Computing modular forms: a very explicit perspective

Nils Skoruppa

Universität Siegen

July 11, 2012

Tenth Algorithmic Number Theory Symposium 2012 — San Diego

Background 1

Background

Interest in (elliptic) modular forms arise from various facts:

- Connection to geometric-Diophantine problems.
- Provide (the only) way to prove desired analytic properties of L-functions.
- Occurrence in the theory of lattices, codes, designs.
- Encode data of representations of Kac-Moody and vertex operator algebras (quantum field theory).

Conclusion

We want to compute elliptic modular forms.

Background 2

Historical review

- Hecke computed them using theta series (mid 1930th).
- Cohen, Zagier, S. computed them using the trace formula method (mid 1980th).
- In the 1970th Manin proposed the most efficient method to compute modular forms.
- In the 1990th various people (Cremona, Merel, S. etc.) turned Manin's ideas into effective algorithms
- Magma and Sage have implementations of these algorithms (mid 2000th).

Background 3

But . . .

- The underlying algorithms could yield more than what they produce currently as output.
- Modular forms of half integral weight are not yet (effectively) implemented.

Plan of the talk

- A (hopefully) very easy and explicit review of Manin's method with some modifications (at least in the description) though.
- Indications concerning the theoretical background.
- Proposals how to extend/modify the current implementations.
- An effective algorithm to compute modular forms of half integral weight.

The algorithm for integral weight

A number theorist's Sudoku

Notations

- $\mathbb{P}^1(\mathbb{Z}/N)$: set of relatively prime pairs (x, y) in $\mathbb{Z}/N$ modulo $(\mathbb{Z}/N)^*$.
- $[x : y]$ class of (x, y).
- $\mathrm{SL}(2, \mathbb{Z})$ acts naturally on $\mathbb{P}^1(\mathbb{Z}/N)$ from the right (matrix multiplication).
- $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $R = ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ $(S^2 = R^3 = -1)$.

Definition (The N-board)

The N-board is a colored graph:

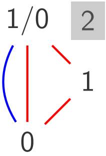
- Vertices: the points of $\mathbb{P}^1(\mathbb{Z}/N)$.
- Connect p and q by a blue edge if $p = qS$.
- Connect p and q by a red edge if $p = qR$ or $p = qR^2$.

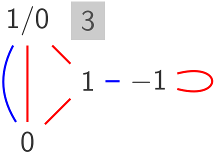
The game (or labeling Schreier coset graphs)

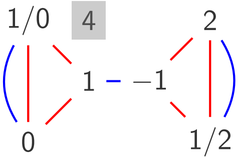
Recall

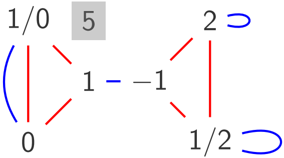
$$x/y = \frac{x}{y} := [x : y]$$

$$\frac{x}{y}S = -\frac{y}{x}, \quad \frac{x}{y}R = \frac{y}{y-x}$$



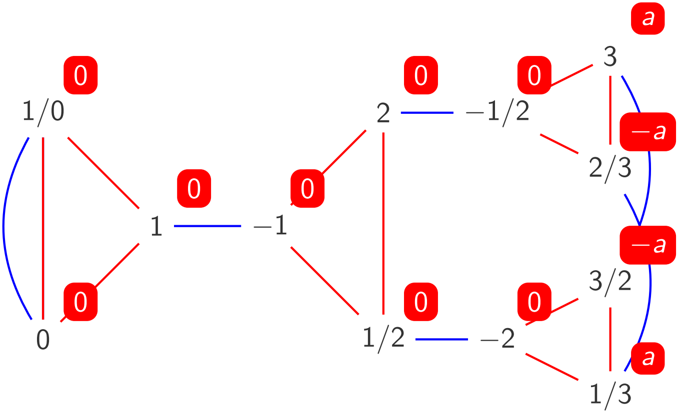




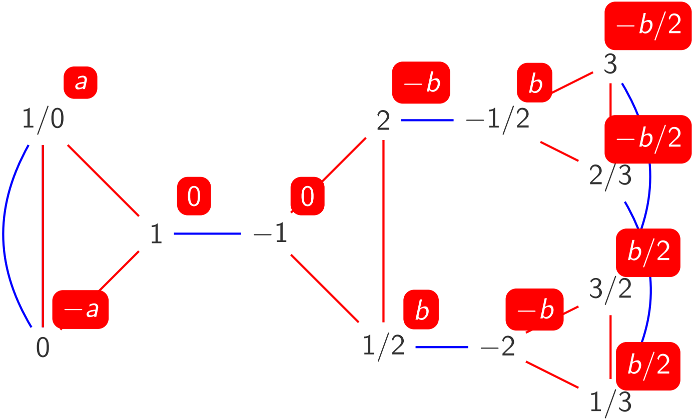


Problem (The N riddle)

Odd solution of the 11-riddle



Even solutions of the 11-riddle



Where are the modular forms?

