UNCG Summer School in Computational Number Theory

Modular Forms and Geometry

May 19 to May 23, 2014

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

"Modular Forms are functions on the complex plane that are inordinately symmetric. They satisfy so many internal symmetries that their mere existence seem like accidents. But they do exist."

(Barry Mazur)

Speakers

Avner Ash
(Boston College)

Paul Gunnells
(University of Massachusetts)

Matt Greenberg
(University of Calgary)

Organizers: Brett Tangedal, Dan Yasaki, Filip Saidak, Sebastian Pauli

uncg.edu/mat/numbertheory/summerschool

Thing Wil likes to Think About

Wil Cocke

BYU
Department of Mathematics

UNCG Computational Number Theory Summer School

Generalizations of Serre's Conjecture

- $\{n\text{-dim Galois Rep.}\} \longleftrightarrow \{\text{Arithmetic Cohomology}\}$
- The connection comes from the Hecke operators on the cohomology.
- In my research I compute the Hecke eigenvalues and then experimentally find a corresponding Galois-representation.

Nice Types of Cayley Tables

- Consider a group G with n elements labeled $1, \ldots, n$ such that:
  - If $ij \leq n$ the element ij is the product of i, j.
  - If $ij \geq n$ the element ij can be anything else.

Nice Types of Cayley Tables

- Consider a group G with n elements labeled $1, \ldots, n$ such that:
  - If $ij \leq n$ the element ij is the product of i, j.
  - If $ij \geq n$ the element ij can be anything else.
- We call such a group an FLP-group.
  - Such groups exist for some n and not others. (Consider $\mathbb{F}_p^\times$ and 195).
  - For a given n if there is a prime of the form $kn + 1$ such that the kth powers of $1, \ldots, n$ are distinct modulo $kn + 1$, then there is an FLP-group of order n.

Nice Types of Cayley Tables

- Consider a group G with n elements labeled $1, \ldots, n$ such that:
  - If $ij \leq n$ the element ij is the product of i, j.
  - If $ij \geq n$ the element ij can be anything else.
- We call such a group an FLP-group.
  - Such groups exist for some n and not others. (Consider $\mathbb{F}_p^\times$ and 195).
  - For a given n if there is a prime of the form $kn + 1$ such that the kth powers of $1, \ldots, n$ are distinct modulo $kn + 1$, then there is an FLP-group of order n.
- If we take $n = 7$ what primes that are of the form $k7 + 1$ will separate the kth powers of $1, \ldots, 7$?

My Research Interest

Lance Everhart

Department of Mathematics and Statistics
University of North Carolina at Greensboro

May 16, 2014

Currently, I do not have have a thesis problem that I have decided on. I do, however, have many interests.

Some of my interest:

- Galois Theory
- Cryptography
- Open algebra problems
- Applications of number theory and algebra
- solving all the problems in Abstract Algebra by Dummit and Foote

Some interesting past work of mine:

- Multi-user Dynamic Proofs of Data Possession using Trusted Hardware
  - Crytography and programming
  - Published by CODASPY
- 3D engine for possible future virtual tours of UNCG
  - Calculus application
  - Linear algebra based engine
  - Curve fitting with B-spline curves

Fractional Derivatives of Hurwitz Zeta Functions

Ricky Farr Joint Work With Sebastian Pauli

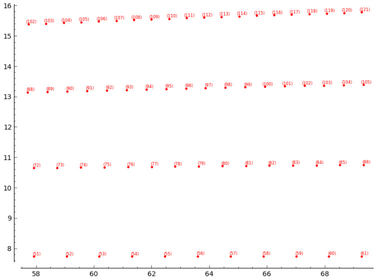
University of North Carolina at Greensboro

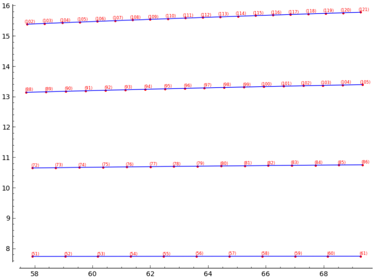
19 May 2014

Fractional Derivative of Hurwitz Zeta Functions

Let $s = \sigma + ti$ where $\sigma > 1$, $0 < a \leq 1$, and $\alpha > 0$

$$\zeta^{(\alpha)}(s, a) = (-1)^{\alpha} \sum_{n=1}^{\infty} \frac{\log^{\alpha}(n+a)}{(n+a)^{s}}.$$



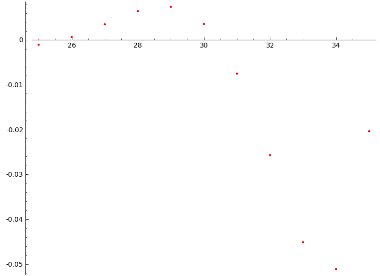


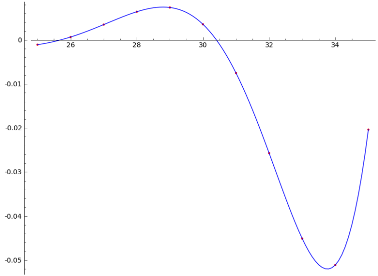
Generalized Non-Integer Stieltjes Constants

Definition

The non-integral generalized Stieltjes Constants is the sequence of numbers $\{\gamma_{\alpha+n}(a)\}_{n=0}^{\infty}$ with the property

$$\sum_{n=0}^{\infty} \frac{\log^{\alpha}(n+a)}{(n+a)^s} = \frac{\Gamma(\alpha+1)}{(s-1)^{\alpha+1}} + \sum_{n=0}^{\infty} \frac{(-1)^n \gamma_{\alpha+n}(a)}{n!}(s-1)^n, \quad s \neq 1$$



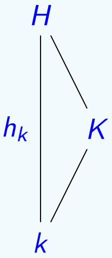


Class groups via elliptic units

Alden Gassert
University of Massachusetts, Amherst

Sumer School at UNCG
May 19-23, 2014

Class groups and elliptic units



k – imaginary quadratic field

H – Hilbert class field of k

K – any unramified, abelian extension of k

E_K – unit group of K (that is, $E_K = \mathcal{O}_K^\times$)

Theorem (Greene, Hajir, 2013)

There is an optimal order of elliptic units $\mathcal{E}$ satisfying $[E_K : \mathcal{E}] = \dfrac{h_K}{[H : K]}$.

Elliptic units are special values of modular functions.

Class groups and elliptic units

Elliptic units are special values of modular functions.

