Computing polynomials attached to modular Galois representations

Johan Bosman

Workshop
'Computations with modular forms'
Thursday 21 August 2008, Bristol

Netherlands Organisation for Scientific Research

The Ramanujan tau function

Definition:

$$\Delta = q \prod_{n \geq 1} (1 - q^n)^{24} =: \sum_{n \geq 1} \tau(n) q^n \in S_{12}(\mathrm{SL}_2(\mathbb{Z}))$$

First few values:

$$\Delta = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 + \cdots$$

Properties:

$$\begin{array}{ll} \tau(mn) = \tau(m)\tau(n) & \text{if } (m,n) = 1 \\ \tau(p^{r+1}) = \tau(p)\tau(p^r) - p^{11}\tau(p^{r-1}) & \text{for } p \text{ prime} \\ |\tau(p)| \leq 2p^{11/2} & \text{for } p \text{ prime} \end{array}$$

Question (Schoof to Edixhoven)**.** Is it possible to compute $\tau(p)$ for p prime in time polynomial in $\log(p)$?

Computing $\tau(p)$

Theorem (Edixhoven, Couveignes, R. de Jong, Merkl)**.** *There exists a probabilistic algorithm that on input primes p and ℓ with $p \neq \ell$ can compute $\underline{\tau(p) \bmod \ell}$ in expected time polynomial in $\log p$ and ℓ.*

Corollary. *There exists a probabilistic algorithm that on input a prime number p can compute $\tau(p)$ in expected time polynomial in $\log p$.*

Congruences. For $\ell \in \{2, 3, 5, 7, 23, 691\}$ we have simple formulas for $\tau(p)$ modulo (a power of) ℓ, e.g.

$$\tau(p) \equiv p^{41} + p^{70} \bmod 5^3 \text{ for } p \neq 5$$
$$\tau(p) \equiv 1 + p^{11} \bmod 691 \text{ for all } p$$

Galois representations for $\tau(p)$ mod ℓ

Theorem (Deligne). *For each prime ℓ there exists a continuous representation*

$$\rho_\ell = \overline{\rho}_{\Delta,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell)$$

that is unramified outside ℓ and that satisfies

$$\mathrm{charpol}(\rho(\mathrm{Frob}_p)) \equiv x^2 - \tau(p)x + p^{11} \bmod \ell$$

for each prime $p \neq \ell$.

Remark (Serre). We have a simple formula for $\tau(p)$ mod ℓ iff $\mathrm{Im}(\rho_\ell)$ does not contain $\mathrm{SL}_2(\mathbb{F}_\ell)$, which is exactly the case for $\ell \in \{2, 3, 5, 7, 23, 691\}$.

Assume $\mathrm{Im}(\rho_\ell) \supset \mathrm{SL}_2(\mathbb{F}_\ell)$ from now. There is a number field K_ℓ through which ρ_ℓ factors:

$$\begin{array}{ccc} \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \xrightarrow{\rho_\ell} & \mathrm{GL}_2(\mathbb{F}_\ell) \\ & \searrow\!\!\!\!\searrow \quad \nearrow & \\ & \mathrm{Gal}(K_\ell/\mathbb{Q}) & \end{array}$$

Computing K_ℓ

$$\begin{array}{ccc} \mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \xrightarrow{\quad\rho_\ell\quad} & \mathsf{GL}_2(\mathbb{F}_\ell) \\ & \searrow\!\!\!\!\searrow \quad\quad \nearrow & \\ & \mathsf{Gal}(K_\ell/\mathbb{Q}) & \end{array}$$

The action of $\mathsf{Im}(\rho_\ell)$ on $\mathbb{F}_\ell^2 - \{0\}$ is *faithful*. So there is a polynomial P_ℓ of degree $\ell^2 - 1$ with

$$K_\ell = \mathsf{Spf}(P_\ell).$$

Once we have P_ℓ, the field K_ℓ can be obtained by adjoining 2 roots of P_ℓ to $\mathbb{Q}$. This enables us *in theory* to compute $\rho_\ell(\mathsf{Frob}_p)$ for all $p \neq \ell$ using standard algorithms in number theory (computing $\mathsf{Gal}(K_\ell/\mathbb{Q})$, Frobenius classes, etc).

More generally

Theorem (Deligne). *Let $f = \sum a_n q^n \in S_k(\Gamma_1(N))$ be a newform of character ε. Put $K_f = \mathbb{Q}(a_1, a_2, \ldots)$ and let $\lambda \mid \ell$ be a prime of K_f. Then there exists a continuous representation*

$$\rho = \overline{\rho}_{f,\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\lambda)$$

that is unramified outside $N\ell$ and that satisfies

$$\mathrm{charpol}(\rho(\mathrm{Frob}_p)) \equiv x^2 - a_p x + \varepsilon(p) p^{k-1} \bmod \lambda$$

for all primes $p \nmid N\ell$.

