,

ON MOD p MODULAR FORMS OF WEIGHT ONE

CNTA/ACTN VII, MONTREAL, MAY 25 MAI, 2002

Bas Edixhoven
Université de Rennes 1

Universiteit Leiden (from september 1)

`http://www.maths.univ-rennes1.fr`

`edix@univ-rennes1.fr`

TSVP

Aim of the talk:

to convince you that mod p modular forms (and especially weight one forms modulo 2) deserve to be studied, and that they are not scary.

Aim of the talk:

to convince you that mod p modular forms (and especially weight one forms modulo 2) deserve to be studied, and that they are not scary.

Importance: representations $G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$

Aim of the talk:

to convince you that mod p modular forms (and especially weight one forms modulo 2) deserve to be studied, and that they are not scary.

Importance: representations $G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$

Why not scary: one can compute with them quite easily, without doing algebraic geometry but just group cohomology (even for weight one).

TSVP

SERRE'S CONJECTURE (1987):

Let p be prime, $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ continuous, irreducible and odd.

Then ρ comes from a mod p modular form of type $(N(\rho), k(\rho), \varepsilon(\rho))$.

SERRE'S CONJECTURE (1987):

Let p be prime, $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ continuous, irreducible and odd.

Then ρ comes from a mod p modular form of type $(N(\rho), k(\rho), \varepsilon(\rho))$.

$N(\rho)$ (the level) is the Artin conductor away from p.

$k(\rho)$ (the weight) is given by a complicated recipe in terms of $\rho|I_p$.

$\varepsilon(\rho)\colon (\mathbb{Z}/N(\rho)\mathbb{Z})^* \to \overline{\mathbb{F}}_p^*$ given by:

$$\det \circ \rho = \varepsilon(\rho)\chi^{k(\rho)-1}.$$

$N(\rho)$ and $k(\rho)$ are meant to be minimal.

TSVP

WHAT ARE MOD p MODULAR FORMS?

For $N \geq 5$, p not dividing N, and k integer one defines, *à la Katz*:

$$S(N,k)_{\mathbb{F}_p} = \mathrm{H}^0(X_1(N)_{\mathbb{F}_p}, \underline{\omega}^{\otimes k}(-\mathrm{cusps})).$$

WHAT ARE MOD p MODULAR FORMS?

For $N \geq 5$, p not dividing N, and k integer one defines, *à la Katz*:

$$S(N,k)_{\mathbb{F}_p} = \mathrm{H}^0(X_1(N)_{\mathbb{F}_p}, \underline{\omega}^{\otimes k}(-\mathrm{cusps})).$$

$S(N,k)_{\mathbb{F}_p}$ is a finite dimensional $\mathbb{F}_p$-vector space, equipped with Hecke operators T_n ($n \geq 1$) and diamond operators $\langle a \rangle$ (a in $(\mathbb{Z}/N\mathbb{Z})^*$).

q-expansions: $S(N,k)_{\mathbb{F}_p} \hookrightarrow \mathbb{F}_p[[q]]$.

WHAT ARE MOD p MODULAR FORMS?

For $N \geq 5$, p not dividing N, and k integer one defines, *à la Katz*:

$$S(N,k)_{\mathbb{F}_p} = \mathrm{H}^0(X_1(N)_{\mathbb{F}_p}, \underline{\omega}^{\otimes k}(-\mathrm{cusps})).$$

$S(N,k)_{\mathbb{F}_p}$ is a finite dimensional $\mathbb{F}_p$-vector space, equipped with Hecke operators T_n ($n \geq 1$) and diamond operators $\langle a \rangle$ (a in $(\mathbb{Z}/N\mathbb{Z})^*$).

q-expansions: $S(N,k)_{\mathbb{F}_p} \hookrightarrow \mathbb{F}_p[[q]]$.

To $f = \sum a_n(f)q^n$ in $S(N,k)_{\overline{\mathbb{F}}_p}$ a normalized eigenform one can associate a semisimple continuous

$$\rho_f \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

(Deligne).

