On the Computation of the Coefficients of a Modular Form

ANTS VII, Berlin

Bas Edixhoven, Universiteit Leiden

Joint work with Jean-Marc Couveignes, Robin de Jong, Franz Merkl, and Johan Bosman.

Motivated by a question by René Schoof.

Detailed text available on arxiv.

The main results

Definition of Ramanujan's τ-function:

$$x \prod_{n \geq 1} (1 - x^n)^{24} = \sum_{n \geq 1} \tau(n) x^n \quad \text{in } \mathbb{Z}[[x]].$$

Theorem 1 *There exists a probabilistic algorithm that on input a prime number p gives $\tau(p)$, in expected running time polynomial in $\log p$.*

THE MAIN RESULTS

Behind the theorem is the existence of certain Galois representations. The function Δ on the complex upper half plane $\mathbb{H}$ given by:

$$\Delta : \mathbb{H} \to \mathbb{C}, \quad z \mapsto \sum_{n \geq 1} \tau(n) e^{2\pi i n z}$$

is a modular form, the so-called discriminant modular form. It is a new-form of level 1 and weight 12.

THE MAIN RESULTS

Deligne showed (1969) that, as conjectured by Serre, for each prime number l there is a (necessarily unique) semi-simple continuous representation:

$$\rho_l \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(K_l/\mathbb{Q}) \hookrightarrow \mathrm{Aut}(V_l),$$

with V_l a two-dimensional $\mathbb{F}_l$-vector space, such that $\mathbb{Q} \to K_l$ is unramified at all primes $p \neq l$, and such that for all $p \neq l$ the characteristic polynomial of $\rho_l(\mathrm{Frob}_p)$ is given by:

$$\det(1 - x\mathrm{Frob}_p, V_l) = 1 - \tau(p)x + p^{11}x^2.$$

In particular, we have $\mathrm{trace}(\rho_l \mathrm{Frob}_p) = \tau(p)$ mod l for all primes $p \neq l$.

Serre and Swinnerton-Dyer: for l not in $\{2, 3, 5, 7, 23, 691\}$ we have $\mathrm{im}(\rho_l) \supset \mathrm{SL}(V_l)$.

The main results

Theorem 2 *There exists a probabilistic algorithm that computes ρ_l in time polynomial in l. It gives:*

1. the extension $\mathbb{Q} \to K_l$, given as a $\mathbb{Q}$-basis e and the products $e_ie_j = \sum_k a_{i,j,k}e_k$;

2. a list of the elements σ of $\mathrm{Gal}(K_l/\mathbb{Q})$, where each σ is given as its matrix with respect to e;

3. the injective morphism $\rho_l \colon \mathrm{Gal}(K_l/\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{F}_l)$.

Theorem 2 implies Theorem 1 via “standard” algorithms.

Note: $|\tau(p)| < 2p^{11/2}$ by Deligne.

Context and motivation

0. More congruences for $\tau(p)$ than the classical ones.

1. Relation to Schoof's algorithm for elliptic curves and Pila's generalisation to curves of fixed genus and abelian varieties of fixed dimension.

2. Computation of non-solvable global field extensions predicted by Langlands' program.

3. Computation of higher degree etale cohomology with $\mathbb{F}_l$-coefficients, with its Galois action.

4. Evidence towards existence of polynomial time computation of $\#X(\mathbb{F}_p)$ for X a fixed $\mathbb{Z}$-scheme of finite type.

WHERE TO FIND V_l

Deligne's work shows that V_l occurs in:

$$H^{11}(E^{10}_{\overline{\mathbb{Q}},\mathrm{et}}, \mathbb{F}_l)^\vee,$$

$$H^1(j\text{-line}_{\overline{\mathbb{Q}},\mathrm{et}}, \mathrm{Sym}^{10}(R^1\pi_*\mathbb{F}_l))^\vee,$$

$$J_l(\overline{\mathbb{Q}})[l].$$

Here $J_l = \mathrm{jac}(X_l)$, and $X_l = X_1(l)$, $X_1(l)(\mathbb{C}) = \Gamma_1(l)\backslash(\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}))$.

Problem: $g_l := \mathrm{genus}(X_l)$ is approximately $l^2/24$.