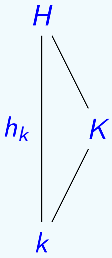
$$\omega_i = \begin{cases} N_{H/K} \dfrac{\prod_{j=1}^{r} \Delta(\overline{\mathfrak{p}}_{s+j})^{m(i,j)}}{\Delta(\mathfrak{o})^{-m(i,r+1)} \Delta(\prod_{j=1}^{r} \overline{\mathfrak{p}}_{s+j}^{m(i,j)})} & 1 \le i \le s \\ N_{H/K} \dfrac{\Delta(\overline{\mathfrak{p}}_i)^{f_i}}{\Delta(\mathfrak{o})^{f_i - 1} \Delta(\overline{\mathfrak{p}}_i^{f_i})} & s+1 \le i \le n-1 \\ e^{2\pi i / w_K} & i = n. \end{cases}$$

Theorem (Greene, Hajir, 2013)

The group $\Omega = \langle \omega_1, \ldots, \omega_n \rangle$ has finite index in E_K given by

$$[E_K : \Omega] = \frac{24^{n-1}}{w_K/2} \frac{h_K}{[H : K]}.$$

Class groups and elliptic units



k – imaginary quadratic field

H – Hilbert class field of k

K – any unramified, abelian extension of k

E_K – unit group of K (that is, $E_K = \mathcal{O}_K^\times$)

Theorem (Greene, Hajir, 2013)

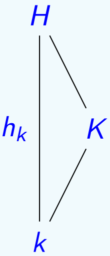
There is an optimal order of elliptic units $\mathcal{E}$ satisfying $[E_K : \mathcal{E}] = \dfrac{h_K}{[H : K]}$.

Elliptic units are special values of modular functions.

G-H produce units from quotients of the Dedekind eta function.

Code: www.math.umass.edu/~gassert/units.txt

Current work



Theorem (Greene, Hajir, 2013)

There is an optimal order of elliptic units $\mathcal{E}$ satisfying $h_K = [H\colon K][E_K : \mathcal{E}]$.

Note that $h_H = [E_H\colon \mathcal{E}]$.

Goal: Identify unusual class groups (e.g., large p-rank).

When $h_k = 2p$, it is unlikely that h_H is even.

- $h_k = 6$: h_H is even in 7 out of 51 cases
- $h_k = 10$: h_H is even in 0 out of 64 cases
- $h_k = 14$: h_H is even in 0 out of 39 cases checked (89 total)

Artin L-function Defined

Paula Hamby

Department of Mathematics and Statistics
University of North Carolina at Greensboro

May 16, 2014

Let $K/\mathbb{Q}$ be a Galois number field with $G = \mathrm{Gal}(K/\mathbb{Q})$. Let $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ be a representation.
The Artin L-Function is defined as

$$L(s, \rho, K/\mathbb{Q}) = \prod_p \det(1 - \rho(\sigma_\mathfrak{p}) \mid_{V^{I_\mathfrak{p}}} p^{-s})^{-1}$$

where σ_p is a Frobenius automorphism and $V^{I_\mathfrak{p}}$ is the subspace of the representation fixed by inertia subgroup $I_\mathfrak{p}$.

The Dedekind Zeta function is defined as

$$\zeta_K(s) = \sum_{\mathfrak{a}}^{\infty} (\mathcal{N}(\mathfrak{a})^s)^{-1} = \prod_{\mathfrak{p}} (1 - \mathcal{N}(\mathfrak{p})^{-s})^{-1}$$

where the product is taken over all non-zero prime ideals in O_K.

Theorem (Artin)

$$\zeta_K(s) = \prod_{\rho} L(s, \rho, K/\mathbb{Q})^{\dim \rho}$$

where the product is taken over all irreducible representations.

My Research Interests

Jeffery Hein
Dartmouth College

UNCG Summer School
May 19, 2014

Algebraic Modular Forms

What are algebraic modular forms?

Algebraic Modular Forms

What are algebraic modular forms?

These are objects defined by purely algebraic/arithmetic means (without analytic hypotheses) and are intimately related to various types of modular forms.

Algebraic Modular Forms

What are algebraic modular forms?

These are objects defined by purely algebraic/arithmetic means (without analytic hypotheses) and are intimately related to various types of modular forms.

My interest in these stems primarily from the following deep theorem:

Algebraic Modular Forms

What are algebraic modular forms?

These are objects defined by purely algebraic/arithmetic means (without analytic hypotheses) and are intimately related to various types of modular forms.

My interest in these stems primarily from the following deep theorem:

Theorem (H. (2013))

- *ALGEBRA* = *EASY*
- *ANALYSIS* = *HARD*

Seriously though, algebraic modular forms provide fertile ground for studying a wide array of beautiful mathematics, including analysis!

Algebraic Modular Forms

What are algebraic modular forms?

These are objects defined by purely algebraic/arithmetic means (without analytic hypotheses) and are intimately related to various types of modular forms.

My interest in these stems primarily from the following deep theorem:

Theorem (H. (2013))

- *ALGEBRA* = *EASY*
- *ANALYSIS* = *HARD*

Seriously though, algebraic modular forms provide fertile ground for studying a wide array of beautiful mathematics, including analysis!

In particular, I've recently been studying orthogonal algebraic modular forms. These arise from (totally) positive definite quadratic forms.

Example: Ternary Quadratic Forms

Let $Q(x, y, z) = x^2 + 4y^2 + 4z^2 + 3yz - xy$ be a quadratic form.

Example: Ternary Quadratic Forms

Let $Q(x, y, z) = x^2 + 4y^2 + 4z^2 + 3yz - xy$ be a quadratic form.

For each prime p, there are various forms related to Q called p-neighbors.

Example: Ternary Quadratic Forms

Let $Q(x, y, z) = x^2 + 4y^2 + 4z^2 + 3yz - xy$ be a quadratic form.

For each prime p, there are various forms related to Q called p-neighbors.

Utilizing these p-neighbors, we compute various Hecke matrices T_p.

Example: Ternary Quadratic Forms

Let $Q(x, y, z) = x^2 + 4y^2 + 4z^2 + 3yz - xy$ be a quadratic form.

For each prime p, there are various forms related to Q called p-neighbors.

Utilizing these p-neighbors, we compute various Hecke matrices T_p.

For the Q above, we have

$$T_2 = \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix}, T_5 = \begin{pmatrix} 5 & 2 \\ 1 & 4 \end{pmatrix}, T_7 = \begin{pmatrix} 4 & 8 \\ 4 & 0 \end{pmatrix}, T_{11} = \begin{pmatrix} 7 & 10 \\ 5 & 2 \end{pmatrix}, \ldots$$

Example: Ternary Quadratic Forms

Let $Q(x, y, z) = x^2 + 4y^2 + 4z^2 + 3yz - xy$ be a quadratic form.

For each prime p, there are various forms related to Q called p-neighbors.

Utilizing these p-neighbors, we compute various Hecke matrices T_p.

For the Q above, we have

$$T_2 = \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix}, T_5 = \begin{pmatrix} 5 & 2 \\ 1 & 4 \end{pmatrix}, T_7 = \begin{pmatrix} 4 & 8 \\ 4 & 0 \end{pmatrix}, T_{11} = \begin{pmatrix} 7 & 10 \\ 5 & 2 \end{pmatrix}, \ldots$$

The eigenvalues associated to the column vector $(1, -1)$ are

$$a_2 = 0, \quad a_5 = 3, \quad a_7 = -4, \quad a_{11} = -3, \quad a_{13} = -1, \ldots$$

Example: Ternary Quadratic Forms

Let $Q(x, y, z) = x^2 + 4y^2 + 4z^2 + 3yz - xy$ be a quadratic form.

For each prime p, there are various forms related to Q called p-neighbors.

Utilizing these p-neighbors, we compute various Hecke matrices T_p.

