My talk at the NT-lunch seminar

"A different look at $\tau(p) \equiv p^{11}+1$ (691)"

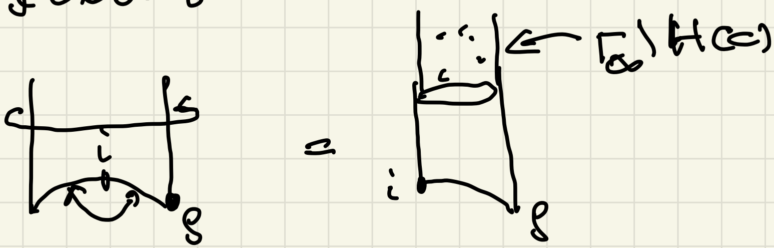
In the following

$$\Gamma = Sl_2(\mathbb{Z})$$

this group acts on the upper half plane

$$\mathbb{H} = \{ z \mid \operatorname{Im}(z) > 0 \}$$

The quotient $\Gamma \backslash \mathbb{H}$ looks as follows



The quotient is not compact we define neighbourhoods of infinity:

$\partial(\Gamma\backslash\mathbb{H}) = \Gamma_\infty \backslash \mathbb{H}(c)$

where $\mathbb{H}(c) = \{ z \in \mathbb{H} \mid \operatorname{Im}(z) \geq c \}$

and

$$\Gamma_\infty = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \,\middle|\, n \in \mathbb{Z} \right\} \subset \Gamma$$

We have the elements of finite order

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$$

the fix the points i and $\rho = \frac{1+\sqrt{-3}}{2}$.

We introduce the Γ-module

$$\mathcal{M}_n = \left\{ \sum a_\nu X^\nu Y^{n-\nu} \,\middle|\, a_\nu \in \mathbb{Z} \right\}$$

for $P(X,Y) \in \mathcal{M}_n$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$

$$(\gamma P)(X,Y) = P(aX+cY, bX+dY)$$

We define the sheaves $\tilde{\mathcal{M}}_n$: If

$\pi : \mathbb{H} \longrightarrow \Gamma\backslash\mathbb{H}$ is the projection and $V \subset \Gamma \backslash \mathbb{H}$ is open then

$$\tilde{\mathcal{M}}_n(V) = \{ f : \pi^{-1}(V) \to \mathcal{M}_n \mid f \text{ locally con} \quad t \text{ and } f(\gamma v) = \gamma f(v) \}.$$

we are interested in the sheaf cohomology $H^1(\Gamma \backslash \mathbb{H}, \tilde{\mathcal{M}}_n)$.

These cohomology group are finitely generated $\mathbb{Z}$-modules and in this case

$$H^1(\Gamma \backslash \mathbb{H}, \tilde{\mathcal{M}}_n) = \frac{\mathcal{M}_n}{\mathcal{M}_n^{\langle S \rangle} + \mathcal{M}_n^{\langle R \rangle}}$$

$$\left(\mathcal{M}_n^{\langle S \rangle} = \{ f \in \mathcal{M}_n \mid Sf = f \}, \mathcal{M}_n^{\langle R \rangle} = \cdots \right)$$

There is some more structure on the cohomology groups

1) We have the fundamental exact sequence

$$\begin{tikzcd}
\arrow[r] & H^1_c(\Gamma\backslash\mathbb{H},\tilde{\mathcal{M}}_n) \arrow[rr] \arrow[dr, "\text{surj}"] & & H^1(\Gamma\backslash\mathbb{H},\tilde{\mathcal{M}}_n) \arrow[r] & H^1(\partial(\Gamma\backslash\mathbb{H}),\tilde{\mathcal{M}}_n) \arrow[r] & {} \\
& & H^1_!(\Gamma\backslash\mathbb{H},\tilde{\mathcal{M}}_n) \arrow[ur, "\text{inj}"] \arrow[dr] & & & \\
& 0 \arrow[ur] & & 0 & &
\end{tikzcd}$$

cohom with compact supports

Inner cohomology

2) We have an action of the Hecke algebra on this diagram

$$\mathcal{H} = \mathbb{Z}[T_2, T_3, T_5, \ldots, T_p, \ldots]$$

i.e for each prime p we have an endomorphism T_p on the diagram and the T_p commute

(*) For any finitely generated $\mathbb{Z}$-module X we introduce the notation $X_{int} := X/\mathrm{Torsion}$

this module X_{int} is also the image of X in $X \otimes \mathbb{Q}$ (*)

3) From our fundamental exact sequence we get

$$
\begin{array}{c}
0 \to H^1_!(\Gamma\backslash\mathbb{H}, \tilde{\mathcal{M}}_n)_{int} \to H^1(\Gamma\backslash\mathbb{H}, \tilde{\mathcal{M}}_n)_{int} \xrightarrow{\ r\ } H^1(\partial\overline{\Gamma\backslash\mathbb{H}}, \tilde{\mathcal{M}}_n)_{int} \to 0 \\
\hspace{22em} \| \\
\hspace{22em} \mathbb{Z}\,\omega_n
\end{array}
$$

this is a short exact sequence of free $\mathbb{Z}$-modules with an action of $\mathcal{H}$.

