Computations of weight 1 modular forms over finite fields

Gabor Wiese*

(Institut de Recherche Mathématique de Rennes)

(Universiteit Leiden)

Intercity Number Theory Seminar

Utrecht, 7 March 2003

* Supported by the European Research Training Network "Arithmetic Algebraic Geometry".

Plan of the talk

Created MAGMA functions for the computation of Katz cusp forms of weight 1 for $\Gamma_0(N)$ over $\overline{\mathbb{F}_2}$.

In this talk I want to tell you:

- *how* we compute them,
  (theorem by Bas Edixhoven)
- *why* we compute them and
  (Galois representations)
- *what* we got so far.
  (You'll see some numbers.)

Modular forms

Cusp forms of *weight* $k \geq 1$ and *level* $N \geq 5$:

analytic/classical	algebro-geometric
$\mathcal{S}_k^{\mathsf{cl}}(\Gamma_1(N), \mathbb{C})$	$\mathcal{S}_k^{\mathsf{Katz}}(\Gamma_1(N), R)$ for $\mathbb{Z}[1/N]$-alg. R
$f : \mathbb{H} \to \mathbb{C}$ hol. s.t. $\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$: $f(\frac{a\tau+b}{c\tau+d}) = (c\tau + d)^k f(\tau)$ + cond. on cusps	global sections of some sheaf of differentials on $Y_1(N)_R$ + cond. on cusps

Modular forms

In both settings one has a

q-expansion at ∞: $f = \sum_{n \geq 1} a_n(f) q^n$

$$\mathcal{S}_k^{\mathrm{cl}}(\Gamma_1(N), \mathbb{Z}) := \{ f = \sum_{n \geq 1} a_n q^n \mid a_n \in \mathbb{Z} \}$$

$$\mathcal{S}_k^{\mathrm{cl}}(\Gamma_1(N), R) := \mathcal{S}_k^{\mathrm{cl}}(\Gamma_1(N), \mathbb{Z}) \otimes_{\mathbb{Z}} R$$

"Classical setting = Katz setting" if

(i) $k \geq 2$ or

(ii) R flat over $\mathbb{Z}$ (in part.: $R \subseteq \mathbb{C}$)

In general: "classical" $\subseteq$ "Katz"

$\Rightarrow$ weight 1 over finite fields is special!

Modular forms

Diamond operators $< a >$ for $a \in (\mathbb{Z}/N)^*$

$\Rightarrow$ group action by $(\mathbb{Z}/N)^*$

For a character $\epsilon : (\mathbb{Z}/N)^* \to R$ set

$\mathcal{S}_k(\Gamma_1(N), \epsilon, R) := \{ f \mid < a > f = \epsilon(a) f \ \forall a \}.$

$\mathcal{S}_k(\Gamma_0(N), R) = \mathcal{S}_k(\Gamma_1(N), \text{trivial}, R)$

Hecke operators T_n for $n \in \mathbb{N}$

For a prime l, set

$$a_n(T_l f) = \begin{cases} a_{ln}(f) & (l \mid N) \\ a_{ln}(f) + l^{k-1} a_{n/l}(< l > f) & (l \nmid N) \end{cases}$$

$$T_{l^{r+1}} = \begin{cases} T_l \circ T_{l^r} & (l \mid N) \\ T_l \circ T_{l^r} - l^{k-1} < l > \circ T_{l^{r-1}} & (l \nmid N) \end{cases}$$

$$T_{nm} = T_n \circ T_m \qquad ((n,m) = 1)$$

In particular:

$$\boxed{a_1(T_n f) = a_n(f)}$$

Hecke algebra

$\mathbb{T}_k(\mathbb{Z})$: $\mathbb{Z}$-alg. gen. by $T_n \in \mathrm{End}_{\mathbb{C}}(\mathcal{S}_k(\mathbb{C}))$,

$\mathbb{T}_k(\mathbb{F})$: $\mathbb{F}$-alg. gen. by $T_n \in \mathrm{End}_{\mathbb{F}}(\mathcal{S}_k(\mathbb{F}))$.

They are free of finite rank, commutative and generated by the T_n as modules.