Definition

- $\mathcal{L}(N)$ the $\mathbb{Z}$-module of all solutions of the N-riddle.
- $\mathcal{L}(N)^-$ and $\mathcal{L}(N)^+$ the submodule of all odd $(\lambda([-x:y]) = -\lambda([x:y]))$ and even $(\lambda([-x:y]) = +\lambda([x:y]))$ solutions, respectively.

Theorem

- *For every λ in $\mathcal{L}(N)$ and every $[x:y]$ in $\mathbb{P}^1(\mathbb{Z}/N)$, the series*

$$f_{\lambda,[x:y]} = \sum_{\substack{a,b,c,d \in \mathbb{Z} \\ a>b\geq 0,\ d>c\geq 0}} \lambda\big([ax+cy : bx+dy]\big)\, q^{ad-bc}$$

  defines an element of $M_2(N)$ (up to addition of a constant term).
- *The series $f_{\lambda,[x:y]}$ span $M_2(N)$.*

Modular forms on $\Gamma_0(N)$

Definition (Modular form of weight 2 on $\Gamma_0(N)$)

$M_2(N)$: space if holomorphic functions f on $\mathbb{H}$ such that

1. $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z)$ for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N) = \left(\begin{smallmatrix} \mathbb{Z} & \mathbb{Z} \\ N\mathbb{Z} & \mathbb{Z} \end{smallmatrix}\right) \cap \mathrm{SL}(2,\mathbb{Z})$
2. $f = \sum_{n\geq 0} a_f(n)\, q^n$ (and a similar regularity in the other cusps).

Theorem (Hecke operators)

For any f in $M_2(N)$, the Dirichlet series $L(f,s) = \sum_{n\geq 1} a_f(n) n^{-s}$ has an Euler product iff f is a simultaneous eigenform of all Hecke operators $T(l)$ ($l = 1, 2, 3, \ldots$), where $T(l)f := \sum_{l\geq 0} \Big[\sum_{d|l,n,\ \gcd(d,N)=1} d\, a_f(ln/d^2) \Big] q^n$.

Remark (Magical equation)

$$a_{T(l)f}(n) = a_{T(n)f}(l)$$

The super riddle

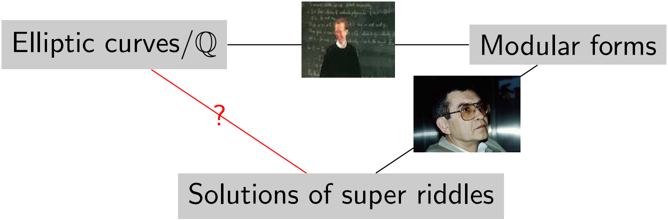
Problem (Super solutions)

Find solutions λ of the N-riddles which correspond to Hecke eigen forms:

$$\big(T(l)\lambda\big)([x:y]) = \sum_{\substack{ad-bc=l \\ a>c\geq 0,\ d>b\geq 0}} \lambda\big([ax+cy:bx+dy]\big) = e(l)\lambda(P)$$

for all $[x:y]$ *and all* $l \geq 1$. *(possibly with labels in* $\overline{\mathbb{Q}}$*).*

Related problem



Theoretical background

Eichler-Shumura isomorphism plus Manin trick

Theorem

The following maps B and C define isomorphisms of Hecke modules:

$$M_2^{\mathrm{Eis}}(N) \oplus S_2(N) \oplus \overline{S_2(N)} \xrightarrow{B} \mathrm{Hom}_{\mathbb{Z}[\Gamma_0(N)]}\left(\mathbb{Z}[\mathbb{P}^1(\mathbb{Q})]^0, \mathbb{C}\right) \xrightarrow{C} \mathcal{L}(N) \otimes \mathbb{C},$$

where

- $B : f \mapsto c_f,\ c_f(e_p - e_q) = \int_q^p f(z)\,dz.$
- $C : c \mapsto \lambda,\ \lambda\big([\tilde{c} : \tilde{d}]\big) = c\big(e_{A\infty} - e_{A0}\big)\ \left(A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})\right).$

C follows from

Lemma (Manin)

$\mathbb{Z}[\mathbb{P}^1(\mathbb{Q})]^0$ *is an* $\mathbb{Z}[\mathrm{SL}(2,\mathbb{Z})]$*-module of rank* 1.

