Modular Forms & Their Applications

From Sums of Squares to Modularity

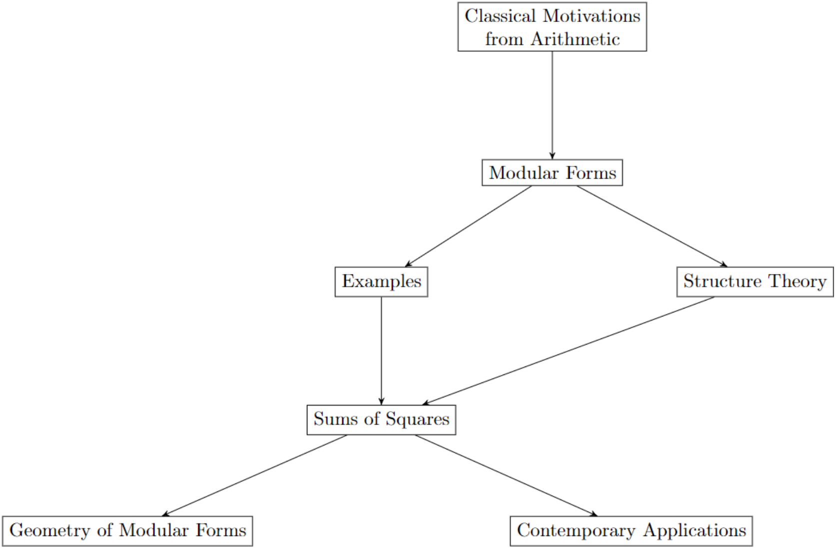
Joseph R. Heavner

University of Maryland

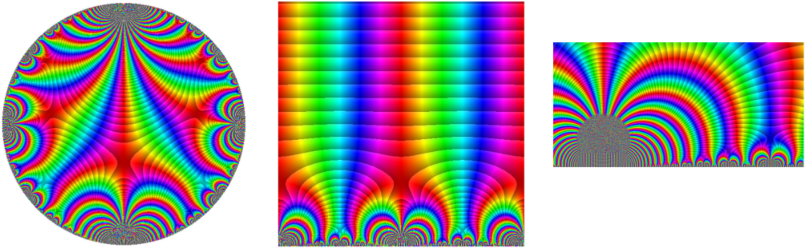
jheavner@umd.edu

December 2023

Overview


Classical Motivations from Arithmetic
Modular Forms
Examples
Structure Theory
Sums of Squares
Geometry of Modular Forms
Contemporary Applications

The Δ Modular Form



Courtesy of David Lowry-Duda (arXiv:2002.05234 [cs.GR]).

Color represents phase while contours express magnitude.

Sums of Squares

Theorem (Fermat's Sum of Two Squares Theorem)

Let $n > 1$ be an integer. Then, there exist integers a and b so that $n = a^2 + b^2$ if and only if n contains no factor of the form p^{2k+1} where $p = 3 \mod 4$ in its prime decomposition where k is odd.

The following is our goal for the first part of this talk.

Theorem (Lagrange's Four-Square Theorem)

Every natural number n can be written as a sum of four squares:

$$n = a^2 + b^2 + c^2 + d^2 \quad \text{for some } a, b, c, d \in \mathbb{N}.$$

Our First q-Series

We can rephrase such problems with a kind of *generating function*.

Definition

Let $q \in \mathbb{C}$ with $|q| < 1$. Then, define the **Jacobi θ function** as

$$\theta(q) := \sum_{n \in \mathbb{Z}} q^{n^2} = 1 + 2q + 2q^4 + 2q^9 + \cdots .$$

Definition

Let $k \in \mathbb{Z}_+$. Define the **sum of squares function** by

$$r_k(n) := \left| \left\{ (a_1, a_2, \ldots, a_k) \subset \mathbb{Z}^k : \sum_{j=1}^{k} a_j^2 = n \right\} \right| .$$

Jacobi's Theorem on Sums of Four Squares

Lemma (Euler, 1750)

For k a positive integer,

$$\theta(q)^k = \sum_{n=0}^{\infty} r_k(n) q^n.$$

From this viewpoint, we prove a sharper result than Lagrange.

