ON COMPUTING COEFFICIENTS OF MODULAR FORMS

BAS EDIXHOVEN

Question (asked by **Schoof**): Let $f = \sum_n a_n q^n$ be a modular form. Can one compute for p prime, a_p in time polynomial in $\log p$?

Example. For example, we consider

$$\Delta = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n \geq 1} \tau(n) q^n.$$

Remark. We reduce to cuspidal eigenforms with integral weight (say for a congruence subgroup), normalized with $a_1 = 1$ (for a fixed level and weight, the space is finite-dimensional so one can choose a basis). For Eisenstein forms there are simple formulas that give the a_p.

From the a_p one can get the a_n (by multiplicativity) if one factors n.

One must restrict to a_p with p prime because, for example for Eisenstein series, the formulae for the coefficients a_n are given in terms of sums of divisors of n, and therefore computing the coefficients amounts to factorization.

The main idea: As in Schoof's algorithm, use that a_p is the trace of a Frobenius element at p, and compute it modulo ℓ for sufficiently many small ℓ.

Notation: let k be the weight of f and N the level. Suppose f is given by the coefficients $a_2, a_3, \ldots, a_{N^2 k}$ (or sufficiently many to determine the form). Henri Cohen has a method which relates the coefficients to a sum of class numbers which is not polynomial in $\log p$.

Basic facts:

1. The extension $E_f = \mathbb{Q}(\ldots, a_n, \ldots)$ is finite.
2. For all ℓ, there exists a continuous semi-simple representation
$$\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{F}_\ell \otimes \mathfrak{O}_{E_f}),$$
unramified outside ℓN such that for all $p \nmid N\ell$, $\mathrm{tr}(\mathrm{Frob}_p) = a_p$.
3. For all $\sigma : E_f \hookrightarrow \mathbb{C}$, $|\sigma(a_p)| \leq 2p^{(k-1)/2}$.

Suppose that $k = 1$. Here one has $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathfrak{O}_{E_f})$ that gives all of the ρ_ℓ, and the trace formula holds over $\mathfrak{O}_{E_f}$. Therefore ρ factors through a finite extension $\mathrm{Gal}(K/\mathbb{Q})$, and one then computes this field to compute the coefficients.

Date: December 14, 2000, 11:00 a.m.

Notes from Workshop on Arithmetic Geometry at MSRI, December 11–15, 2000, by John Voight, `jvoight@math.berkeley.edu`.

Suppose that $k = 2$. Then ρ_ℓ is given by $A_f(\overline{\mathbb{Q}})[\ell]$. Computation of the abelian variety with the action of the Hecke operators therefore gives the representation.

Suppose that $k \geq 3$. We may dualize to obtain $\rho_\ell^\vee$ which occurs in $H^{k-1}_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{F}_\ell)$ where X is a $(k-1)$-dimensional variety (the $(k-2)$-fold fiber product of the universal elliptic curve E^{univ}). By the usual methods of etale cohomology, we reduce to computing $H^1_{\text{ét}}(X_1(N)_{\overline{\mathbb{Q}}}, \mathcal{F}_{k,\ell})$, where $\mathcal{F}_{k,\ell} = \text{Sym}^{k-2}_{\mathbb{F}_\ell}(E^{\text{univ}}[\ell]^\vee)$, which is the set of isomorphism classes of $\mathcal{F}_{k,\ell}$-torsors on $X_1(N)_{\overline{\mathbb{Q}}}$. One could write down (analytically or otherwise) these varieties, but in order to compute the Galois action, one must compute the algebraic variety which is much harder. In practice, there are too many variables in too high a degree, making this method impractical.

We consider ρ_ℓ in $J_1(N\ell)(\overline{\mathbb{Q}})[\ell]$ (if $k \leq \ell + 1$): over $X_1(N\ell)$, $E^{\text{univ}}[\ell]$ acquires a 1-dimensional constant subsheaf $\mathbb{F}_\ell$ (since E^{univ} acquires a point of order ℓ), giving a surjection from $\mathcal{F}_{k,\ell}$ to the constant sheaf $\mathbb{F}_\ell$, which explains that ρ_ℓ occurs in $J_1(N\ell)$. The dimension of $J_1(N\ell)(\overline{\mathbb{Q}})[\ell])$ is very large (the genus of $X_1(N\ell)$ is quadratic in ℓ), so we have to specify the small subspace of it that gives ρ_ℓ.

Let $X_\ell = X_1(N\ell)$, and suppose that we have a surjection $\mathfrak{O}_{E_f} \to \mathbb{F}_\ell$ (E_f has enough prime ideals of degree one for our purposes). Then we have a 2-dimensional $\mathbb{F}_\ell$-subvector space $V_{f,\ell} \subset J_\ell(\overline{\mathbb{Q}})[\ell]$, cut out by $T_r - a_r$ for $r \leq N^2\ell^2$ (this bound on r is indeed polynomial in ℓ). It is impractical to compute these as algebraic varieties (using equations) again because this system is so large.