For the Q above, we have

$$T_2 = \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix}, T_5 = \begin{pmatrix} 5 & 2 \\ 1 & 4 \end{pmatrix}, T_7 = \begin{pmatrix} 4 & 8 \\ 4 & 0 \end{pmatrix}, T_{11} = \begin{pmatrix} 7 & 10 \\ 5 & 2 \end{pmatrix}, \ldots$$

The eigenvalues associated to the column vector $(1, -1)$ are

$$a_2 = 0, \quad a_5 = 3, \quad a_7 = -4, \quad a_{11} = -3, \quad a_{13} = -1, \ldots$$

In other words, traces of Frobenius for the elliptic curve (51a1)

$$E/\mathbb{Q} : y^2 + y = x^3 + x^2 + x - 1.$$

Hi! My Name Is...

Brian Hwang

May 19, 2014

http://hwang.caltech.edu

What do I do?

The dream: "All motives are automorphic."

Slightly more precisely, let X be a variety over a number field K, and $\zeta_X(s)$ its (Hasse–Weil) Zeta function. For the zeta function (or the variety) to be "automorphic," it should be equal to some (product of) L-functions of some automorphic forms, i.e.

$$\zeta_{X,K}(s) := \sum_{\mathfrak{p} \text{ prime}} \exp\left(\sum_{n\geq 1} \frac{\#\overline{X}(\mathbb{F}^n_{q(\mathfrak{p})})}{n} t^n)\right) \overset{?}{=} \prod_{\pi} L(\pi, s).$$

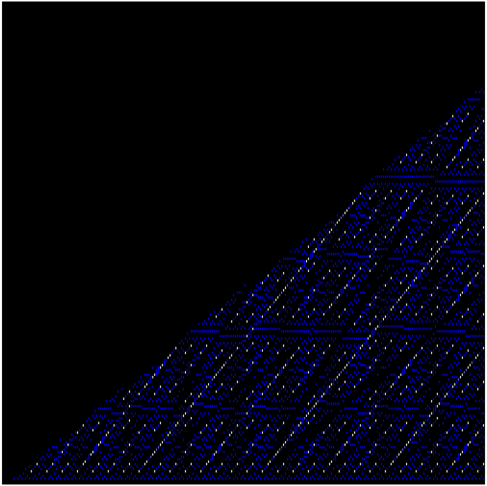
(Really The Only) Example. Modularity of elliptic curves E over $\mathbb{Q}$ or real quadratic extensions.

Main Project: Compute the zeta functions of Shimura varieties attached to $GSp(2n)$ (with parahoric level structure) and determine whether they are automorphic.

Cool things that I've been trying to understand

1. Applying a modified Faltings–Serre–Livné method to get some modularity results for (Galois representations) in some non-regular cases. (Here "non-regular" means: don't have $h^{p,q} \leq 1$.)
   - If you (or somebody you know) have some candidate pairs of abelian surfaces and Siegel modular forms, please tell me! I may be able to check that for you.
   - If you know of easy ways to compute Frobenii or "exhaustion" results related to such methods, please talk to me!
2. The picture on the next slide.

Graph of Slopes of p-adic Modular Forms



Teaser: There's some strange behavior e.g. at $p = 59$ that is related to [a different notion of] irregularity of the image of the associated Galois representations.

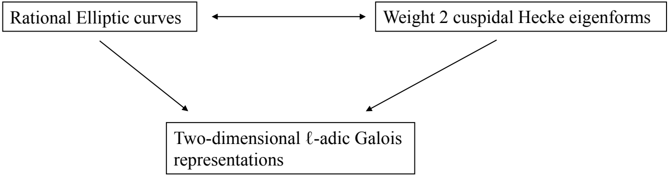
Modularity of Elliptic Curves over Quartic CM Fields

UNCG Summer School in Computational Number Theory, 2014

Andrew Jones, University of Sheffield

The Modularity Theorem

- The Modularity Theorem plays a key role in the proof of Fermat's Last Theorem, and establishes a connection between rational elliptic curves and modular forms in the following manner:



- It was known previously how to attach such Galois representations to each of these objects. The theorem states that, given an elliptic curve, the associated Galois representation is equivalent to one arising from a modular form.
- In particular, the traces of these representations at Frobenius elements of the absolute Galois group are equal. These traces are familiar to us: for elliptic curves they are the values $a_p(\mathrm{E})$ obtained by looking at reductions of the curve over finite fields, while for modular forms they are the eigenvalues $a_p(f)$ of the Hecke operators T_p.

- Langlands' conjectures predict that the same should hold over *any* number field, not just the rationals (where we replace modular forms, which rapidly become very, very ugly, with the equivalent notions of *automorphic forms*, or *automorphic representations*).
- It's long been known how to attach Galois reps to elliptic curves defined over a number field, and we know a fair amount about modular forms over quadratic and totally real fields (in fact, we now know that modularity holds for all real quadratic fields!).
- Recently, it's been proven that one can attach Galois reps to automorphic representations defined over *CM* fields, which are totally imaginary quadratic extensions of totally real fields, so we'd like to see if we can find modular elliptic curves.
- Methods exist to compare Galois reps, which as input require only the traces at finitely many Frobenius elements. Since we can work out the local data for an elliptic curve easily, the task boils down to computing Hecke eigenvalues.
- A method for this exists (at least for quartic CM fields). It turns out that modular forms over a field F "live in" the cohomology of the arithmetic group $\mathrm{Res}_{F/Q}(\mathrm{GL}_2)$, and that the Hecke action translates to this setting.
- The group cohomology turns out to be equivalent to the homology of a combinatorial cell complex (equipped with an action of $\mathrm{Res}_{F/Q}(\mathrm{GL}_2)$) which can be modelled by a *finite* sub-complex, which has connections with a space of binary Hermitian forms over the field F.
- Unfortunately the Hecke action doesn't preserve this sub-complex, but Paul Gunnells and Dan Yasaki have come up with an algorithm to "break down" elements of the general complex so that they fit into the smaller space, thus allowing us to compute the action of the Hecke operators, and prove modularity of specific elliptic curves.

Research Interests - Dirichlet Series and Distributions

Tianyi Mao

City University of New York, Graduate Center

tmao@gc.cuny.edu

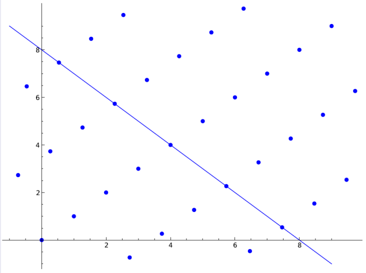
May 13, 2014

Counting Elements of Given Trace

Given totally real number field K and a fractional ideal $\mathfrak{a}$ of K. Let N_a be the number of totally positive elements in $\mathfrak{a}$ with trace a.

Geometric Estimate

Natural geometric estimate of N_a: r_a=the volume of the intersection in $\mathfrak{a} \otimes \mathbb{R}$ of the totally positive cone with hyperplane Trace=a.