Theorem (Jacobi's Four-Square Theorem, 1834)

Let $n \in \mathbb{N}$. Then,

$$r_4(n) = 8 \sum_{\substack{d \mid n \\ d \not\equiv 0 \bmod 4}} d.$$

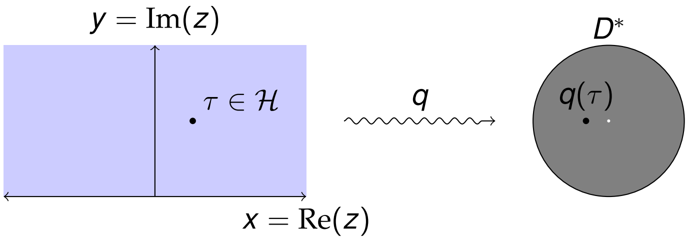
Some Notation from Analysis

Definition

The set $\mathcal{H} := \{z \in \mathbb{C} \colon \mathrm{Im}(z) > 0\}$ is called the **upper half plane**.

Lemma

Let $D^* := \{z \in \mathbb{C} \colon |z| < 1\} \setminus \{0\}$ be the punctured unit disk. The map $q : \mathcal{H} \to D^*$ given by $q(\tau) = e^{2\pi i \tau}$ is a holomorphic surjection.



Action on the Upper Half Plane

Definition

The **modular group** is the following set under matrix multiplication

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc = 1 \text{ and } a, b, c, d \in \mathbb{Z} \right\}.$$

Theorem

The modular group is generated by $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ & $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.
Moreover, $\mathrm{SL}_2(\mathbb{Z})$ *acts on* $\mathcal{H}$ *by fractional linear transformations*

$$\mathrm{SL}_2(\mathbb{Z}) \times \mathcal{H} \to \mathcal{H} \text{ by } \gamma\tau \mapsto \frac{a\tau + b}{c\tau + d} \quad \text{where } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Recall Riemann's zeta function $\zeta(s) := \sum_{n=1}^{\infty} n^{-s}$. Consider:

Eisenstein Series

For $\tau \in \mathcal{H}$, the **Eisenstein series of weight** k is

$$G_k(\tau) := \sum_{\substack{(m,n)\neq(0,0) \\ (m,n)\in\mathbb{Z}^2}} (m\tau + n)^{-k}.$$

Theorem

Let $k \geq 4$ be an even integer. Let B_k be the k^{th} ***Bernoulli number*** *and let $\sigma_k(n) = \sum_{d|n} d^k$ be the* ***sum of divisors function****. Then,*

$$E_k(\tau) := \frac{G_k(\tau)}{2\zeta(k)} = 1 - \frac{2k}{B_k} \sum_{k=1}^{\infty} \sigma_{k-1}(n) q^n.$$

Definition

Let k be an integer. A *holomorphic* function $f : \mathcal{H} \to \mathbb{C}$ is called a **modular form of weight** k **for** $\mathrm{SL}_2(\mathbb{Z})$ provided:

1. For all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, f satisfies the **weight** k **modularity condition**

$$f(\gamma\tau) = (c\tau + d)^k f(\tau) \quad \forall \tau \in \mathcal{H},$$

   which is equivalent to the conditions that

$$f(\tau + 1) = f(\tau) \quad \text{and} \quad f\left(-\frac{1}{\tau}\right) = \tau^k f(\tau) \quad \forall \tau \in \mathcal{H};$$

2. The function is holomorphic at ∞, i.e., $\lim_{\mathrm{Im}\,\tau \to \infty} f(\tau)$ exists.

Theorem

For each even $k \geq 4$, the Eisenstein series $G_k(\tau)$ is a modular form of weight k for $\mathrm{SL}_2(\mathbb{Z})$.

Theorem

*Every modular form has a q-**expansion (or Fourier expansion)***

$$f(\tau) = g(q(\tau)) = \sum_{n=0}^{\infty} a_n q^n = \sum_{n=0}^{\infty} a_n \left(e^{2\pi i \tau}\right)^n \quad \text{for } q \in D.$$

*If a modular form has 0 as the constant term in its Fourier expansion, then it is called a **cusp form**.*

Theorem

1. *The space $M_k(\mathrm{SL}_2(\mathbb{Z}))$ of all weight k modular forms is a $\mathbb{C}$-vector space. The space of cusp forms $S_k(\mathrm{SL}_2(\mathbb{Z}))$ is a subspace.*
2. *The spaces $M(\mathrm{SL}_2(\mathbb{Z}))$ and $S(\mathrm{SL}_2(\mathbb{Z}))$ of <u>all</u> modular and <u>all</u> cusp forms, respectively, are graded rings.*

Examples of Modular Forms

The archetypal example of a modular form is the Eisenstein series.

