Efficient computations of p-adic L-functions via overconvergent modular symbols

(and applications to Stark-Heegner points)

Robert Pollack — Boston University

http://math.bu.edu/~rpollack/

Main results

1) An algorithm that computes p-adic L-functions of elliptic curves in polynomial time.

(joint with Glenn Stevens)

2) This algorithm then leads to a (conjectural) algorithm to compute Stark-Heegner points in polynomial time. (These are global points on elliptic curves defined over ring class fields of real quadratic extensions of $\mathbf{Q}$.)

(joint with Henri Darmon)

Heegner points

Let E be an elliptic curve over $\mathbf{Q}$ of conductor N.
Let K be a imaginary quadratic extension of $\mathbf{Q}$ in which N splits completely.

Heegner points $\longrightarrow$ systematic collections of global points on elliptic curves (over ring class fields of K)

To construct Heegner points on E, first consider the points on $X_0(N)$ which correspond to elliptic curves with complex multiplication by K.

Heegner points

By Wiles, Taylor-Wiles, *et al.*, E corresponds to a modular form f_E which gives rise to a map

$$X_0(N) \xrightarrow{\pi} E.$$

Heegner points are then the images of these CM points on $X_0(N)$ under the map π.

By the theory of complex multiplication, these Heegner points are actually defined over finite extensions of $\mathbf{Q}$ (precisely, over ring class fields of K).

More explicitly...

If $\mathcal{H}$ is the upper half plane, the modular parametrization of E comes from a composition of maps,

$$\mathcal{H}/\Gamma_0(N) \longrightarrow \mathbf{C}/\Lambda \longrightarrow E(\mathbf{C}),$$

where the second map is the Weierstrauss $\wp$-function and the first map is given by complex integration; namely,

$$z \mapsto \int_z^{i\infty} f_E \, dz.$$

The CM points we are considering are then simply the elements of $(\mathcal{H} \cap K)/\Gamma_0(N)$.

Computing Heegner points

One can efficiently compute Heegner points in practice.

First one computes $\int_z^{i\infty} f_E$ to high precision using $f_E = \sum_{n\geq 1} a_n e^{2\pi i z/n}$. (This series converges very quickly if $\mathrm{Im}(z) \gg 0$.)

Then one applies $\wp$ and $\wp'$ to some estimate of this line integral to obtain an approximate point on E.

As long as this point is computed with enough accuracy, one then identifies it as an algebraic number.

Stark-Heegner points

Fix a prime p. Let $K/\mathbf{Q}$ be a real quadratic extension with p inert in K.

Let $E/\mathbf{Q}$ be an elliptic curve of conductor N with $p \mid\mid N$. (For simplicity, we take $N = p$.)

Stark-Heegner points are a p-adic variant of Heegner points (conjecturally) defined over ring class fields of K.

To define them, instead of beginning with the upper half plane $\mathcal{H}$, we now use the p-adic upper half plane $\mathcal{H}_p = \mathbf{C}_p - \mathbf{Q}_p$.

(Note that $\mathbf{C} - \mathbf{R}$ equals two copies of $\mathcal{H}$.)

New notion of CM points

Instead of using the CM points $(\mathcal{H} \cap K)/\Gamma_0(N)$, we now use the points

$$(\mathcal{H}_p \cap K)/\Gamma$$

where $\Gamma = \mathrm{SL}_2(\mathbf{Z}[1/p])$.

The assumption that p is inert in K implies that this last set is non-empty as any embedding of K into $\mathbf{C}_p$ will not land entirely within $\mathbf{Q}_p$.

(Note that in the classical case, if K is an imaginary quadratic extension, then ∞ is inert in K and thus $\mathcal{H} \cap K$ is non-empty.)

p-adic uniformization of E

Instead of using the complex uniformization

$$\mathbf{C}/\Lambda \longrightarrow E(\mathbf{C})$$

we use the (p-adic) Tate uniformization

$$\mathbf{C}_p^\times/q^{\mathbf{Z}} \longrightarrow E(\mathbf{C}_p)$$

where q is the Tate period of E at p.

(Here we are exploiting the fact that $p \mid\mid N$.)

Integration on $\mathcal{H}_p \times \mathcal{H}$

Complex integration was used to define the map

$$\mathcal{H}/\Gamma_0(N) \longrightarrow \mathbf{C}/\Lambda.$$

In place of this, Darmon defines a notion of "integration" on $\mathcal{H}_p \times \mathcal{H}$ combining both complex and p-adic methods!