TSVP

NAIVE MOD p MODULAR FORMS.

One may reduce characteristic zero modular forms mod p:

$$S(N,k)_{\mathbb{Z}[1/N]} \to S(N,k)_{\mathbb{F}_p}.$$

NAIVE MOD p MODULAR FORMS.

One may reduce characteristic zero modular forms mod p:

$$S(N,k)_{\mathbb{Z}[1/N]} \to S(N,k)_{\mathbb{F}_p}.$$

One has: $S(N,k)_{\mathbb{Z}[1/N]} =$

$$\{f \in S(N,k)_{\mathbb{C}} \mid a_n(f) \in \mathbb{Z}[1/N]\}$$

NAIVE MOD p MODULAR FORMS.

One may reduce characteristic zero modular forms mod p:

$$S(N,k)_{\mathbb{Z}[1/N]} \to S(N,k)_{\mathbb{F}_p}.$$

One has: $S(N,k)_{\mathbb{Z}[1/N]} =$

$$\{f \in S(N,k)_{\mathbb{C}} \mid a_n(f) \in \mathbb{Z}[1/N]\}$$

Unfortunately: $S(N,k)_{\mathbb{Z}[1/N]} \to S(N,k)_{\mathbb{F}_p}$ is not surjective for $k = 1$.

NAIVE MOD p MODULAR FORMS.

One may reduce characteristic zero modular forms mod p:

$$S(N,k)_{\mathbb{Z}[1/N]} \to S(N,k)_{\mathbb{F}_p}.$$

One has: $S(N,k)_{\mathbb{Z}[1/N]} =$

$$\{f \in S(N,k)_{\mathbb{C}} \mid a_n(f) \in \mathbb{Z}[1/N]\}$$

Unfortunately: $S(N,k)_{\mathbb{Z}[1/N]} \to S(N,k)_{\mathbb{F}_p}$ is not surjective for $k=1$.

Even worse: $S(N,k,\tilde{\varepsilon})_{\overline{\mathbb{Z}}_p} \to S(N,k,\varepsilon)_{\overline{\mathbb{F}}_p}$ is not always surjective even if $k>1$. (Carayol's lemma.)

TSVP

Conclusion:

Serre's conjecture comes out much more natural if one considers mod p modular forms à la Katz.

For example: $k(\rho) = 1$ if and only if ρ is unramified at p.

TSVP

SERRE'S CONJECTURE (1987):

Let p be prime, $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ continuous, irreducible and odd.

Then ρ comes from a mod p modular form of type $(N(\rho), k(\rho), \varepsilon(\rho))$.

TSVP

WHAT IS KNOWN, AND WHAT IS NOT.

THEOREM (SMRGCECVD...) If ρ is modular, then Serre's conjecture is true for ρ, except possibly if $p = 2$, ρ is unramified at 2 and $\rho(\mathrm{Frob}_2)$ has a double eigenvalue.

WHAT IS KNOWN, AND WHAT IS NOT.

THEOREM (SMRGCECVD...) If ρ is modular, then Serre's conjecture is true for ρ, except possibly if $p = 2$, ρ is unramified at 2 and $\rho(\mathrm{Frob}_2)$ has a double eigenvalue.

In the last case, one only does not know if ρ comes from a form of weight one (it does come from weight two).

Conversely, it is not known if ρ_f is unramified at two for f mod 2 of weight one.

What is known, and what is not.

Theorem (SMRGCECVD...) If ρ is modular, then Serre's conjecture is true for ρ, except possibly if $p = 2$, ρ is unramified at 2 and $\rho(\mathrm{Frob}_2)$ has a double eigenvalue.

In the last case, one only does not know if ρ comes from a form of weight one (it does come from weight two).

Conversely, it is not known if ρ_f is unramified at two for f mod 2 of weight one.

Is ρ modular? Ask Ramakrishna and Taylor. (A p-adic lift of ρ is potentially modular.)

TSVP

WHY ONE CANNOT ALWAYS LIFT IN WEIGHT ONE.