Isom. of $\mathbb{T}_k(\mathbb{Z})$-modules

$$\mathcal{S}_k(\mathbb{Z}) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_k(\mathbb{Z}), \mathbb{Z})$$

$$f \mapsto (T_n \mapsto a_1(T_n f) = a_n(f)).$$

$f \in \mathcal{S}_k(\overline{\mathbb{F}_p})$ *Hecke eigenform*

$$\Rightarrow a_1(T_n f) = \lambda_n a_1(f) = a_n(f)$$

f normalised eigenform $\Leftrightarrow T_n f = a_n(f) f \ \forall n$

Coeff. of norm. eigenforms = eigenvalues of Hecke operators

Hecke algebra

- $\mathcal{S}_k^{\mathsf{cl}}(\Gamma_1(N), \overline{\mathbb{Q}})$ has a basis of normalized eigenforms if N is prime.

- For $\mathcal{S}_k(\overline{\mathbb{F}_p})$ wrong in general: $f \in \mathbb{Z}[X]$ prime can have multiple roots mod p.
- $\mathbb{T}_k(\mathbb{F}_p) = \prod_i^n \mathbb{T}_i$ with $\mathbb{T}_i$ local $\mathbb{F}_p$-algebras
- $\mathbb{T}_i \otimes \overline{\mathbb{F}_p} = \prod_j^{m_i} \mathbb{T}_{i,j}$ with $\mathbb{T}_{i,j}$ local $\overline{\mathbb{F}_p}$-algebras
- Each $T_{i,j}$ corresponds to an eigenform with coefficients in $\mathbb{T}_i/\mathfrak{m}_i = \mathbb{F}_{p^{m_i}}$ ($\mathfrak{m}_i =$ max.id.)
- For fixed i, these eigenforms are conjugate via $G_{\mathbb{F}_{p^{m_i}}|\mathbb{F}_p}$.
- I define $\mathsf{UPO}(\mathbb{T}_i) = \min \{ n \mid (\mathfrak{m}_i)^n = (0) \}$.

Computing the Hecke algebra

$$\boxed{k \geq 2}$$

Isomorphisms of Hecke modules:

$$\begin{array}{c} H^1_{\mathrm{par}}(\Gamma_1(N), \mathcal{F}_k(\mathbb{C}))(\epsilon) \\ \sim \big\downarrow \\ \text{Cuspidal modular symbols}_k(\Gamma_1(N), \epsilon, \mathbb{C}) \\ \sim \big\downarrow \\ \mathcal{S}_k^{\mathrm{cl}}(\Gamma_1(N), \epsilon, \mathbb{C}) \oplus \overline{\mathcal{S}_k^{\mathrm{cl}}(\Gamma_1(N), \epsilon, \mathbb{C})} \end{array}$$

MAGMA provides functions to compute the T_n on cuspidal modular symbols for $\Gamma_1(N)$ <u>with character</u> in weight $k \geq 2$.

$$\boxed{k = 1 \text{ is different!}}$$

Computing eigenforms of weight 1

$N \geq 5$, $\mathbb{F}|\mathbb{F}_p$ finite extension,

$\epsilon : (\mathbb{Z}/N)^* \to \mathbb{F}^*$ character

Frobenius:

$F : \mathcal{S}_1^{\mathsf{Katz}}(\Gamma_1(N), \epsilon, \mathbb{F}) \to \mathcal{S}_p^{\mathsf{Katz}}(\Gamma_1(N), \epsilon, \mathbb{F})$

$$a_n(Ff) = \begin{cases} a_{n/p}(f) & (p \mid n) \\ 0 & (p \nmid n) \end{cases}$$

Proposition.

$B := \frac{p+2}{12} N \prod_{l|N,\mathsf{prime}} (1 + \frac{1}{l})$.

Let $f \in \mathcal{S}_p^{\mathsf{Katz}}(\Gamma_1(N), \epsilon, \mathbb{F})$.