That is, for any $z_1, z_2 \in \mathcal{H}_p$ and $r, s \in \mathcal{H}$, he constructs a number

$$\int_{z_1}^{z_2} \int_r^s f_E \in \mathbf{C}_p$$

as a p-adic limit of line integrals involving f_E.

Basic properties

This suggestive notation is used since this "double integral" is linear in both the p-adic and complex variables. For instance,

$$\int_{z_1}^{z_2}\int_{r}^{s} f_E + \int_{z_2}^{z_3}\int_{r}^{s} f_E = \int_{z_1}^{z_3}\int_{r}^{s} f_E.$$

Also, it is invariant under the action of $\Gamma = \mathrm{SL}_2(\mathbf{Z}[1/p])$; that is

$$\int_{\gamma z_1}^{\gamma z_2}\int_{\gamma r}^{\gamma s} f_E = \int_{z_1}^{z_2}\int_{r}^{s} f_E$$

for $\gamma \in \Gamma$.

Stark-Heegner points

Using the above double integral, Darmon (conjecturally) constructs a map

$$(\mathcal{H}_p \cap K)/\Gamma \longrightarrow K_p^\times / q^{\mathbf{Z}}$$

where again q is the Tate period of E at p.

Composing with Tate uniformization yields a map

$$(\mathcal{H}_p \cap K)/\Gamma \longrightarrow E(K_p).$$

Stark-Heegner points are then defined to be points in the image of this map.

Fields of definition

Note that in the classical case when K is a quadratic imaginary field, we know that the image of $(\mathcal{H} \cap K)/\Gamma_0(N)$ is not merely contained in $E(\mathbf{C})$, but in $E(\overline{\mathbf{Q}})$.

In the real quadratic case, Darmon conjectures that the image of $(\mathcal{H}_p \cap K)/\Gamma$ is not merely in $E(K_p)$, but in $E(\overline{\mathbf{Q}})$.

Also, as in the classical case, Darmon makes precise conjectures about the field of definition of these points (being a certain ring class field of K) and about the Galois action on these (conjecturally) global points.

Evidence

To test these conjectures, Darmon and Green took elliptic curves E of prime conductor with rank one over K.

They computed approximations to the trace of the basic Stark-Heegner point down to K and compared this to multiples of a generator of $E(K)$.

In each case, the approximation of the Stark-Heegner point agreed with a global point (modulo a power of p equal to the accuracy of their computation).

Accuracy

Unfortunately, they were only able to compute modulo a small power of p and thus were not able in general to recognize a global point from their p-adic computation.

For instance, for $E = X_0(11)$ and $K = \mathbf{Q}(\sqrt{13})$, the basic Stark-Heegner point should equal

$$2 \cdot \left(\frac{105557507041}{21602148048}, -\frac{1}{2} + \frac{15613525573072201}{1144766951937273 6}\sqrt{13} \right)$$

and so very high accuracy is needed to recognize this point!

Thus, without high accuracy, this algorithm cannot be used to find global points.

Obstruction to high accuracy

The most difficult part of the computing Stark-Heegner points is in computing the "double integral"

$$\int_{z_1}^{z_2} \int_r^s f_E \in \mathbf{C}_p.$$

For instance,

$$\int_{z_1}^{z_2} \int_0^{i\infty} f_E = \int_{\mathbf{Z}_p^\times} \log\left(\frac{x - z_1}{x - z_2}\right) \, dL_p(E)$$

where $L_p(E)$ is the p-adic L-function of E. To compute this expression, one needs to be able to compute with the p-adic L-function of the elliptic curve E.

p-adic L-functions

The p-adic L-function of E (denoted by $L_p(E)$) is a distribution on $\mathbf{Z}_p^\times$. (That is, one can "integrate" any nice function on $\mathbf{Z}_p^\times$ against $L_p(E)$.)

The p-adic L-function is uniquely characterized by the fact that

$$\int_{\mathbf{Z}_p^\times} \chi \, dL_p(E) = c \cdot \frac{L(E,\chi,1)}{\Omega_E}$$

where χ is a Dirichlet character of conductor a power of p and c is some explicit constant.