On the modular forms side:

$$S(N,1)_{\mathbb{F}_p} = \mathrm{H}^0(X_1(N)_{\mathbb{F}_p}, \underline{\omega}(-\mathrm{cusps})).$$

The degree $\deg(\underline{\omega}(-\mathrm{cusps}))$ is about half the genus of $X_1(N)$.

WHY ONE CANNOT ALWAYS LIFT IN WEIGHT ONE.

On the modular forms side:

$S(N, 1)_{\mathbb{F}_p} = \mathrm{H}^0(X_1(N)_{\mathbb{F}_p}, \underline{\omega}(-\mathrm{cusps}))$.

The degree $\deg(\underline{\omega}(-\mathrm{cusps}))$ is about half the genus of $X_1(N)$.

On the Galois side: if $\tilde{f}$ lifts f, then have

$$\rho_{\tilde{f}} \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$$

lifting ρ_f.

But then the image of $\rho_{\tilde{f}}$ in $\mathrm{PGL}_2(\mathbb{C})$ is very small.

TSVP

FROM WEIGHT ONE TO WEIGHT p.

Hasse:

$$S(N,1)_{\mathbb{F}_p} \to S(N,p)_{\mathbb{F}_p}, \quad f \mapsto Af.$$

On q-expansions:

$$\sum a_n q^n \mapsto \sum a_n q^n.$$

From weight one to weight p.

Hasse:

$$S(N,1)_{\mathbb{F}_p} \to S(N,p)_{\mathbb{F}_p}, \quad f \mapsto Af.$$

On q-expansions:

$$\sum a_n q^n \mapsto \sum a_n q^n.$$

Frobenius:

$$S(N,1)_{\mathbb{F}_p} \to S(N,p)_{\mathbb{F}_p}, \quad f \mapsto f^p.$$

On q-expansions:

$$\sum a_n q^n \mapsto \sum a_n q^{pn}.$$

Each leads to an algorithm.

TSVP

THE HASSE ALGORITHM.

Suppose $N \geq 5$ is odd. Let $\mathbb{T}$ be the Hecke algebra of $S(2N, 2)_{\mathbb{C}}$. Put:

$$M := (\mathbb{T}^\vee / \mathbb{T}^\vee \cap w_2 \mathbb{T}^\vee)_2.$$

Then $4M = 0$, and:

$$S(N, 1)_{\mathbb{F}_2} = M/M[2],$$

as Hecke modules (except for T_2).

THE HASSE ALGORITHM.

Suppose $N \geq 5$ is odd. Let $\mathbb{T}$ be the Hecke algebra of $S(2N,2)_{\mathbb{C}}$. Put:

$$M := (\mathbb{T}^{\vee}/\mathbb{T}^{\vee} \cap w_2\mathbb{T}^{\vee})_2.$$

Then $4M = 0$, and:

$$S(N,1)_{\mathbb{F}_2} = M/M[2],$$

as Hecke modules (except for T_2).

Principle of proof: geometry over $\mathbb{Z}_2$.

Motivation from a question by Agashe and Stein (comparison of two lattices).

THE HASSE ALGORITHM.

Suppose $N \geq 5$ is odd. Let $\mathbb{T}$ be the Hecke algebra of $S(2N,2)_{\mathbb{C}}$. Put:

$$M := (\mathbb{T}^\vee/\mathbb{T}^\vee \cap w_2\mathbb{T}^\vee)_2.$$

Then $4M = 0$, and:

$$S(N,1)_{\mathbb{F}_2} = M/M[2],$$

as Hecke modules (except for T_2).

Principle of proof: geometry over $\mathbb{Z}_2$.

Motivation from a question by Agashe and Stein (comparison of two lattices).

Note: $\mathbb{T}$ can be computed using modular symbols.

TSVP

THE FROBENIUS ALGORITHM.

Let $N \geq 5$ and p a prime not dividing N.

Let $\mathbb{T}$ be the Hecke algebra of $S(N,p)_{\mathbb{C}}$.