We have a number field K_λ as in the diagram for which we want to compute a splitting polynomial $P_{f,\lambda}$:

$$\begin{array}{ccc} \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \xrightarrow{\quad\overline{\rho}_{f,\lambda}\quad} & \mathrm{GL}_2(\mathbb{F}_\lambda) \\ & \searrow\!\!\!\!\searrow \qquad \nearrow & \\ & \mathrm{Gal}(K_\lambda/\mathbb{Q}) & \end{array}$$

Inside the Jacobian of $X_1(N')$

Assume $k \leq \ell + 1$ and that $\overline{\rho}_{f,\lambda}$ is absolutely irreducible. Put

$$N' = \begin{cases} N & \text{for } k = 2, \\ N\ell & \text{otherwise.} \end{cases}$$

Let $\mathbb{T} = \mathbb{Z}[T_1, T_2, \ldots] \subset \mathrm{End}_{\mathbb{Q}}(J_1(N'))$ be the Hecke algebra and put

$$\theta = \overline{\theta}_{\lambda,f} : \mathbb{T} \to \mathbb{F}_\lambda, \quad T_n \mapsto a_n \bmod \lambda$$

Put $\mathfrak{m} = \mathrm{Ker}\,\theta$, then $J_1(N')(\overline{\mathbb{Q}})[\mathfrak{m}]$ is a $\mathbb{T}/\mathfrak{m}$-module with an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. It is non-zero and contains a submodule that is isomorphic to $\overline{\rho}_{f,\lambda}$ (Mazur).

In most cases, $J_1(N')(\overline{\mathbb{Q}})[\mathfrak{m}] \sim \overline{\rho}_{f,\lambda}$. In any case, $\overline{\rho}_{f,\lambda}$ is the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on some $V_\lambda \subset J_1(N')(\overline{\mathbb{Q}})[\ell]$.

The Jacobian of $X_1(N')$

We have $\overline{\rho}_{f,\lambda}$ as the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $V_\lambda \subset J_1(N')(\overline{\mathbb{Q}})[\ell]$.

Pick a suitable $h \in \mathbb{Q}(J_1(N'))$, then

$$P_{f,\lambda} = \prod_{Q \in V_\lambda - \{0\}} (x - h(Q))$$

Let D be an effective divisor on $X_1(N')_{\mathbb{Q}}$ of degree $g = g(X_1(N'))$ (e.g. $D = g \cdot 0$), then we have a birational morphism

$$\phi : \mathrm{Sym}^g X_1(N') \to J_1(N'), \quad (Q_1, \ldots, Q_g) \mapsto \left[\left(\sum_{i=1}^{g} Q_i \right) - D \right].$$

So $\mathbb{Q}(J_1(N')) \cong \mathbb{Q}(\mathrm{Sym}^g X_1(N'))$. Pick $\psi \in \mathbb{Q}(X_1(N'))$ and put

$$h(Q_1, \ldots, Q_g) := \sum_{i=1}^{g} \psi(Q_i).$$

The Jacobian of $X_1(N')$ over $\mathbb{C}$

Pick a basis $f_1, \ldots, f_g$ of $S_2(\Gamma_1(N'))$. Put

$$\Lambda = \left\{ \int_\gamma (f_1, \ldots, f_g) \frac{dq}{q} \; : \; [\gamma] \in H_1(X_1(N')(\mathbb{C}), \mathbb{Z}) \right\} \subset \mathbb{C}^g.$$

Then (Abel-Jacobi) we have

$$J_1(N')(\mathbb{C}) \xrightarrow{\sim} \mathbb{C}^g/\Lambda, \quad \sum (Q_i - P_i) \mapsto \sum \int_{P_i}^{Q_i} (f_1, \ldots, f_g) \frac{dq}{q}$$

so that we get a birational morphism

$$\phi : \mathrm{Sym}^g X_1(N')(\mathbb{C}) \to \mathbb{C}^g/\Lambda, \quad (Q_1, \ldots, Q_g) \mapsto \sum_{i=1}^{g} \int_0^{Q_i} (f_1, \ldots, f_g) \frac{dq}{q}.$$

We can evaluate (integrals of) modular forms easily using q-expansions at various cusps.