B follows from the Eichler-Shimura isomorphism ...

Eichler-Shumura isomorphism plus Manin trick (cont.)

Proof.

...by analyzing the long exact sequence associated to the short exact sequence of $\Gamma_0(N)$-modules:

$$0 \to \mathbb{C} \cdot \deg \to \mathrm{Hom}\left(\mathbb{Z}[\mathbb{P}^1(\mathbb{Q})], \mathbb{C}\right) \xrightarrow{\text{res}} \mathrm{Hom}\left(\mathbb{Z}[\mathbb{P}^1(\mathbb{Q})]^0, \mathbb{C}\right) \to 0,$$

namely, the sequence

$$\begin{aligned} \mathbb{C} \to \mathrm{Hom}_{\Gamma_0(N)}\left(\mathbb{Z}[\mathbb{P}^1(\mathbb{Q})], \mathbb{C}\right) &\to \mathrm{Hom}_{\Gamma_0(N)}\left(\mathbb{Z}[\mathbb{P}^1(\mathbb{Q})]^0, \mathbb{C}\right) \\ &\to \mathrm{H}^1\left(\Gamma_0(N), \mathbb{C}\right) \to \mathrm{H}^1\left(\Gamma_0(N), \mathrm{Hom}\left(\mathbb{Z}[\mathbb{P}^1(\mathbb{Q})], \mathbb{C}\right)\right) \end{aligned}$$

and using the Eichler-Shimura isomorphism

$$\mathrm{H}^1_{cusp}\left(\Gamma_0(N), \mathbb{C}\right) \cong S_1(N) \oplus \overline{S_1(N)}.$$

□

Modular forms and solutions of N-riddles

Corollary

The spaces $\mathcal{L}(N)^{-}$ and $\mathcal{L}(N)^{+}$ are isomorphic as Hecke modules to $S_2(N) \oplus M_2^{\mathrm{Eis},-}(N)$ and $S_2(N) \oplus M_2^{\mathrm{Eis},+}(N)$, respectively.

Theorem (Basic principle for computing modular forms)

Let X be a Hecke module which is isomorphic (as Hecke module) to a submodule M of $M_2(N)$. Then, for every ϕ in X^*, the application

$$S_\phi(x) := \sum_{l \geq 1} \phi(T(l)x)\, q^l$$

defines a Hecke equivariant map $S_P : X \to M$. Moreover, M equals the sum of the images of the S_P.

The theorem follows rom the magic identity $a_{T(l)}f(n) = a_{T(n)}f(l)$.

Proof of the basic principle

Proof.

Let $p : X \xrightarrow{\cong} M$ an isomorphism of Hecke modules. Note that M^* is generatedby the $\phi_n : f \mapsto a_f(n)$ $(n = 1, 2, 3, \dots)$. Accordingly, X^* is generated by the $p^*\phi_n$. Suppose $\phi = p^*\phi_n$. Let $f = p(x)$. Then

$$S_\phi(x) = \sum_l \phi\big(T(l)x\big)\, q^l = \sum_l \phi\big(T(l)p(f)\big)\, q^l = \sum_l p^*\phi\big(T(l)f\big)\, q^l$$
$$= \sum_l a_{T(l)f}(n)\, q^l = \sum_l a_{T(n)}(l)\, q^l = T(n)f.$$

□

Solutions of N-riddles and modular forms

Remark

If λ is a solution of the N-riddle, say, λ corresponding to f in $M_2(N)$, then

$$\sum_{l\geq 1}\big(T(l)\lambda\big)([x:y]) \sum_{\text{finitly mamy } n} T(n)f.$$

Comments and Supplements

Open problems

Questions

- What is the nature of super solutions to N-riddles?
- What is the precise connection between such a solution and the underlying algebro-arithmetic object (elliptic curve, Galois representations, ...)?
- How can one derive *nice* formulas for elements of $\mathrm{Hom}_{\mathbb{Z}[\Gamma_0(N)]}\left(\mathbb{Z}[\mathbb{P}^1(\mathbb{Q})]^0, \mathbb{C}\right)$?
  (The inverse of the map B to solutions of the N-riddle is not very explicit since it contains continued fraction expansions of rational numbers).
- Is there an *explicit* way to distinguish super solutions from the others. (Algorithmically it suffices to check for $T(l)$ for l below an effective bound depending on N only.)