Computing p-adic L-functions

These p-adic L-functions arise from measures on $\mathbf{Z}_p^\times$. Namely,

$$L_p(E)(a + p^n\mathbf{Z}_p) := \frac{1}{a_p^n}\left(\int_{a/p^n}^{i\infty} f_E + \int_{-a/p^n}^{i\infty} f_E\right) \cdot \Omega_E^{-1}$$

which lies in $\mathbf{Z}$.

To naively compute the moments of $L_p(E)$ one would use Riemann sums; that is

$$\int_{\mathbf{Z}_p^\times} x^j \, dL_p(E) \equiv \sum_{a \in (\mathbf{Z}/p^n\mathbf{Z})^\times} a^j \cdot L_p(E)(a + p^n\mathbf{Z}_p) \pmod{p^n}.$$

Computing p-adic L-functions

To compute $L_p(E)(a + p^n\mathbf{Z}_p)$ is relatively easy. On an Athlon 2800 processor, one can compute approximately 1000 per second for $X_0(11)$.

However, to compute the j-th moment $\int_{\mathbf{Z}_p^\times} x^j \, dL_p(E)$ to n p-adic digits of accuracy would take p^n computations of $L_p(E)(a + p^n\mathbf{Z}_p)$.

For instance, to compute the first moment of $L_p(E)$ to 10 p-adic digits would take approximately 1 year of CPU time, 11 digits would take 11 years, $etc.$

This is why DG only computed to low levels of accuracy.

Modular symbols

Let $\Delta = \mathbf{P}^1(\mathbf{Q}) \times \mathbf{P}^1(\mathbf{Q})$. Then $\mathrm{Hom}(\Delta, \mathbf{Q}_p)$ is naturally a right $\mathrm{GL}_2(\mathbf{Q})$-module. If $r, s \in \mathbf{P}^1(\mathbf{Q})$, then

$$(\phi|\gamma)(r,s) = \phi(\gamma r, \gamma s)$$

where γ acts on r, s by linear fractional transformations.

We define the space of $\mathbf{Q}_p$-valued modular symbols of level $\Gamma := \Gamma_0(p)$ to be

$$\begin{aligned} \mathsf{MS}_\Gamma(\mathbf{Q}_p) &:= \mathrm{Hom}_\Gamma(\Delta, \mathbf{Q}_p) \\ &= \left\{ \phi : \Delta \to \mathbf{Q}_p \;\middle|\; \phi|\gamma = \phi \text{ for } \gamma \in \Gamma \right\}. \end{aligned}$$

Modular symbols

An example of a modular symbol of level Γ is

$$\phi_E(r,s) := \left(\int_r^s f_E + \int_{-r}^{-s} f_E \right) \cdot \Omega_E^{-1}$$

The space $\mathsf{MS}_\Gamma(\mathbf{Q}_p)$ has a Hecke action defined by

$$\phi_E \big| U_p = \sum_{a=0}^{p-1} \phi \ \Big| \begin{pmatrix} 1 & a \\ 0 & p \end{pmatrix}$$

and similarly for T_ℓ with $\ell \neq p$.

The symbol ϕ_E is an eigensymbol in that $\phi_E | U_p = a_p \cdot \phi_E$.

Connection to p-adic L-functions

Since

$$L_p(E)(a + p^n\mathbf{Z}_p) = \frac{1}{a_p^n} \cdot \phi_E(a/p^n, i\infty),$$

in order to compute moments of p-adic L-functions, one must compute ϕ_E at p^n points.

We wish to construct a more elaborate modular symbol so that evaluating it at a single ordered pair yields moments of the p-adic L-function.

Overconvergent modular symbols

Set $\mathcal{A}(\mathbf{Z}_p)$ equal to all locally analytic functions on $\mathbf{Z}_p$ and let $\mathcal{D}(\mathbf{Z}_p)$ be the continuous $\mathbf{Q}_p$-dual of $\mathcal{A}(\mathbf{Z}_p)$ – the space of $\mathbf{Q}_p$-valued distributions on $\mathbf{Z}_p$. (Note that $\mathcal{A}(\mathbf{Z}_p)$ is a left Γ-module and thus $\mathcal{D}(\mathbf{Z}_p)$ is a right Γ-module.)

We consider the large space of modular symbols given by

$$\mathrm{MS}_\Gamma(\mathcal{D}(\mathbf{Z}_p)) := \mathrm{Hom}_\Gamma(\Delta, \mathcal{D}(\mathbf{Z}_p))$$

which we will refer to as the space of overconvergent modular symbols of level Γ.