Put $B := \frac{p+2}{24} N^2 \prod_{l|N}(1 - l^{-2})$.

Then:

$$S(N,1)_{\mathbb{F}_p} =$$

$\{f\colon \mathbb{T} \to \mathbb{F}_p \mid f(T_n) = 0$, for $p \nmid n \leq B\}$,
as Hecke modules.

THE FROBENIUS ALGORITHM.

Let $N \geq 5$ and p a prime not dividing N.

Let $\mathbb{T}$ be the Hecke algebra of $S(N,p)_{\mathbb{C}}$.

Put $B := \frac{p+2}{24} N^2 \prod_{l|N}(1 - l^{-2})$.

Then:

$$S(N,1)_{\mathbb{F}_p} =$$

$\{f\colon \mathbb{T} \to \mathbb{F}_p \mid f(T_n) = 0$, for $p \not| n \leq B\}$,
as Hecke modules.

Principle of proof:

$$qd/dq\colon\ S(N,p)_{\mathbb{F}_p} \to S(N,p+2)_{\mathbb{F}_p},$$

and a result of Jacob Sturm (for B).

TSVP

MODULAR SYMBOLS MODULO p.

In the Frobenius algorithm, one only needs to compute $\mathbb{F}_p \otimes \mathbb{T}$.

Modular symbols modulo p.

In the Frobenius algorithm, one only needs to compute $\mathbb{F}_p \otimes \mathbb{T}$.

THEOREM $\mathrm{H}^1(X_1(N)(\mathbb{C}), \mathbb{F}_2)$ is a faithful $\mathbb{F}_2 \otimes \mathbb{T}$-module.

The proof uses group schemes over $\mathbb{F}_2$, Dieudonné modules, and de Rham cohomology.

MODULAR SYMBOLS MODULO p.

In the Frobenius algorithm, one only needs to compute $\mathbb{F}_p \otimes \mathbb{T}$.

THEOREM $\mathsf{H}^1(X_1(N)(\mathbb{C}), \mathbb{F}_2)$ is a faithful $\mathbb{F}_2 \otimes \mathbb{T}$-module.

The proof uses group schemes over $\mathbb{F}_2$, Dieudonné modules, and de Rham cohomology.

THEOREM For $2 \leq k < p$,

$$\mathsf{H}^1_{\mathsf{par}}(\Gamma_1(N), \mathsf{Sym}^{k-2}(\mathbb{F}_p^2))$$

is a faithful $\mathbb{F}_p \otimes \mathbb{T}(N, k)$-module.

The proof uses Fontaine-Laffaille theory. One should be able to treat the important case $k = p$.

TSVP

A RESULT ON EIGENSPACES.

Let $N \geq 1$, p prime not dividing Nx.

Let V be a common non-zero eigenspace in $S(N,p)_{\overline{\mathbb{F}}_p}$ for all T_l, $l \neq p$ prime, with system of eigenvalues a.

A RESULT ON EIGENSPACES.

Let $N \geq 1$, p prime not dividing Nx.

Let V be a common non-zero eigenspace in $S(N,p)_{\overline{\mathbb{F}}_p}$ for all T_l, $l \neq p$ prime, with system of eigenvalues a.

Then V is of dimension at most two.

If $\dim(V) = 1$, then a does not occur in $S(N,1)_{\overline{\mathbb{F}}_p}$.

If $\dim(V) = 2$, then the a-eigenspace V_1 in $S(N,1)_{\overline{\mathbb{F}}_p}$ is of dimension one, with T_p eigenvalue the trace of T_p on V.

TSVP

Computations.

There are published methods to compute $S(N,1)_{\mathbb{C}}$.

Kiming, *On the experimental verification of the Artin conjecture for 2-dimensional odd Galois representations over* $\mathbb{Q}$. In Lecture Notes in Mathematics 1585 (1994).

As far as I know, there are no published tables of mod p modular forms of weigt 1. But there is a letter from Mestre to Serre (october 1987).