4) For all p the generator ω_n is an eigenvector, i.e.

$$T_p\,\omega_n = (p^{n+1}+1)\,\omega_n$$

5) The "complex conjugation"

$$c : z \longrightarrow -\bar{z}$$

induces an involution on the

cohomology (commuting with $\mathcal{H}$)

We have $c\omega_n = -\omega_n$ and

$$H^1_!(\Gamma\backslash\mathbb{H}, \tilde{\mathcal{M}}_n \otimes \mathbb{Q}) = H^1_{!,+} \oplus H^1_{!,-}$$

where the two summands are isomorphic Hecke modules.

Now we can write a computer program, which does the following:

It produces a basis (set of free generators)

$$f_n, \underbrace{f_{n-1}, \dots, f_k}_{\text{basis of } H^1_!} \qquad \omega_n$$

and for any p it produces the matrix with respect to this basis

$$T_p = \begin{pmatrix} p^{n+1}+1 & 0 & t_{n-2}^{(p)} & 0 & \cdots \\ 0 & x & x & & \cdots x \\ \vdots & & & & \\ \vdots & & & & \\ 0 & x & \cdots & \cdots & x \end{pmatrix}$$

Now I come back to the title of the talk. I consider the case $n = 10$. The the computer program spits out the matrix for T_2,

$$T_2 = \begin{pmatrix} 2049 & 0 & -68040 \\ 0 & -24 & 0 \\ 0 & 0 & -24 \end{pmatrix}$$

we see that f_{10} is not an eigenvector. We try to modify it and look for an x s.t.

$\tilde{f}_{10} = f_{10} + x f_8$

is an eigenvector. This means

we want

$$T_2(f_{10} + x f_8) = (2^{11}+1)(f_{10} + x f_8)$$

and this says we have to solve

$$2073 \cdot x = -68040$$

i.e

$$691 \cdot x = -22680$$

We see: We can decompose

$$H^1(\Gamma\backslash\mathbb{H}, \tilde{\mathcal{M}}_{10} \otimes \mathbb{Q}) = H^1_!(\Gamma\backslash\mathbb{H}, \tilde{\mathcal{M}}_{10} \otimes \mathbb{Q}) \oplus \mathbb{Q}\tilde{f}_{10}$$

where $\tilde{f}_{10}$ maps to ω_{10} and

$$T_2 \tilde{f}_{10} = (2^{11}+1)\tilde{f}_{10}$$

The element $\tilde{f}_{10}$ is uniquely defined by these conditions.

We say $\tilde{f}_{10}$ is the Eisenstein class

But we see the Eisenstein class has the denominator 691

this means that

$$f^{+}_{,10} = 691 \cdot \tilde{f}_{10} \in H^1(\Gamma\backslash\mathbb{H}, \tilde{\mathcal{M}}_{10})_{int}$$

is a primitive element.

We consider the matrix for T_p

$$T_p = \begin{pmatrix} p^{11}+1 & 0 & t^{(p)} \\ 0 & \tau(p) & 0 \\ 0 & 0 & \tau(p) \end{pmatrix}$$

the above computation yields that the equation

$$(p^{11}+1-\tau(p))\, x = t^{(p)}$$

can not be solved with $x \in \mathbb{Z}$, there must be a 691 in the denominator of x. Hence we conclude

For all prime p we have the congruence

$$\tau(p) \equiv p^{11} + 1 \mod 691$$

Of course at this point we do not know that the number $\tau(p)$ is Ramanujan's $\tau(p)$ which is defined by

$$\Delta(q) = q \cdot \prod_{n=1}^{\infty} (1-q^n)^{24} = \sum \tau(n) q^n$$

For this we need the Eichler-Shimura isomorphism.

Main message: Knowing the denominator is better than only knowing the resulting congruences.

We know from Serre and Deligne

that there is a representation of the Galois group (Now $\ell = 691$!)

$$\rho_{10} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}(H^1(\Gamma\backslash\mathbb{H}, \tilde{\mathcal{M}}_{10} \otimes \mathbb{Z}_\ell))$$

which has the following properties

i) The representation is unramified outside ℓ.