Couveignes' suggestion: don't use computer algebra, but approximation and height bounds instead.

STRATEGY

We have:

$$J_l(\mathbb{C}) = \mathbb{C}^{g_l}/\Lambda, \quad \Lambda = H_1(X_l(\mathbb{C}), \mathbb{Z})$$

$$V_l \subset J_l(\mathbb{C})[l] = (l^{-1}\Lambda)/\Lambda$$

$$V_l = \bigcap_{1 \le i \le l^2} \ker (T_i - \tau(i))$$

$$\infty \in X_l(\mathbb{Q})$$

We choose:

$$f : X_{l,\mathbb{Q}} \twoheadrightarrow \mathbb{P}^1_{\mathbb{Q}}$$

as simple as possible.

STRATEGY

$$\phi\colon X_l(\mathbb{C})^{g_l} \twoheadrightarrow J_l(\mathbb{C}) = \mathbb{C}^{g_l}/\Lambda$$

$$Q \longmapsto [Q_1 + \cdots + Q_{g_l} - g_l \cdot \infty] = \sum_{i=1}^{g_l} \int_{\infty}^{Q_i} (\omega_1, \ldots, \omega_{g_l}),$$

where $(\omega_1, \ldots, \omega_{g_l})$ is a basis of normalised newforms.

For x in $V_l \subset l^{-1}\Lambda/\Lambda$, there are $Q_{x,1}, \ldots, Q_{x,g_l}$, unique up to permutation, such that $\phi(Q_x) = x$ (well, $\ldots$).

Consider:

$$P_l := \prod_{x \neq 0} (T - \sum_i f(Q_{x,i})) \quad \text{in } \mathbb{Q}[T].$$

STRATEGY

Then K_l is the splitting field of P_l.

Show that the *(logarithmic) height* of the coefficients of P_l are $O(l^c)$. Recall: $h(a/b) = \log(\max(|a|, |b|))$ if $a, b \in \mathbb{Z}$, $b \neq 0$ and $\gcd(a, b) = 1$.

Show that P_l can be approximated in $\mathbb{C}[T]$ with a precision of n digits, in time $O((ln)^c)$. Or approximated p-adically, or reductions mod many small primes. . . .

Theorem 3 (Edixhoven, de Jong) *There is an integer c such that for all l we can take f in such a way that the height of the coefficients of P_l are bounded above by l^c.*

Tool: Arakelov theory on X_l (Faltings' arithmetic Riemann-Roch, etc.).

To get an impression ($D := g_l{\cdot}\infty$, $B := \mathrm{Spec}(O_{K_l})$, $\mathcal{X}$ a model of X_l, $D'_x = \sum_i Q_{x,i}$):

$$(D'_x, \infty) + \log \#\mathrm{R}^1 p_* O_{\mathcal{X}}(D'_x) \leq -\frac{1}{2}(D, D - \omega_{\mathcal{X}/B}) + 2g_l^2 \sum_{s \in B} \delta_s \log \#k(s) + \sum_{\sigma} \log \|\vartheta\|_{\sigma,\mathrm{sup}} + \frac{g_l}{2}[K_l : \mathbb{Q}] \log(2\pi) + \frac{1}{2} \deg \det p_* \omega_{\mathcal{X}/B} + (D, \infty)\,,$$

Height bound

$$\log \|\vartheta\|_{\mathrm{sup}} = O(l^6),$$

$$h_{\mathrm{abs}}(X_l) = O(l^2 \log(l)), \quad \text{(absolute Faltings height)}$$

$$\sup_{a \neq b} g_{a,\mu}(b) = O(l^6), \quad \text{(Arakelov's Green function; Merkl).}$$

HEIGHT BOUND, A BYPRODUCT.

