Polynomial time computation of Galois representations attached to modular forms

Bas Edixhoven

Universiteit Leiden

FOCM, Montevideo, 2014/12/11

joint work with Jean-Marc Couveignes, Robin de Jong, Johan Bosman, Franz Merkl

and more recent work by Peter Bruin, Ila Varma, Ariyan Javan Peykar, Nicolas Mascot, Jinxiang Zeng, and Tian Peng

What *are* modular forms?

Let k be in $\mathbb{Z}$. A *modular form of weight k on* $\mathrm{SL}_2(\mathbb{Z})$ is a function $f\colon \mathbb{H} \to \mathbb{C}$, holomorphic, such that

$$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), \quad \forall z \in \mathbb{H}: \quad f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z),$$

and such that for all $y \in \mathbb{R}_{>0}$, the restriction of f to $\{z \in \mathbb{H} : \Im(z) > y\}$ is bounded.

Let $q\colon \mathbb{H} \to \mathbb{C}$, $z \mapsto e^{2\pi i z}$. Then

$$f = \sum_{n \geq 0} a_n(f) q^n.$$

The $a_n(f)$ are called the *coefficients of f*. There is a more general notion of modular form on *congruence subgroups* of $\mathrm{SL}_2(\mathbb{Z})$.

Why are we interested in modular forms?

One among many reasons: coefficients of modular forms arise in counting problems in number theory, combinatorics, algebraic geometry, lattices.

The function $\theta = \sum_{x_1 \in \mathbb{Z}} q^{x_1^2}$ is a modular form of weight $1/2$ on $\Gamma_1(4) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv 1(4) \text{ and } c \equiv 0(4)\}$.

Then for all $d \in \mathbb{Z}_{\geq 0}$:

$$\theta^d = \left(\sum_{x_1 \in \mathbb{Z}} q^{x_1^2}\right) \cdots \left(\sum_{x_d \in \mathbb{Z}} q^{x_d^2}\right) = \sum_{x \in \mathbb{Z}^d} q^{x_1^2 + \cdots + x_d^2} = \sum_{n \geq 0} r_d(n) q^n$$

with $r_d(n) = \#\{x \in \mathbb{Z}^d : x_1^2 + \cdots + x_d^2 = n\}$, is in $M_{d/2}(\Gamma_1(4))$, the $\mathbb{C}$-vector space of modular forms of weight $d/2$ on $\Gamma_1(4)$.

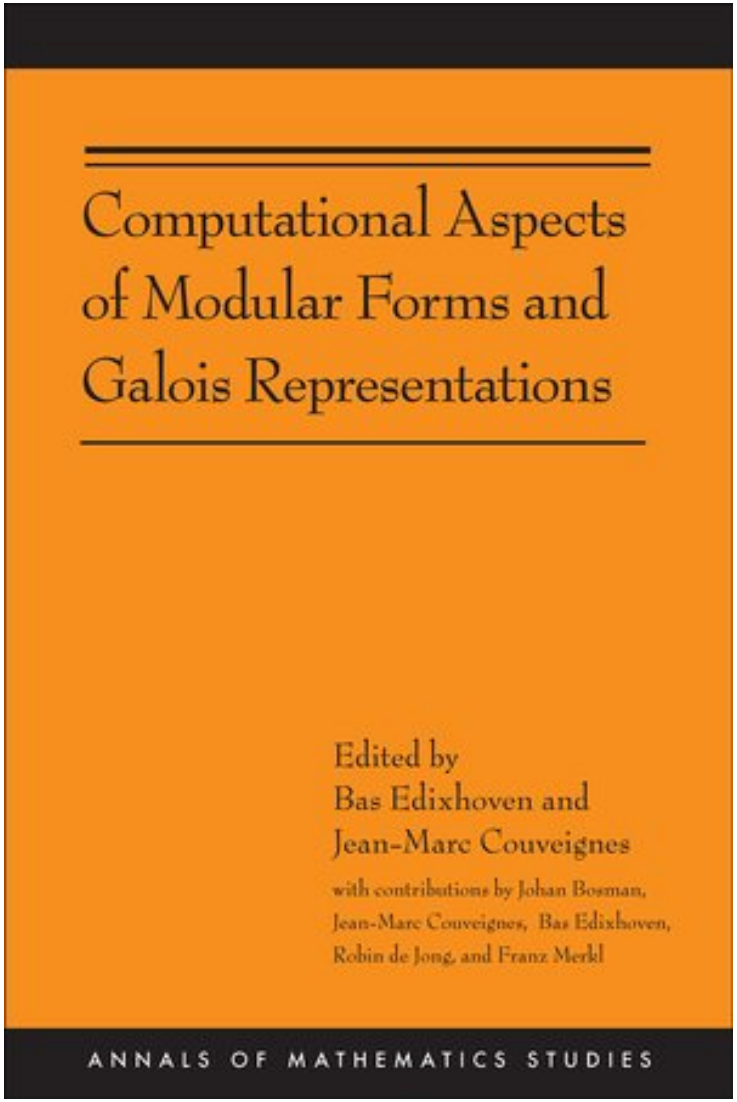
The first results

Fact: the $M_k(\Gamma_1(N))$ are finite dimensional, and have a $\mathbb{C}$-basis of forms with integer coeffients.