Using Newton-Raphson to compute $\phi^{-1}(V_\lambda - \{0\})$

$$\phi' : (X_1(N')(\mathbb{C}))^g \to \mathbb{C}^g/\Lambda, \quad (Q_1, \ldots, Q_g) \mapsto \sum_{i=1}^{g} \int_0^{Q_i} (f_1, \ldots, f_g) \frac{dq}{q},$$

We have a function $\psi \in \mathbb{Q}(X_1(N'))$ and a set of torsion points

$$V_\lambda(\mathbb{C}) \subset J_1(N')(\mathbb{C})[\ell] = \frac{1}{\ell}\Lambda/\Lambda \subset \mathbb{C}^g/\Lambda.$$

Use *Newton-Raphson* to compute $\phi'^{-1}(V_\lambda(\mathbb{C}))$: For $U \subset \mathbb{C}^g$ open and $F : U \to \mathbb{C}^g$ analytic we have

$$F(Q+h) = F(Q) + \left(\frac{\partial F_i}{\partial z_j}(Q)\right)_{i,j} \cdot h + O(\|h\|^2).$$

So for P close to $F(Q)$ take

$$h = \left(\frac{\partial F_i}{\partial z_j}(Q)\right)_{i,j}^{-1} \cdot (P - F(Q)),$$

Then $F(Q+h)$ will be much closer to P than $F(Q)$.

Computing rational coefficients

So we have

$$P_\lambda = \prod_{Q\in\phi^{-1}(V_\ell(\mathbb{C})-\{0\})} \left(x - \sum_{i=1}^{g} \psi(Q_i) \right) \approx x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{R}[x].$$

We seek $p_0, \ldots, p_{n-1}, q$ with $\frac{p_i}{q} \approx a_i$. Choose a small $C > 0$ and use LLL on the lattice

$$\{(p_0 - a_0 q, \ \ldots\ , p_{n-1} - a_{n-1}q, Cq) \ : \ p_0, \ldots, p_{n-1}, q \in \mathbb{Z}.\}$$

One can always get $|p_i - a_i q| \approx \frac{1}{q^{1/(n-1)}}$ but almost never better. So if

$$|p_i - a_i q| <<< \frac{1}{q^{1/(n-1)}} \quad \text{for all } i$$

then we guess

$$P_\lambda = x^n + \frac{p_{n-1}}{q}x^{n-1} + \cdots + \frac{p_0}{q}.$$

Otherwise, double the precision and repeat.

Projective representations: smaller polynomials

Compose $\overline{\rho}_{f,\lambda}$ with $\mathsf{GL}_2(\mathbb{F}_\lambda) \twoheadrightarrow \mathsf{PGL}_2(\mathbb{F}_\lambda)$ to get

$$\tilde{\rho}_{f,\lambda} : \mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathsf{PGL}_2(\mathbb{F}_\lambda)$$

with a field $\tilde{K}_\lambda$:

$$\begin{array}{ccc} \mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \xrightarrow{\quad\tilde{\rho}_{f,\lambda}\quad} & \mathsf{PGL}_2(\mathbb{F}_\lambda) \\ & \searrow\!\!\!\!\searrow \qquad \nearrow & \\ & \mathsf{Gal}(\tilde{K}_\lambda/\mathbb{Q}) & \end{array}$$

We get a splitting polynomial $\tilde{P}_{f,\lambda}$ for $\tilde{K}_\lambda$:

$$\tilde{P}_{f,\lambda} = \prod_{L \in \mathbb{P}(V_\lambda)} \left(x - \sum_{Q \in L - \{0\}} h(Q) \right).$$

The polynomial $\tilde{P}_{f,\lambda}$ is small enough to do computational verifications. We have Galois group computations and Serre's conjecture.

Applications

Conjecture (Lehmer). *The number $\tau(n)$ is never zero.*

Theorem (B.). *Holds for $n < 22798241520242687999$.*

Previously this was known for $n < 22689242781695999$.

The proof uses projective representations: a matrix in $\mathrm{GL}_2(\mathbb{F}_\ell)$ has trace zero iff its action on $\mathbb{P}^1(\mathbb{F}_\ell)$ has a 2-cycle.

Computational inverse Galois theory

The polynomials $\tilde{P}_{f,\lambda}$ will have certain Galois groups. Computing polynomials with prescribed Galois group is a challenge as such (Klüners & Malle).

