362}{729}\right) T + \left(-\frac{152569}{2187}\alpha - \frac{71186}{729}\right) \end{split}$$

again to 20 digits of 47-adic accuracy. Both of these do in fact cut out the Hilbert Class field of K.

BASE CHANGE

 $g \in S_2(\Gamma_0(N))$ - modular form on \mathcal{H} , F imaginary quadratic field of class number 1.

base change
$$\begin{array}{ccc} g & \leftrightarrow & E_{/\mathbb{Q}} \\ \downarrow & & \downarrow \\ \vec{g} & \leftrightarrow & E_{/F} \end{array}$$

Periods over \mathbb{Q} . Modular symbols of g (over \mathbb{Q}):

$$\{a \to b\}_{\mathbb{Q}} = \int_{a}^{b} g(z)dz,$$
$$\{a \to b\}_{\mathbb{Q}}^{\pm} = \frac{\{a \to b\}_{\mathbb{Q}} \pm \{-a \to -b\}_{\mathbb{Q}}}{2}.$$

 $\Omega_+, \Omega_- \in \mathbb{R}_+$: smallest real and imaginary parts of periods $\{a \to b\}_{\mathbb{Q}}$.

 $\Omega_{\mathbb{C}} = \Omega_{+}\Omega_{-}$: area of $E(\mathbb{C})$ for E the strong Weil curve corresponding to g.

Proposition 2. a) (Manin-Drinfeld Lemma) For any two cusps $a, b \in \mathbb{P}^1(\mathbb{Q})$, there exist $r_+, r_- \in \mathbb{Q}$ with

$$\{a \to b\}_{\mathbb{Q}}^+ = r_+\Omega_+, \{a \to b\}_{\mathbb{Q}}^- = r_-i\Omega_-.$$

b) (Birch Lemma) Let $\chi : (\mathbb{Z}/f\mathbb{Z})^{\times} \to \mathbb{C}^{\times}$ be a primitive Dirichlet character. Denote by

$$\tau_{\mathbb{Q}}(\chi) = \sum_{k=0}^{f-1} \chi(a) e^{\frac{2\pi i a}{f}}$$

its Gauss sum. Set $\Omega = \Omega_+$ if χ is even, and $\Omega = i\Omega_-$ if χ is odd. The special value of the twisted L-function of g is given by

$$L(g,\chi,1) = \overline{\tau_{\mathbb{Q}}(\chi)}^{-1} \sum_{k \in \mathbb{Z}/f\mathbb{Z}} \bar{\chi}(k) \left\{ \frac{k}{f} \to \infty \right\}_{\mathbb{Q}} = r_{\chi}\Omega,$$

for some $r_{\chi} \in \mathbb{Q}(\chi)$.

Periods over F. Modular symbol of \vec{g} (over F):

$$\{a \to b\}_F = \frac{16\pi^2}{w |D|} \int_a^b \vec{g} \cdot \vec{\beta}.$$

 $\Omega_F \in \mathbb{R}_+$: smallest positive real period of \vec{f} .

Proposition 3. a) (Manin-Drinfeld Lemma) For any two cusps $a, b \in \mathbb{P}^1(F)$, there exists $r \in \mathbb{Q}$ with

$$\{a \to b\}_F = r\Omega_F.$$

b) (Birch Lemma) Let $\chi : (\mathcal{O}_F/\varphi)^{\times}/\mathcal{O}_F^{\times} \to \mathbb{C}^{\times}$ be a primitive 'Dirichlet' character (i.e. a Hecke character with trivial archimedean component) with Gauss sum

$$\tau_F(\chi) = \sum_{\alpha \in \mathcal{O}_F/\varphi} \chi(\alpha) e^{2\pi i \operatorname{Tr}_{F/\mathbb{Q}} \frac{\alpha}{\varphi \sqrt{D}}}.$$

Then the special value $L(\vec{f}, \chi, 1)$ is given by

$$L(\vec{g},\chi,1) = \overline{\tau_F(\chi)}^{-1} \sum_{\kappa \in \mathcal{O}_F/\varphi} \bar{\chi}(\kappa) \left\{ \frac{\kappa}{\varphi} \to \infty \right\}_F = r_{\chi} \Omega_F,$$

for some $r_{\chi} \in \mathbb{Q}(\chi)$.

Proposition 4. Let F be an imaginary quadratic field of class number 1. Let $g \in S_2(N)$ be a newform on \mathcal{H} and \vec{g} its base-change to $\mathcal{H}^{(3)}$. Let $\Omega_{\mathbb{C}} = \Omega_+\Omega_-$ be the complex period of g, and let Ω_F be the smallest positive real period of \vec{g} . Then

(1)
$$\frac{1}{\sqrt{|D|}}\frac{\Omega_{\mathbb{C}}}{\Omega_F} \in \mathbb{Q}.$$

Proof. $\chi : (\mathbb{Z}/f\mathbb{Z})^{\times} \to \mathbb{C}^{\times}$ - primitive Dirichlet character of conductor prime to ND. By definition of base change

$$L(\vec{g},\chi \circ N_{F/\mathbb{Q}},1) = L(g,\chi,1)L(g,\chi \varepsilon_F,1) = L(g,\chi,1)L(g_{\varepsilon_F},\chi,1),$$

Expressing in terms of modular symbols,

$$\overline{\tau_F(\chi \circ N_{F/\mathbb{Q}})^{-1}}r_F\Omega_F = \left[\overline{\tau_{\mathbb{Q}}(\chi)}\overline{\tau_{\mathbb{Q}}(\chi\varepsilon_F)}\right]^{-1}r_{\mathbb{Q}}i\Omega_+\Omega_-.$$

with $r_F, r_{\mathbb{Q}} \in \mathbb{Q}(\chi)$ (we get both Ω_+ and Ω_- since F is imaginary, so the associated character ϵ_F is odd). The Gauss sums are related by

$$\tau_F(\chi \circ N_{F/\mathbb{Q}}) = -i \frac{\tau_{\mathbb{Q}}(\chi) \tau_{\mathbb{Q}}(\chi \varepsilon_F)}{\sqrt{|D|}},$$

which yields

$$\sqrt{|D|}r_F\Omega_F = -r_{\mathbb{Q}}\Omega_{\mathbb{C}}.$$

A theorem of Rohrlich guarantees the existence of infinitely many characters χ such that $L(g, \chi, 1) \neq 0 \neq L(g_{\varepsilon_F}, \chi, 1)$, i.e. such that $r_F \neq 0$. Divide by r_F :

$$\frac{1}{\sqrt{|D|}} \frac{\Omega_{\mathbb{C}}}{\Omega_F} \in \mathbb{Q}(\chi).$$

Repeating this argument with a χ' of conductor prime to that of χ , we get that

$$\frac{1}{\sqrt{|D|}} \frac{\Omega_{\mathbb{C}}}{\Omega_F} \in \mathbb{Q}(\chi) \cap \mathbb{Q}(\chi') = \mathbb{Q},$$

as desired

		l
		l
		L
		L

Remark: The base change identity

$$L(\vec{g}, \chi \circ N_{F/\mathbb{Q}}, 1) = L(g, \chi, 1)L(g, \chi \varepsilon_F, 1)$$

can be read as a linear equation in $\left\{\frac{\alpha}{f} \to \infty\right\}_F$

Can we choose enough χ 's to completely determine $\{a \to b\}_F$ in terms of $\{x \to y\}_{\mathbb{Q}}$?

Can we get an explicit formula in this way?

If so, in base change cases there might be hope of relating the Stark-Heegner points over F with classical Heegner points, and use that to provide evidence for the conjecture that Stark-Heegner points are global.