Classical Modular Forms

Introduction

William Stein

Department of Mathematics
University of Washington

July 31, 2006 / MSRI Workshop

Outline

1. Definition of Modular Forms (of Level 1)
2. Applications of Modular Forms
3. Workshop Goals

Some Objects

Definition (Upper Half Plane)

The **complex upper half plane** is $\mathfrak{h} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$.

Definition (Modular Group)

The **modular group**

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

acts on $\mathfrak{h}$ via **linear fractional transformations**.

Definition (Congruence Subgroup)

A **congruence subgroup** Γ of $\mathrm{SL}_2(\mathbb{Z})$ is one that contains $\Gamma(N) = \ker(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}))$ for some N.

Weakly modular functions

Definition (Weakly Modular Function for Γ)

A **weakly modular function** of **weight** $k \in \mathbb{Z}$ for Γ is a meromorphic function f on $\mathfrak{h}$ such that for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ and all $z \in \mathfrak{h}$ we have

$$f(z) = (cz + d)^{-k} f(\gamma(z)). \tag{1.1}$$

When k is even:

$$f(\gamma(z))(d(\gamma(z)))^{k/2} = f(z)(dz)^{k/2}.$$

In this case (1.1) says that the weight k “differential form” $f(z)(dz)^{k/2}$ is fixed under the action of every element of Γ.

Fourier Expansions

Suppose f is a weakly modular function of weight k for Γ. Then $f(z) = f(z+h)$ for some integer $h > 0$.

Definition (Fourier Expansion)

A **Fourier expansion** of f, if it exists, is a representation of f as $f(z) = \sum_{n=m}^{\infty} a_n e^{2\pi i n/hz}$, for all $z \in \mathfrak{h}$.

The Fourier expansion of f **at a cusp** $\alpha \in \Gamma\backslash\mathbb{P}^1(\mathbb{Q})$ is the Fourier expansion of

$$f^{[\gamma]_k} = \det(\gamma)^{k-1}(cz+d)^{-k} f(\gamma(z))$$

at ∞, for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma(\infty) = \alpha$. (One of the problems for this workshop is to investigate efficient computation of these expansions at cusps.)

Modular Forms Are...

Definition (Modular Function)

A **modular function** of **weight** k for Γ is a weakly modular function of weight k that is meromorphic at all cusps.

Definition (Modular Form)

A **modular form** of **weight** k for Γ is a modular function of weight k for Γ that is holomorphic on $\mathfrak{h}$ and at all cusps.

Definition (Cusp Form)

A **cusp form** of **weight** k for Γ is a modular form of weight k such that $f(\alpha) = 0$ for all cusps α.

Are Modular Forms Interesting?

- The definition of modular forms might leave the impression that modular forms occupy an **obscure corner of complex analysis**.
- This is **not the case**!
- Modular forms are highly geometric, arithmetic, and topological objects that are of **extreme interest all over mathematics**, as the following examples illustrate.

Fermat's last theorem

- **Wiles's proof of Fermat's last theorem** uses modular forms extensively.
- The work of Wiles, Taylor, etc., on **modularity of elliptic curves** also massively extends computational methods for elliptic curves over $\mathbb{Q}$, because many elliptic curve algorithms, e.g., for computing L-functions, modular degrees, etc., rely on modular forms.
- Work of Kolyvagin, Kato, etc., on the **Birch and Swinnerton-Dyer conjecture** all uses modularity extensively. E.g., Construction of Heegner points require that the elliptic curve is modular.

Diophantine equations

- Andre Wiles's **proof of Fermat's last theorem** has made available a wide array of new techniques for solving certain diophantine equations.
- Such work relies crucially on having access to **tables or software for computing modular forms**.
- Wiles did not need a computer, because the relevant spaces of modular forms that arise in his proof have dimension 0!
- Also, according to Samir Siksek (personal communication) some of his papers about diophantine equations would "**have been entirely impossible** to write without the algorithms you'll talk about."

(I'll talk about modular symbols algorithms for computing modular forms in my lecture 2.)

