# Serre's Conjecture and Computational Aspects of the Langlands Program

Chandrashekhar Khare

UCLA

VANTAGE Talk 5th April 2022

Bas Edixhoven (1962-2022)

# Bas Edixhoven

I learnt with great sadness of Bas passing on from Ronald van Luijk. I had spoken to Bas a few months ago via Zoom and he seemed his usual self to me. We had spoken after a long time, although he did give a seminar at UCLA via Zoom during the pandemic. His illness and eventual succumbing to it this January, after a very short illness, came as a great shock. He was not yet 60.

I knew of Bas since 1991, when I was a second year graduate student at Caltech. I had gone to an AMS meeting on Serre's conjecture in San Francisco, and Bas spoke there on his very recent proof of the weight part of Serre's conjecture. Bas's work was very prominent at that AMS session which had many of the leaders of the subject speaking in it like Gross, Ribet,... I understood very little of the mathematics, but was dazzled by it and the personalities of the mathematicians present. It left me determined and inspired to understand the subject.

Bas gave a brilliant talk, and this was the first of his talks that I enjoyed over the years. They were always enlightening and taught me something every time. I wrote him around then to send me his thesis on stable reduction of modular curves (and his use of it to prove the then best known results about the Manin constant) and he sent me his beautifully bound and deep work which he never fully published I think.

The depth and sureness of his understanding of arithmetic geometry impressed and thrilled me. He was ever willing to talk about mathematics and other things and give a patient ear to questions others asked. Unlike many researchers he was not just focused on his own work but also wanted to help others to do their best mathematics. The human side of him was something that drew me to him, he had a rare quality of empathy which came through in his conversations. His contribution to the community from his taking care of Compositio Mathematica for a number of years is of course widely known and valued in the mathematical world.

Bas came to visit TIFR, Mumbai for a few weeks around 1996 or so. I worked there at the time and I greatly enjoyed his visit. He gave scintillating lectures (perhaps on the Andre-Oort conjecture and his proof of it for the product of modular curves).

I invited him over for a lunch at my parents' flat in Bombay which was right on the Arabian Sea (on Worli Seaface). I think he enjoyed the visit and the warm, even slightly excessive and grand, hospitality of an Indian home. Meeting my father then seemed to have left an impression on Bas. (My father who led a large accountancy firm in Bombay that he had built up from scratch left an impression on most people he met. ) My father asked Bas about my prospects in mathematics which seemed very uncertain then. Bas liked reminding me of his visit to our flat, and also recounting the story to anyone who knew me when they met him!

I visited Bas in Rennes around 2000 or so (perhaps slightly later) through an Indo-French program (I was still working at TIFR then) and that's where we wrote our one paper together.

It was a short note about finding a cohomological explanation why mod $p$ modular forms in weight 2 also occur in weight $p+1$ (multiplication by the Hasse invariant).

This suggests that for integers $N$ prime to $p$ there is an injective map

$$H^1(\Gamma_0(N), \mathbb{F}_p) \to H^1(\Gamma_0(N), \mathrm{Symm}^{p-1}(\mathbb{F}_p^2))$$

which is puzzling as at the level of the locally constant sheaves/coefficients, $\mathbb{F}_p$ and $\mathrm{Symm}^{p-1}(\mathbb{F}_p^2)$ are distinct irreducible representations of $\mathrm{GL}_2(\mathbb{F}_\mathrm{p})$.

We found that the explanation lies in considering maps induced from $X_0(Np) \to X_0(N)$ by the $p$th degeneracy map $z \to pz$. This gives a map $H^1(\Gamma_0(N), \mathbb{F}_p) \to H^1(\Gamma_0(Np), \mathbb{F}_p)$.