Polynomials for $\tau(p)$

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

$$\widetilde{P}_{17} =$$
$$x^{18} - 9x^{17} + 51x^{16} - 238x^{15} + 884x^{14} - 2516x^{13} + 5355x^{12} - 7225x^{11} - 1105x^{10} + 37468x^9 - 111469x^8 + 192355x^7 - 211803x^6 + 134793x^5 - 17323x^4 - 50660x^3 + 47583x^2 - 19773x + 3707$$

$$\widetilde{P}_{19} =$$
$$x^{20} - 7x^{19} + 76x^{17} - 38x^{16} - 380x^{15} + 114x^{14} + 1121x^{13} - 798x^{12} - 1425x^{11} + 6517x^{10} + 152x^9 - 19266x^8 - 11096x^7 + 16340x^6 + 37240x^5 + 30020x^4 - 17841x^3 - 47443x^2 - 31323x - 8055$$

A polynomial with Galois group $\mathrm{SL}_2(\mathbb{F}_{16})$

$$x^{17} - 5x^{16} + 12x^{15} - 28x^{14} + 72x^{13} - 132x^{12} + 116x^{11} - 74x^9$$
$$+ 90x^8 - 28x^7 - 12x^6 + 24x^5 - 12x^4 - 4x^3 - 3x - 1$$

A polynomial with Galois group $\mathrm{PSL}_2(\mathbb{F}_{25})$

$$x^{26} - 10x^{25} + 75x^{23} + 1150x^{22} - 1465x^{21} - 10950x^{20}$$
$$- 57925x^{19} + 40300x^{18} - 8525x^{17} + 407000x^{16}$$
$$- 1812800x^{15} + 1894425x^{14} - 2057375x^{13} + 15778750x^{12}$$
$$- 11055625x^{11} - 12123500x^{10} - 13762875x^9 - 16007875x^8$$
$$+ 91035625x^7 - 49044875x^6 + 13600625x^5 - 9798125x^4$$
$$- 21934375x^3 + 13825625x^2 + 2507500x - 2546875$$

A polynomial with Galois group $\mathrm{SL}_2(\mathbb{F}_{32})$

$$
\begin{aligned}
&x^{33} + 13x^{32} + 108x^{31} + 744x^{30} + 4768x^{29} + 27172x^{28} \\
&+ 132412x^{27} + 569936x^{26} + 2254864x^{25} + 8014936x^{24} \\
&+ 24146112x^{23} + 58070720x^{22} + 103024676x^{21} \\
&+ 105307300x^{20} - 50671036x^{19} - 451423176x^{18} \\
&- 931969758x^{17} - 950145182x^{16} + 258579596x^{15} \\
&+ 3324485088x^{14} + 8626891432x^{13} + 15770332836x^{12} \\
&+ 21389501380x^{11} + 14825199448x^{10} - 13660027232x^{9} \\
&- 54239325496x^{8} - 68496746608x^{7} - 35204682152x^{6} \\
&+ 25928111596x^{5} + 49552492980x^{4} + 32492001580x^{3} \\
&- 3814250752x^{2} - 11970016119x - 5786897139
\end{aligned}
$$

A polynomial with Galois group $\mathrm{PSL}_2(\mathbb{F}_{49})$

$$
\begin{aligned}
&x^{50} + 15x^{49} + 98x^{48} + 189x^{47} + 1232x^{46} + 16541x^{45} + 87885x^{44} + 19614x^{43} \\
&+ 1532146x^{42} + 15094730x^{41} + 40321246x^{40} - 31974033x^{39} + 1219687658x^{38} \\
&+ 5123805862x^{37} + 3377791081x^{36} + 3846199665x^{35} + 386041136138x^{34} \\
&+ 152969547283x^{33} - 993121604167x^{32} + 4283901756078x^{31} \\
&+ 29070603927785x^{30} - 150060184671551x^{29} - 35582774083038x^{28} \\
&+ 482188564174744x^{27} - 4599849367725563x^{26} - 2995173366528385x^{25} \\
&+ 7559080337542671x^{24} - 106554688226971957x^{23} - 2492477007160988 4x^{22} \\
&+ 243960897715362468 9x^{21} - 1139482401054234937 0x^{20} \\
&+ 2674840188547587162 2x^{19} + 3622811199622386587 2x^{18} \\
&- 17072450324828156781 6x^{17} + 44095132630018107099x^{16} \\
&+ 220575599569292221559 2x^{15} - 730939533408212365518 4x^{14} \\
&+ 819102422021080734314 4x^{13} + 172205764857967865528 56x^{12} \\
&- 134381254167088687376800x^{11} + 246189220202902763028690x^{10} \\
&+ 2008852910842223066286 26x^{9} - 1770532501735302384701776x^{8} \\
&+ 10046016828906440618776 33x^{7} + 13328116569913120063486965x^{6} \\
&- 32320727666048199017631033x^{5} + 81862443383654393090895 18x^{4} \\
&+ 112612247529381480642588848x^{3} - 239863254860651584214525249x^{2} \\
&+ 217464362272825263861712698x - 963692431975476049811246 95
\end{aligned}
$$