Theorem 4 *A prime number* $p \nmid l$ *is said to be* l-good *if for all* x *in* $V_l - \{0\}$ *the following two conditions are satisfied:*

1. at all places v *of* K_l *over* p *the specialisation* $(D'_x)_{\overline{\mathbb{F}}_p}$ *at* v *is the unique effective divisor on the reduction* $X_l, \overline{\mathbb{F}}_p$ *such that the difference with* $D_{\overline{\mathbb{F}}_p}$ *represents the specialisation of* x*;*

2. the specialisations of the non-cuspidal part D''_x *of* D'_x *at all* v *above* p *are disjoint from the cusps.*

Then we have:

$$\sum_{p \text{ not } l\text{-good}} \log p \leq c{\cdot}l^{14}.$$

Couveignes' finite field method

Theorem 5 (Couveignes) *There is a probabilistic algorithm that on input l computes for p a prime that is l-good, the reductions $(D'_x)_{\overline{\mathbb{F}}_p}$ of the divisors D'_x on $X_{l,\overline{\mathbb{F}}_p}$, with an expected running time that is polynomial in l and p.*

Tool: computer algebra on $X_{l,\mathbb{F}_{p^r}}$, projecting random divisor classes into V_l using Hecke operators (well . . .).

Why not polynomial in $\log p$? Only because one needs the numerator of the zeta function of $X_{l,\mathbb{F}_p}$.

Examples

Using Magma to do computations over $\mathbb{C}$, Johan Bosman has found, for $l = 13, 17$ and 19, polynomials P_l , of degrees $l^2 - 1$, and polynomials P_l' of degree $l + 1$.

We have no proof that these polynomials are correct, but they do pass the following tests:

1. the ring of integers of the corresponding number field ramifies only at l,

2. the reductions modulo small primes p correspond to the orbit structures of $\rho_l(\mathrm{Frob}_p)$ on $V_l - \{0\}$ and $\mathbb{P}(V_l)$.

Examples

$$
\begin{aligned}
2535853P'_{13} = {} & 2535853x^{14} - 127713190x^{13} - 9947603692x^{12} \\
& + 795085450224x^{11} - 29425303073920x^{10} \\
& + 667684302673440x^{9} - 9974188441308416x^{8} \\
& + 106364914419352576x^{7} - 1012336515218109952x^{6} \\
& + 9094902359324720640x^{5} - 60847891441699468288x^{4} \\
& + 324814691085008943104x^{3} \\
& - 1761495929112889016320x^{2} \\
& + 6235371687080448827392x \\
& - 10767442738728520761344.
\end{aligned}
$$

Examples

A polynomial that gives the same extension (found using LLL):

$$x^{14} + 7x^{13} + 26x^{12} + 78x^{11} + 169x^{10} + 52x^9 - 702x^8 - 1248x^7 + 494x^6 + 2561x^5 + 312x^4 - 2223x^3 + 169x^2 + 506x - 215,$$

EXAMPLES

Required precision as suggested by Bosman's computations:

about 80 digits for $l = 13$ (genus 2),

400 digits for $l = 17$ (genus 5),

and 830 digits for $l = 19$ (genus 7).

For $l = 19$ the computations were distributed over several machines and still took a couple of months.

It seems that it is hard to get much further.

EXAMPLES

Using same methods, Johan Bosman could also produce a polynomial that gives a $\mathtt{SL}_2(\mathbb{F}_{16})$ extension of $\mathbb{Q}$ (was still missing in tables of Jürgen Klüners), corresponding to a weight 2 modular form on $\Gamma_0(137)$ (genus 11).

Klüners has checked that the Galois group is indeed $\mathtt{SL}_2(\mathbb{F}_{16})$.

In this case, Bosman tries to *prove*, using Khare-Wintenberger, that his representation is right one.

DETERMINISTIC VERSION?

Theorem 6 (Couveignes, arxiv) *The operations of addition and subtraction in the complex Jacobian $J_0(l)(\mathbb{C})$ of $X_0(l)$ can be done in deterministic polynomial time in l and the required precision. More precisely, given elements P, Q and R of $X_0(l)^g$, elements S and D of $X_0(l)^g$ can be computed in time polynomial in l and the required precision, such that $\phi(S) = \phi(Q) + \phi(R)$ and $\phi(D) = \phi(Q) - \phi(R)$ hold within the required precision. Moreover, for x in $\mathbb{C}^g/\Lambda$, one can compute Q in $X_0(l)^g$ in time polynomial in l and the required precision, such that $\phi(Q) = x$ holds within the required precision.*

This result will almost certainly be generalised to all curves $X_1(n)$, giving deterministic versions of Theorems 1 and 2.

THE END

Thank you for your attention!

Questions?