Some examples

Example

$M_2(11) = \mathbb{C}\cdot\big(E_2(z) - 11E_2(11z)\big) \oplus \mathbb{C}\cdot\eta(z)^2\,\eta(11z)^2$. Recall $\operatorname{rank}\mathcal{L}\big(11\big)^{+} = 2$, $\operatorname{rank}\mathcal{L}\big(11\big)^{-} = 1$. One even super solution is $\infty \mapsto 1$, $0 \mapsto -1$. Resulting formula:

$$E_2(z) - 11E_2(11z) = -10 + 288\Big(\sum_{\substack{a>b\geq 0,\ d>c\geq 0\\ \frac{a}{c}\equiv\frac{1}{0} \bmod 11}} - \sum_{\substack{a>b\geq 0,\ d>c\geq 0\\ \frac{a}{c}\equiv 0 \bmod 11}}\Big)q^{ad-bc}.$$

The odd (super)solution is $3, 1/3 \mapsto 1$, $2/3, 3/2 \mapsto -1$. Hence

$$\eta(z)^2\,\eta(11z)^2 = \Big(\sum_{\substack{a>b\geq 0,\ d>c\geq 0\\ \frac{3a+c}{3c+d}\equiv\frac{1}{3},3 \bmod 11}} - \sum_{\substack{a>b\geq 0,\ d>c\geq 0\\ \frac{3a+c}{3c+d}\equiv\frac{3}{2},\frac{2}{3} \bmod 11}}\Big)q^{ad-bc}.$$

Partial answers

Explicit formulas for eigenform in the Hom-space

- For Eisenstein series such formulas can be set up.
- For eigenforms associated to groessencharacters: work in progress.

Theorem

For any integral binary quadratic form Q whose discriminant is positive and not a square, the application

$$c \mapsto \sum_{A \in \Gamma_0(N)_Q \backslash \Gamma_0(N)} \sum_{[p:q] \in \mathbb{P}^1(\mathbb{Q})} c([p:q]) \operatorname{sign}\big(Q(p,q)\big)$$

defines an element λ_Q in $\mathrm{Hom}_{\mathbb{Z}[\Gamma_0(N)]}\big(\mathbb{Z}[\mathbb{P}^1(\mathbb{Q})]^0, \mathbb{C}\big)$. The λ_Q span the cuspidal part in $\mathrm{Hom}_{\mathbb{Z}[\Gamma_0(N)]}\big(\mathbb{Z}[\mathbb{P}^1(\mathbb{Q})]^0, \mathbb{C}\big)$.

Comments on current implementations

- Current implementations work with modular symbols instead of $\mathrm{Hom}_{\mathbb{Z}[\Gamma_0(N)]}\left(\mathbb{Z}[\mathbb{P}^1(\mathbb{Q})]^0, \mathbb{C}\right)$.
  Modular symbols can be identified with elements in the space of coinvariants $\left(\mathbb{C}[\mathbb{P}^1(\mathbb{Q})]^0\right)_{\Gamma_0(N)}$, which in turn can be identified with the dual of the Hom space.
- Current implementations determine the modular symbol eigenforms and compute from them on request the first so and so many eigenvalues.
- Current implementations ignore the fact that with less more effort they could output explicit formulas instead of only finitely many Fourier coefficients.
- Analysing the labeling procedure and adding more intelligence to the algorithms, what levels can one reach? (Ongoing project wih Martin Raum).

An algorithm for half integral weight

Basic notions

Notations

For an even Dirichlet character modulo $4N$, denote by $M_{3/2}(N,\chi)$ the space of holomorphic functions F on $\mathbb{H}$ such that

1. $Q := F/\theta^3$ satisfies $Q\left(\frac{az+b}{cz+d}\right) = \chi(d)\,Q(z)$ for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(4N)$. $(\theta(z) = \sum_{n\in\mathbb{Z}} q^{n^2})$.
2. f is holomorphic at the cusps.

$S_{3/2}(N,\chi)$ denotes the subspace of non trivial cusp forms.
Trivial cusp form: $\sum_{n\in\mathbb{Z}} n\psi(n)q^{tn^2}$ (t fixed positive integer, ψ a periodic function)

Example

For $\lambda \equiv 15 \bmod 24$: $\frac{\eta(3\tau)\,\eta(12\tau)\,\eta(2\lambda\tau)^3}{\eta(6\tau)\,\eta(\lambda\tau)\,\eta(4\lambda\tau)}\theta(z) \in S_{3/2}\left(3\lambda, \left(\frac{3\lambda}{\cdot}\right)\right)$

Arithmetic significance

Theorem (Shimura, Niwa)

For each squarefree integer t there is a Hecke equivariant map $S_t : S_{3/2}(N, \chi) \to S_2(2N, \chi^2)$.