A version of Shapiro's lemma gives that:

$$H^1(\Gamma_0(Np), \mathbb{F}_p) \simeq H^1(\Gamma_0(N), \mathbb{F}_p[\mathbb{P}^1(\mathbb{F}_p)]).$$

One further observes that as $\mathrm{GL}_2(\mathbb{F}_\mathrm{p})$-modules

$$\mathbb{F}_p[\mathbb{P}^1(\mathbb{F}_p)] = \mathbb{F}_p \oplus \mathrm{Symm}^{p-1}(\mathbb{F}_p^2).$$

A version of Ihara's lemma gives that the composition of maps

$$H^1(\Gamma_0(N), \mathbb{F}_p) \to H^1(\Gamma_0(Np), \mathbb{F}_p) \simeq H^1(\Gamma_0(N), \mathbb{F}_p \oplus \mathrm{Symm}^{p-1}(\mathbb{F}_p^2))$$

$$\to H^1(\Gamma_0(N), \mathrm{Symm}^{p-1}(\mathbb{F}_p^2))$$

where the last map is induced by projection, is injective.

Thus we get the desired injective map

$$H^1(\Gamma_0(N), \mathbb{F}_p) \to H^1(\Gamma_0(N), \mathrm{Symm}^{p-1}(\mathbb{F}_p^2))$$

# Computational aspects of the Langlands program

I now want to talk about Bas's book *"Computational aspects of modular forms and Galois representations"* ( how one can compute in polynomial time the value of Ramanujan's $\tau$ at a prime) which was edited by Jean-Marc Couveignes and Bas Edixhoven.

In the introduction he starts with the observation:
*There is a deterministic algorithm, that on input positive integers $N, k \geq 2$, computes $\mathbb{T}(N, k)$: it gives a $\mathbb{Z}$-basis and the multiplication table for this basis, in running time polynomial in $N$ and $k$. Moreover, the Hecke operator $T_n$ can be ex- pressed in this $\mathbb{Z}$-basis in deterministic polynomial time in $N, k, n$.*

Then he describes the main result of the book which improves on the above result (for level $N = 1$).
*Let us now state one of the main results in this book, Theorem 15.2.1: Assume that the generalised Riemann hypothesis (GRH) holds. There exists a deterministic algorithm that on input positive integers n and k, together with the factorisation of n into prime factors, computes the element $T_n$ of $\mathbb{T}(1, k)$ in running time polynomial in k and* $\log n$.

Schoof's algorithm and Galois representations associated to modular forms reduces this to proving the following:

*There is a deterministic algorithm that on input a positive integer $k$, a finite field $\mathbb{F}$, and a surjective ring morphism $f$ from $\mathbb{T}(1,k) \to \mathbb{F}$ such that the associated Galois representation $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ is reducible or has image containing $\mathrm{SL}_2(\mathbb{F})$, computes $\rho_f$ in time polynomial in $k$ and $\#\mathbb{F}$.*

Bas deduces as a consequence:
*For $p$ prime, Ramanujan's $\tau(p)$ can be computed in time polynomial in $\log p$.*

# Bas's hope and philosophy for computational Langlands program

Bas goes on to say:
*More generally, we hope that non-solvable global field extensions whose existence and local properties are implied by the Langlands program can be made accessible to computation and so become even more useful members of the society of mathematical objects. Explicit descriptions of these fields make the study of global properties such as class groups and groups of units possible. Certainly, if we only knew the maximal abelian extension of $\mathbb{Q}$ as described by general class field theory, then roots of unity would be very much welcomed.*

I want to start from scratch and talk about Ramanujan's $\tau$-function, and explain how Serre's modularity conjecture is used to justify a step in the proof of:
*For p prime, Ramanujan's* $\tau(p)$ *can be computed in time polynomial in* $\log p$.
Here one is starting with the Ramanujan $\Delta$ function, which is a modular form, but yet needs Serre's conjecture to verify the algorithm to compute the Fourier coefficients of $\Delta$ (which are the $\tau(p)$).

# Modular forms of level one

We consider the space $M_k = M_k(\mathrm{SL}_2(\mathbb{Z}), \mathbb{C})$ of modular forms of weight $k$ for the group $\mathrm{SL}_2(\mathbb{Z})$, or level one. These are holomorphic functions $f$ defined on the upper half plane $\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$, with the following properties:

- They have a Fourier series expansion $f(z) = \sum_{n \geq 0} a_n q^n$ with $q = e^{2\pi i z}$, and $a_n \in \mathbb{C}$, that is absolutely convergent for $|q| < 1$.
- $f(\frac{-1}{z}) = z^k f(z)$.