Examples of Modular Forms

1. For <u>all</u> weights k, 0 is a modular form of weight k.
2. For weight zero, the constant functions are modular forms.
3. The j**-invariant** $j(\tau) := 1728\frac{E_4(\tau)^3}{E_4(\tau)^3 - E_6(\tau)^2}$ is a modular *function* of weight zero for $\mathrm{SL}_2(\mathbb{Z})$.
4. The **Dedekind eta function**

$$\eta(\tau) := q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1 - q^n)$$

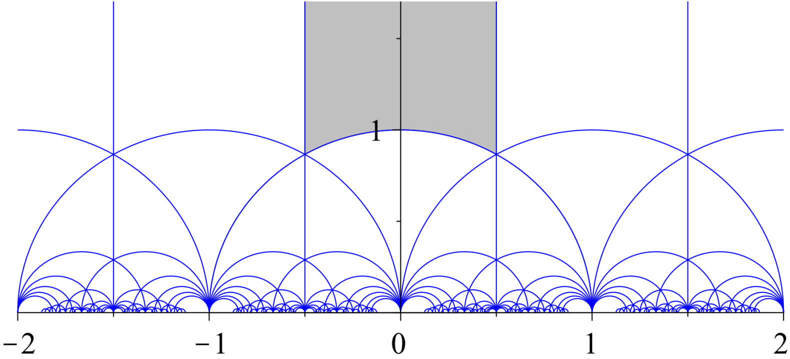
is a modular form of weight $1/2$.

A Fundamental Domain

The group $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathcal{H}$. The fundamental domain

$$\mathcal{F} := \{\tau \in \mathcal{H} \colon |\tau| \geq 1 \text{ and } |\mathrm{Re}(\tau)| \leq 1/2\}$$

provides a visualization of the set of representatives of the orbits so that a unique point of each orbit lies in $\mathcal{F}$.



Courtesy of Wikimedia: The Modular Group's Fundamental Domains.

The Valence Formula

Definition

For a modular form $f\colon \mathcal{H} \to \mathbb{C}$ and for $\tau_0 \in \mathcal{H}$, define the **order of f at τ_0**, denoted $v_{\tau_0}(f)$, to be the unique integer n such that $\frac{f(\tau)}{(\tau-\tau_0)^n}$ is non-zero and holomorphic. Further define $v_\infty(f)$ to be the first index in the q-expansion that is non-zero.

Theorem (Valence Formula)

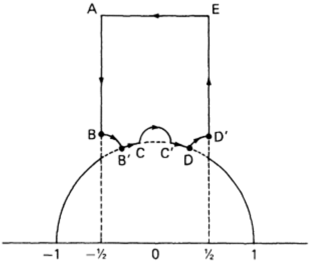
Let $\mathcal{D} = \{\tau \in \mathcal{F}\colon \mathrm{Re}\tau = \frac{1}{2}\} \cup \{\tau \in \mathcal{F}\colon |\tau| = 1, \mathrm{Re}\tau \geq 0\} \cup \left\{e^{\frac{2\pi i}{3}}\right\}$.
If $f \in M_k(\mathrm{SL}_2(\mathbb{Z}))$ is nonzero, then

$$v_\infty(f) + \frac{1}{2}v_{\mathrm{i}}(f) + \frac{1}{3}v_{e^{\frac{2\pi \mathrm{i}}{3}}}(f) + \sum_{\mathcal{F}-\mathcal{D}} v_\tau(f) = \frac{k}{12}.$$

Theorem (Valence Formula)

Let $\mathcal{D} = \{\tau \in \mathcal{F} \colon \mathrm{Re}\tau = \frac{1}{2}\} \cup \{\tau \in \mathcal{F} \colon |\tau| = 1, \mathrm{Re}\tau \geq 0\} \cup \left\{e^{\frac{2\pi i}{3}}\right\}$. *If* $f \in M_k(\mathrm{SL}_2(\mathbb{Z}))$ *is nonzero, then*

$$v_\infty(f) + \frac{1}{2}v_{\mathrm{i}}(f) + \frac{1}{3}v_{e^{\frac{2\pi\mathrm{i}}{3}}}(f) + \sum_{\mathcal{F}-\mathcal{D}} v_\tau(f) = \frac{k}{12}.$$



Courtesy of Serre's Course in Arithmetic: The Valence Contour.