Dirichlet Series

Let $\sigma_1, \ldots, \sigma_n$ be all embeddings of K, $\sigma_i(\alpha) = \alpha^{(i)}$. Let $v(\alpha) = \prod_{i=1}^{n} sgn(\alpha^{(i)})^{e_i}$ where $e_i = 0$ or 1, and let $\Psi(s, v, \mathfrak{a}) = \sum_{0 \neq \alpha \in \mathfrak{a}} \frac{v(\alpha)}{(|\alpha^{(1)}| + \ldots + |\alpha^{(n)}|)^s}$. Summing over all 2^n choices of v:

$$\sum_{v} \Psi(s, v, \mathfrak{a}) = 2^n \sum_{0 << \alpha \in \mathfrak{a}} Tr(\alpha)^{-s} = 2^n \sum_{a > 0} N_a a^{-s} \quad (1)$$

Theorem (Ash & Friedberg, 2005)

For $\epsilon > 0$, $\sum_{a<X} (N_a - r_a) = O(X^{n-1-\frac{2n-2}{2n+1}+\epsilon})$

Note: When $K = \mathbb{Q}(D)$, *the Dirichlet series* $\sum (N_a - r_a) a^{-s}$ *describes the distribution of fractional parts of* $m\sqrt{D}$.*(Hecke)*

My Interests

Ash and Friedberg did that by studying the general form of the Ψ above: $\Phi(s, y, p, k, \mathfrak{b}) = \sum_{0 \neq \alpha \in \mathfrak{b}} \frac{p(\alpha)}{(\sum_{i=1}^{n-1} |\alpha^{(i)}|^k y_i^k y_n^{k/n} + |\alpha^{(n)}|^k y_n^{k/n})^s}$

Question: How do we generalize their result to non-totally real case?

Ramanujan-type congruences

James Martin

University of North Texas

May 19, 2014

Ramanujan Congruences

Let $p(n)$ be the *partition function*. Recall that

$$G(q) := \sum_{n=0}^{\infty} p(n)q^n = \prod_{n=1}^{\infty} \frac{1}{1-q^n},$$

i.e., $q^{\frac{1}{24}} \frac{1}{G(q)}$ is the *Dedekind eta-function*.

Ramanujan Congruences

Let $p(n)$ be the *partition function*. Recall that

$$G(q) := \sum_{n=0}^{\infty} p(n)q^n = \prod_{n=1}^{\infty} \frac{1}{1-q^n},$$

i.e., $q^{\frac{1}{24}} \frac{1}{G(q)}$ is the *Dedekind eta-function*.

Theorem (Ramanujan, 1919)

$$p(5n+4) \equiv 0 \pmod 5$$
$$p(7n+5) \equiv 0 \pmod 7$$
$$p(11n+6) \equiv 0 \pmod{11}$$

Let $p(n)$ be the *partition function*. Recall that

$$G(q) := \sum_{n=0}^{\infty} p(n) q^n = \prod_{n=1}^{\infty} \frac{1}{1-q^n},$$

i.e., $q^{\frac{1}{24}} \frac{1}{G(q)}$ is the *Dedekind eta-function*.

Theorem (Ramanujan, 1919)

$$p(5n+4) \equiv 0 \pmod{5}$$
$$p(7n+5) \equiv 0 \pmod{7}$$
$$p(11n+6) \equiv 0 \pmod{11}$$

Theorem (Ahlgren & Boylan, Inventiones 2003)

These are the only such congruences for the partition function.

Ramanujan-type Congruences

An elliptic modular form with coefficients $a(n)$ has a Ramanujan congruence at $b \pmod{p}$ if $a(pn + b) \equiv 0 \pmod{p}$.

Ramanujan-type Congruences

An elliptic modular form with coefficients $a(n)$ has a Ramanujan congruence at $b \pmod{p}$ if $a(pn+b) \equiv 0 \pmod{p}$. This notion has been extended to Jacobi forms and Siegel modular forms.

Ramanujan-type Congruences

An elliptic modular form with coefficients $a(n)$ has a Ramanujan congruence at $b \pmod{p}$ if $a(pn + b) \equiv 0 \pmod{p}$. This notion has been extended to Jacobi forms and Siegel modular forms.

Richter (2008-09): Jacobi forms at $b \equiv 0 \pmod{p}$.

Ramanujan-type Congruences

An elliptic modular form with coefficients $a(n)$ has a Ramanujan congruence at $b \pmod{p}$ if $a(pn+b) \equiv 0 \pmod{p}$. This notion has been extended to Jacobi forms and Siegel modular forms.

Richter (2008-09): Jacobi forms at $b \equiv 0 \pmod{p}$.

Choi, Choie, and Richter (2011): Siegel modular forms of degree 2 at $b \equiv 0 \pmod{p}$.

Ramanujan-type Congruences

An elliptic modular form with coefficients $a(n)$ has a Ramanujan congruence at $b \pmod{p}$ if $a(pn+b) \equiv 0 \pmod{p}$. This notion has been extended to Jacobi forms and Siegel modular forms.

Richter (2008-09): Jacobi forms at $b \equiv 0 \pmod{p}$.

Choi, Choie, and Richter (2011): Siegel modular forms of degree 2 at $b \equiv 0 \pmod{p}$.

Dewar and Richter (2010): Jacobi forms and Siegel modular forms of degree 2 at $b \not\equiv 0 \pmod{p}$.

Ramanujan-type Congruences

An elliptic modular form with coefficients $a(n)$ has a Ramanujan congruence at $b \pmod{p}$ if $a(pn+b) \equiv 0 \pmod{p}$. This notion has been extended to Jacobi forms and Siegel modular forms.

Richter (2008-09): Jacobi forms at $b \equiv 0 \pmod{p}$.

Choi, Choie, and Richter (2011): Siegel modular forms of degree 2 at $b \equiv 0 \pmod{p}$.

Dewar and Richter (2010): Jacobi forms and Siegel modular forms of degree 2 at $b \not\equiv 0 \pmod{p}$.

Raum and Richter (2014): Jacobi forms of higher degree and Siegel modular forms of arbitrary degree at $b \equiv 0 \pmod{p}$.

Non-vanishing of fundamental Fourier coefficients of Siegel modular forms

Jolanta Marzec

University of Bristol

UNCG Summer School, May 2014
Computational Number Theory: Modular Forms and Geometry

Classical modular form:

$$f\left(\frac{az+b}{cz+d}\right)=(cz+d)^k f(z) \text{ finite at cusps of } \Gamma, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma \subset \mathrm{SL}_2(\mathbb{Z})$$

Classical modular form:

$$f\left(\frac{az+b}{cz+d}\right)=(cz+d)^k f(z) \text{ finite at cusps of } \Gamma, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma \subset \mathrm{SL}_2(\mathbb{Z})$$

Siegel modular form of degree 2:

$$F((AZ+B)(CZ+D)^{-1}) = \det(CZ+D)^k F(Z) \ \text{ for } \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma^{(2)},$$

$Z = Z^t, \mathrm{Im}\, Z > 0$, where $\Gamma^{(2)}$ a congruence subgroup of $\mathrm{Sp}_4(\mathbb{Q})$,

Classical modular form:

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z) \text{ finite at cusps of } \Gamma, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma \subset \mathrm{SL}_2(\mathbb{Z})$$

Siegel modular form of degree 2:

$$F((AZ+B)(CZ+D)^{-1}) = \det(CZ+D)^k F(Z) \ \text{ for } \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma^{(2)},$$

$Z = Z^t, \mathrm{Im}\, Z > 0$, where $\Gamma^{(2)}$ a congruence subgroup of $\mathrm{Sp}_4(\mathbb{Q})$, e.g.

