Constructing modular forms as Sudoku for number theorists

Nils Skoruppa

Universität Siegen and Tongji University

November 13, 2015

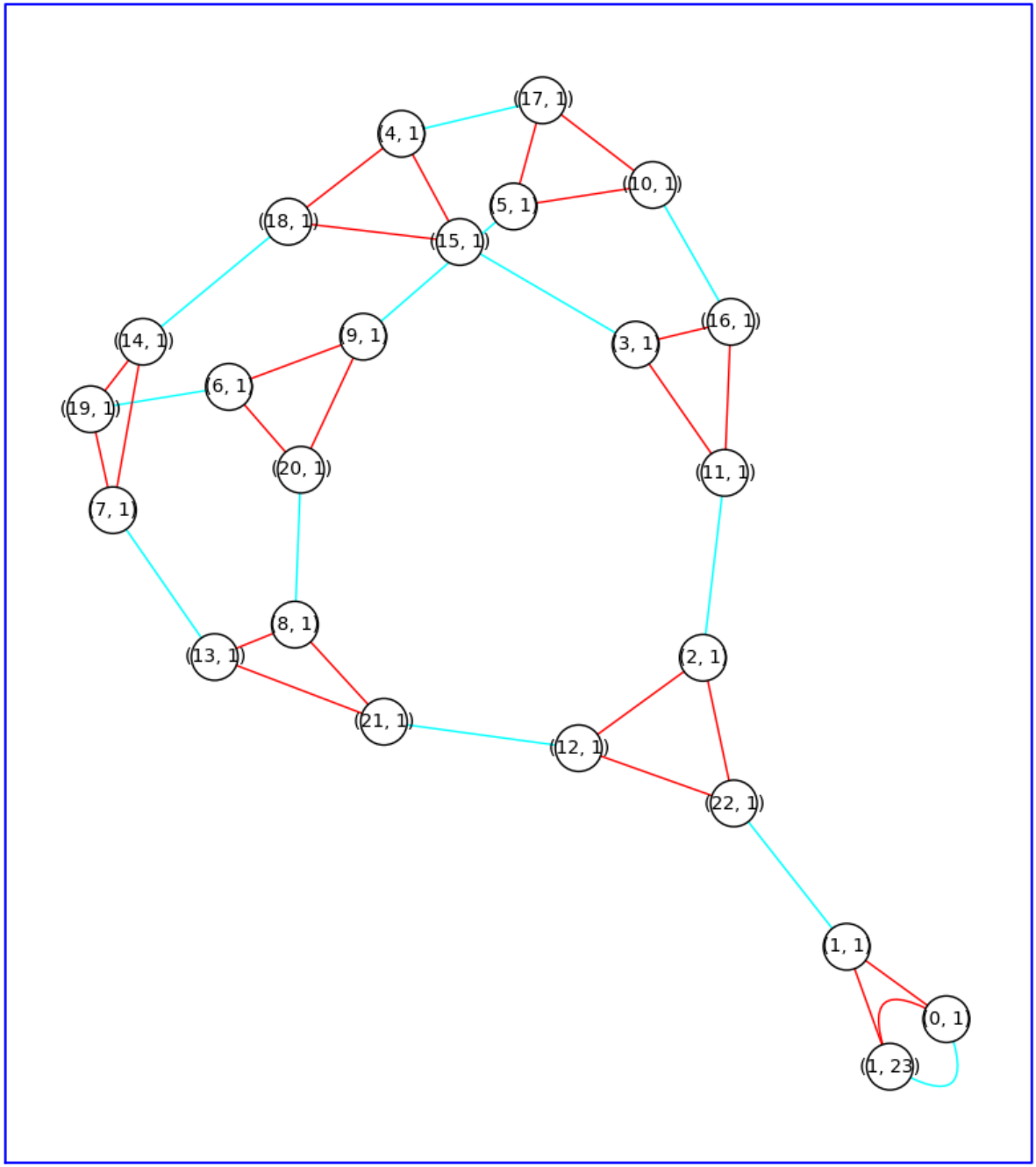
Seminar

Waseda University

The game

Assign numbers to the vertices so that:

- Numbers connected by a blue line sum to zero.
- Numbers at the vertices of a red triangle sum to zero.