Couveignes has suggested that we do numerical computations: we have

$$J_\ell(\mathbb{C}) = H_1(X_\ell(\mathbb{C}), \mathbb{R})/H_1(X_\ell(\mathbb{C}), \mathbb{Z}) \supset V_{f,\ell},$$

and suppose $0 \neq x \in V_{f,\ell}$. One should try to:

1. Approximate $F(x) \in \mathbb{C}$ for F some rational function on J_ℓ (defined over $\mathbb{Q}$) such that $\mathbb{Q}(x) = \mathbb{Q}(F(x))$.
2. Bound the height and degree of $F(x)$ (allowing us to compute the algebraic number via its minimal polynomial).

The degree here is no problem because $V_{f,\ell}$ has ℓ^2-elements (and one of these is zero) so the degree is $\leq \ell^2 - 1$. So the main problem is to approximate F and to bound the height.

One may try to ϑ-functions, but these are usually defined as sums over lattices which do not converge quickly enough (the rank of the lattices tends to infinity). Instead, we try to use divisors on X_ℓ. The curves X_ℓ all lie over $X_1(N)$, so we can consider the following kind of functions on X_ℓ: consider the universal elliptic curve over $X_1(N)$ given by a Weierstrass equation, then take the x-coordinate of the given torsion point. Use symmetric expressions to get functions of divisors.

We choose $P_1, \ldots, P_g$ on $X_\ell(K)$ with $K/\mathbb{Q}$ Galois, solvable, of degree polynomial in ℓ, P_i of height polynomial in ℓ. For example, we may take

CM elliptic curves in a isogeny class (such as those with CM by $\mathbb{Q}(i)$). Put $D = P_1 + \cdots + P_g$, a divisor on $X_{\ell,K}$. Let $\mathcal{L}$ be the line bundle on $X_{\ell,K(x)}$ given by x. With probability 1, $H^0(X_{\ell,K(x)}, \mathcal{L}(D))$ is of dimension 1 (by Riemann-Roch). Define $D' = \mathrm{div}(s)$, with $s \neq 0$ is any section of $\mathcal{L}(D)$. Then $\mathcal{L} \simeq \mathcal{O}_{X_{\ell,K(x)}}(D' - D)$. Approximate D' over $\mathbb{C}$:

$$X_\ell(\mathbb{C})^g \to J_\ell(\mathbb{C}) = \mathbb{C}^g/\Lambda$$

$$(Q_1, \ldots, Q_g) \mapsto \sum_i \int_{P_i}^{Q_i} (\omega_1, \ldots, \omega_g),$$

where $x \in \mathbb{C}^g/\Lambda$, specified say by modular symbols.

There are three options to do this.

1. Take random Q_i and start Newton's method. (This converges fast when we start close to a solution; but it works well for polynomials, even if one does not start close to a solution (work of Shub and Smale), but our map is not very polynomial.)
2. Approximate s by using the complex uniformization of $\mathcal{L}$ and then approximate the zeros. This gives a good starting point for Newton's method. To approximate s, one has to approximate solutions of the differential equation $\overline{\partial} f = 0$, for f in the space of C^∞-sections of $\mathcal{L}(D)$; maybe this is standard stuff for people in numerical analysis.
3. **Couveignes** has suggested: do the numerical computations over some $\mathbb{Q}_p$, which involves a p-adic uniformization, which exists only if the reduction is totally degenerate (which does not happen for modular curves). But this does work for modular forms which live on Shimura curves, and in this case we need only to start with a solution modulo p for Newton's method, which involves only solving systems of linear equations.

Suppose we are in case (3). The crucial element is the height estimate; intuitively, the height of D' is not bigger than the height of D plus the height of $\mathcal{L}$ (where the latter is small since it is a torsion bundle). The tool we use is Arakelov theory. In the function field analogue, where $\pi : X \to S$ smooth and proper with $\mathcal{L}$ on X with a section $P : S \to X$, then $\mathcal{L} \simeq \mathcal{O}_X(D' - D - \pi^*E)$, and $D' \equiv D + \pi^*E$, and by Grothendieck-Riemann-Roch we obtain a good bound on $\deg E$.

Problems caused by singular fibres of π give reasonable error terms (still polynomial in ℓ in the case of X_ℓ). In the number field case, I still have to understand better the archimedean contributions to Arakelov intersection theory (Green's functions), and probably also the difference between the Arakelov metric and the hyperbolic metric. Nevertheless, what is lacking is only a proof for a polynomial height estimate for $F(x)$. Even without that one could already start doing some experiments.