A Gentle Introduction to the Langlands Program

Jeremy Booher, University of Canterbury

Popular Account:
'Amazing' Math Bridge Extended Beyond Fermat's Last Theorem"
in Quanta Magazine

Example: $f(q) = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2 = \sum a_n(f)q^n = q - 2q^2 - q^3 + \dots$

n	2	3	5	7	11	13	17	19	23	29	31	37	41	
$a_n(f)$	−2	−1	1	−2	1	4	−2	0	−1	0	7	3	−8	…

$E: \; y^2 + y = x^3 - x \quad \bigstar \qquad a_p(E) = p - \#\text{solutions to } \bigstar \bmod p.$

p	2	3	5	7	11	13	17	19	23	29	31	37	41	
$a_p(E)$	−2	−1	1	−2	−5	4	−2	0	−1	0	7	3	−8	…

Observe: $a_p(f) = a_p(E) \quad (p \neq 11) \qquad a_p(f) \equiv p+1 \bmod 5$

Topics

I Modular Forms ~ Complex analysis

II Elliptic Curves

III Galois Representations - Galois theory

Limitations:

- Can't be technical
- Won't give exhaustive overview of current developments.
- ignoring Langlands and L-functions

Logistics: Slides available via link on my University of Canterbury homepage:

math.canterbury.ac.nz/~j.booher

and on conference site?

Modular Forms

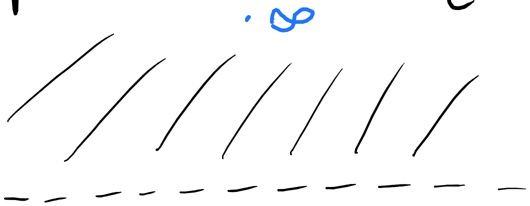
References: Serre: A Course in Arithmetic Chapter VII

Diamond + Shurman: A First Course in Modular Forms

"There are five elementary arithmetical operations: addition, subtraction, multiplication, division, and ... modular forms"

– Martin Eichler?

Upper Half Plane: $\mathcal{H} = \{ z \in \mathbb{C} : \operatorname{Im}(z) > 0 \}$ ↺ $SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \begin{array}{l} ad-bc=1 \\ a,b,c,d \in \mathbb{Z} \end{array} \right\}$



$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}$$

$\boxed{\text{Fractional Linear Transformations}}$

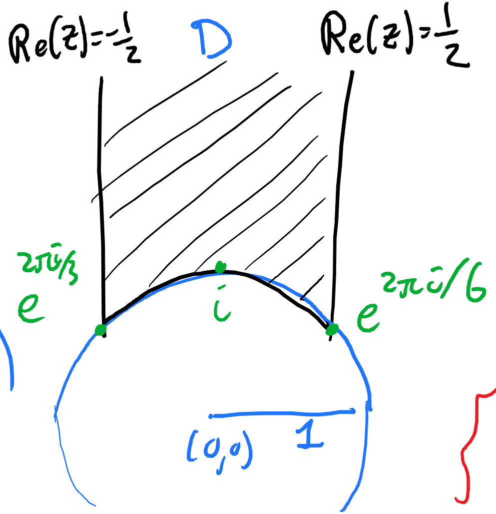
Definition: A function $f: \mathcal{H} \to \mathbb{C}$ is weakly modular of weight k with respect to $\Gamma \subset SL_2(\mathbb{Z})$ if

$$\star \quad f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} . z\right) = f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z) \quad \text{for } z \in \mathcal{H},\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma.$$

Example: $\Gamma = SL_2(\mathbb{Z})$

$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ $\quad f(z+1) = f(z)$

$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ $\quad f\left(-\frac{1}{z}\right) = z^k f(z)$

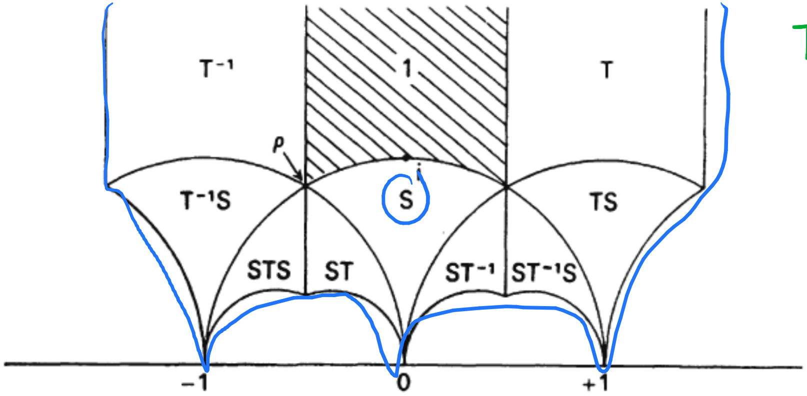


D fundamental domain

every orbit of $SL_2(\mathbb{Z})$ on $\mathcal{H}$ intersects D exactly once*

$k=0$: function on $\mathcal{H}/\Gamma$

$k=2$: modular form on $\mathcal{H}/\Gamma$



$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

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

Observe: a weakly modular function of weight k is determined by restriction to fundamental domain.