We deduce from this that

$$f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$$

for all

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

We consider the subspace $S_k = S_k(\mathrm{SL}_2(\mathbb{Z}), \mathbb{C})$ of $M_k$ cut out by the condition that $a_0 = 0$ ($\lim_{y\to+\infty} f(iy) = 0$).
This is a co-dimension one subspace of $M_k$ whenever $M_k \neq 0$.
We see easily that $M_k = 0$ unless $k \geq 0$ is an even integer.
Further $M_2$ is 0, and $M_k \neq 0$ for even $k \geq 4$.

# Eisenstein series

For any even integer $k \geq 4$ one can write down a modular form of weight $k$:

$$G_k(z) = -B_k/2k + \sum_{n \geq 1} \sigma_{k-1}(n) q^n = \zeta(1-k)/2 + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

Here $B_k$ is the $k$ th Bernoulli number

$$\frac{t}{1-e^t} = \sum_k B_k t^k / k!;$$

and $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$.

We define the normalized Eisenstein series of weight k and level 1,

$$E_k(z) = -\frac{2k}{B_k} G_k(z) = 1 - \frac{2k}{B_k} \sum \sigma_{k-1}(n) q^n.$$

In particular:

- $E_4 = 240 G_4 = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n$
- $E_6 = -504 G_6 = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n$

The series $E_4$ and $E_6$ were denoted by $Q$ and $R$ by Ramanujan. We have that $M_k = \mathbb{C}.E_k \oplus S_k$.

# The algebra of modular forms

We can consider the algebra $\mathcal{M} = \oplus M_k(\mathrm{SL}_2(\mathbb{Z}), \mathbb{C})$ of modular forms of all weights and level 1. This is a graded algebra, and is the polynomial algebra $\mathbb{C}[Q, R]$ where $Q$ and $R$ have weights 4 and 6 respectively. For example

$$E_8 = Q^2$$

$$E_{10} = QR$$

$$E_{12} = \frac{441Q^3 + 250R^2}{691}$$

One may compute the dimensions of $M_k$ as $\mathbb{C}$ vector spaces for instance using the Riemann Roch theorem and the dimension is roughly $k/12$.
$S_k(\mathrm{SL}_2(\mathbb{Z})) = 0$ for $k < 12$ and $S_{12}(\mathrm{SL}_2(\mathbb{Z}))$ is one dimensional, and $= \mathbb{C}.\Delta$ where $\Delta$ is the famous Ramanujan $\Delta$ function.

# $\Delta$-function

The Ramanujan $\Delta$ function is defined by

$$\Delta = \frac{Q^3 - R^2}{1728} = q\Pi_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n$$

with $q = e^{2\pi iz}$.
It is up to scalars the unique cusp form of weight 12 on $\mathrm{SL}_2(\mathbb{Z})$.
The Fourier coefficients $\tau(n)$ are the Ramanujan $\tau$-function.
Ramanujan conjectured

1. $\tau(mn) = \tau(m)\tau(n)$ when $m, n$ are coprime integers.
2. $\tau(p^{n+1}) = \tau(p^n)\tau(p) - p^{11}\tau(p^{n-1})$ for $n \geq 1$
3. $|\tau(p)| \leq 2p^{\frac{11}{2}}$

# Hecke operators

The first two statements were proved by Mordell soon after Ramanujan conjectured them.
He defined operators $T_n$ (later called Hecke operators!) on $M_k(\mathrm{SL}_2(\mathbb{Z}))$ and $S_k(\mathrm{SL}_2(\mathbb{Z}))$ for each $n \geq 1$ that commute with each other and can be diagonalised. They satisfy the multiplicativity properties:

- $T_{mn} = T_m T_n$ for $(m, n) = 1$
- $T_{p^{n+1}} = T_{p^n} T_p - p^{11} T_{p^{n-1}}$ for $n \geq 1$

Further if $f \in S_k$ is an eigenform for all the $T_n$ then $a_1 \neq 0$ and if we normalize it to be 1, then $f|T_n = a_n f$.
The Eisenstein series $G_k$ are (Hecke) eigenforms for $T_n$ with eigenvalues $\sigma_{k-1}(n)$.

