Using algebraic values of modular forms to obtain models of modular curves

Kamal Khuri-Makdisi
Center for Advanced Mathematical Sciences
American University of Beirut
kmakdisi@aub.edu.lb

Preprint on arXiv:
http://arxiv.org/abs/0903.1439

Rational Points 3, Bayreuth, July 2010

Models of curves: the basic idea

Setup: X/K a smooth projective curve of genus g, embedded as a curve of degree d in projective space $\mathbf{P}^n$. Homogeneous ideal $I = I_X$ defining X.

Ambient polynomial ring: $\mathcal{R} = K[x_0 \cdots x_n] = K \oplus V \oplus \operatorname{Sym}^2 V \oplus \cdots$.

Projective coordinate ring of X: $\mathcal{R}/I_X = K \oplus V \oplus V_2 \oplus \cdots$, where $V_k = \operatorname{Sym}^k V/I_k$. Example: $\mathcal{L}$ line bundle of degree $d \geq 2g+1$, then $V = H^0(X, \mathcal{L})$ gives a projectively normal embedding and $V_k = H^0(X, \mathcal{L}^k)$.

Further assumption: we know k such that I is generated by elements of degree $\leq k$. In the above example, if $d \geq 2g+2$, then we can take $k = 2$, i.e., I is generated by $I_2 = \ker(\operatorname{Sym}^2 V \to V_2)$ (Castelnuovo-Mumford-Fujita-St. Donat).

Interpolating to find I: Knowing $kd+1$ points $P_0, \ldots, P_{kd}$ on $X \subset \mathbf{P}^n$ uniquely determines $I_{\leq k}$. (Sections of $\mathcal{L}^k$ vanish at exactly kd points.)

Modular curves

We will stick to the case of $X = X(N)$ for $N \geq 3$, over a field $K \supset \mathbf{Q}(\zeta_N)$.

Complex points: $X(N)(\mathbf{C}) = \widehat{\Gamma\backslash\mathcal{H}}$, where $\Gamma = \Gamma(N)$.

Moduli space: Points on the open set "$\Gamma\backslash\mathcal{H}$" parametrize (E, P_1, P_2) where E is an elliptic curve, and P_1, P_2 are a basis for $E[N]$ with $e_N(P_1, P_2) = \zeta_N$ (e_N Weil pairing, ζ_N fixed primitive Nth root of 1).

Line bundle: Since $N \geq 3$, there exists a line bundle $\mathcal{L}$ on X such that $H^0(X, \mathcal{L}^k) = \mathcal{M}_k(\Gamma) =$ space of modular forms of weight k on $\Gamma(N)$. Can view modular forms algebraically as functions of (E, η, P_1, P_2) where $\eta \in \Omega^1(E)$. $f \in \mathcal{M}_k$ means $f(E, c\eta, P_1, P_2) = c^{-k} f(E, \eta, P_1, P_2)$. Example: the choice of η normalizes an equation $E : y^2 = x^3 + ax + b$ with $\eta = dx/2y$. Then a, b are essentially weight 4,6 Eisenstein series on $\Gamma(1)$.

Eisenstein series on $\Gamma(N)$

Analytic definition: For $i, j \in \mathbf{Z}/N\mathbf{Z}$, let $Q = [i]P_1 + [j]P_2 \in E[N]$. Then $G_{k,(i,j)} = G_{k,Q} \in \mathcal{M}_k(\Gamma)$ is defined as a function of (E, η, P_1, P_2) by:

$$(E, \eta, Q) \cong (\mathbf{C}/\Lambda, dz, \alpha \in N^{-1}\Lambda/\Lambda) \mapsto G_{k,Q} = \sum_{\ell \in \Lambda - \{-\alpha\}} (\ell + \alpha)^{-k}.$$

As written, this converges only for $k > 2$, but can be fixed for $k = 1, 2$. Note above that Λ is the lattice of periods of η on E.

Algebraic values: For example, if $Q = (x_Q, y_Q)$, then $x_Q \sim \wp(\alpha) \sim G_{2,Q}$ and $y_Q \sim \wp'(\alpha) \sim G_{3,Q}$. In weight 1, the G_1's can be related to slopes $(y_P - y_Q)/(x_P - x_Q)$.

Theorem (KKM): All the $G_{k,Q}$'s for $k \geq 1$ can be evaluated purely algebraically (exact arithmetic, no infinite series) and all belong to the ring of modular forms generated by weight 1 Eisenstein series. In fact this ring contains all forms in weights ≥ 2, and misses just $\mathcal{S}_1(\Gamma(N))$.