As before, $\mathrm{MS}_\Gamma(\mathcal{D}(\mathbf{Z}_p))$ is naturally a Hecke-module.

Slopes of OMS

Let the slope of an eigensymbol to be equal to the p-adic valuation of its U_p-eigenvalue.

For $h \in \mathbf{R}$, let $\mathsf{MS}_\Gamma(\mathbf{Q}_p)^{(<h)}$ and $\mathsf{MS}_\Gamma(\mathcal{D}(\mathbf{Z}_p))^{(<h)}$ denote the direct sum of the generalized eigenspaces of U_p whose slope is less than h.

For example, since $p \mid\mid N$, we have that $a_p(E) = \pm 1$. Thus ϕ_E has slope 0.

Fact: The operator U_p is a completely continuous operator on the space $\mathsf{MS}_\Gamma(\mathcal{D}(\mathbf{Z}_p))$. In this context, this means that $\mathsf{MS}_\Gamma(\mathcal{D}(\mathbf{Z}_p))^{(<h)}$ is finite dimensional for any h.

Specialization

There is a natural (Hecke-equivariant) map

$$\rho : \mathsf{MS}_\Gamma(\mathcal{D}(\mathbf{Z}_p)) \longrightarrow \mathsf{MS}_\Gamma(\mathbf{Q}_p)$$

given by taking total measure. That is,

$$\rho(\Phi)(r,s) = \int_{\mathbf{Z}_p} 1_{\mathbf{Z}_p} \, d\Phi(r,s).$$

This map must have huge kernel since the target is finite dimensional. Moreover, by Eichler-Shimura theory, the slope of any classical modular symbol is ≤ 1.

Comparison theorem

Theorem (Stevens): The specialization map restricted to symbols of slope less than 1

$$\rho : \mathsf{MS}_\Gamma(\mathcal{D}(\mathbf{Z}_p))^{(<1)} \longrightarrow \mathsf{MS}_\Gamma(\mathbf{Q}_p)^{(<1)}$$

is an isomorphism.

Corollary (Stevens): There exists a unique Hecke-eigensymbol $\Phi_E \in \mathsf{MS}_\Gamma(\mathcal{D}(\mathbf{Q}_p))$ such that $\rho(\Phi_E) = \phi_E$. Moreover,

$$\Phi_E(0, i\infty) = L_p(E)$$

the p-adic L-function of E.

Strategy to compute Φ_E

First lift ϕ_E to any overconvergent modular symbol Φ (not necessarily a Hecke-eigensymbol). Then

$$\Phi = \Phi_E + (\text{something of slope} \geq 1).$$

Then repeatedly apply the operator $\frac{1}{a_p}U_p$ to Φ to yield

$$\frac{1}{a_p^n}\Phi\Big|U_p^n = \Phi_E + p^n \cdot (\text{something of slope} \geq 1).$$

In particular, $\left\{\frac{1}{a_p^n}\Phi\Big|U_p^n\right\} \longrightarrow \Phi_E$ and we are gaining an extra p-adic digit of accuracy with each application of U_p!

Computing in practice

To carry out this algorithm in practice, we need a way to store distributions on a computer and a way to store modular symbols on a computer.

The latter problem is standard. It is well known that one can find a finite set of ordered pairs

$$(r_1, s_1), (r_2, s_2), \dots (r_n, s_n) \in \mathbf{P}^1(\mathbf{Q}) \times \mathbf{P}^1(\mathbf{Q})$$

such that any $\Phi \in \mathsf{MS}_\Gamma(\mathcal{D}(\mathbf{Z}_p))$ is uniquely determined by its values on these elements.

Representing distributions

The functions $\{x^j\}_{j=0}^{\infty}$ are dense in $\mathcal{A}(\mathbf{Z}_p)$ and thus any distribution $\mu \in \mathcal{D}(\mathbf{Z}_p)$ is uniquely determined by its sequence of moments $\{\mu(x^j)\}_{j=0}^{\infty}$.

A natural approach then is to fix some large number $M \gg 0$ and approximate μ by the sequence $\{\mu(x^j) \pmod{p^M}\}_{j=0}^{M-1}$; that is, store the first M moments each modulo p^M.