The operators $T_\ell$ for $\ell$ primes are defined by

$$f|T_\ell = \sum_n a_{n\ell} q^n + \ell^{k-1} \sum_n a_n q^{\ell n}.$$

As $\Delta$ is the unique cusp form of weight 12, it is an eigenform for the Hecke operators $T_\ell$ for each prime $\ell$, where the action of $T_\ell$ is given by:

$$\Delta(z)|T_\ell = \Sigma\tau(n\ell)q^n + \ell^{11}\Sigma\tau(n)q^{n\ell}.$$

The fact that $\Delta$ is an eigenfunction means that

$$\Delta(z)|T_\ell = \tau(\ell)\Delta(z).$$

Thus we deduce the multiplicativity properties of $\tau(n)$ that were conjectured by Ramanujan as a consequence of the properties of the operators $T_n$.

# $L$-function

Consider the $L$-function

$$L(\Delta, s) = \sum_{n=1}^{\infty} \frac{\tau(n)}{n^s}$$

attached to the $\Delta$-function. The multiplicativity properties of $\tau(n)$ are equivalent to the Euler product expansion

$$L(\Delta, s) = \Pi_p \frac{1}{1 - \tau(p)p^{-s} + p^{11-2s}}.$$

Hecke proved that the completed $L$-function $\Lambda(\Delta, s) = (2\pi)^{-s}\Gamma(s)L(\Delta, s)$ has the functional equation $\Lambda(12 - s) = \Lambda(s)$ as a consequence of $\Delta(\frac{-1}{z}) = z^{12}\Delta(z)$.

The third property conjectured by Ramanujan turned out to be much deeper and was proved by Deligne only in the early 1970's.

Note that the "almost as good" bound $\tau(p) = O(p^6)$ is easy (deduced from the maximum modulus principle). Hardy was slightly skeptical about the importance of the sharpening that Ramanujan conjectured.

"We seem to have drifted into one of the backwaters of mathematics."

Hardy qualified this by saying that the problem "might have some features which made it not unworthy of Ramanujan's attention".

The conjecture, and its natural generalizations, has turned into one of the central problems in the theory of authomorphic forms.

# Congruences for the $\tau$-function

Ramanujan also discovered a remarkable congruence for $\tau(n)$:

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691}.$$

Here it is relevant to note that 691 divides the numerator of $B_{12}$ which is the numerator of the constant term of $G_{12}$.

There were other similar congruences for $\ell = 2, 3, 5, 7, 23, 691$. We call these the *exceptional primes* (for the Ramanujan $\Delta$-function).
The congruence for $\ell = 23$ is a little different from that for the other exceptional primes. For $p \neq 23$:

- $\tau(p) = 0 \pmod{23}$ if $(\frac{p}{23}) = -1$
- $\tau(p) = 2 \pmod{23}$ if $p = u^2 + 23v^2$
- $\tau(p) = -1 \pmod{23}$ otherwise.

The explanation for these congruences, given by Swinnerton-Dyer and Serre, and the Ramanujan bound, proved by Deligne, lay in the *Galois representations* attached to $\Delta$.

# Galois representations

Let $G_{\mathbb{Q}}$ be the absolute Galois group of $\mathbb{Q}$.
For each prime $\ell$, Deligne constructed a Galois representation

$$\rho_{\Delta,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_\ell),$$

that is irreducible for all $\ell$, and unramified outside $\ell$. Deligne proved the existence of these representations shortly after they were conjectured to exist by Serre in his article in Séminaire Delange-Pisot-Poitou of 1967-68.
The representation is characterised for by the property that the characteristic polynomial of $\rho_{\Delta,\ell}(\mathrm{Frob}_p)$ for all primes $p \neq \ell$ is $X^2 - \tau(p)X + p^{11}$.

# Work of Eichler and Shimura

Such representations attached to new forms of weight $k \geq 2$ and level $N$ had been constructed by Eichler and Shimura in the 1950's using the $\ell$-adic Tate module of Jacobians $J_1(N)$ of modular curves $X_1(N)_{/\mathbb{Q}}$. This is also the dual of the étale cohomology group $H^1_{et}(X_1(N), \mathbb{Z}_\ell)$.