$$f \in \mathrm{Image(F)} \Leftrightarrow$$

$$a_n(f) = 0 \; \forall n \leq B, p \nmid n$$

Computing eigenforms of weight 1

$$\mathbb{T} := \mathbb{T}_p^{\mathsf{cl}}(\Gamma_1(N), \mathbb{Z})$$

$$\begin{array}{ccc}
f & & \mathcal{S}_1^{\mathsf{Katz}}(\Gamma_1(N), \epsilon, \mathbb{F}) \\
\Big\downarrow & & \Big\downarrow F \\
 & & \mathcal{S}_p^{\mathsf{Katz}}(\Gamma_1(N), \epsilon, \mathbb{F}) \\
 & & \sim \Big\downarrow \\
 & & \Big(\mathcal{S}_p^{\mathsf{Katz}}(\Gamma_1(N), \mathbb{F})\Big)(\epsilon) \\
 & & \sim \Big\downarrow \\
 & & \Big((\mathcal{S}_p^{\mathsf{cl}}(\Gamma_1(N), \mathbb{Z})) \otimes \mathbb{F}\Big)(\epsilon) \\
 & & \sim \Big\downarrow \\
 & & \Big((\mathsf{Hom}_{\mathbb{Z}}(\mathbb{T}, \mathbb{Z}) \otimes \mathbb{F}\Big)(\epsilon) \\
 & & \sim \Big\downarrow \\
 & & (\mathbb{T} \otimes \mathbb{F})^{\vee_{\mathbb{F}}}(\epsilon) \\
 & & \Big\| \\
\phi & & (\mathbb{T} \otimes \mathbb{F})^{\vee_{\mathbb{F}}}\Big[\ \epsilon(a) - < a > \ \mid a \in (\mathbb{Z}/N)^*\ \Big]
\end{array}$$

$$\phi = \Big(T_n \otimes 1 \mapsto \begin{cases} a_{n/p}(f) & (p \mid n) \\ 0 & (p \nmid n) \end{cases}\Big)$$

Computing eigenforms of weight 1

Theorem (Edixhoven).

Isomorphism of Hecke modules

$$\mathcal{S}_1^{\mathsf{Katz}}(\Gamma_1(N), \epsilon, \mathbb{F}) \cong \Big((\mathbb{T} \otimes \mathbb{F})/\mathcal{R}\Big)^{\vee \mathbb{F}}$$

with $\mathcal{R} \leq \mathbb{T} \otimes \mathbb{F}$ the sub-$\mathbb{F}$-v.s. gener. by

- $T_n \,\forall\, n \leq B, p \nmid n$ and
- $\epsilon(l) - < l > \;\forall\, l \in (\mathbb{Z}/N)^*$.

T_l corresponds to T_l ($l \neq p$ prime),

T_p corresponds to $T_p + < p > F$.

⇒ Know $\mathbb{T}_1^{\mathsf{Katz}}(\Gamma_1(N), \epsilon, \mathbb{F})$.
⇒ Can compute weight 1 eigenforms.

Problem: Computation of $\mathbb{T}$ very slow!

Computing eigenforms of weight 1

$\epsilon =$ trivial character, $\mathbb{F}|\mathbb{F}_2$,

$\mathbb{T}^{(i)} := \mathbb{T}_2^{\mathrm{cl}}(\Gamma_i(N), \mathbb{Z})$ for $i \in \{ 0, 1 \}$

$\left(\mathbb{T}^{(1)}/(1- < l >)\right)_{\mathrm{free}} \cong \mathbb{T}^{(0)}$

Get injection of Hecke modules:

$\phi : ((\mathbb{T}^{(0)} \otimes \mathbb{F})/(T_n \mid 2 \nmid n))^\vee \hookrightarrow \mathcal{S}_1^{\mathrm{Katz}}(\Gamma_0(N), \mathbb{F})$

Proposition:

If $\exists q$ prime s.t. $q \mid N$ and $q \equiv 3$ (4),

then ϕ above is an isomorphism.

We calculate Hecke operators on $(\mathbb{T}^{(0)} \otimes \mathbb{F})/(T_n \mid 2 \nmid n, n \leq B)$.

Galois representations

Theorem (Deligne).

Let $f \in \mathcal{S}_k^{\mathsf{Katz}}(\Gamma_1(N), \epsilon, \overline{\mathbb{F}_p})$ an eigenform.

$\Rightarrow$ $\exists!$ contin., semi-simple, odd repres.

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

- ρ_f unramified outside pN,
- $\mathrm{Tr}(\rho_f(\mathrm{Frob}_l)) = a_l(f)$ and

  $\mathrm{Det}(\rho_f(\mathrm{Frob}_l)) = \epsilon(l) l^{k-1} \; \forall \, l \nmid Np$.

f is reduction of a char. 0 form of weight 1,

$\Rightarrow$ ρ_f is the reduction of a rep. over $\mathbb{C}$.