Example: $\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \underset{c \equiv 0 \bmod N}{} \right\}$

"level N"

More generally: Γ finite index in $SL_2(\mathbb{Z})$

fundamental domain built out of copies of D

$\gamma_i D$ $\quad$ γ_i coset reps for Γ in $SL_2(\mathbb{Z})$

Important Definition:

A <u>modular form</u> of weight k with respect to $\Gamma \subset SL_2(\mathbb{Z})$ is

$f: \mathcal{H} \to \mathbb{C}$ such that

1) f weakly modular of weight k with respect to Γ

$$f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} . z\right) = (cz+d)^k f(z)$$

2) holomorphic on $\mathcal{H}$

3) holomorphic "at infinity"

It is a <u>cusp form</u> if it vanishes "at infinity".

Warning: ignoring detail that there may be multiple cusps "at infinity"

How to Describe a Modular Form: q-Series

Example: $\boxed{q = e^{2\pi i z}}$

$$f(z) = q \prod_{n=1}^{\infty} (1-q^n)^2 (1-q^{11n})^2 \quad \text{is a modular form}$$

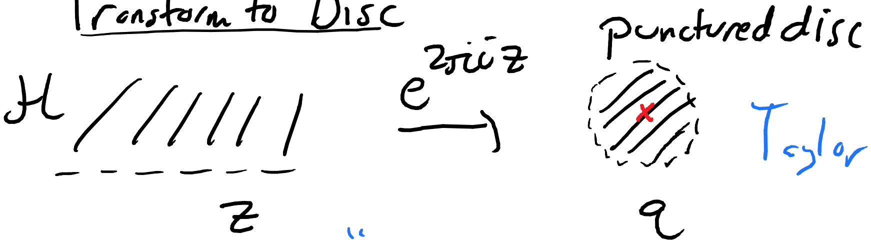
$$= \underline{q - 2q^2 - q^3 + 2q^4 + 2q^6 + \dots} = e^{2\pi i z} - 2e^{4\pi i z} - e^{6\pi i z} + \dots$$

Fourier Series

$$\boxed{f(z) = f(z+1)}$$

$$q^n = e^{2\pi i n z} = \cos(2\pi n z) + i \sin(2\pi n z)$$

Transform to Disc



Taylor.

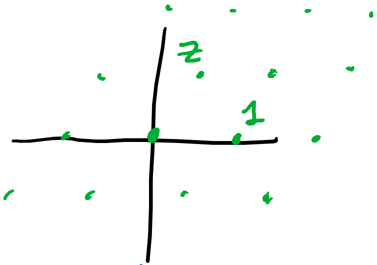
"∞" $\rightarrow$ 0

cusp form: no constat term.

Examples of Modular Forms

A) Eisenstein Series:

Definition: $G_k(z) = \sum'_{m,n\in\mathbb{Z}} \frac{1}{(mz+n)^k}$. $\boxed{k \geq 4}$ even.



lattice

Modular Form weight k for $SL_2(\mathbb{Z})$: how transform?

interpret $\underline{G_k\left(\frac{az+b}{cz+d}\right)}$ summing over $\mathrm{span}_{\mathbb{Z}}(az+b, cz+d)$

$= \mathrm{span}_{\mathbb{Z}}(1, z)$

q-expansion: $G_k(z) = (*) + (*)\sum_{n=1}^{\infty}\Big(\underbrace{\sum_{d|n} d^{k-1}}_{\sigma_{k-1}(n)}\Big)q^n$

not cusp form

$$2\zeta(k) + \frac{2\cdot(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}\sigma_{k-1}(n)\,q^n$$

Variants of Eisenstein Series:

Weight 2: $G_2(z) = \sum_{m,n \in \mathbb{Z}} \frac{1}{(mz+n)^2}$ Conditionally convergent not modular form.