$$\Gamma_0^{(2)}(N) := \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{Z}) : C \equiv 0 \ (\mathrm{mod} N) \right\},$$

$$\Gamma^{\mathrm{para}}(N) := \left\{ \begin{pmatrix} * & N* & * & * \\ * & * & * & */N \\ * & N* & * & * \\ N* & N* & N* & * \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{Q}) : * \in \mathbb{Z} \right\}.$$

Classical modular form:

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z) \text{ finite at cusps of } \Gamma, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma \subset \mathrm{SL}_2(\mathbb{Z})$$

Siegel modular form of degree 2:

$$F((AZ+B)(CZ+D)^{-1}) = \det(CZ+D)^k F(Z) \;\text{ for }\; \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \Gamma^{(2)},$$

$Z = Z^t, \mathrm{Im}\, Z > 0$, where $\Gamma^{(2)}$ a congruence subgroup of $\mathrm{Sp}_4(\mathbb{Q})$, e.g.

$$\Gamma_0^{(2)}(N) := \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{Z}) : C \equiv 0 \pmod{N} \right\},$$

$$\Gamma^{\mathrm{para}}(N) := \left\{ \begin{pmatrix} * & N* & * & * \\ * & * & * & */N \\ * & N* & * & * \\ N* & N* & N* & * \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{Q}) : * \in \mathbb{Z} \right\}.$$

$$F(Z) = \sum_{\substack{T=T^t, T\geq 0 \\ \text{half-integral}}} a(F,T) e^{2\pi i \operatorname{tr}(TZ)}$$

Why fundamental Fourier coefficients?

(Those $a\left(F, \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}\right)$ for which $D := b^2 - 4ac < 0$ is a fundamental discriminant).

Why fundamental Fourier coefficients?

(Those $a\left(F,\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}\right)$ for which $D := b^2 - 4ac < 0$ is a fundamental discriminant).

- (A version of) Böcherer's conjecture: If F is a newform w.r.t. $\Gamma_0^{(2)}(N)$ (or $\Gamma^{\mathrm{para}}(N)$) and D is a fundamental discriminant, then:

$$\sum_{\{T>0:\mathrm{disc}(T)=D\}/\sim} a(F,T)\Lambda^{-1}(T) \neq 0 \Longrightarrow L(1/2, \pi_F \times \theta_\Lambda) \neq 0\,,$$

  where $T \sim T'$ if $T' = A^t T A$ for some $A \in \mathrm{SL}_2(\mathbb{Z})$ (or $\Gamma_0(N)$), and $\theta_\Lambda(z) = \sum_{0\neq\mathfrak{a}\subset\mathcal{O}_{\mathbb{Q}\sqrt{-D}}} \Lambda(\mathfrak{a}) e^{2\pi i \mathcal{N}(\mathfrak{a}z)}$.

Why fundamental Fourier coefficients?

(Those $a\left(F, \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}\right)$ for which $D := b^2 - 4ac < 0$ is a fundamental discriminant).

- (A version of) Böcherer's conjecture: If F is a newform w.r.t. $\Gamma_0^{(2)}(N)$ (or $\Gamma^{\text{para}}(N)$) and D is a fundamental discriminant, then:

$$\sum_{\{T>0:\mathrm{disc}(T)=D\}/\sim} a(F,T)\Lambda^{-1}(T) \neq 0 \Longrightarrow L(1/2, \pi_F \times \theta_\Lambda) \neq 0\,,$$

  where $T \sim T'$ if $T' = A^t TA$ for some $A \in \mathrm{SL}_2(\mathbb{Z})$ (or $\Gamma_0(N)$), and $\theta_\Lambda(z) = \sum_{0 \neq \mathfrak{a} \subset \mathcal{O}_{\mathbb{Q}\sqrt{-D}}} \Lambda(\mathfrak{a}) e^{2\pi i \mathcal{N}(\mathfrak{a}z)}$.
- L-function of a paramodular form is equal to some L-function of an abelian surface over $\mathbb{Q}$ (paramodular conjecture).

Why fundamental Fourier coefficients?

(Those $a\left(F, \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}\right)$ for which $D := b^2 - 4ac < 0$ is a fundamental discriminant).

- (A version of) Böcherer's conjecture: If F is a newform w.r.t. $\Gamma_0^{(2)}(N)$ (or $\Gamma^{\text{para}}(N)$) and D is a fundamental discriminant, then:

$$\sum_{\{T>0:\mathrm{disc}(T)=D\}/\sim} a(F,T)\Lambda^{-1}(T) \neq 0 \Longrightarrow L(1/2, \pi_F \times \theta_\Lambda) \neq 0\,,$$

  where $T \sim T'$ if $T' = A^t TA$ for some $A \in \mathrm{SL}_2(\mathbb{Z})$ (or $\Gamma_0(N)$), and $\theta_\Lambda(z) = \sum_{0\neq\mathfrak{a}\subset\mathcal{O}_{\mathbb{Q}\sqrt{-D}}} \Lambda(\mathfrak{a})e^{2\pi i\mathcal{N}(\mathfrak{a}z)}$.
- L-function of a paramodular form is equal to some L-function of an abelian surface over $\mathbb{Q}$ (paramodular conjecture).
- Their non-vanishing is related to the existence of global Bessel models of fundamental type for Siegel cusp forms.

The Computation of Galois Groups over Local Fields

Jonathan Milstead, UNCG

1. Splitting Field Method

W

wildly ramified
extension of
degree p^m

$T = \mathbb{Q}_p(\zeta, \sqrt[e_0]{\zeta^r p})$

normal, tamely ramified
extension given by
$g(x) = x^{e_0} - \zeta^r p$

$U = \mathbb{Q}_p(\zeta)$

unramified extension degree f
given by cyclotomic polynomial,
ζ is primitive root of unity.

$\mathbb{Q}_p$ p-adic numbers

A variation of an OM Algorithm is used

See upcoming paper (Milstead, Pauli, Sinclai

2.**Ramification Polygon**: Newton polygon of $\dfrac{\varphi(\alpha x + \alpha)}{\alpha^n}$. Interested in 1 or 2 segment cases.

Polynomials over Q.

3. Stauduhar's method (1973):

- Key Challenge: finding a G-relative H-invariant $F \in \mathbb{Z}[X_1, ..., X_n]$, i.e., F so that $\text{Stab}_G F := \{\sigma \in G \mid F^\sigma = F\} = H$ where $H < G \leqslant S_n$

- Uses resolvents
$$R_F := \prod_{\sigma \in G//H} (T - F^\sigma(\alpha_1, ..., \alpha_n)) \in \mathbb{Z}[T]$$
to see if $\text{Gal}(f) \leqslant H^g$. Global ($G = S_n$) and Relative.

4. Fieker, Kluners

- General method for computing invariants of large degree.

- The "first" practical degree independent algorithm.