I call the group $\mathrm{Im}(\rho_f) \subset \mathrm{GL}_2(\overline{\mathbb{F}_p})$

the *group of* ρ_f (resp. f).

Galois representations

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ a contin., irreducible, odd representation, unramified at p.

$\Rightarrow$ $\mathrm{Det} \circ \rho = \epsilon_\rho \circ \chi_{N_\rho}$

for unique $\epsilon_\rho : (\mathbb{Z}/N_\rho)^* \to \overline{\mathbb{F}_p}^*$, where

N_ρ Artin conductor, χ_{N_ρ} cyclotomic char.

Serre-Conjecture (1^{st} version 1987).

$\exists$ eigenform $f \in \mathcal{S}_1^{\mathrm{Katz}}(\Gamma_1(N_\rho), \epsilon_\rho, \overline{\mathbb{F}_p})$

such that $\rho = \rho_f$.

Theorem (many people).

$p \neq 2$ and $\rho = \rho_g$ for some eigenform g

$\Rightarrow \rho = \rho_f$ with f as in conjecture.

$p = 2$ unknown, *exceptional case*

Galois representations

Let $\rho : G_{\mathbb{Q}} \to \mathrm{SL}_2(\overline{\mathbb{F}_2}) = \mathrm{PSL}_2(\overline{\mathbb{F}_2})$.

Some facts:

- $\#\mathrm{SL}_2(\mathbb{F}_{2^r}) = (2^r - 1)2^r(2^r + 1)$

- $\mathrm{SL}_2(\mathbb{F}_{2^r})$ simple if $r > 1$

- subgroups of $\mathrm{SL}_2(\mathbb{F}_{2^r})$ are (up to conj.)

  - $\mathrm{SL}_2(\mathbb{F}_{2^s})$ with $s \mid r$ ($\Rightarrow \rho$ irreducible)
  - dihedral groups D_{2n} with

    $n \mid 2^r - 1$ or $n \mid 2^r + 1$ ($\Rightarrow \rho$ irreducible)
  - cyclic groups of order n with

    $n \mid 2^r - 1$ or $n \mid 2^r + 1$ ($\Rightarrow \rho$ reducible)
  - subgroups of upper triang. matrices

    (order $\mid 2^r(2^r - 1)$) ($\Rightarrow \rho$ reducible)

- can often distinguish elements of different

  order by their traces

Galois representations

Theorem (essentially Hecke).

Serre's conjecture is true for

representations with dihedral image.

Let $N \in \mathbb{N}$ square-free.

Let $K = \begin{cases} \mathbb{Q}(\sqrt{N}) & \text{if } N \equiv 1(4) \\ \mathbb{Q}(\sqrt{-N}) & \text{if } N \equiv 3(4). \end{cases}$

Take $\mathbb{Q} \subset K \subseteq L \subseteq H_K$, with

$[L : K] =: u$ maximal odd.

$\Rightarrow \exists (u-1)$ non-trivial $\chi : G_{L|K} \to \overline{\mathbb{F}_2}^*$.

$\Rightarrow \exists (u-1)/2$ irreducible dihedral repres.

$\mathrm{Ind}_{G_{L|K}}^{G_{L|\mathbb{Q}}} \chi : G_{L|\mathbb{Q}} \to \mathrm{SL}_2(\overline{\mathbb{F}_2})$

(Artin conductor $= N$)

$\Rightarrow \exists \; \frac{u-1}{2}$ dihedral eigenforms of
weight 1, level N, trivial character

Some data

First calculations done by Mestre in 1987(!).

Written down in a letter to Serre.

Verified them nearly completely.

We did (can do much more):

- prime levels $5 \leq N < 2100$,
- odd levels $5 \leq N < 1000$

Results in prime levels:

- all representation irreducible,
- all Hecke algebras locally $\mathbb{F}_{2^m}[x]/(x^n)$

In non-prime level some non-Gorenstein cases.

Today focus on eigenforms for

- dihedral group,
- $\mathrm{SL}_2(\mathbb{F}_{2^2}) \cong A_5$,
- $\mathrm{SL}_2(\mathbb{F}_{2^3})$.