Pick N

$$G_{2,N}(z) = G_2(z) - N\, G_2(Nz)$$ modular of weight 2 for $\Gamma_0(N)$

Note:

$$G_2\left(N \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z\right)$$

$$= G_2\left(\frac{aNz + Nb}{cz+d}\right)$$

$$= G_2\left(\begin{pmatrix} a & bN \\ c/N & d \end{pmatrix} (Nz)\right)$$

Example: $G_{2,4}(z) = -\pi^2\left(1 + 8 \sum_{n=1}^{\infty} \left(\sum_{\substack{d \mid n \\ 4 \nmid d}} d \right) q^n\right)$

weight 2 for $\Gamma_0(4)$

B) Dedekind Eta Function

$$\eta(z) = e^{2\pi i z/24} \prod_{n=1}^{\infty} \left(1 - e^{2\pi i z n}\right) = q^{1/24} \prod_{n=1}^{\infty} (1-q^n)$$

Compute: $\eta(z+1) = e^{2\pi i/24}\, \eta(z)$

$\eta(-1/z) = \sqrt{-iz}\, \eta(z)$ } not modular close

1) $\boxed{\Delta(z) = \eta(z)^{24}}$

weight 12 for $SL_2(\mathbb{Z})$

$$\Delta(z) = q \prod_{n=1}^{\infty} (1-q^n)^{24} = \sum_{n \geq 1} \tau(n)\, q^n$$

Ramanujan τ function.

initial example

2) $\boxed{f(z) = \eta(z)^2 \eta(11z)^2}$

$$= q \prod (1-q^n)^2 (1-q^{11n})^2$$

weight 2 for $\Gamma_0(11)$

c) Theta Function

$$\Theta_4(z) = \sum_{v \in \mathbb{Z}^4} q^{\|v\|^2} = \sum_{n \geq 0} r_4(n) q^n$$

Can use other lattices or quadratic forms

$r_4(n) =$ # ways to write n as sum of 4 squares

1) $\Theta_4(z) = \Theta_4(z+1)$ ✓

2) $\Theta_4\left(-\frac{1}{4z}\right) = (4z+1)^2 \Theta_4(z)$

Poisson Summation

Conclusion: $\Theta_4(z)$ modular of wt 2 for $\Gamma_0(4)$

Application: Use mod. forms to study representing ints as sum of 4 squares.

Key Idea about Modular Forms for Today:

The vector space of modular forms of weight k for $\Gamma_0(N)$ is finite dimensional, and its dimension is computable.

Application: Modular forms of weight 8 for $SL_2(\mathbb{Z})$ is one dimensional.

Eisenstein Series $G_8(z) = (\cancel{*}) + (*) \sum_{n=1}^{\infty} \sigma_7(n) q^n$ is an example.

Another Example: $\left[G_4(z)\right)^2 = \left[(*) + (*)\sum_{n=1}^{\infty} \sigma_3(n) q^n\right]^2 \Big)$

$$\sigma_m(n) = \sum_{d \mid n} d^m$$

Conclusion: $\sigma_3(n) + 120 \sum_{m=1}^{n-1} \sigma_3(m)\sigma_3(n-m) = \sigma_7(n)$

Key Idea about Modular Forms for Today:

The vector space of modular forms of weight k for $\Gamma_0(N)$ is finite dimensional, and its dimension is computable.

Application: Modular Forms of weight 2 for $\Gamma_0(4)$ is two dimensional

$$\left.\begin{aligned} -\frac{3}{\pi^2} G_{2,2}(z) &= 1 + 24q + \cdots \\ -\frac{1}{\pi^2} G_{2,4}(z) &= 1 + 8q + \cdots \end{aligned}\right\} \text{basis}$$

Theta function $\Theta_4(z) = 1 + 8q + \cdots$

Conclusion: $r_4(n) = 8 \sum_{\substack{d \mid n \\ 4 \nmid d}} (d)$

$G_{2,N}(z) =$

$G_2(z) - N\,G_2(Nz)$

$= (*) + (*) \sum_{n=1}^{\infty} \Big(\sum_{\substack{0<d \mid n \\ N \nmid d}} d \Big) q^n$

$\Theta_4(z) = \sum_{n=1}^{\infty} r_4(n) q^n$

Key Idea about Modular Forms for Today:

The vector space of modular forms of weight k for $\Gamma_0(N)$ is finite dimensional, and its dimension is computable.

Sketchy Application: Cusp forms of weight 2 for $\Gamma_0(11)$ is one dim.

Example: $f(z) = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2 = \sum_{n\geq 1} a_n(f)q^n$.