# Ramanujan's conjectured bound on $\tau(p)$

The sequence of numbers $\{\tau(p)\}$ now acquire a meaning as traces of the representation $\rho_{\Delta,\ell}$.
Even for $\ell = p$ one can interprete $\tau(p)$ as the trace of the crystalline Frobenius acting on $D_{cris}(\rho_{\Delta,p}|_{G_p})$ with $G_p$ a decomposition group at p in $G_{\mathbb{Q}}$.
Deligne realized the representations $\rho_{\Delta,\ell}$ inside the $\ell$-adic étale cohomology

$$H^1_{et}(\mathbb{P}^1(j), \mathrm{Symm}^{10}(\mathbb{Z}^2_\ell)),$$

interpreted $\tau(p)$ as the trace of Frobenius at $p$ acting on this cohomology group, and deduced the Ramanujan bound

$$|\tau(p)| \leq 2p^{\frac{11}{2}}$$

as a consequence of his proof of the Weil conjectures.

Serre in his article in DPP had shown how the existence of $\rho_{\Delta,\ell}$ could help in understanding the congruences for $\tau(n)$. Swinnerton-Dyer showed that the image of $\rho_{\Delta,2}$ is a subgroup of $\mathrm{GL}_2(\mathbb{Z}_2)$ of index $3.2^{25}$ which explained the congruence of Lehmer:

$$\tau(p) \equiv 1 + p^{11} + 8(41 + x)(p - x)^{2+x}$$

modulo $2^{11}$ with $x = (-1)^{\frac{p-1}{2}}$.

# Congruence mod 691

The congruence mod 691 is equivalent to the fact that $\bar{\rho}_{\Delta,691} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_{691})$ is of the form

$$\begin{pmatrix} 1 & * \\ 0 & \chi_{691}^{11} \end{pmatrix}.$$

# Congruence mod 23

The congruence in the case of $\ell = 23$ is accounted for by the fact that $\bar{\rho}_{\Delta,23}$ is an induced representation $\mathrm{Ind}_{\mathbb{Q}(\sqrt{-23})}^{\mathbb{Q}}(\psi)$ where $\psi$ is one of the two (conjugate) characters of $G_{\mathbb{Q}(\sqrt{-23})}$ of order 3 into $\mathbb{F}_{529}^*$.

# Images of $\rho_{\Delta,\ell}$

Swinnerton-Dyer and Serre proved in that the representation $\rho_{\Delta,\ell}$ has large image, i.e., $\rho_{\Delta,\ell}(G_{\mathbb{Q}})$ contains $\mathrm{SL}_2(\mathbb{Z}_\ell)$ for $\ell$ different from $2, 3, 5, 7, 23, 691$, and has open image in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ for all $\ell$.
The key step was to prove that the mod $\ell$ image contains $\mathrm{SL}_2(\mathbb{F}_\ell)$ for these primes. Then one can use:

**Lemma**

*For $\ell > 3$, a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ that contains $\mathrm{SL}_2(\mathbb{F}_\ell)$ in its reduction mod $\ell$, contains $\mathrm{SL}_2(\mathbb{Z}_\ell)$.*

# Mod $\ell$ modular forms and Ramanujan's $\Theta$-operator

In proving their results about the mod $\ell$ images of the Galois representations attached to the $\Delta$-function, the main tool Serre and Swinnerton-Dyer used was the study of congruences between modular forms which has been an intense focus of research ever since.

We consider the set of ($\ell$-integral) modular forms of weight $k$ and level one whose Fourier coefficients are $\ell$-integral and denote the reduction by $\bar{M}_k$. We consider the sub algebra $\bar{M}$ of $\mathbb{F}_\ell[[q]]$ which is the span of $\bar{M}_k$ for all $k$. This is the space of modular forms mod $\ell$ (of level one). We have an inclusion $\bar{M}_K \to \bar{M}_{k+\ell-1}$ given by multiplication by the Hasse invariant. One of the basic results is that $\bar{M} = \mathbb{F}_\ell[\bar{Q}, \bar{R}]/(A-1)$ where $A(\bar{Q}, \bar{R}) = \bar{E}_{p-1}$, the Hasse invariant.