Small Dimensions Computed

For small k, the Valence Formula is an easy-to-solve non-negative integral equation of the form $A + \frac{1}{2}B + \frac{1}{3}C = \frac{k}{12}$, which has no solution or a unique one for a given k.

Almost immediately then, we obtain:

Corollary

$$\dim_{\mathbb{C}}(M_k(\mathrm{SL}_2(\mathbb{Z})) = \begin{cases} 0 & k < 0, k = 2, \text{ or } k \text{ odd} \\ 1 & k = 0, 4, 6, 8, 10. \end{cases}$$

The Modular Discriminant

$$\Delta(\tau) := \frac{E_4(\tau)^3 - E_6(\tau)^2}{1728} = q\prod_{n=1}^{\infty}(1-q^n)^{24}$$

is a weight 12 cusp form for $\mathrm{SL}_2(\mathbb{Z})$.

Theorem (The Dimension Formula for Full Level)

Let $k \geq 0$ be an even integer. Then,

$$\dim(M_k(\mathrm{SL}_2(\mathbb{Z})) = \begin{cases} \lfloor \frac{k}{12} \rfloor & k = 2 \mod 12 \\ \lfloor \frac{k}{12} \rfloor + 1 & k \neq 2 \mod 12 \end{cases}$$

and

$$\dim(S_k(\mathrm{SL}_2(\mathbb{Z})) = \dim(M_k(\mathrm{SL}_2(\mathbb{Z})) - 1.$$

A Basis for Modular Forms

Using Hecke's Dimension Formula, we can characterize modular forms for $\mathrm{SL}_2(\mathbb{Z})$ in terms of Eisenstein series.

Theorem

The set

$$\mathcal{B}_k = \left\{ E_4(\tau)^a E_6(\tau)^b \colon 4a + 6b = k \text{ with } a, b \in \mathbb{Z}_{\geq 0} \right\}$$

is a basis for $M_k(\mathrm{SL}_2(\mathbb{Z}))$.

Modular Forms for Subgroups of $\mathrm{SL}_2(\mathbb{Z})$

The basic theory is similar to the full level case seen so far.

Definition

The **principal congruence subgroup of level N** is

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \colon \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}.$$

Any subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ is a **congruence subgroup** if $\Gamma(N) \subset \Gamma$.

Definition

$$\Gamma_0(4) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \colon c = 0 \mod 4 \right\}$$
$$= \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle.$$

Jacobi's Four Squares

Lemma

Define $E_{2,N} := E_2(\tau) - NE_2(N\tau)$*. Then,* $E_{2,N} \in M_2(\Gamma_0(N))$*. Moreover,* $M_2(\Gamma_0(4))$ *is a 2-dimensional vector space with basis* $\{E_{2,2}(\tau), E_{2,4}(\tau)\}$*.*

Proof Idea.

Because $\theta^4 \in M_2(\Gamma_0(4))$, we can expand in the basis

$$\theta^4(\tau) = \sum_{n=0}^{\infty} r_4(n)q^n = -\frac{1}{3}E_{2,4}(\tau) = 1 + 8\sum_{n=1}^{\infty}\left(\sum_{\substack{0<d|n \\ 4\nmid d}} d\right) q^n,$$

so reading off coefficients gives $r_4(n) = 8 \sum_{\substack{d|n \\ d\neq 0 \bmod 4}} d$ as desired. $\square$

The Geometry of Modular Forms

Associated to any congruence subgroup Γ, there is a curve $Y(\Gamma) = \{\Gamma\tau : \tau \in \mathcal{H}\}$ that can be made into a Riemann surface $X(\Gamma)$.