Congruent number problem

- **A thousand year old open problem**
- Give an algorithm to decide whether an integer is the **area of a right triangle with rational sides lengths**.
- There is a **"potential" solution** that uses modular forms (of weight $3/2$) extensively (the solution is conditional on truth of the Birch and Swinnerton-Dyer conjecture, which is not yet known).

Topology

Topological modular forms are a major area of research (see work of Mike Hopkins et al.)...

Construction of Ramanujan graphs

- Modular forms can be used to construct **almost optimal expander graphs**, which play a role in communications network theory.
- Lassina Dembele and David Kohel's lectures will likely be very relevant to this problem.

Cryptography and Coding Theory

- **Point counting** on elliptic curves over finite fields is crucial to the construction of elliptic curve cryptosystems. Modular forms are very relevant to such algorithms.
- Algebraic curves that are associated to modular forms are useful in constructing **error-correcting codes**.

The Birch and Swinnerton-Dyer conjecture

- This central open problem in arithmetic geometry relates **arithmetic properties of elliptic curves** (and abelian varieties) to **special values of *L*-functions**.
- Many **deep results toward this conjecture** use modular forms extensively (e.g., work of Kolyvagin, Gross-Zagier, Kato, Skinner-Urban, etc.).
- Also, modular forms are used to compute and prove results about **special values** of these *L*-functions.

(I'll talk about computational verification of the Birch and Swinnerton-Dyer conjecture in my lecture 4.)

Serre's Conjecture on modularity of Galois representation

- Let $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.
- Serre conjectured and many people (Khare, Wintenberger) **have (nearly!!) proved** that every continuous homomorphism $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_q)$, where $\mathbb{F}_q$ is a finite field and $\det(\rho(\text{complex conjugation})) = -1$, "arises" from a modular form.
- Arises: For almost all primes p the coefficients a_p of a modular (eigen-)form $\sum a_n q^n$ are congruent to the traces of elements $\rho(\mathrm{Frob}_p)$, where Frob_p are certain special elements of $G_{\mathbb{Q}}$ called **Frobenius elements**.

Generating functions for partitions

- The **generating functions** for various kinds of partitions of an integer can often be related to modular forms.
- **Deep theorems** about modular forms then translate into results about partitions.
- See work of Ramanujan, Gordon, Andres, and Ahlgren and Ono.

Lattices

- If $L \subset \mathbb{R}^n$ is an even **unimodular lattice** (the basis matrix has determinant ± 1 and $\lambda \cdot \lambda \in 2\mathbb{Z}$ for all $\lambda \in L$), then the theta series
$$\theta_L(q) = \sum_{\lambda \in L} q^{\lambda \cdot \lambda}$$
is a modular form of weight $n/2$.
- The coefficient of q^m is the **number of lattice vectors** with squared length m.
- Theorems and computational methods for modular forms translate into theorems and computational methods for lattices. For example, **the 290 theorem of M. Bharghava and J. Hanke (who is here!)** is (almost) proved; it involves many calculations with modular forms (both theoretical and with a computer).

Workshop Goals

What we will create:

1. Papers
2. Software
3. Web pages and Online databases
4. Pretty pictures (fun!)

Our Target Audience: The results should be of interest to active researchers in modular forms like Barry Mazur, Karl Rubin, Richard Taylor, Ralph Greenberg, Matt Emerton, Frank Calegari, etc.

You will **learn** a lot about **something** in particular, have a lot of fun, meet people, and do some research.

1. Papers – Solve Problems

See the **problem book**.

- Many of the problems are **not very easy**.
- In fact, many are **VERY HARD**.
- Some of the problems are sufficiently **cutting edge** that they could lead to research papers, or even a Ph.D. thesis.

2. Write Software

Build a free open source infrastructure for modular forms research.

