Computing coefficients of modular forms, part 2: explicit calculations

Johan Bosman
(joint work with Bas Edixhoven)

// Many thanks go to John Voight for for making and supplying me the notes that he took from my talk about this subject.

Let $\tau(n)$ be defined by $\Delta(q) = q\prod_{n\geq 1}(1-q^n)^{24} = \sum_{n\geq 1}\tau(n)q^n$. We wish to calculate $\tau(p) \bmod \ell$. For all ℓ, there exists a representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(K_\ell/\mathbb{Q}) \to GL_2(\mathbb{F}_\ell)$ such that $\mathrm{tr}(\mathrm{Frob}_p) \equiv \tau(p) \bmod \ell$ and $\det(\mathrm{Frob}_p) \equiv p^{11} \bmod \ell$ for $p \neq \ell$. For $\ell \geq 11$, there exists a 2-dimensional subspace $V_\ell \subset \mathrm{Jac}(X_1(\ell))[\ell]$ such that ρ is given by the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on V_ℓ.

Let $f_1, \ldots, f_g$ be a basis of newforms for the modular forms space $S_2(\Gamma_1(\ell))$. This space is isomorphic to $H^0(X_1(\ell), \Omega^1)$ by $f \mapsto f(dq/q)$. We have $J_1(\ell)(\mathbb{C}) \cong \mathbb{C}^g/\Lambda$ where $\Lambda = \{\int_\gamma (f_1, \ldots, f_g)dq/q : [\gamma] \in H_1(X_1(\ell)(\mathbb{C}), \mathbb{Z})\}$ is a lattice.

We have

$$\phi : X_1(\ell)^g \to \mathbb{C}^g/\Lambda \supset V_\ell$$
$$(Q_1, \ldots, Q_g) \mapsto \sum_{i=1}^{g} \int_0^{Q_i} (f_1, \ldots, f_g)\, dq/q.$$

If we choose $Y_1(\ell) \subset X_1(\ell)$ to be the moduli space of pairs (E, P) where E is an elliptic curve and P is a point on E of order ℓ, then this gives us a model for $X_1(\ell)$ over $\mathbb{Q}$ in which the cusp at 0 is rational. Hence the map ϕ is defined over $\mathbb{Q}$ in this setting.

For each $x \in V_\ell$ we want to approximate $Q \in X_1(\ell)^g$ such that $\phi(Q) = x$. Pick a random Q and compute $\phi(Q)$. Then draw a small vector from $\phi(Q)$ in the direction of x. Getting the Jacobian matrix, we then find a Q' such that $\phi(Q')$ is closer to x. Repeat this step until we are really close. Once in a neighborhood of x, we use Newton-Raphson iteration. We use a low calculation precision until we get in the Newton-Raphson part, where we start increasing the precision. This way the first part of the approximation can be performed much faster than the NR part, in spite of the fact that it needs more steps.

What we need to show is that we can calculate $f_i(z)$ and $\int_0^z f_i(z)(dq/q)$ to a high precision.

Let F be the standard fundamental domain for the action of $SL_2(\mathbb{Z})$ and let f be a newform. Write $z = \gamma z'$ with $\gamma \in SL_2(\mathbb{Z})$ and $z' \in F$. This is for computational reasons: in $SL_2(\mathbb{Z})$ we can do exact calculations and in the upper half plane we

want to stay away from the real line.

Because f is a newform, there is a character $\epsilon : (\mathbb{Z}/\ell\mathbb{Z})^* \to \mathbb{C}^*$ such that $f\left(\frac{az+b}{cz+d}\right) = \epsilon(d)(cz+d)^2 f(z)$ for all matrices in $\Gamma_0(l)$. Furthermore, $\Gamma_0(\ell)\backslash SL_2(\mathbb{Z})$ has the following set of coset representatives:

$$S = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} 0 & -1 \\ 1 & j \end{pmatrix} : j \in \{-(\ell-1)/2, \ldots, (\ell+1)/2\} \right\}.$$

So if we write $\gamma = \gamma_1\gamma_2$ with $\gamma_1 \in \Gamma_0(\ell)$ and $\gamma_2 \in S$, then the calculation of $f(\gamma z)$ is reduced to the calculation of $f(\gamma_2 z)$.

Now, $S \cdot F$ is a fundamental domain for $\Gamma_0(\ell)\backslash\mathbb{H}$, in which 0 is the only cusp apart from ∞. If $\Im z \gg 0$, then $|q| \ll 1$ so $\sum_n a_n(f)q^n$ converges rapidly, so we can calculate $f(z)$. This works if z is not near the cusp 0. If $z \in S \cdot F$ is near 0, then we have an Atkin-Lehner operator on $S_2(\Gamma_1(\ell))$ by $(w_\ell f)(z) = \ell z^{-2} f(-1/\ell z)$. If f is a newform, then $w_\ell f = c_f \widetilde{f}$, where $\widetilde{f} = \sum \overline{a_n(f)} q^n$, the complex conjugate and c_f is a constant depending on f.

Plug in a value of z such that $\Im z \gg 0$, $\Im(-1/\ell z) \gg 0$ to get c_f. For points in $S \cdot F$ near the cusp 0, $-1/\ell z$ is near ∞, so we can calculate $\widetilde{f}(-1/\ell z)$. From this we can get $w_\ell f(-1/\ell z)$, hence also $f(z)$.

With similar tricks plus some more we can also calculate integrals of modular forms to a high precision (think of at least hundreds of decimals).

Given $\psi \in \mathbb{Q}(X_1(\ell))$ (quotients of two modular forms of the same weight), we obtain

$$P_\ell = \prod_{Q \in V_\ell \setminus \{0\}} (X - \sum_{i=1}^{g} \psi(Q_i)) \in \mathbb{Q}[X].$$

We can approximate $P_\ell \in \mathbb{R}[X]$. Using continued fractions, we find rational numbers near the coefficients. If $|p/q - \alpha| \ll 1/q^2$, then we are psychologically convinced that $\alpha = p/q$, although a mathematical proof still lacks. This polynomial should define the field of definition of a nonzero point in V_ℓ and its splitting field should be K_ℓ.

We do this for $\ell = 13$, $\ell = 17$.

We also have another polynomial

$$P'_\ell = \prod_{L \in \mathbb{P}^1(V_\ell)} (X - \sum_{Q \in L \setminus \{0\}} \sum_i \psi(Q_i))$$

which gives the extension $PGL_2(\mathbb{F}_\ell)$.

Multiplication by n on V_ℓ gives a map $x \mapsto \psi_n(x)$ in $\mathbb{Q}[x]/P_\ell(x)$, which we want to calculate. The cycle type of Frob_p acting on V_ℓ is the same as the decomposition type of $P_\ell \bmod p$. One ends up with a set of candidate matrices M for $\rho(\mathrm{Frob}_p)$. Find an r such that $M^r = nI$ for all candidates. Then, in $\mathbb{F}_p[x]/(P_\ell)$, the congruence $\psi_n \equiv x^{p^r} \mod P_\ell$ holds. If you do this for sufficiently many p, one can use LLL to find the polynomial ψ_n.

We can use this to calculate $\tau(p) \mod \ell$ if $\rho(\mathrm{Frob}_p)$ has its eigenvalues in $\mathbb{F}_\ell$. Factor P_ℓ in $\mathbb{F}_p[x]$, say $P_\ell(x) = P_1 \dots P_k$. Then n is an eigenvalue of $\rho(\mathrm{Frob}_p)$ iff $x^p \equiv \psi_n \mod P_i$ for some i.