Coleman Integration on Modular Curves

Mingjie Chen, Kiran Kedlaya, Jun Bo Lau
University of California, San Diego

UC San Diego

Motivation

Rational points on modular curves hold importance in number theory and Coleman integrals have been used in computing various arithmetic-geometric invariants, including rational points on curves. Current methods employ Dwork's principle of analytic continuation along the Frobenius, and we investigate the effect of Hecke operators on these p-adic line integrals and thus circumvent the use of Frobenius.

Modular Curves

Let $\mathbb{H}$ denote the upper half plane, $\Gamma \leq SL_2(\mathbb{R})$ an arithmetic subgroup, $X(\Gamma) := \Gamma\backslash(\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}))$ a modular curve . For the purpose of demonstration, we consider

$$\Gamma = \Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}), N|c \right\}$$

Points on modular curves parametrise elliptic curves with certain data. In our case, a $\mathbb{Q}$-point $P = (E, C) \in X_0(N) := X(\Gamma_0(N))$ corresponds to an elliptic curve E defined over $\mathbb{Q}$ with a cyclic subgroup C of order N. Equivalently, a point on $X_0(N)$ is a pair of elliptic curves with a cyclic isogeny $\varphi : E \to E'$ of degree N.

For ℓ not dividing the level N, we have two degeneracy maps $\pi_1, \pi_2 : X_0(\ell N) \to X_0(N)$. Note that $X_0(\ell N)$ parametrises pairs (E, G) where $G = C \oplus D$ with C cyclic of order ℓ and D cyclic of order N. Then π_1 forgets the subgroup C of order ℓ and π_2 quotients by C:

$$\begin{tikzcd} & X_0(\ell N) \arrow[dl, "\pi_1"'] \arrow[dr, "\pi_2"] & \\ X_0(N) \arrow[rr, dashed] & & X_0(N) \end{tikzcd}$$

We define the Hecke correspondence T_ℓ on divisors and differential forms on $X_0(N)$ via the formula $T_\ell(D) := \pi_{2*}\pi_1^* D$. More concretely,

$$(E, D) \mapsto \sum_{C \in E[\ell]} (E, C \oplus D) \mapsto \sum_{C \in E[\ell]} (E/C, (C + D)/C)$$

Coleman Integration

In the 1980s, Coleman defined a p-adic line integral $\int_P^Q \omega \in \mathbb{C}_p$ on a curve X over $\mathbb{Q}_p$ with good reduction at the prime p where ω is a holomorphic differential on X, $P, Q \in X(\mathbb{C}_p)$. These integrals satisfy, among many others, nice properties [4]:

- Linearity:
$$\int_P^Q a\eta + b\omega = a\int_P^Q \eta + b\int_P^Q \omega$$
- Additivity in endpoints:
$$\int_P^Q \omega = \int_P^R \omega + \int_R^Q \omega$$
- Defining it on divisors:
$$\int_P^Q \omega + \int_{P'}^{Q'} \omega = \int_P^{Q'} \omega + \int_{P'}^Q \omega$$
- Change of variables: If $U \subseteq X, V \subseteq Y$ are wide open subspaces of the rigid analytic spaces X, Y, ω a 1-form on V, $\phi : U \to V$ a rigid analytic map, then:
$$\int_P^Q \phi^*\omega = \int_{\phi(P)}^{\phi(Q)} \omega$$
- Fundamental theorem of calculus: Let f be a rigid analytic function on $U \subseteq X$ wide open subspace, then:
$$\int_P^Q df = f(Q) - f(P)$$
- Tiny integrals: For $P, Q \in X(\mathbb{Q}_p)$ in the same residue disc, we have $\int_P^Q \omega = \int_{t(P)}^{t(Q)} \omega(t)$, where t is a local coordinate.