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 and, in particular, simplifications though.
- Indications concerning the theoretical background.
- Proposals how to extend/modify the current implementations.
- Some additional remarks on "Sudoka boards".

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).
- $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $R = ST = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$ $(S^2 = R^3 = -1)$.

Definition (The N-board)

The N-board is a colored graph:

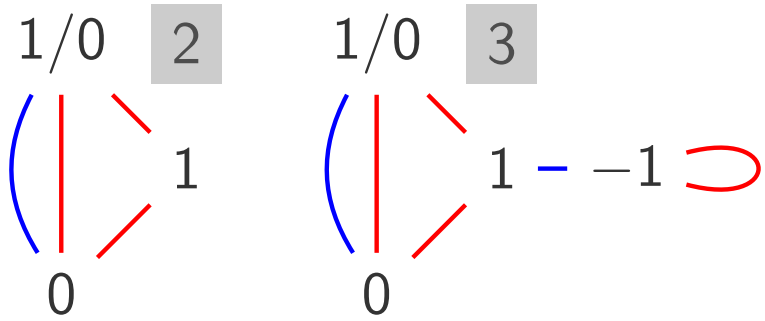
- Vertices: the points of $\mathbb{P}^1(\mathbb{Z}/N)$.
- Connect p and q by a blue edge if $p = qS$.
- Connect p and q by a red edge if $p = qR$ or $p = qR^2$.

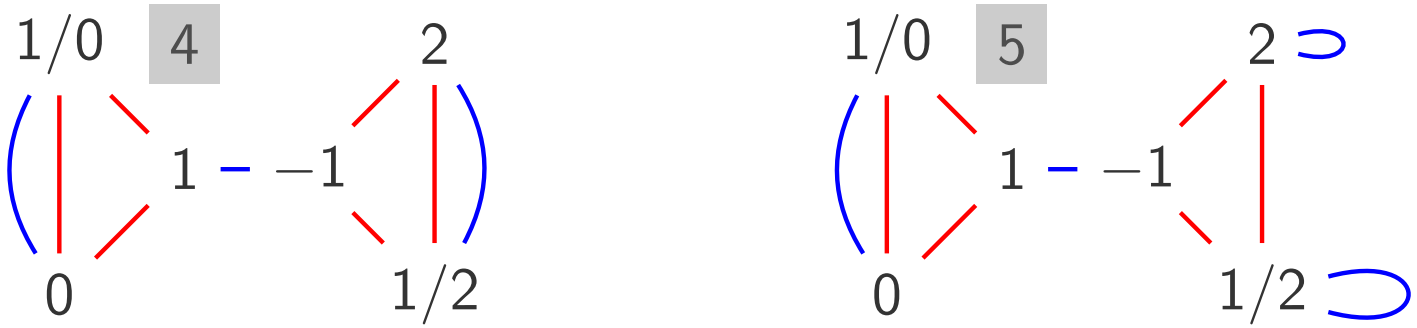
The game (or labeling Schreier coset graphs)