Congruences, Galois Representations, Discriminants, and Modular Forms

UNCG Summer School 2014

Richard Moy
Northwestern University

May 19, 2014

Interests

Interests

- Congruences and classical modular forms

Interests

- Congruences and classical modular forms
- Partial weight one Hilbert modular forms

Interests

- Congruences and classical modular forms
- Partial weight one Hilbert modular forms
- Ethereal modular forms

Interests

- Congruences and classical modular forms
- Partial weight one Hilbert modular forms
- Ethereal modular forms
- Statistics of discriminant of polynomials over finite fields

Interests

- Congruences and classical modular forms
- Partial weight one Hilbert modular forms
- Ethereal modular forms
- Statistics of discriminant of polynomials over finite fields

Table : Number of Monic Square Free Polynomials over $\mathbb{F}_7$ with Given Discriminant

Δ	Degree 2	Degree 3	Degree 4	Degree 5
1				
2				
3				
4				
5				
6				
Total				

Interests

- Congruences and classical modular forms
- Partial weight one Hilbert modular forms
- Ethereal modular forms
- Statistics of discriminant of polynomials over finite fields

Table : Number of Monic Square Free Polynomials over $\mathbb{F}_7$ with Given Discriminant

Δ	Degree 2	Degree 3	Degree 4	Degree 5
1	7			
2	7			
3	7			
4	7			
5	7			
6	7			
Total	42			

Interests

- Congruences and classical modular forms
- Partial weight one Hilbert modular forms
- Ethereal modular forms
- Statistics of discriminant of polynomials over finite fields

Table : Number of Monic Square Free Polynomials over $\mathbb{F}_7$ with Given Discriminant

Δ	Degree 2	Degree 3	Degree 4	Degree 5
1	7	56		
2	7	14		
3	7	21		
4	7	77		
5	7	84		
6	7	42		
Total	42	294		

Interests

- Congruences and classical modular forms
- Partial weight one Hilbert modular forms
- Ethereal modular forms
- Statistics of discriminant of polynomials over finite fields

Table : Number of Monic Square Free Polynomials over $\mathbb{F}_7$ with Given Discriminant

Δ	Degree 2	Degree 3	Degree 4	Degree 5
1	7	56	392	
2	7	14	98	
3	7	21	147	
4	7	77	539	
5	7	84	588	
6	7	42	294	
Total	42	294	2058	

Interests

- Congruences and classical modular forms
- Partial weight one Hilbert modular forms
- Ethereal modular forms
- Statistics of discriminant of polynomials over finite fields

Table : Number of Monic Square Free Polynomials over $\mathbb{F}_7$ with Given Discriminant

Δ	Degree 2	Degree 3	Degree 4	Degree 5
1	7	56	392	2041
2	7	14	98	2041
3	7	21	147	2041
4	7	77	539	2041
5	7	84	588	2041
6	7	42	294	2041
Total	42	294	2058	14406

Monic Degree 3 Polynomials over $\mathbb{F}_p$ with Discriminant 1

Monic Degree 3 Polynomials over $\mathbb{F}_p$ with Discriminant 1

- Consider an arbitrary degree 3 monic polynomial $f = z^3 + w \cdot z^2 + x \cdot z + y \in \mathbb{F}_p[z]$ where $2, 3 \nmid q$.

Monic Degree 3 Polynomials over $\mathbb{F}_p$ with Discriminant 1

- Consider an arbitrary degree 3 monic polynomial $f = z^3 + w \cdot z^2 + x \cdot z + y \in \mathbb{F}_p[z]$ where $2, 3 \nmid q$.
- By sending $z \mapsto \frac{z-w}{3}$, we can eliminate the z^2 term and leave Δf unchanged. Therefore, consider $g = z^3 + x \cdot z + y$.

Monic Degree 3 Polynomials over $\mathbb{F}_p$ with Discriminant 1

- Consider an arbitrary degree 3 monic polynomial $f = z^3 + w \cdot z^2 + x \cdot z + y \in \mathbb{F}_p[z]$ where $2, 3 \nmid q$.
- By sending $z \mapsto \frac{z-w}{3}$, we can eliminate the z^2 term and leave Δf unchanged. Therefore, consider $g = z^3 + x \cdot z + y$.
- Since $\Delta g = -27y^2 - 4x^3$, we are counting the number of solutions to $1 = -27y^2 - 4x^3$ over $\mathbb{F}_p$, or $y^2 + y = x^3 - 7$.

Monic Degree 3 Polynomials over $\mathbb{F}_p$ with Discriminant 1

- Consider an arbitrary degree 3 monic polynomial $f = z^3 + w \cdot z^2 + x \cdot z + y \in \mathbb{F}_p[z]$ where $2, 3 \nmid q$.
- By sending $z \mapsto \frac{z-w}{3}$, we can eliminate the z^2 term and leave Δf unchanged. Therefore, consider $g = z^3 + x \cdot z + y$.
- Since $\Delta g = -27y^2 - 4x^3$, we are counting the number of solutions to $1 = -27y^2 - 4x^3$ over $\mathbb{F}_p$, or $y^2 + y = x^3 - 7$.
- The elliptic curve $E: \; y^2 + y = x^3 - 7$ has conductor 27 and CM by $\zeta_3: \; (x, y) \mapsto (\zeta_3 x, y)$. It's associated modular form $h \in M_2(\Gamma_0(27))$ is $h = q - 2q^4 - q^7 + 5q^{13} + 4q^{16} - 7q^{19} - 5q^{25} + 2q^{28} + \dots$

Monic Degree 3 Polynomials over $\mathbb{F}_p$ with Discriminant 1

- Consider an arbitrary degree 3 monic polynomial $f = z^3 + w \cdot z^2 + x \cdot z + y \in \mathbb{F}_p[z]$ where $2, 3 \nmid q$.
- By sending $z \mapsto \frac{z-w}{3}$, we can eliminate the z^2 term and leave Δf unchanged. Therefore, consider $g = z^3 + x \cdot z + y$.
- Since $\Delta g = -27y^2 - 4x^3$, we are counting the number of solutions to $1 = -27y^2 - 4x^3$ over $\mathbb{F}_p$, or $y^2 + y = x^3 - 7$.
- The elliptic curve $E: \; y^2 + y = x^3 - 7$ has conductor 27 and CM by $\zeta_3 : \; (x, y) \mapsto (\zeta_3 x, y)$. It's associated modular form $h \in M_2(\Gamma_0(27))$ is $h = q - 2q^4 - q^7 + 5q^{13} + 4q^{16} - 7q^{19} - 5q^{25} + 2q^{28} + \dots$
- Therefore, for a prime p, if a_p is the p^{th} coefficient of f, then $\#E(\mathbb{F}_p) = p - a_p + 1$ (but we don't want to count the point at infinity). So the number of solutions to $\Delta g = 1$ should be $p - a_p$, and the number of solutions to $\Delta f = 1$ should be $p^2 - a_p \cdot p$.