Remark

There is a *theta kernel* $\theta_t \in M_{3/2}^{\mathrm{alc}}(N, \chi) \otimes \overline{M_2^{\mathrm{alc}}(2N, \chi^2)}$ such that $S_t(F)(z) = \langle F, \theta_{t,\chi}(., z)\rangle$.

Main Property (Waldspurger's theorem)

Let f in $M_2(2N, \chi^2)$ be the Shimura lift of F, both Hecke eigenforms. Then, for every squarefree t, one has

$$\frac{|a_F(t)|^2}{\langle F, F\rangle} = \mathrm{const}(N)\sqrt{t}\,\frac{L(f \otimes \chi_{\mathbb{Q}(\sqrt{-t})}, 1)}{\langle f, f\rangle}.$$

Current implementations

Naive algorithm

For computing the (subspace of) eigenforms in $S_{3/2}(N, \chi)$ lifting to a given Hecke eigenform in $S_2(2N, \chi^2)$:

1. Choose a modular form of weight $1/2$ (e.g. Hecke's θ).
2. Compute a basis for $M_2(4N, \chi)$.
3. Determine the image of the maps $\times\theta : S_{3/2}(N, \chi) \to M_2(4N, \chi)$ (i.e. determine the forms which are divisible by θ).
4. Divide the forms of a basis of the image by θ for obtaining a basis for $S_{3/2}(N, \chi)$.
5. Proceed with standard linear algebra on this basis to determine the desired eigenspace.

Remark

There is a variant to minimize the computational effort in 3. (Basmaji).

A different approach: the final result

Theorem

Set

$$C(2N) = \ker\Big((\mathbb{C}[\mathbb{P}^1(\mathbb{Q})]^0)_{\Gamma_0(2N)} \to (\mathbb{C}[\mathbb{P}^1(\mathbb{Q})])_{\Gamma_0(2N)} \Big).$$

Let χ be a quadratic Dirichlet character modulo $4N$. For every positive squarefree integer t, the application

$$[c] \mapsto \sum_{\substack{a,b,c\in\mathbb{Z} \\ t\mid Nb^2-ac>0}} \Big(\sum_{[x:y]\in\mathbb{P}^1(\mathbb{Q})} c([x:y])\,\mathrm{sign}(aNx^2+2Nbxy+cy^2)\Big) \cdot \chi(a)\left(\frac{-4t}{a}\right) q^{(Nb^2-ac)/t} + \sum_{\delta\mid 4Nt}\sum_{n\in\mathbb{Z}} * q^{\delta n^2}.$$

defines a Hecke equivariant map $L_t : C(2N) \to S_{3/2}(N,\chi)$. The images of the L_t span $S_{3/2}(N,\chi)$.

A different approach: the idea

The ansatz

- Consider the composition of the maps

$$S_{3/2}(N,\chi\cdot) \xrightarrow{S_t} M_2(N) \xrightarrow{B} \mathrm{Hom}_{\mathbb{Z}[\Gamma_0(N)]}\left(\mathbb{Z}[\mathbb{P}^1(\mathbb{Q})]^0, \mathbb{C}\right),$$

- and dualize, to obtain a Hecke equivariant map

$$L_t : \left(\mathbb{C}[\mathbb{P}^1(\mathbb{Q})]^0\right)_{\Gamma_0(2N)} \to S_{3/2}(N,\chi\cdot)^* \cong S_{3/2}(N,\chi\left(\tfrac{4N}{\cdot}\right)).$$

- One has

$$L_t([c]) \equiv W_{4N}\iota \int_c \overline{\theta_{t,\chi}(\cdot,z)}\,dz \bmod M_{3/2}^{\mathrm{Eis\&triv}}(N,\chi\left(\tfrac{4N}{\cdot}\right)).$$

The essential step

Conclusion

Conclusion

Summary

- We showed how to compute closed formulas for modular forms of integral and half integral weight by hand (at least for small levels).
- The challenge is to develop algorithms to find rapidly super solutions (Hecke eigenforms), if possible in closed form.
- We indicated that it is possible to compute directly the Shimura inverse half integral weight forms corresponding to a given Hecke eigenform (without generating the whole space to search for the needles in the haystack).

Material

At `data.countnumber.de/ANTS-X` you can download

- Articles containing (parts of) the ideas presented here.
- An N-board generator for N-riddles for computing modular forms by hand.

...

Thank you.