Some data - a dihedral example

- Example $N = 2063$: prime, $N \equiv 3\ (4)$
- $\dim \mathcal{S}_1^{\mathsf{Katz}}(\Gamma_0(N), \overline{\mathbb{F}_2}) = 26$
- $K := \mathbb{Q}(\sqrt{-2063})$, $\mathsf{CL}_K = \mathbb{Z}/45$
- $22 = (45-1)/2$ dihedral reps; concretely:
  - $\varphi(45)/2 = 12$ with group D_{90} over $\mathbb{F}_{2^{12}}$,
  - $\varphi(15)/2 = 4$ with group D_{30} over $\mathbb{F}_{2^4}$,
  - $\varphi(9)/2 = 3$ with group D_{18} over $\mathbb{F}_{2^3}$,
  - $\varphi(5)/2 = 2$ with group D_{10} over $\mathbb{F}_{2^2}$,
  - $\varphi(3)/2 = 1$ with group D_6 over $\mathbb{F}_2$.
- Find $\mathbb{T} = \prod_{i=1}^{5} \mathbb{T}_i$ over $\mathbb{F}_2$ with:
  - $\mathbb{T}_1$: dim = 12, UPO = 1, 12 max. ideals,
  - $\mathbb{T}_2$: dim = 4, UPO = 1, 4 max. ideals,
  - $\mathbb{T}_3$: dim = 3, UPO = 1, 3 max. ideals,
  - $\mathbb{T}_4$: dim = 6, UPO = 3, 2 max. ideals,
  - $\mathbb{T}_5$: dim = 1, UPO = 1, 1 max. ideal.

Some data - A_5-fields

- $p = 2$ allows also totally real fields.
- Prime levels with an A_5-eigenform:

  $653, 1061, 1381, 1553, 1733, 2029,$

  $2053, 2083$

- Example $N = 2083$: prime, $N \equiv 3$ (4)
- $\dim \mathcal{S}_1^{\mathrm{Katz}}(\Gamma_0(N), \overline{\mathbb{F}_2}) = 7$
- $K := \mathbb{Q}(\sqrt{-2083})$, $\mathrm{CL}_K = \mathbb{Z}/7$
- Expect $3 = (7-1)/2$ dihedral reps.
- Find $\mathbb{T} = \mathbb{T}_1 \times \mathbb{T}_2$ over $\mathbb{F}_2$ with:
  - $\mathbb{T}_1$: dim = 3, UPO = 1, 3 max. ideals, corresponds to D_{14} ($\varphi(7)/2 = 3$),
  - $\mathbb{T}_2$: dim = 4, UPO = 2, 2 max. ideals, corresponds to A_5.

Some data - $\mathrm{SL}_2(\mathbb{F}_8)$-fields

- $\mathrm{SL}_2(\mathbb{F}_8) \not\subseteq \mathrm{GL}_2(\mathbb{C})$

  $\Rightarrow$ $\mathrm{SL}_2(\mathbb{F}_8)$-eigenforms are not reductions from char. 0, i.e. "Katz $\neq$ classical".

- Prime levels with an $\mathrm{SL}_2(\mathbb{F}_8)$-eigenform:

  $1429, 1567, 1613, 1693, 1997, 2017, 2089$

Some data - $\mathrm{SL}_2(\mathbb{F}_8)$-fields

- Example $N = 1567$: prime, $N \equiv 3$ (4)
- $\dim \mathcal{S}_1^{\mathrm{Katz}}(\Gamma_0(N), \overline{\mathbb{F}_2}) = 13$
- $K := \mathbb{Q}(\sqrt{-1567})$, $\mathrm{CL}_K = \mathbb{Z}/15$
- Expect $7 = (15-1)/2$ dihedral reps.
- Find $\mathbb{T} = \prod_{i=1}^4 \mathbb{T}_i$ over $\mathbb{F}_2$ with:
  - $\mathbb{T}_1$: dim = 4, UPO = 1, 4 max. ideals, corresponds to D_{30} ($\varphi(15)/2 = 4$),
  - $\mathbb{T}_2$: dim = 2, UPO = 1, 2 max. ideals, corresponds to D_{10} ($\varphi(5)/2 = 2$),
  - $\mathbb{T}_3$: dim = 1, UPO = 1, 1 max. ideal, corresponds to D_6 ($\varphi(3)/2 = 1$),
  - $\mathbb{T}_4$: dim = 6, UPO = 2, 3 max. ideals, corresponds to $\mathrm{SL}_2(\mathbb{F}_8)$