Monic Degree 3 Polynomials over $\mathbb{F}_p$ with Discriminant 1

- Consider an arbitrary degree 3 monic polynomial $f = z^3 + w \cdot z^2 + x \cdot z + y \in \mathbb{F}_p[z]$ where $2, 3 \nmid q$.
- By sending $z \mapsto \frac{z-w}{3}$, we can eliminate the z^2 term and leave Δf unchanged. Therefore, consider $g = z^3 + x \cdot z + y$.
- Since $\Delta g = -27y^2 - 4x^3$, we are counting the number of solutions to $1 = -27y^2 - 4x^3$ over $\mathbb{F}_p$, or $y^2 + y = x^3 - 7$.
- The elliptic curve $E: \; y^2 + y = x^3 - 7$ has conductor 27 and CM by $\zeta_3: \; (x, y) \mapsto (\zeta_3 x, y)$. It's associated modular form $h \in M_2(\Gamma_0(27))$ is
  $h = q - 2q^4 - q^7 + 5q^{13} + 4q^{16} - 7q^{19} - 5q^{25} + 2q^{28} + \dots$

Table : Number of Degree 3 Polynomials over $\mathbb{F}_p$ with $\Delta = 1$

p	5	7	11	13	17	19
#	5^2	$7^2 - (-1) \cdot 7$	11^2	$13^2 - 5 \cdot 13$	17^2	$19^2 - (-7) \cdot 19$

UNCG Summer School Introduction

Jesse Patsolic
Jeremy Rouse, PhD

WAKE FOREST
UNIVERSITY
Department of Mathematics

May 2014

Introduction

- My thesis research with Jeremy Rouse has involved the study of number fields and their defining polynomials.

Introduction

- My thesis research with Jeremy Rouse has involved the study of number fields and their defining polynomials.
- Given a number field K, how does one find polynomials $f(x)$ that have a small number of nonzero terms? Specifically, is it possible to make this method work to classify all the trinomials that generate a given field?

Introduction

- My thesis research with Jeremy Rouse has involved the study of number fields and their defining polynomials.
- Given a number field K, how does one find polynomials $f(x)$ that have a small number of nonzero terms? Specifically, is it possible to make this method work to classify all the trinomials that generate a given field?
- We have made progress with the specific case where $f(x) = x^5 + x + 3$.

Introduction

- My thesis research with Jeremy Rouse has involved the study of number fields and their defining polynomials.
- Given a number field K, how does one find polynomials $f(x)$ that have a small number of nonzero terms? Specifically, is it possible to make this method work to classify all the trinomials that generate a given field?
- We have made progress with the specific case where $f(x) = x^5 + x + 3$.
- We have proven that if the number field, $K = \mathbb{Q}[\alpha]$, is defined by $f(x) = x^5 - 5x + 12$, where α is a root of f, then f is the only trinomial of the form $x^5 + ax + b$ defining K.

$$C_K = \begin{cases} n_4 = -5a + 4e = 0 \\ n_3 = 10a^2 - 16ae + 4bd + 15be + 2c^2 + 15cd + 6e^2 = 0 \\ n_2 = -10a^3 + 4b^2c - 6ac^2 + 15bc^2 - 12abd + 15b^2d \\ \quad - 45acd - 4cd^2 - 9d^3 + 24a^2e - 45abe + 4c^2e \\ \quad + 8bde + 6cde - 45d^2e - 18ae^2 + 33be^2 - 45ce^2 + 4e^3 = 0. \end{cases}$$

$$C_K = \begin{cases} n_4 = -5a + 4e = 0 \\ n_3 = 10a^2 - 16ae + 4bd + 15be + 2c^2 + 15cd + 6e^2 = 0 \\ n_2 = -10a^3 + 4b^2c - 6ac^2 + 15bc^2 - 12abd + 15b^2d \\ \quad - 45acd - 4cd^2 - 9d^3 + 24a^2e - 45abe + 4c^2e \\ \quad + 8bde + 6cde - 45d^2e - 18ae^2 + 33be^2 - 45ce^2 + 4e^3 = 0. \end{cases}$$

Magma was unable to compute the curve quotient by the automorphism group. Doing this computation manually, we obtain a map whose image is a cubic curve that can then be transformed into an elliptic curve:

$$C_K = \begin{cases} n_4 = -5a + 4e = 0 \\ n_3 = 10a^2 - 16ae + 4bd + 15be + 2c^2 + 15cd + 6e^2 = 0 \\ n_2 = -10a^3 + 4b^2c - 6ac^2 + 15bc^2 - 12abd + 15b^2d \\ \quad - 45acd - 4cd^2 - 9d^3 + 24a^2e - 45abe + 4c^2e \\ \quad + 8bde + 6cde - 45d^2e - 18ae^2 + 33be^2 - 45ce^2 + 4e^3 = 0. \end{cases}$$

Magma was unable to compute the curve quotient by the automorphism group. Doing this computation manually, we obtain a map whose image is a cubic curve that can then be transformed into an elliptic curve:

$$E : y^2 = x^3 + a_4x + a_6.$$

$$C_K = \begin{cases} n_4 = -5a + 4e = 0 \\ n_3 = 10a^2 - 16ae + 4bd + 15be + 2c^2 + 15cd + 6e^2 = 0 \\ n_2 = -10a^3 + 4b^2c - 6ac^2 + 15bc^2 - 12abd + 15b^2d \\ \quad - 45acd - 4cd^2 - 9d^3 + 24a^2e - 45abe + 4c^2e \\ \quad + 8bde + 6cde - 45d^2e - 18ae^2 + 33be^2 - 45ce^2 + 4e^3 = 0. \end{cases}$$

Magma was unable to compute the curve quotient by the automorphism group. Doing this computation manually, we obtain a map whose image is a cubic curve that can then be transformed into an elliptic curve:

$$E : y^2 = x^3 + a_4 x + a_6.$$

E has positive rank and the methods we use are inadequate to determine $C_K(\mathbb{Q})$. We may possibly be able to use elliptic curve Chabauty in the future.

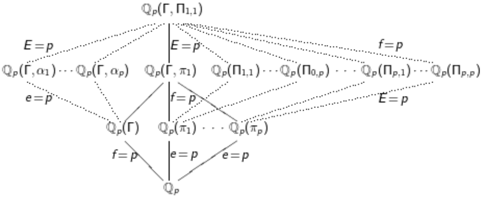
Algorithms for Local Fields and Zeros of Derivatives of Zeta

Sebastian Pauli

University of North Carolina at Greensboro

Algorithms for Local Fields

- OM Algorithms – Round 4, Montes algorithm, Polynomial factorization and other applications
- Galois groups
- Construction of Extensions with given invariants – Krasner, Class fields ...

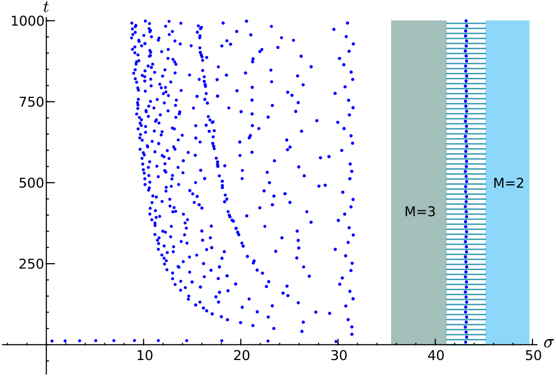


$$\pi_k^p + (p-1)p\pi_k^{p-1} + p + (k-1)p^2 = 0$$

$$\Pi_{k,l}^p + (p-1)\pi_k\Pi_{k,l}^{p-1} + \pi_k + (l-1)\pi_k^2 = 0$$

Zeros of Derivatives of the Riemann Zeta function

Zero free regions



(with Thomas Binder and Filip Saidak)

The Representation Problem and Regular Quadratic Polynomials

James Ricci

Wesleyan University

May 19th, 2014

The Representation Problem

A polynomial $H(\mathbf{x})$ with rational coefficients is said to represent an integer a if the Diophantine equation

$$H(\mathbf{x}) = a$$

has a solution over the integers.