Theorem 1(Couveignes, Edixhoven, de Jong, Merkl). *There is a deterministic algorithm that on input the weight k and the coefficients $a_i(f) \in \mathbb{Z}$ for $0 \leq i \leq k/12$ of a modular form on $\mathrm{SL}_2(\mathbb{Z})$ with integer coefficients, and an integer $n \geq 1$ with its factorisation into primes, computes the integer $a_n(f)$. For fixed k, the running time is polynomial in $\log n$. If the Generalised Riemann Hypothesis for number fields holds, then the running time is polynomial in k and $\log n$.*

Remarks. This is very fast.
Necessity of getting n with factorisation: $E_4 = 1 + 240 \sum_{n \geq 1} \sigma_3(n) q^n$ is in $M_4(\mathrm{SL}_2(\mathbb{Z})$, with $\sigma_3(n) = \sum_{d|n} d^3$.
By the way: $E_4(q^2)$ is the theta function of the $E8$-lattice. The theorem gives coefficients of the powers of E_4.

How does it work? Read our book! PUP, 2011.



The commercial by PUP:

. . . Such fast computation of Fourier coefficients is itself based on the main result of the book: the computation, in polynomial time, of Galois representations over finite fields attached to modular forms by the Langlands program. Because these Galois representations typically have a nonsolvable image, this result is a major step forward from explicit class field theory, and it could be described as the start of the explicit Langlands program.

The computation of the Galois representations uses their realization, following Shimura and Deligne, in the torsion subgroup of Jacobian varieties of modular curves. The main challenge is then to perform the necessary computations in time polynomial in the dimension of these highly nonlinear algebraic varieties. Exact computations involving systems of polynomial equations in many variables take exponential time. This is avoided by numerical approximations with a precision that suffices to derive exact results from them. Bounds for the required precision. . . are obtained from Arakelov theory. . .

Generalisation by Peter Bruin, PhD thesis 2010

Theorem 2(Bruin). *Let a be a positive integer. There is a probabilistic algorithm that, given a positive integer k, a squarefree positive integer b coprime to a, the q-expansion of a Hecke eigenform f of weight k for $\Gamma_1(ab)$ up to sufficient precision to determine f uniquely, and a positive integer m in factored form, computes $a_m(f)$, and that runs in expected time polynomial in b, k and* $\log m$ *under GRH for number fields.*

Remarks *probabilistic, Las Vegas*: because based on numerical computations over *finite fields*, and not as before over $\mathbb{C}$.

The Arakelov theory is more involved (in the level one case we had a very special *non-special* divisor).

In these theoretical results, it is the length of the proofs that is minimised, not the running time. I will describe real computations a bit later in this lecture.

A nice theoretical consequence: sums of squares

Let $\chi\colon \mathbb{Z} \to \mathbb{C}$, $\chi(d) = 0, 1, 0, -1$ if $d \equiv 0, 1, 2, 3(4)$.
Fermat, Gauss, Legendre, Jacobi, Eisenstein, Smith and Liouville:

$$r_2(n) = 4 \sum_{d|n} \chi(d),$$

$$r_3(n) = 12 \cdot h(\mathbb{Z}[\sqrt{-n}]), \quad \text{for } n > 1 \text{ squarefree, 1 or 2 mod 4,}$$

$$r_4(n) = 8 \sum_{2 \nmid d|n} d + 16 \sum_{2 \nmid d|(n/2)} d,$$

$$r_6(n) = 16 \sum_{d|n} \chi\left(\frac{n}{d}\right) d^2 - 4 \sum_{d|n} \chi(d) d^2,$$

$$r_8(n) = 16 \sum_{d|n} d^3 - 32 \sum_{d|(n/2)} d^3 + 256 \sum_{d|(n/4)} d^3,$$

$$r_{10}(n) = \frac{4}{5} \sum_{d|n} \chi(d) d^4 + \frac{64}{5} \sum_{d|n} \chi\left(\frac{n}{d}\right) d^4 + \frac{8}{5} \sum_{d \in \mathbb{Z}[i],\, |d|^2 = n} d^4.$$

A nice theoretical consequence

Theorem 3 (Ila Varma, masters thesis, Leiden, 2010). *There is no even $d > 10$ for which θ^d is a linear combination of Eisenstein series and modular forms attached to Hecke characters.*

Theorem 4 (book+Bruin). *Assume GRH. Then there is a probabilistic algorithm that for even d and n with factorisation computes $r_d(n)$ in time polynomial in d and* $\log n$.