This space has a $\mathbb{Z}/(\ell-1)\mathbb{Z}$-grading $\bar{M} = \oplus_{i \in \mathbb{Z}/(p-1)\mathbb{Z}} \bar{M}^i$.

There is a weight filtration $w(f)$ for $f \in \bar{M}$, defined as the least weight $k$ for which $f \in \bar{M}_k$ if $\neq 0$ and $w(0) = -\infty$.

One of the key operators on the space $\bar{M}$ is the Ramanujan theta operator $\Theta$ which on $q$ expansions is given by $q\frac{d}{dq}$. One of the key results in the analysis of Serre and Swinnerton-Dyer is that $w(\Theta(f)) \leq w(f) + \ell + 1$ with inequality if and only if $\ell | w(f)$ in which case $w(\Theta(f)) = w(f) + 2$. There is a cohomological interpretaion of the corresponding map

$$\Theta : H^1(\Gamma_0(N), \mathrm{Symm}^k(\mathbb{F}_\ell{}^2)) \to H^1(\Gamma_0(N), \mathrm{Symm}^{k+\ell-1}(\mathbb{F}_\ell^2)),$$

namely its given by multiplication by $X^\ell Y - XY^\ell$.

# Example of a congruence

Consider the following formal manipulation:

$$\Delta(z) = q\Pi(1-q^n)^{24} = q\Pi(1-q^n)^2\Pi(1-q^n)^{22}$$

$$\equiv q\Pi(1-q^n)^2\Pi(1-q^{11n})^2 \pmod{11}$$

and the latter is the $q$-expansion of the unique cusp form in $S_2(\Gamma_0(11))$. This is the $\ell = 11$ case of Serre's Hecke-equivariant isomorphism

$$S_{\ell+1}(\mathrm{SL}_2(\mathbb{Z}), \mathbb{F}_\ell) \simeq \mathrm{S}_2(\Gamma_0(\ell), \mathbb{F}_\ell).$$

# Image of $\bar{\rho}_{\Delta,\ell}$

The results Swinnerton-Dyer and Serre proved were:

- $\rho_{\Delta,\ell}$ is absolutely irreducible and odd, i.e. complex conjugation is not mapped to a scalar.
- For $\ell \neq 2, 3, 5, 7, 691$, the reduction $\bar{\rho}_{\Delta,\ell}$ is absolutely irreducible (which by a theorem of Carayol and Serre we now know means that $\rho_{\Delta,\ell}$ has an unique integral model up to isomorphism).
- For $\ell = 23$, $\bar{\rho}_{\Delta,23}$ factors through the Hilbert class field of $\mathbb{Q}(\sqrt{-23})$ (which is the splitting field of the polynomial $X^3 - X - 1$), and has image isomorphic to $S_3$.
- The determinant of $\rho_{\Delta,\ell}$ is $\chi_\ell^{11}$ where $\chi_\ell$ is the $\ell$-adic cyclotomic character.
- For $\ell \neq 2, 3, 5, 7, 23, 691$, the image of $\bar{\rho}_{\Delta,\ell}$ contains $\mathrm{SL}_2(\mathbb{F}_\ell)$.

This then implies the following theorem which essentially proves that the congruences that had been found for the Ramanujan $\tau$ function mod $2, 3, 5, 7, 23, 691$ were the only ones.

**Theorem**

*Given positive integers $m, n$ and integers $a, b$, such that $(b, n) = 1$, and with $m$ not divisible by any of the exceptional primes, there is set of primes $\{p\}$ of positive density such that $\tau(p)$ is $a$ mod $m$ and $p$ is $b$ mod $n$.*

Thus a congruence on $p$ (an abelian condition by the Kronecker-Weber theorem) does not determine any congruence on $\tau(p)$ outside moduli that are not coprime to the exceptional primes.

