Computing congruences between spaces of cusp forms*

Amod Agashe

September 14, 2009

Let $N > 5$ be an integer. In this paragraph, the symbol g stands for a newform of level N_g dividing N. Let S'_g denote the subspace of $S_2(\Gamma_0(N), \mathbf{C})$ spanned by the forms $g(dz)$ where d ranges over the divisors of N/N_g. Let $[g]$ denote the Galois orbit of g, and let $S_{[g]}$ denote the $\mathbf{Q}$-subspace of forms in $\oplus_{h \in [g]} S'_h$ with rational Fourier coefficients. We have $S_2(\Gamma_0(N), \mathbf{Q}) = \oplus_{[g]} S_{[g]}$, where the sum is over Galois conjugacy classes of newforms of some level dividing N. If T is a subset of the set of Galois conjugacy classes of newforms of some level dividing N, then let T' denote its complement, let $S_T = \oplus_{[g] \in T} S_{[g]}$, and let $I_T = \mathrm{Ann}_{\mathbf{T}} S_T$.

Let T_1 and T_2 denote two disjoint subsets of the set of Galois conjugacy classes of newforms of some level dividing N. The example I am really interested in is where T_1 consists of the Galois conjugacy class of a given newform and T_2 consists of the set of Galois conjugacy classes of all newforms of level strictly less than N. Let I_1 denote I_{T_1} for simplicity and let I'_1 denote $I_{T'_1}$ (similarly with 1 replaced by 2). Let $S = S_2(\Gamma_0(N), \mathbf{Z})$. Consider the "congruence module"

$$C = \frac{S[I_1 \cap I_2]}{S[I_1] + S[I_2]},$$

which is a finite group. A prime p divides the order of this module if and only if some eigenform in $S_2(\Gamma_0(N), \mathbf{C})[I_1]$ is congruent to some eigenform in $S_2(\Gamma_0(N), \mathbf{C})[I_2]$ modulo a prime ideal over p in the ring of integers generated by the Fourier coefficients of these eigenforms. One goal is to compute the structure or order of the congruence module C and a weaker (more immediate) goal is to decide if a given prime p divides its order.

If one can compute C efficiently (e.g., by considering the corresponding quotient group involving the Hecke algebra), then that would be great. Otherwise, let $H = H_1(X_0(N), \mathbf{Z})$, and consider the finite group

$$C' = \frac{H}{H[I'_1] + H[I'_2]}.$$

Then the exponent of C' divides the exponent of C, and if $p^2 \nmid N$, then the two exponents are the same (this requires some justification). I believe that in fact that if $p^2 \nmid N$, then the p-primary components of C' is isomorphic to the direct sum of two copies of C (using a multiplicity one argument). Anyhow, if $p^2 \nmid N$, then to decide if a given prime p divides the order of C, one may instead check if p divides the order of C', which is the problem I will focus on in the rest of this article.

Here is how one may compute the group C' above: Firstly, $I_1 H \subseteq H[I'_1]$ and $I_2 H \subseteq H[I'_2]$ and both inclusions have finite cokernels (as one sees by tensoring with $\mathbf{Q}$). Now the inclusions $H[I'_1] \subseteq H$ and $H[I'_2] \subseteq H$ have torsion-free cokernels. So one can first compute the order of

$$\frac{H}{I_1 H + I_2 H},$$

*This is a preliminary rough draft, and will probably need some corrections.

and then divide by the product of the orders of the torsion subgroups of H/I_1H and H/I_2H. In order to compute the above, one uses modular symbols to get a presentation for H, and the only thing left to explain is how one finds generators for I_1 and I_2.

Instead of finding these generators, what one may do instead is first find a $\mathbf{Q}$-basis for $I_1 \otimes \mathbf{Q}$ and $I_2 \otimes \mathbf{Q}$. This may be done as follows: let n denote the dimension of $S_2(\Gamma_0(N), \mathbf{C})[I_1]$ and find a basis $v_1, \ldots, v_n$ for $S_2(\Gamma_0(N), \mathbf{C})[I_1]$ (or perhaps for the corresponding modular symbols space). Find a basis $t_1, \ldots, t_g$ for $\mathbf{T} \otimes \mathbf{Q}$ (here g is the genus of $X_0(N)$) – this may be done by just starting with one Hecke operator, and then adding another one at a time, checking for linear independence, etc. (or there may be better methods). Consider the system of equations $(t_1x_1 + \ldots + t_gx_g)v_i = 0$ for $i = 1, \ldots, n$. This is a system of n equations with $g \geq n$ unknowns, and so a basis for the solution set will give a basis for $I_1 \otimes \mathbf{Q}$ (similarly for $I_2 \otimes \mathbf{Q}$).

One then clears the denominators in these bases (more precisely in the x_i's) – the resulting sets need not be generators for I_1 and I_2, but the subgroups of H generated by these sets (call these subgroups H' and H'' respectively) are still of finite index in I_1H (hence in $H[I_1']$) and in I_2H (hence in $H[I_2']$) respectively, so one can play the same game as two paragraphs above, i.e. take the ratio of the order of $H/(H' + H'')$ to the product of the orders of the torsion subgroups of H/H' and H/H''. I believe one can do theses calculations using the Smith normal form, but there may be better methods. Also, since we only want to check if a prime p divides the ratio of certain orders, perhaps one can work over $\mathbf{F}_p$ for the last step. Finally, if p is odd, then one can work with H^+ (the elements of H fixed by complex conjugation) instead of H throughout.