Conclusion. From an algorithmic perspective this classical problem now has a satisfactory answer for *all* even d. The question for *formulas* has a negative answer, but for *computing* that negative answer does not matter and we now have a *positive* answer. For odd $d > 3$, see Shimura, Bull. AMS 43, 2006.

Galois representations attached to modular forms

It is better to consider just one typical case, the *discriminant modular form* in $S_{12}(\mathrm{SL}_2(\mathbb{Z}))$:

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

Deligne showed (1969) that for each prime number ℓ there is a representation:

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(K_\ell/\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{F}_\ell),$$

such that $\mathbb{Q} \to K_\ell$ is unramified at all primes $p \neq \ell$, and such that for all $p \neq \ell$ the characteristic polynomial of $\rho_\ell(\mathrm{Frob}_p)$ is given by:

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

In particular: $\mathrm{trace}(\rho_\ell(\mathrm{Frob}_p)) = \tau(p) \bmod \ell$ for all primes $p \neq \ell$.
Serre and Swinnerton-Dyer: for ℓ not in $\{2, 3, 5, 7, 23, 691\}$ we have $\mathrm{im}(\rho_\ell) \supset \mathrm{SL}_2(\mathbb{F}_\ell)$.

Main theorem of the book (in this special case)

Theorem 5 *There exists an algorithm that on input ℓ computes ρ_ℓ in time polynomial in ℓ. It gives:*

- *the extension $\mathbb{Q} \to K_\ell$, given as a $\mathbb{Q}$-basis e and the products $e_i e_j = \sum_k a_{i,j,k} e_k$;*
- *a list of the elements σ of $\mathrm{Gal}(K_\ell/\mathbb{Q})$, where each σ is given as its matrix with respect to e;*
- *the injective morphism $\rho_\ell \colon \mathrm{Gal}(K_\ell/\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$.*

Theorem 5 implies Theorem 1 via "standard algorithms".

One can compute $\tau(p)$ mod ℓ in time $O((\ell \cdot \log p)^c)$.

Note: $|\tau(p)| < 2p^{11/2}$ by Deligne, and $\prod_{\ell < x} \ell \approx e^x$.

Where to find ρ_ℓ

Deligne's work shows that ρ_ℓ is realised on a subspace V_ℓ in:

- $\mathrm{H}^{11}(E^{10}_{\overline{\mathbb{Q}},\mathrm{et}}, \mathbb{F}_\ell)^\vee$, this *is* computable! (Poonen–Testa–van Luijk, Madore–Orgogozo (and Jinbi Jin, in progress)),
- $\mathrm{H}^1(j\text{-line}_{\overline{\mathbb{Q}},\mathrm{et}}, \mathrm{Sym}^{10}(R^1\pi_*\mathbb{F}_\ell))^\vee$,
- $J_\ell(\overline{\mathbb{Q}})[\ell]$.

Here $J_\ell = \mathrm{jac}(X_\ell)$, $X_\ell = X_1(\ell)$, $X_1(\ell)(\mathbb{C}) = \Gamma_1(\ell)\backslash(\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}))$.

X_ℓ is the (compactified) moduli space of (E, P), elliptic curves with a point of order ℓ. Smooth and proper over $\mathbb{Z}[1/\ell]$.

Problem: $g_\ell := \mathrm{genus}(X_\ell) = \dim(J_\ell) = (\ell - 5)(\ell - 7)/24$.

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

Strategy for computing ρ_ℓ

X_ℓ has Hecke correspondences. For $n \geq 1$:

$$T_n \colon (E, P) \mapsto \sum_C (E/C, \overline{P}), \quad C \subset E \text{ subgroup of order } n, \text{ with } P \notin C.$$

The T_n commute, generate a commutative subring $\mathbb{T}_\ell \subset \mathrm{End}(J_\ell)$.

$$\omega_1, \ldots, \omega_{g_\ell} \quad \text{a basis of normalised eigenforms of } \Omega^1(X_\ell)$$

$$J_\ell(\mathbb{C}) = \mathbb{C}^{g_\ell}/\Lambda, \quad \Lambda = H_1(X_\ell(\mathbb{C}), \mathbb{Z})$$

$$V_\ell \subset J_\ell(\mathbb{C})[\ell] = (\ell^{-1}\Lambda)/\Lambda, \quad V_\ell = \bigcap_{1 \leq i \leq \ell^2} \ker(T_i - \tau(i))$$

Modular symbols algorithms (Magma, Sage): $\mathbb{T} \subset \mathrm{End}(\mathrm{H}_1(X_\ell(\mathbb{C}), \mathbb{Z}))$.