If we denote by $K_{\Delta,\ell}$ the extension of $\mathbb{Q}$ through which $\bar{\rho}_{\Delta,\ell}$ factors then:

1. $K_{\Delta,\ell}$ is unramified outside $\ell, \infty$.
2. We have an embedding

$$\iota_\ell : G_{\Delta,\ell}(= \mathrm{Gal}(K_{\Delta,\ell}/\mathbb{Q})) \hookrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$$

   that (for $\ell \neq 2, 3, 5, 7, 691$) gives an irreducible action of $G_{\Delta,\ell}$ on $\mathbb{F}_\ell^2$.
3. If further $\ell \neq 23$, then the image of $G_{\Delta,\ell}$ contains $\mathrm{SL}_2(\mathbb{F}_\ell)$.
4. The determinant of the matrix $\iota_\ell(c)$ is $-1$.
5. The semisimplification of the image of the inertia group at $\ell$, $I_\ell$, under $\iota_\ell$, is either:
   (i) $1 \oplus \bar{\chi}_\ell^{11}$ with $\bar{\chi}_\ell$ the reduction of the cyclotomic character $\chi_\ell$, or
   (ii) $\psi_\ell \oplus \psi_\ell^{11}$ where $\psi_\ell$ is a fundamental character of level 2 of $I_\ell$.

# Lehmer's Conjecture

(i) is equivalent, by results of Deligne and Fontaine, to asking that $\ell$ does not divide $\tau(\ell)$. This is a generic condition and holds true for all primes $\ell < 7,000,000$ and $\ell \neq 2, 3, 5, 7, 2411$ .
The only solutions up to $10^{10}$ to the equation $\tau(\ell) = 0 \pmod{\ell}$ are $\ell = 2, 3, 5, 7, 2411$, and $7,758,337,633$.
Lehmer has conjectured that $\tau(\ell) \neq 0$ for all $\ell$. One knows this is true outside a density 0 set of primes. The congruences satisfied by $\tau(\ell)$ show that the smallest value of $\ell$ for which Lehmer's conjecture might fail is large.

# Serre's modularity conjecture

A rough version of Serre's conjecture would ask that any $K/\mathbb{Q}$ that verifies (1), (2), (4) and (5) arises from the Ramanujan $\Delta$-function, i.e., $K = K_{\Delta,\ell}$. This was proved in joint work with Jean-Pierre Wintenberger (thus in particular no such $K$ exists for $\ell = 2, 3, 5, 7, 691$) and was the initial breakthrough in our work on the conjecture.

If we drop (5), then the conjecture says that $K$ arises from a suitable newform of level 1 and of a weight which depends on $\iota_\ell(I_\ell)$.

When we drop (1) then the conjecture predicts that $K$ arises from a newform of level $N$ and weight $k$, with the numerical invariants defined by Serre using the ramification data of $K$.

# Numerical example

For $\ell = 11$, if we have an irreducible odd representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_{11})$ unramified outside 11 and satisfying the conditions on inertia at 11 as above, then Serre's conjecture, and the congruence recalled above, predicts that $\rho$ arises from the 11-torsion of the elliptic curve over $\mathbb{Q}$ of smallest conductor, namely 11. This is the curve given by the equation

$$y^2 + y = x^3 - x^2 - 10x - 20.$$

The Ramanujan $\Delta$-function is significant in another way: it gives rise to the smallest rank 2 motive $M_\Delta$ over $\mathbb{Q}$ with good reduction everywhere. Here size is measured by the Hodge type which for $M_\Delta$ is $(11, 0)$ and $(0, 11)$.

# Bosman's computation of $\Delta$ mod $\ell$

The explicit computation of the $K_{\Delta,\ell}$'s, or the subfield which corresponds to the fixed fixed of the center of the Galois group, for small primes $\ell$ in the book is done in Chapter 7: *Polynomials for projective representations of level one forms* written by J. Bosman. It is a step in computing explicitly the mod $\ell$ Galois representations arising from $\Delta$. There we find the following result.

**Corollary 3.** Let $\tilde{\rho} : G_{\mathbb{Q}} \to PGL_2(\mathbb{F})$ be an irreducible projective representation and let $\rho$ be a lifting of $\tilde{\rho}$ of minimal Serre weight $k(\rho)$. Let $K$ be the number field belonging to a point of $\mathbb{P}^1(\mathbb{F})$. If $k \geq 3$ is such that $v_\ell(\mathrm{Disc}(K/\mathbb{Q})) = k + \ell - 2$ holds, then we have $k(\rho) = k$.