Recall

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

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



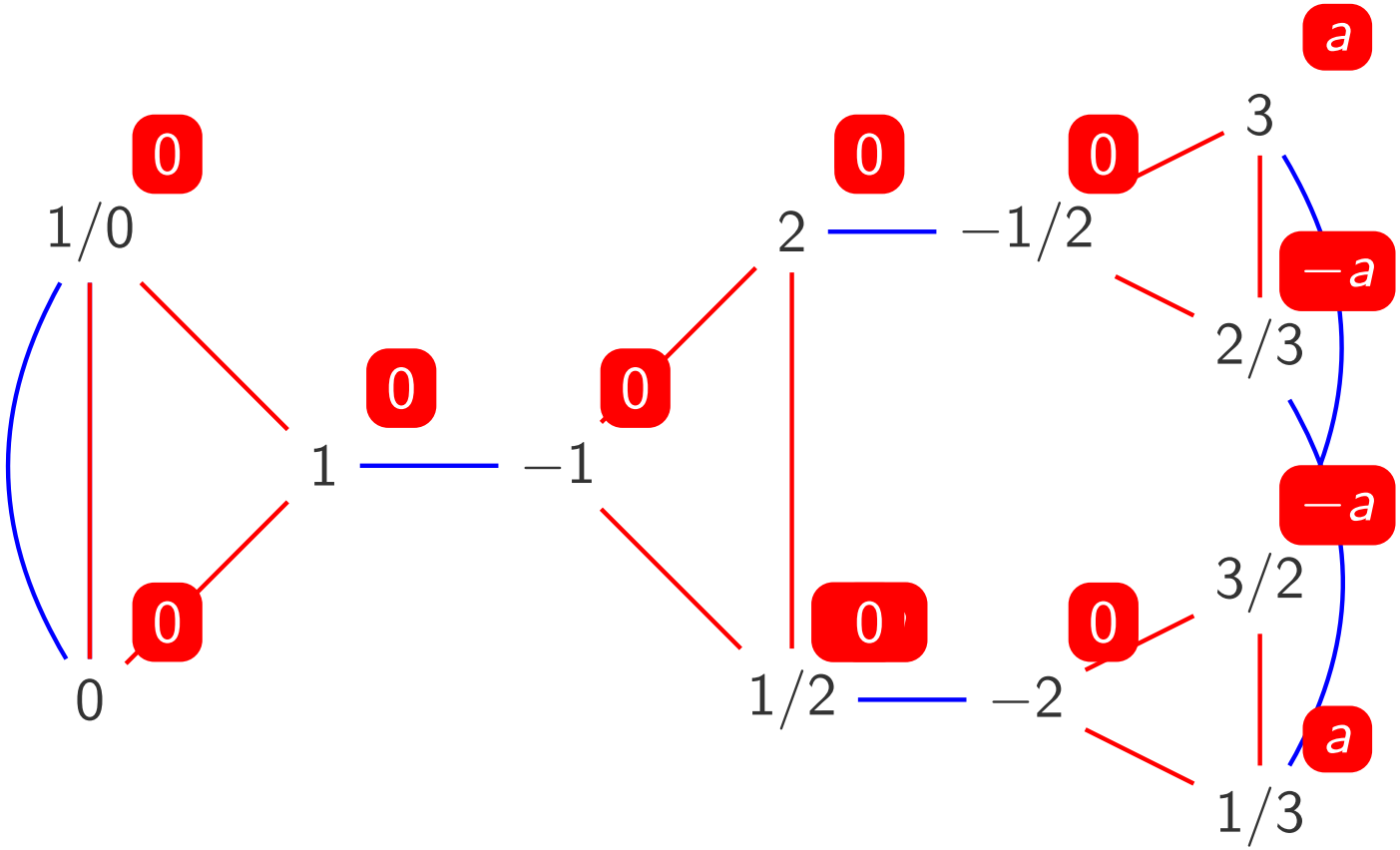


Problem (The N-riddle)