Theorem (Riemann-Roch)

Let X be a compact Riemann surface and $\mathrm{div}(\lambda)$ be a canonical divisor on X. Then for any $D \in \mathrm{Div}(X)$,

$$\ell(D) = \deg(D) - g + 1 + \ell(\mathrm{div}(\lambda) - D).$$

Theorem (Riemann-Hurwitz)

Let $f : X \to Y$ be nonconstant holomorphic between compact Riemann surfaces of degree d. Let g_X and g_Y be the genus of X and Y respectively. Then,

$$2g_X - 2 = d(2g_Y - 2) + \sum_{x \in X} (e_x - 1).$$

The Dimension Formula in General

Theorem

For $k = 0$, $\dim(\mathcal{M}_k(\Gamma)) = 1$. *For* $k < 0$, $\dim(\mathcal{M}_k(\Gamma)) = 0$.
For even $k \geq 2$,

$$\dim(\mathcal{M}_k(\Gamma)) = \ell(\lfloor \mathrm{div}(f) \rfloor) = (k-1)(g-1) + \left\lfloor \frac{k}{4} \right\rfloor \epsilon_2 + \left\lfloor \frac{k}{3} \right\rfloor \epsilon_3 + \frac{k}{2}\epsilon_\infty,$$

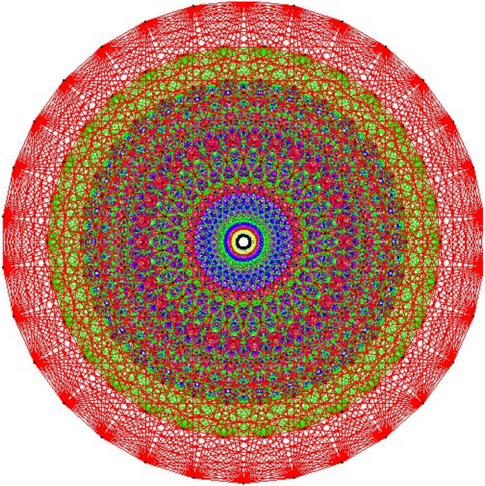
$$\dim(\mathcal{S}_k(\Gamma)) = \ell(\lfloor \mathrm{div}(f) - \sum_i x_i \rfloor) = \ell(\lfloor \mathrm{div}(f) \rfloor) - \epsilon_\infty = \dim(\mathcal{M}_k(\Gamma)) - \epsilon_\infty.$$

The odd case is similar but more technical.

Contemporary Applications

1. Operator theory on modular forms.
2. Count the number of partitions of an integer, $p(n)$.
3. Provide natural functions on elliptic curves through lattice view.
4. The Modularity Theorem and its classical partial converse: For any rational newform $f \in S_2(\Gamma_0(N))$, there is an elliptic curve $E/\mathbb{Q}$ such that the L-function of f is the L-function of E.
5. Monstrous moonshine (Borcherds, et al.).
6. Sphere packing in 8D and 24D (Viazovska, et al.).
7. Physics: quantum and statistical mechanics, CFT, string theory.
8. Properties of ζ and irrationality proofs ($\zeta(2k)$, $\zeta(3)$, etc.).
9. "Explain why" $e^{\pi\sqrt{163}} \approx 262537412640768743.99999999999992$.
10. "LMFDB universe" of automorphic forms, Galois representations, L-functions, motives.

The E_8 Lattice



Courtesy of the American Institute of Mathematics.

Further Reading

1. 2021 AWS: *A friendly introduction to the theory of modular forms* (Alex Barrios). *An introduction to modular groups* (Lori Watson).
2. *A Course in Arithmetic.* J.P. Serre.
3. *The 1-2-3 of Modular Forms.* Don Zagier, et al.
4. *Introduction to Modular Forms.* Keith Conrad. CTNT 2016.
5. *A First Course in Modular Forms*. Fred Diamond & Jerry Shurman.
6. *Elliptic Curves, Modular Forms, and Their L-Functions.* Álvaro Lozano-Robledo.
7. *Modular Forms: A Computational Approach.* William Stein.
8. *Tutorial on modular forms.* Sam Marks. Harvard, Summer 2020.
9. *Modular Forms.* Richard Borcherds. YouTube.
10. *The Geometry of SL(2,Z).* Kristaps Balodis ("K-Theory"). YouTube.
11. *A Beautiful Group, SL2(Z).* Roy Williams.

Thank You!

Questions? Comments?