To explicitly compute a Coleman integral of a genus g curve X, the approach using Frobenius is as follows [3]:

1. Find a model for the curve X.
2. Obtain a basis $\{\omega_i\}$ in the Monsky-Washnitzer cohomology.
3. Find a lift of ϕ Frobenius mod p to dagger algebras.
4. Compute the action of ϕ on $\{\omega_i\}$ using Kedlaya's algorithm [6, 3]:
$$\phi^*\omega_i = df_i + \sum_{j=0}^{2g-1} M_{ji}\omega_j$$
5. We note that $M - I$ is invertible by the proof of Weil Conjectures. And using properties listed above, we have the following:
$$\begin{pmatrix} \vdots \\ \int_P^Q \omega_j \\ \vdots \end{pmatrix} = (M - I)^{-1} \begin{pmatrix} \vdots \\ f_i(P) - f_i(Q) - \int_P^{\phi(P)} \omega_i - \int_{\phi(Q)}^Q \omega_i \\ \vdots \end{pmatrix}$$

Coleman integrals on modular curves

On modular curves, the differentials correspond to weight 2 Hecke eigenforms. Using properties of the integral and the Hecke correspondence defined earlier would give (here $\ell = p$ as discussed in the previous sections):

$$\begin{aligned} \int_P^Q T_\ell(\omega) &= a_\ell \int_P^Q \omega \\ &= \sum_{i=1}^{\ell+1} \int_{P_i}^{Q_i} \omega \end{aligned}$$

And using the Ramanujan bound, we obtain a nonzero integral where the right hand side consists of tiny integrals as P and $T_\ell P$ each consist of points in the same residue disc:

$$(\ell + 1 - a_\ell)\int_P^Q \omega = \sum_{i=1}^{\ell+1} \Big(\int_{Q_i}^Q \omega - \int_{P_i}^P \omega \Big)$$

One of the issues with modular curves is that it is not easy to find good models for them. We provide a "model-free" algorithm to resolve this problem using the modular j-invariant: Let $P = (E, C) \in X(\mathbb{Q})$, $\omega \leftrightarrow f(z)dz$.

1. Find $\tau_0 \in \mathbb{H}$ such that $\Gamma_0(N)\tau_0$ corresponds to P, with j-invariant j_0.
2. Expand ω as a power series in $j - j_0$ where ω could be expressed as a power series in $\tau - \tau_0$:
$$\omega = \sum_{i=0}^{\infty} a_i (j - j_0)^i d(j - j_0)$$
3. Use linear algebra and algdep from `PARI/GP` or `SAGE` to recover the a_i's.
4. Find $j(P_i)$ via the modular polynomial $\Phi_\ell(X, j(P)) = 0$.
5. Compute $\int_P^Q \omega = \sum_{i=1}^{\ell+1} \int_0^{j(P_i)-j_0} a_0 + a_1 t + \ldots dt$.

Remarks and future work

We have computed examples for small N in the case of $\Gamma = \Gamma_0(N), \Gamma_0^+(N)$ and verified the hyperelliptic cases with the already implemented codes on `Magma` and `SAGE`.
There are several observations that arise from the calculations:

- The denominators appearing in the coefficients obtained in the model free method are somehow related to the trace of Frobenius of P mod p for any prime p of good reduction (e.g. $X_0(37)$) [5].
- Iterated integrals (such as the double integrals appearing in quadratic Chabauty [2, 1]) do not yield to this method due to the lack of additivity in endpoints of the Hecke correspondence.
- The height of the a_i's are large for the expansion of $(j - j_0)^i$. A good replacement would be uniformisers with smaller q-coefficients on the curve, such as Hauptmoduls (e.g. eta quotients).

References

[1] Jennifer Balakrishnan and Netan Dogra. "Quadratic Chabauty and rational points II: Generalised height functions on Selmer varieties". In: (Apr. 2017).

[2] Jennifer Balakrishnan and Netan Dogra. "Quadratic Chabauty and rational points, I: P-adic heights". In: *Duke Mathematical Journal* 167 (Jan. 2016). DOI: 10.1215/00127094-2018-0013.

[3] Jennifer Balakrishnan and Jan Tuitman. "Explicit Coleman integration for curves". In: *Mathematics of Computation* (Oct. 2017). DOI: 10.1090/mcom/3542.

[4] Robert F. Coleman. "Torsion Points on Curves and p-Adic Abelian Integrals". In: *Annals of Mathematics* 121.1 (1985), pp. 111–168.

[5] Noam Elkies. "Elliptic and modular curves over finite fields and related computational issues". In: *Computational Perspectives on Number Theory*. Proceedings of a Conference in Honor of A. O. L. Atkin. Ed. by Duncan Buell and Jeremy Teitelbaum. AMS, 1998, pp. 21–76.

[6] Kiran Kedlaya. "Counting Points on Hyperelliptic Curves using Monsky-Washnitzer Cohomology". In: *J. Ramanujan Math. Soc.* 16 (June 2001).