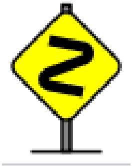
Non-Example: $\dfrac{G_{2,11}(z)}{2\zeta(2)} = \dfrac{5}{12} + \sum_{n=1}^{\infty}\left(\sum_{\substack{0<d\mid n \\ 11\nmid d}} d\right)q^n$

not cusp form

$$f(z) = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2 = \sum_{n\geq 1} a_n(f)\, q^n. = q-2q^2-q^3+\dots$$

$$g(z) := \frac{G_{2,11}(z)}{2\zeta(2)} = \frac{5}{12} + \sum_{n=1}^{\infty}\Big(\sum_{\substack{0<d\mid n \\ 11\nmid d}} d\Big)\, q^n = \frac{5}{12} + q + 3q^2 + 4q^3 + \dots$$

(weight 2 for $\Gamma_0(11)$)



Modulo 5, $g(z)$ is a cusp form. Compare coefficients:

$$f(z) \equiv g(z) \mod 5.$$

Conclusion: $a_p(f) \equiv \underbrace{p+1}_{q\text{-expansion for } g(z)} \mod 5 \qquad p \nmid 11.$

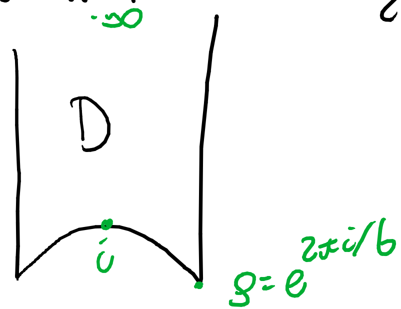
Computing Dimensions of Spaces of Modular Forms

Reminders: 1) When integrating a meromorphic function over a closed contour, can evaluate integral using residues.

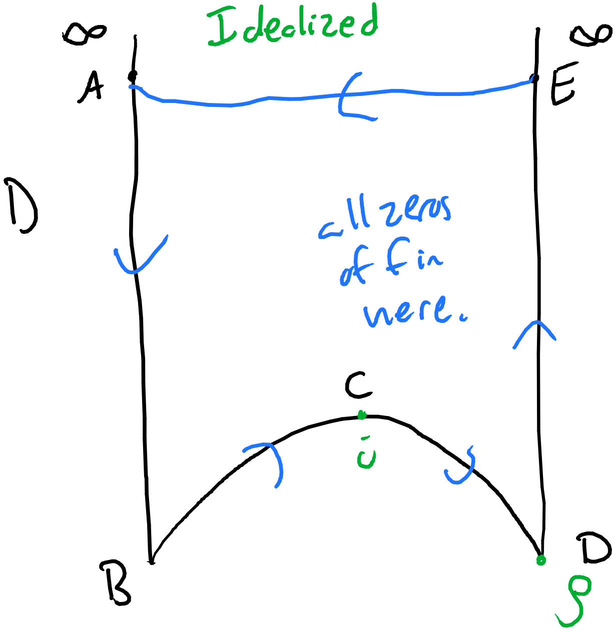
2) $\frac{f'(z)}{f(z)}$ has simple pole of residue $\mathrm{ord}_p(f)$ if p is zero/pole of f.

$\frac{n z^{n-1}}{z^n}$

Sketch for $\Gamma = SL_2(\mathbb{Z})$, k even > 2. f modular form



Claim: $\mathrm{ord}_\infty(f)$ is bounded



Compute $\frac{1}{2\pi i}\int \frac{f'(z)}{f(z)}\,dz$ = sum of residues for $f'(z)/f(z)$ = sum of orders of zeros

Cancel using symmetry: AB, DE

$f(z) = f(z+1)$

BC, CD $\quad f\left(\frac{-1}{z}\right) = z^k f(z)$: leave $k/12$

AE : $-\mathrm{ord}_\infty(f)$

Issues: zero at i, ρ

zero elsewhere on boundary : need to modify contour

f holomorphic as modular form.

Idealized $\frac{1}{2\pi i}\int \frac{f'(z)}{f(z)}\,dz$ gives: $\mathrm{ord}_\infty(f) + \sum_{p\in D} \mathrm{ord}_p(f) = k/12$

Correct Conclusion: $\mathrm{ord}_\infty(f) + \frac{1}{2}\mathrm{ord}_i(f) + \frac{1}{3}\mathrm{ord}_\rho(f) + \sum_{p\neq i,\rho} \mathrm{ord}_p(f) = k/12$

Corollary: $\mathrm{ord}_\infty(f) \leq k/12$

Corollary: If two modular forms of weight k for $SL_2(\mathbb{Z})$ have q-expansions which begin the same (up to $q^{k/12}$ term), they're same.

Corollary: Modular Forms of weight k for $SL_2(\mathbb{Z})$ are finite dimensional.