Strategy for computing ρ_ℓ

We have $\infty \in X_\ell(\mathbb{Q})$, we choose $f\colon X_{\ell,\mathbb{Q}} \twoheadrightarrow \mathbb{P}^1_{\mathbb{Q}}$ as simple as possible.

$$\phi\colon X_\ell(\mathbb{C})^{g_\ell} \longrightarrow J_\ell(\mathbb{C}) = \mathbb{C}^{g_\ell}/\Lambda,$$

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

For x in $V_\ell \subset \ell^{-1}\Lambda/\Lambda$, there are $Q_{x,1}, \ldots, Q_{x,g_\ell}$ in $X_\ell(\overline{\mathbb{Q}})$, unique up to permutation (with a bit of luck), such that $\phi(Q_x) = x$.

Then K_ℓ is the splitting field of:

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

Strategy for computing ρ_ℓ

How to compute P_ℓ?

- Recall the *(logarithmic) height*: $h(a/b) = \log(\max(|a|, |b|))$ if $a, b \in \mathbb{Z}$, $b > 0$ and $\gcd(a, b) = 1$.
  Show that $h(P_{\ell,i}) = O(\ell^c)$.
  Edixhoven and de Jong, with help from Merkl: $h(P_{\ell,i}) = O(\ell^{16})$.
  This uses Arakelov geometry. Has been generalised by Bruin, and by Javan Peykar. The problem is uniformity in the level.
- Show that P_ℓ can be approximated in $\mathbb{C}[T]$ with a precision of n digits, in time $O((n\ell)^c)$.
  Or approximated p-adically, or reductions mod many small primes.
  Couveignes: did *two cases*: in $\mathbb{C}$ (deterministic) and over finite fields (Las Vegas).

Couveignes's complex algorithm

Over $\mathbb{C}$, rough sketch.

1. Let x be in $V_\ell = \ell^{-1}\Lambda/\Lambda$.
2. Lift it to $\tilde{x}$ in $\ell^{-1}\Lambda \subset \mathbb{C}^{g_\ell}$.
3. Take $m \in \mathbb{Z}$ large enough, and let $y = 2^{-m}\tilde{x}$.
4. By integration of power series get R_x in $X_\ell(\mathbb{C})^{g_\ell}$, close to ∞^{g_ℓ} hence good convergence, such that $\phi(R_x) = y$ with desired precision.
5. Then double R_x m times, using algebraic operations in $J_\ell(\mathbb{C})$ involving effective divisors of degree g_ℓ. This gives Q'_x.
6. For general $x \in J_\ell(\mathbb{C})$, $\phi(Q'_x) \approx x$, but for $Q'_x \approx Q_x$, still some Arakelov theory is used (for our $x \in V_\ell$).

We do not know how to make the homotopy lifting method provably work in time polynomial in ℓ.

Bosman's computations

Bosman did the first computations, between 2004 and 2006, using Newton iteration (HLM) globally, randomising initial data.
With Magma he has found, for all $\ell \leq 23$ and all normalised cuspidal eigenforms f_k of level one and weight $k \leq 22$, a polynomial $P_{k,\ell}^{\mathrm{proj}}$ of degree $\ell+1$ that gives:

$$\mathbb{P}(\rho_{f_k,\ell})\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{F}_\ell)$$

To prove that his polynomials are correct, he uses that Serre's modularity conjecture has been proved by Khare, Wintenberger and Kisin.

Convergence gets worse if ℓ increases: one covers $X_\ell(\mathbb{C})$ by disks around the cusps, and one has to work ever closer to the radius of convergence.