Unfortunately, this is not stable under our matrix actions. That is, the first M moments modulo p^M of μ does not determine the same data for $\mu\big|\gamma$.

Representing distributions

The basic problem with this approach is that if $\mathcal{D}_0(\mathbf{Z}_p)$ is the set of distributions all of whose moments are in $\mathbf{Z}_p$, then the subset

$$\{\mu \in \mathcal{D}_0(\mathbf{Z}_p) \mid \mu(x^j) = 0 \ \text{ for } \ 0 \leq j \leq M-1\}$$

is not stable under our matrix actions.

The smallest subset containing this set that is stable under our matrix actions is

$$\{\mu \in \mathcal{D}_0(\mathbf{Z}_p) \mid \mu(x^j) \in p^{M-j}\mathbf{Z}_p \ \text{ for } \ 0 \leq j \leq M-1\}$$

which we denote by $I(M)$.

Finite approximation modules

Let $\mathcal{F}(M)$ denote

$$\mathcal{D}_0(\mathbf{Z}_p)/I(M) \cong (\mathbf{Z}/p^M) \times (\mathbf{Z}/p^{M-1}) \times \cdots \times (\mathbf{Z}/p),$$

the M-th finite approximation module. This set is finite and stable under our matrix actions.

This gives us a way of storing a distribution $\mu \in \mathcal{D}_0(\mathbf{Z}_p)$ on a computer by simply projecting it into $\mathcal{F}(M)$; that is, by storing its first M moments modulo descending powers of p.

Finite approximation modules

Thus, the set $\mathsf{MS}_\Gamma(\mathcal{F}(M))$ can be stored on a computer with a finite amount of data since any symbol in this space can be represented by a finite number of elements of $\mathcal{F}(M)$ which is a finite set.

Also, note that there is a natural map

$$\mathsf{MS}_\Gamma(\mathcal{F}(M)) \xrightarrow{\overline{\rho}} \mathsf{MS}_\Gamma(\mathbf{Z}/p^M)$$

given by taking total measure.

We note that both the source and the target of this map are finite sets.

The algorithm

1) Lift the symbol $\overline{\phi}_E \in \mathrm{MS}_\Gamma(\mathbf{Z}/p^M)$ to a symbol $\overline{\Phi}$ in $\mathrm{MS}_\Gamma(\mathcal{F}(M))$. (This can be done very quickly.)

2) Apply $\frac{1}{a_p}U_p$ to $\overline{\Phi}$ until the answer stabilizes to a symbol $\overline{\Phi}_E$. (This should take M iterations.)

3) Evaluate $\overline{\Phi}_E$ at the point $(0, i\infty)$. (The answer will be an approximation of the p-adic L-function of E.)

We note that each iteration of U_p yields an extra p-adic digit of accuracy. Moreover, an application of U_p can be performed in polynomial time (in p).

Running times

Again consider the curve $E = X_0(11)$. Recall that to compute the p-adic L-function to 10 digits of accuracy with Riemann sums required 1 year of CPU time.

With overconvergent modular symbols, to compute to 100 digits of accuracy takes less than 2 minutes on the same computer. To get 200 digits requires approximately 20 minutes.

Also, note that this computation is independent of K! So once the moments are computed, one can find Stark-Heegner points over many real quadratic fields K.

Example

For $K = \mathbf{Q}(\sqrt{101})$, the class number equals 1.

Thus, the basic Stark-Heegner point should be defined over K.

We recognized it to be the global point

$$\begin{aligned} x &= 108162413664469253966708468511684 9, \\ y &= -19391462977749218369160989980706200472762157755 00 \\ &\quad -45034813271762519727132587561686024065704563549 3\sqrt{101}. \end{aligned}$$

Example

For $K = \mathbf{Q}(\sqrt{79})$, the class number equals 3.

We found that the x-coordinate of the basic Stark-Heegner point satisfies

$$\begin{aligned} h_{316}(x) \;=\; & 7276645376874546352069472809496718 4x^3 \\ & -7191441556618132355922021509724026494 0x^2 \\ & +2653029535749035413574464896382331270516x \\ & -1533378178360194067585720285155061514380 3, \end{aligned}$$

whose splitting field is indeed the Hilbert class field of $\mathbf{Q}(\sqrt{79})$!

Computer Progams

Find your own points! See:

http://www.math.mcgill.ca/darmon/programs/programs.html

to download a package that contains these algorithms.