We have the cyclotomic character $\alpha_\ell : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^\infty})/\mathbb{Q}) = \mathbb{Z}_\ell^\times$

which is defined by

$$\sigma(\zeta) = \zeta^{\alpha_\ell(\sigma)}$$

for any ℓ^m-th root of unity

Then

(ii) $\rho_{10}(\sigma)\,\omega_n = \alpha_\ell(\sigma)^{11}\,\omega_n$

on $H^1(\partial(\Gamma\backslash\mathbb{H}), \tilde{\mathcal{M}}_{10} \otimes \mathbb{Z}_\ell)$

Let $\rho_{10}^!(\sigma)$ be the restriction of ρ_{10} to $H^1_!(\Gamma\backslash\mathbb{H}, \tilde{\mathcal{M}}_{10}\otimes\mathbb{Z}_\ell)$

then we have for any $p \neq \ell$

and the resulting Frobenius

$\Phi_p \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})/\sim$ that

$$\mathrm{tr}(\rho^!_{10}(\Phi_p)) = \tau(p)$$
$$\det(\rho^!_{10}(\Phi_p)) = p^{11}$$

(iii) In $\mathrm{End}(H^1(\Gamma\backslash\mathbb{H}, \tilde{\mathcal{M}}_{10}\otimes\mathbb{Z}_\ell))$

we have the famous

Eichler-Shimura congruence

relation

$$\rho_{10}(\Phi_p^2) - T_p\cdot\rho_{10}(\Phi_p) + p^{11}\cdot\mathrm{Id} = 0$$

We consider the reduction of

our representation mod ℓ. Let

$\alpha_{\ell,1} : \mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/\ell)^\times = \mathbb{F}_\ell^\times$

be the reduction of α_ℓ mod ℓ.

The reduction mod ℓ of our fundamental exact sequence is the exact sequence

$$0 \to H^1_!(\Gamma\backslash\mathbb{H}, \tilde{\mathcal{M}}_{10}\otimes\mathbb{F}_\ell) \to H^1(\Gamma\backslash\mathbb{H}, \tilde{\mathcal{M}}_{10}\otimes\mathbb{F}_\ell) \to H^1(\partial(\Gamma\backslash\mathbb{H}), \tilde{\mathcal{M}}_{10}\otimes\mathbb{F}_\ell) = \mathbb{F}_\ell(-11) \to 0$$

here $\mathbb{F}_\ell(-11)$ is the one dimensional $\mathbb{F}_\ell$ vector space on which $\mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q})$ acts by the character α_ℓ^{11}.

Now there is a simple argument using the denominator that the is a Galois module embedding

$$\mathbb{F}_\ell(-11) \hookrightarrow H^1_!(\Gamma\backslash\mathbb{H}, \tilde{\mathcal{M}}_{10}\otimes\mathbb{F}_\ell)$$

and this says that the reduction mod ℓ of our Galois module is of the form

$$\rho_{\ell,0} \bmod \ell : \sigma \longrightarrow \begin{pmatrix} \alpha_{\ell,1}^{11}(\sigma) & u_{12}(\sigma) & u_{13}(\sigma) \\ 0 & 1 & u_{23}(\sigma) \\ 0 & 0 & \alpha_{\ell,1}^{11}(\sigma) \end{pmatrix}$$

hence we see that the denominator forces the image of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ into the subgroup $B^{(1)}(\mathbb{F}_p)$ where

$$B^{(1)} = \left\{ \begin{pmatrix} t & u & v \\ & 1 & w \\ & & t \end{pmatrix} \right\}$$

<u>Thm.</u> The image of the Galois group is equal to $B^{(1)}(\mathbb{F}_p)$, so it is as large as possible under the present circumstances.

The proof uses the Eichler-Shimura congruences. It plays a role that we can find a prime

$p \equiv 1 \bmod \ell$ and $p^{11}+1-\tau(p) \not\equiv 0 \bmod \ell^2$

This gives us field extensions

$$\begin{tikzcd}[column sep=small, row sep=small] & & K_1 \arrow[dr, phantom, "\subseteq"] & \\ \mathbb{Q} \subset \mathbb{Q}(\zeta_\ell) \arrow[urr, phantom, "\subset"] \arrow[drr, phantom, "\subset"] & & & K \\ & & K_2 \arrow[ur, phantom, "\subseteq"] & \end{tikzcd}$$

where $[K:\mathbb{Q}] = (\ell-1)\cdot \ell^3$.

We have the following "Zerlegungsgesetz"

A prime p splits completely in K_1 or in K_2 if and only if

$p \equiv 1 \bmod \ell$ and

$$\tau(p) \equiv p^{11}+1 \bmod \ell^2$$

I do not see how such a result can be obtained if one only looks at the congruences

For more details and a more extensive discussion I refer to my unfinished book on cohomology of arithmetic groups
https://www.math.uni-bonn/de/people/harder

In the folder Manuscripts/buch you find volume-III.pdf the newest version.

I want to add some remarks which concern the experimental aspects.

I our example we see that the Hecke operator T_2 suffices to verify that the Eisenstein class has denominator 691.

This will very often happen in other situations:

One Hecke operator is enough to compute the denominator.

But then the congruences follow for all eigenvalues of Hecke operators T_p.

On the other hand there are many instances where people have verified the congruences for a certain small number of primes (or for all primes) but where the denominator is not verified.

It seems to be easier to prove the congruences than to compute the denominator.

On the other hand the denominator can be computed in any given case (in principle).

For several years I have bothered people – those people who love to do computations – to write a program that works for cases which go beyond the case above. For instance the case treated in 1-2-3 would be nice.