An example by Bosman

$$
\begin{aligned}
f = x^{24} &- 2x^{23} + 115x^{22} + 23x^{21} + 1909x^{20} + 22218x^{19} \\
&+ 9223x^{18} + 121141x^{17} + 1837654x^{16} - 800032x^{15} \\
&+ 9856374x^{14} + 52362168x^{13} - 32040725x^{12} \\
&+ 279370098x^{11} + 1464085056x^{10} + 1129229689x^{9} \\
&+ 3299556862x^{8} + 14586202192x^{7} + 29414918270x^{6} \\
&+ 45332850431x^{5} - 6437110763x^{4} - 11142992035 8x^{3} \\
&- 12449542097x^{2} + 93960798341x - 31890957224
\end{aligned}
$$

has Galois group $\mathrm{PGL}_2(\mathbb{Z}/23\mathbb{Z})$, and (reduced) discriminant 23^{43}; note that $g_{23} = 12$, and that $\deg(P_{23}) = 23^2 - 1 = 528$. Before "polredding" his polynomial $P^{\mathrm{proj}}_{22,23}$ had coefficients of almost 2000 digits. Computations took months.

Jinxiang Zeng's computations

Couveignes and I lectured on this subject in Beijing in 2011–2012. Jinxiang Zeng (Tsinghua) has implemented Couveignes's finite field method, using Hess's algorithms (already implemented in Magma) for computing in $J_\ell(\mathbb{F}_q)$, and in certain $\mathrm{jac}(X_\ell/H)$, $H \subset (\mathbb{Z}/\ell\mathbb{Z})^\times$. He uses recent algorithms for isogenies between elliptic curves for computing Hecke operators.

He computed (arxiv, 2013) a polynomial P_{19} of degree $19^2 - 1$, with coefficients up to 1681 digits, and a polynomial $P^{\mathrm{proj}}_{12,31}$ of degree 32, with coefficients up to 2426 digits.

He worked with a quotient of X_{31} of genus 6, as suggested by Maarten Derickx, and for which a plane model was provided by Mark van Hoeij.

Nicolas Mascot's computations

Nicolas Mascot (Warwick) has made Couveignes's complex method much more practical. I just describe the main improvements.

He uses Khuri-Makdisi's algorithms for doubling in $J_\ell(\mathbb{C})$ in terms of divisors on $X_\ell(\mathbb{C})$ (Peter Bruin had already used this (theoretically) for finite fields) . This now only involves linear algebra.

He has a much better rational function on J_ℓ to map V_ℓ to $\overline{\mathbb{Q}}$. Let $\mathcal{L}$ be a line bundle of degree g_ℓ on X_ℓ, and let P_0 and P_1 be in $X_\ell(\mathbb{Q})$. For x in V_ℓ, $\mathrm{H}^0(X_{\ell,\overline{\mathbb{Q}}}, \mathcal{L}_x \otimes \mathcal{L}) = \overline{\mathbb{Q}} \cdot s$, then take "$s(P_0)/s(P_1)$".This rational function has poles only along two translates of Θ, whereas the previous function along $deg(f)$ translates ($f\colon X_\ell \to \mathbb{P}^1_{\mathbb{Q}}$).

For the computation of P_{29} (of degree $29^2-1 = 840$) a precision of 4000 bits was already sufficient.
He used Dokchitsers's resolvents. Estimates complexity at $O(\ell^9)$.

Some congruences by Mascot

p	Similarity class of $\rho_{29}(\mathrm{Frob}_p)$	$\tau(p) \bmod 29$
$10^{1000}+453$	$\begin{bmatrix} 0 & 5 \\ 1 & 21 \end{bmatrix}$	21
$10^{1000}+1357$	$\begin{bmatrix} 0 & 28 \\ 1 & 8 \end{bmatrix}$	8
$10^{1000}+2713$	$\begin{bmatrix} 0 & 9 \\ 1 & 11 \end{bmatrix}$	11
$10^{1000}+4351$	$\begin{bmatrix} 0 & 26 \\ 1 & 0 \end{bmatrix}$	0

Tian Peng's computations

Tian Peng (PhD student of René Schoof) used Johan Bosman's code and he trick proposed by Derickx to use appropriate $X_1(\ell)/H$ and found the projective representations for (k, ℓ) equal to $(12, 31)$, $(16, 29)$, $(20, 31)$, $(22, 31)$.

References

Thank you for your attention!

Peter Bruin, *Computing in Jacobians of projective curves over finite fields*. arXiv:1003.2563

Couveignes, Edixhoven, *Approximate computations with modular curves*. arXiv:1205.5896.

Nicolas Mascot, *Computing modular Galois representations*. arXiv:1211.1635

Tian Peng, *Computations of Galois Representations Associated to Modular Forms of Level One*. arXiv:1311.0577

Jinxiang Zeng, *On the computation of coefficients of modular forms: the p-adic approach*. arXiv:1211.1124

Maarten Derickx, Mark van Hoeij, Jinxiang Zeng, *Computing Galois representations and equations for modular curves* $X_H(\ell)$. arXiv:1312.6819