Projective embedding of $X(N)$

The incomplete linear series $V = \mathcal{E}is_1(\Gamma(N)) \subset \mathcal{M}_1(\Gamma) = H^0(X, \mathcal{L})$ gives a projective embedding of X. Over $\mathbf{C}$, the projective coordinate ring is $\mathcal{R}/I = \mathbf{C} \oplus \mathcal{E}is_1 \oplus \mathcal{M}_2 \oplus \cdots$ which is a large subring of the full ring of modular forms on $\Gamma(N)$. It turns out that I is generated by $I_{\leq 3}$.

Computing generators for I: As mentioned before, this can be done by interpolating through sufficiently many points on X. A nice way is to fix one elliptic curve, e.g., $E_0 : y^2 = x^3 + 31416x + 27818$, and to consider all possible level N structures on it. Thus $E_0 \in X(1)$ and we take the points of $\pi^{-1}(E_0)$ where $\pi : X(N) \to X(1)$.

These give enough points to find relations all the way up to $I_{\leq 11}$ if needed. The calculations take place over $\mathbf{Q}(E_0[N])$ but one should be able to lump Galois conjugates together and work over $\mathbf{Q}(\zeta_N)$ or maybe even over $\mathbf{Q}$.

What are the generators of I?

The elements of I_1 are the linear relations between the Eisenstein series $\{G_{1,Q} : Q \in E[N]\}$. These were already known to Hecke. For example, $G_{1,-Q} = -G_{1,Q}$. There is also a second, subtler, symmetry of order 2, that is essentially a duality under the Fourier transform with respect to the Weil pairing. For example, if $N = 13$, then there are 169 possible Q, but the first symmetry reduces the dimension to 84, and the subtle symmetry brings this further down to 42. (General fact: the “easy” symmetries bring you down to the number of cusps, but the space $\mathcal{E}is_1$ has **half** that dimension.)

Several elements of I_2 and I_3 are known. For example, if $P, Q, R \in E[N] - \{O\}$ and $P + Q + R = O$, then $(G_{1,P} + G_{1,Q} + G_{1,R})^2 \sim G_{2,P} + G_{2,Q} + G_{2,R}$. Eliminate the $G_{2,P}$ to get elements of I_2. Observation (Borisov-Gunnells, also work in progress by KKM-Raji): many relations are parallel to the Manin relations between modular symbols. But these do not account for everything.

Example: results on the generators of I, when $N = 13$

To avoid coefficient explosion, I worked modulo $p = 10037$. I chose $E_0/\mathbf{F}_p$ such that $E_0[13] \subset E[\mathbf{F}_p]$. Hence all points of $\pi^{-1}(E_0)$ were defined over $\mathbf{F}_p$, simplifying computations. I computed $I_{\leq 3}$ by interpolation, and studied the ideal J defined by the known relations in weights 1 and 2.

Hilbert-Poincaré series: The Hilbert series for $\mathcal{R}/I$ is $1 + (\dim \mathcal{E}is_1)t + (\dim \mathcal{M}_2)t^2 + \cdots = 1 + 42t + 133t^2 + 224t^3 + 315t^4 + \cdots$. This matches up with the known dimension formulas ($g = 50$, $\deg \mathcal{L} = 91$). On the other hand, the Hilbert series for J is $1 + 42t + \mathbf{161}t^2 + 224t^3 + 315t^4 + \cdots$. (There are 28 "mysterious" relations in weight 2.)

Remarks: In this example, I is generated by $I_{\leq 2}$. With respect to grevlex order in 169 variables, I has a Gröbner basis with 127 elements in weight 1, 770 in weight 2, and 60 in weight 3. The numbers for J are 127 in weight 1, 742 in weight 2, and 174 in weight 3.

Can this be generalized?

This approach using algebraic evaluation of modular forms and interpolation has some hope to systematically allow us to produce equations for Shimura curves attached to an indefinite quaternion algebra B. This would need:

- A source of some "simple" modular forms on B, analogous to using Eisenstein series of weight 1 for modular curves. Perhaps restriction of simple Hilbert modular forms from a real quadratic field $F \subset B$? There is some relation of this to periods and hyperbolic Poincaré series on the Shimura curve.

- The above "simple" forms should have a moduli interpretation so that we can evaluate them algebraically at moduli points of the Shimura curve (e.g., at CM points).

Can this be generalized? (continued)

- We would need to prove a result on products of simple forms giving rise to the whole space of modular forms of slightly higher weight. For modular curves we got all of $\mathcal{M}_k$ for $k \geq 2$ regardless of N. More generally, we can consider Hecke algebra orbits of products of forms; this tends to mix up automorphic representations.

- If the above is not feasible, at least we need to know some bounds on the regularity of the ideal sheaf from the projective embedding to know how high up to go in computing I.

A last question for the elliptic case: can one do these computations for larger N in reasonable time? It would be nice to do Gröbner bases taking into account the action of $SL(2, \mathbf{Z}/N\mathbf{Z})$.