Bosman relying on earlier work in the book and using the fact that $\Delta$ mod $\ell$ also arises from the mod $\ell$ space of modular forms $S_2(\Gamma_0(\ell), \omega_\ell^{10})$ writes down *candidate* polynomials $P_{12,\ell}$ (for $\ell = 11, 13, 17, 19$) of degree $\ell + 1$ whose splitting field $K_\ell/\mathbb{Q}$ he can verify has:

- (i) Galois group $PGL_2(\mathbb{F}_\ell)$;
- (ii) $K_\ell$ is unramified outside $\ell$ and is not totally real;
- (iii) the subfield $K$ of $K_\ell$, of a Borel subgroup of $PGL_2(\mathbb{F}_\ell)$ which corresponds to a point of $\mathbb{P}^1(\mathbb{F}_\ell)$, satisfies $v_\ell(\mathrm{Disc}(K/\mathbb{Q})) = \ell + 10$.

Essentially one can verify only ramification properties of $K_\ell$ and Bosman uses that to tie the field to $\Delta$ mod $\ell$ as follows.
From the above he checks that $K_\ell$ arises from a Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ with Serre invariants $k(\rho) = 12, N(\rho) = 1$. Serre's conjecture implies that $\rho$ arises from $S_{12}(\mathrm{SL}_2(\mathbb{Z}), \mathbb{C})$ which is spanned by $\Delta$. Thus the fixed field of $K_{\Delta,\ell}$ under the center is $K_\ell$!

# Counting mod $\ell$ Galois representations

The number of semisimple mod $\ell$ Galois representations $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_\ell})$ arising from modular forms of level one is finite. Serre in his DPP article shows this by observing that any such representation arises from

$$W_k = M_{k+\ell-1}(\mathrm{SL}_2(\mathbb{Z}), \mathbb{F}_\ell)/\mathrm{M_k}(\mathrm{SL}_2(\mathbb{Z}), \mathbb{F}_\ell)$$

for some integer $k \geq 2$. The dimensions of $W_k$ are bounded and roughly of size $\ell/12$. Thus the fields of definition of such Galois representations are of bounded degree over $\mathbb{F}_\ell$. Then the Hermite-Minkowski theorem implies that there are only finitely many such Galois representations.

# Finiteness of Galois representations

This combined with Serre's conjecture yields the following corollary.

**Corollary.** There are finitely many semisimple Galois representations $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_\ell})$ that are unramified outside $\ell$ and odd.

# Mass formula for mod $\ell$ Galois representations

How many such Galois representations are there?
The reducible ones are easy to count: they are of the form $\chi_\ell^i \oplus \chi_\ell^j$ with $0 \leq i, j \leq \ell - 2$, and $i + j$ odd.
For $\ell \leq 7$, there are no such irreducible representations.
For $\ell = 11$, there are exactly 10 such representations.
In general I conjecture that there are roughly $\ell^3/48$ such representations.

# Heuristic

This number is arrived at by computing

$$(\ell - 1)\Sigma_{2 \leq k \leq \ell+1} \dim S_k(\mathrm{SL}_2(\mathbb{Z}), \mathbb{F}).$$

Recall that up to twisting by powers of the mod $\ell$ cyclotomic character $\chi_\ell$ (or up to applying powers of the Ramanujan operator $\Theta$), any Galois representation as above (or any level 1 mod $\ell$ Hecke eigensystem) arises from $\ell$-restricted weights between 2 and $\ell + 1$. This shows that the conjectured number gives an upper bound. The best lower bound is $\ell^2/8$.

The conjecture is premised on:

- (i) there are few congruences mod $\ell$ between modular forms of level 1 and equal weights in the "$\ell$-restricted" range of weights ;
- (ii) Most of the mod $\ell$ Galois representations $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ arising from modular forms $f$ of level 1 and $\ell$-restricted weights are wildly ramified at $\ell$. Namely most such $f$ do not have a "companion form".

There are interesting computations and theoretical results proved about this by Tommaso Centeleghe.

# End

Thank you for your attention!