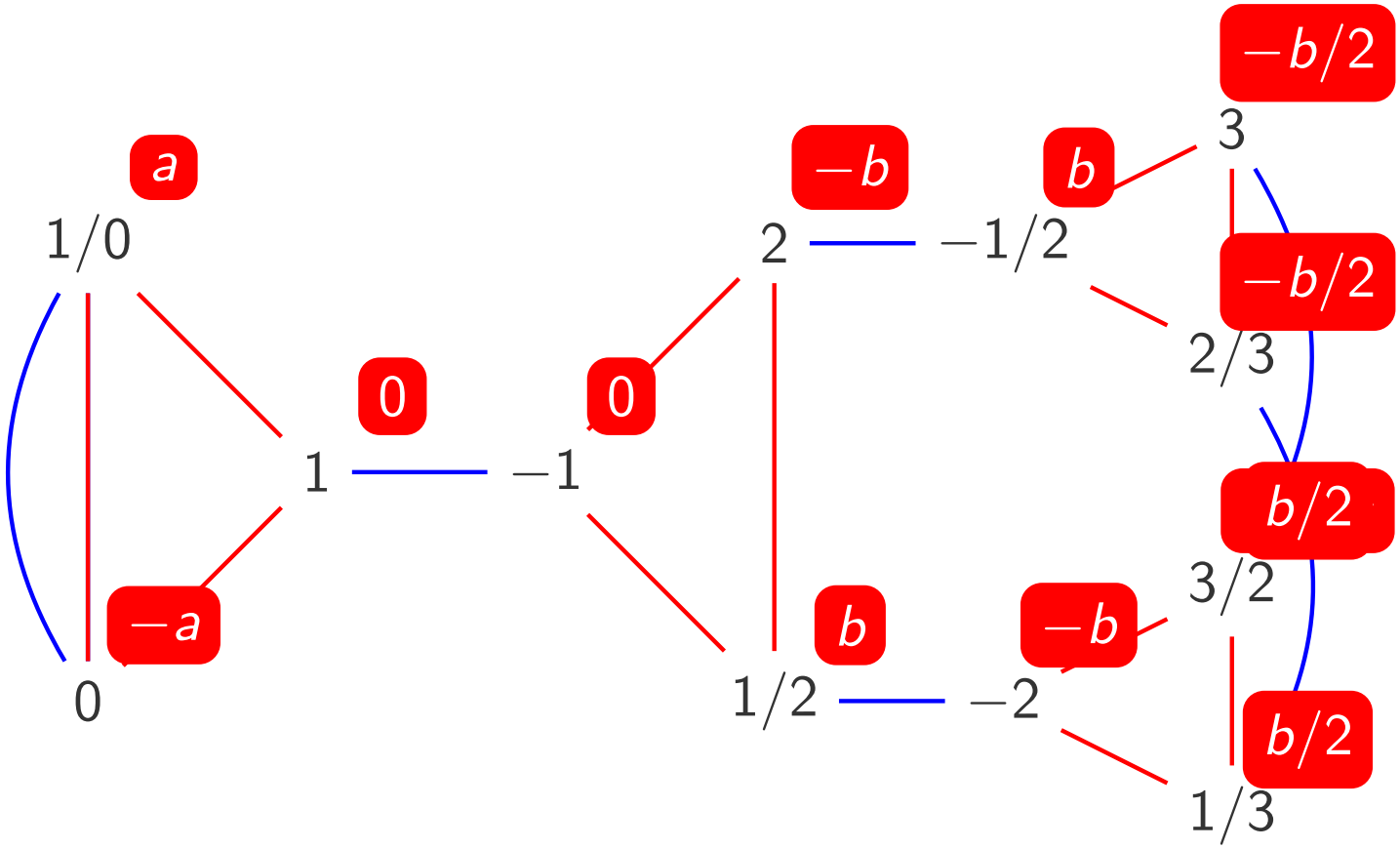
Assign labels (integers) to the vertices such that:

1. *The sum of labels connected by a blue edge is* 0.
2. *The sum of labels along a red triangle is* 0.

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*

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

  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 $T(l)$ $(l = 1, 2, 3, \dots)$, where $T(l)f := \sum_{l \geq 0} \left[\sum_{d \mid l, n,\ \gcd(d,N)=1} d\, a_f(ln/d^2) \right] q^n.$

Remark (Magical equation)

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

The super riddle

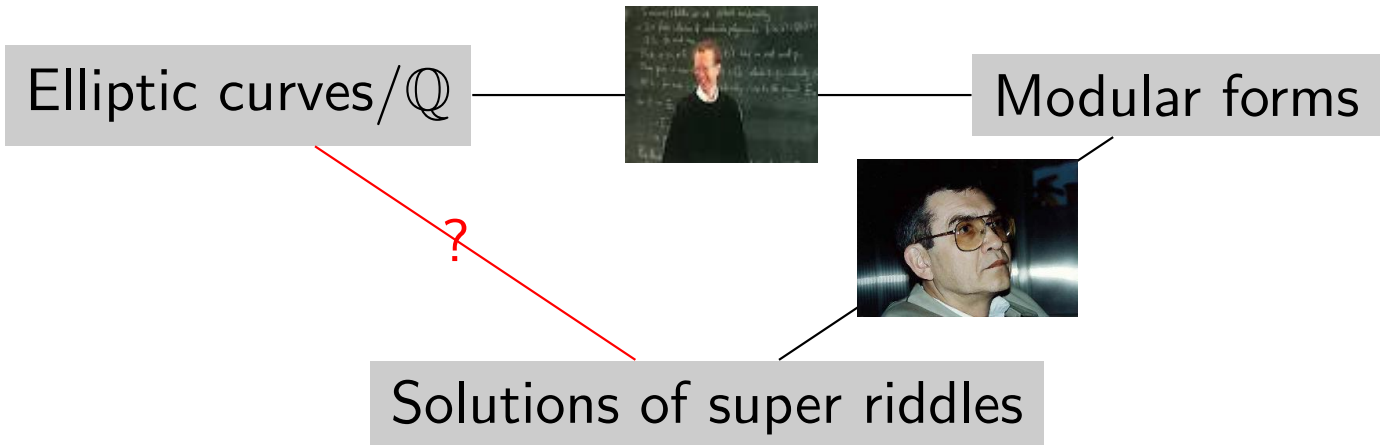
Problem (Super solutions)