- We already have **MAGMA's modular forms code** (written by me and David Kohel) and HECKE which I wrote a long time ago.
- **Now we have** SAGE**, which is the union of the best open source free math software and much more in the context of a mainstream language (Python)...**
- This afternoon: **tutorials** on MAGMA and SAGE.

```
sage: M = ModularForms(Gamma1(13),prec=14)
sage: M.basis()
[
q - 4*q^3 - q^4 + 3*q^5 + 6*q^6 - 3*q^8 + q^9 - 6*q^10 -
q^2 - 2*q^3 - q^4 + 2*q^5 + 2*q^6 - 2*q^8 + q^9 - 3*q^10
1 + 21060/19*q^11 - 36504/19*q^12 - 10270/19*q^13 + O(q^
q + 11709/19*q^11 - 20687/19*q^12 - 17570/57*q^13 + O(q^
q^2 + 262*q^11 - 467*q^12 - 386/3*q^13 + O(q^14),
q^3 + 918/19*q^11 - 1215/19*q^12 - 1115/57*q^13 + O(q^14
q^4 - 882/19*q^11 + 2095/19*q^12 + 1607/57*q^13 + O(q^14
q^5 - 1287/19*q^11 + 2607/19*q^12 + 2114/57*q^13 + O(q^1
q^6 - 1080/19*q^11 + 2024/19*q^12 + 1637/57*q^13 + O(q^1
q^7 - 675/19*q^11 + 1056/19*q^12 + 940/57*q^13 + O(q^14)
q^8 - 360/19*q^11 + 453/19*q^12 + 419/57*q^13 + O(q^14),
q^9 - 153/19*q^11 + 98/19*q^12 + 44/19*q^13 + O(q^14),
q^10 - 54/19*q^11 - 9/19*q^12 + 22/57*q^13 + O(q^14)
]
```

3. Web pages and Online databases

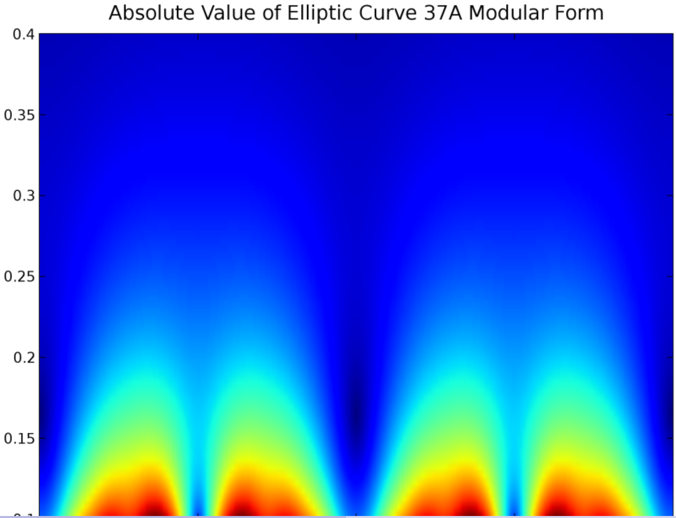
- Contribute to the **"wiki"!!**
- Numerous opportunities to make some **useful new databases**: modular forms of weight 1, modular forms mod *p*, Hilbert modular forms, rework/fix my databases, etc.
- Format:
  - Should be stored in an easy-to-use **plain text file**.
  - Have a **nice interface** via SAGE and/or a web browser.
- These databases **get used!**, e.g.,

```
Dear William Stein,

           What follows is an unsystematic assortment of notes and queries.
 I have now managed to access your database, but again, owing either to my
 own lack of skill or to our netscape software, I cannot always read your
 files beyond the first one or two pages. Thus my queries as to what is not in
 your database may be silly and answerable by "it is". You mentioned in your
 reply to my last email that you used modular symbols, & I refer to these
 below.

 -- Yours sincerely,
                  Oliver Atkin
```

4. Pretty Pictures (a T-shirt??)



General Remarks

1. Each speaker gives four talks; **first two are "mandatory"**, second two are optional.
2. Afternoon sessions will be informally organized, possibly at the last minute. Interesting things may go on in parallel.
3. **Do not burn yourself out** trying to follow everything. The goal is to find something (anything!) that **really excites** you and **dive in**, working **incredibly hard** for the next two weeks.