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:

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

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 $T(I)$ for I 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 $\operatorname{rank} \mathcal{L}(11)^+ = 2$, $\operatorname{rank} \mathcal{L}(11)^- = 1$. One even super solution is $\infty \mapsto 1$, $0 \mapsto -1$. Resulting formula:

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

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

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

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

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

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

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).

Some remarks on Schreier coset graphs

Schreier coset graphs

Definition

The *Schreier coset graph of a subgroup* Γ *of finite index in* $\mathrm{SL}(2,\mathbb{Z})$ is the following directed multigraph $G_\Gamma = (V_\Gamma, F_\Gamma)$:

- The set of vertices is $V_\Gamma = \Gamma \backslash \mathrm{SL}(2,\mathbb{Z})$.
- The set of edges is the set E_Γ of pairs (x, S) and (x, R), where x runs through the set of vertices.
- $F = F_\Gamma = (t, h) : E_\Gamma \to V_\Gamma \times V_\Gamma$ is given by

$$F(x, S) = (x, xS), \quad F(x, R) = (x, xR).$$

Examples

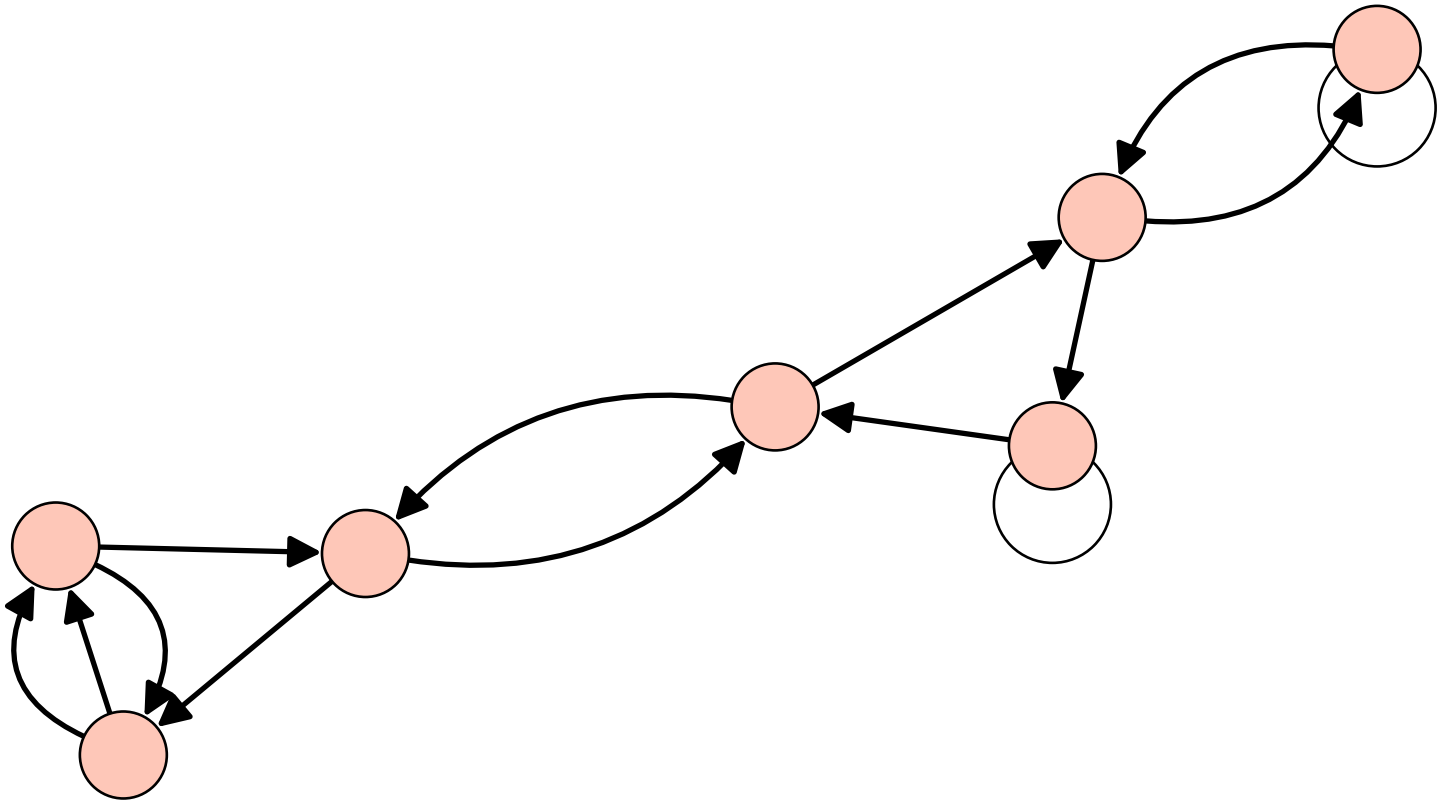


Figure: The Schreier coset graph of a non-congruence subgroup Γ_7 (of smallest possible index 7).

Examples (cont.)

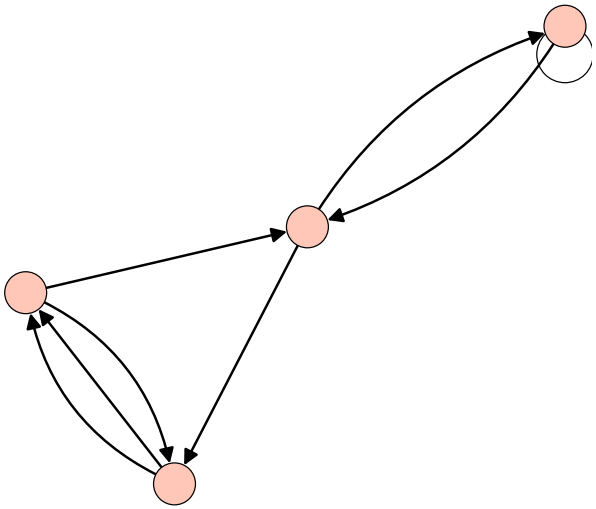


Figure: $\Gamma_0(3)$)

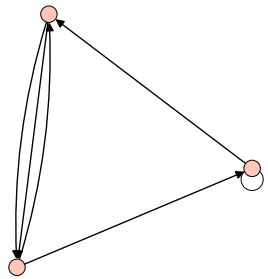


Figure: $\Gamma_0(2)$

How to reconstruct a group from its SCG

Proposition

The Schreier coset graph determines the subgroup Γ *(up to conjugacy).*

Proof.

$$\Gamma = \text{set of closed paths starting and ending in } \Gamma.$$

A closed path has to be read as a word in S and R. □

The zeta function of a SCG

Definition

$$Z(\Gamma, u) = \exp\left(\sum_{n\geq 1} \frac{N_n}{n} u^n\right),$$

where N_n denotes the number of closed paths of length n (say, starting and ending in Γ).

Facts

- $Z(\Gamma, u) = f_\Gamma(u)^{-1}$ for some polynomial f_Γ with integer coefficients.
- One has

$$Z(\Gamma, u) = \prod_{\mathfrak{p}} (1 - u^{|\mathfrak{p}|})^{-1},$$

where $\mathfrak{p}$ runs through all prime cycles of G_Γ.

N	$Z(\Gamma_0(N), u)^{-1}$
1	$(2u-1)$
2	$(-1)(u+1)(2u-1)$
3	$(2u-1)(2u^3+u^2-u-1)$
5	$(2u-1)(2u^5-u^4+u^3+2u^2-1)$
7	$(2u-1)(2u^7+u^6-5u^5-6u^4+3u^3+4u^2-1)$
11	$(2u-1)(2u^{11}+u^{10}-3u^9+7u^7-7u^6-14u^5+2u^4+11u^3+3u^2-2u-1)$
$\vdots$	$\vdots$

Table: Zeta functions of $\Gamma_o(N)$

. . .

Thank you.