The Representation Problem

A polynomial $H(\mathbf{x})$ with rational coefficients is said to represent an integer a if the Diophantine equation

$$H(\mathbf{x}) = a$$

has a solution over the integers.

$$H(\mathbf{x}) = Q(\mathbf{x}) + L(\mathbf{x}) + c.$$

The Representation Problem

A polynomial $H(\mathbf{x})$ with rational coefficients is said to represent an integer a if the Diophantine equation

$$H(\mathbf{x}) = a$$

has a solution over the integers.

$$H(\mathbf{x}) = Q(\mathbf{x}) + 2B(\mathbf{v}, \mathbf{x}) + c.$$

The Representation Problem

A polynomial $H(\mathbf{x})$ with rational coefficients is said to represent an integer a if the Diophantine equation

$$H(\mathbf{x}) = a$$

has a solution over the integers.

$$H(\mathbf{x}) = Q(\mathbf{x}) + 2B(\mathbf{v}, \mathbf{x}) + c.$$

$$H(\mathbf{x}) - c \text{ represents } a \qquad \Leftrightarrow \qquad N + \mathbf{v} \text{ represents } Q(\mathbf{v}) + a.$$

The Representation Problem

A polynomial $H(\mathbf{x})$ with rational coefficients is said to represent an integer a if the Diophantine equation

$$H(\mathbf{x}) = a$$

has a solution over the integers.

$$H(\mathbf{x}) = Q(\mathbf{x}) + 2B(\mathbf{v}, \mathbf{x}) + c.$$

$H(\mathbf{x}) - c$ represents a $\quad\Leftrightarrow\quad$ $N + \mathbf{v}$ represents $Q(\mathbf{v}) + a$.

Research Interests

Finding ways to extend methods and results from the theory of quadratic forms to apply to the realm of quadratic polynomials.

Using Quadratic Forms to Study Quadratic Polynomials

A quadratic polynomial is regular if it represents all of the integers which are represented over $\mathbb{Z}_p$ for all primes p as well as over $\mathbb{Z}_\infty := \mathbb{R}$.

Using Quadratic Forms to Study Quadratic Polynomials

A quadratic polynomial is regular if it represents all of the integers which are represented over $\mathbb{Z}_p$ for all primes p as well as over $\mathbb{Z}_\infty := \mathbb{R}$.

Goal:

Use cosets of quadratic lattices to study regular quadratic polynomials.

Using Quadratic Forms to Study Quadratic Polynomials

A quadratic polynomial is regular if it represents all of the integers which are represented over $\mathbb{Z}_p$ for all primes p as well as over $\mathbb{Z}_\infty := \mathbb{R}$.

Goal:

Use cosets of quadratic lattices to study regular quadratic polynomials.

Theorem (R- 2013)

Given a fixed conductor, there are only finitely many semi-equivalence classes of positive regular quadratic polynomials in three variables.

Perfect and prime numbers, and $\zeta(s)$

FILIP SAIDAK
Department of Mathematics and Statistics
University of North Carolina
Greensboro, NC 27403

May 18, 2014

Topics of interest:

Distribution of prime numbers:

1) Chebyshev-type results (their generalizations and limits)
2) Prime Number Theorem (error term estimates)
3) Twin primes, maximal gaps between primes

Riemann zeta function:

1) zero-free regions of $\zeta(s)$
2) monotonicity results inside the critical strip
3) zeros of higher derivatives of the Riemann zeta function

Arithmetical functions:

1) Erdős-Kac type theorems
2) Extreme values of multiplicative functions
3) Perfect Numbers

Stark's Conjecture as it relates to Hilbert's 12th Problem

Brett A. Tangedal

University of North Carolina at Greensboro, Greensboro NC, 27412, USA
batanged@uncg.edu

May 19, 2014

UNCG

Let F be a real quadratic field, $\mathcal{O}_\mathsf{F}$ the ring of integers in F, and $\mathfrak{m}$ an integral ideal in $\mathcal{O}_\mathsf{F}$ with $\mathfrak{m} \neq (1)$. There are two infinite primes associated to the two distinct embeddings of F into $\mathbb{R}$, denoted by $\mathfrak{p}_\infty^{(1)}$ and $\mathfrak{p}_\infty^{(2)}$. Let $\mathcal{H}_2 := H(\mathfrak{m}\mathfrak{p}_\infty^{(2)})$ denote the ray class group modulo $\mathfrak{m}\mathfrak{p}_\infty^{(2)}$, which is a finite abelian group.

Given a class $\mathcal{C} \in \mathcal{H}_2$, there is an associated partial zeta function $\zeta(s, \mathcal{C}) = \sum \mathsf{N}\mathfrak{a}^{-s}$, where the sum runs over all integral ideals (necessarily rel. prime to $\mathfrak{m}$) lying within the class $\mathcal{C}$. The function $\zeta(s, \mathcal{C})$ has a meromorphic continuation to $\mathbb{C}$ with exactly one (simple) pole at $s = 1$. We have $\zeta(0, \mathcal{C}) = 0$ for all $\mathcal{C} \in \mathcal{H}_2$, but $\zeta'(0, \mathcal{C}) \neq 0$ (if certain conditions are met).

First crude statement of Stark's conjecture: $e^{-2\zeta'(0,\mathcal{C})}$ is an algebraic integer, indeed this real number is conjectured to be a root of a palindromic monic polynomial

$$f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_2x^2 + a_1x + 1 \in \mathbb{Z}[x].$$

For this reason, $e^{-2\zeta'(0,\mathcal{C})}$ is called a "Stark unit". By class field theory, there exists a ray class field $\mathsf{F}_2 := \mathsf{F}(\mathfrak{mp}_\infty^{(2)})$ with the following special property: F_2 is an abelian extension of F with $\mathsf{Gal}(\mathsf{F}_2/\mathsf{F}) \cong \mathcal{H}_2$. Stark's conjecture states more precisely that $e^{-2\zeta'(0,\mathcal{C})} \in \mathsf{F}_2$ for all $\mathcal{C} \in \mathcal{H}_2$.
This fits the general theme of Hilbert's 12th problem: Construct analytic functions which when evaluated at "special" points produce algebraic numbers which generate abelian extensions over a given base field.

Hyperbolic Fourier Coefficients of Modular Forms
A Preliminary Report: UNCG Summer School in Computational Number Theory 2014

Karen Taylor (joint work with Cormac O'Sullivan)

Bronx Community College
City University of New York

May 19, 2014

Introduction

Let $\mathbb{H}$ denote the upper half plane. Let $\Gamma = SL(2, \mathbb{Z})$, Γ acts on $\mathbb{H} \cup \mathbb{R} \cup \{\infty\}$ by linear fractional transformations. Elements in Γ may be classified as parabolic, elliptic or hyperbolic according to their types of fixed points: parabolic elements have one real fixed point, hyperbolic two real fixed points. Let k be a positive even integer and $f : H \longrightarrow \mathbb{C}$ a holomorphic function. We define the slash operator, $|_k$ by

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

Introduction

Let $\mathbb{H}$ denote the upper half plane. Let $\Gamma = SL(2, \mathbb{Z})$, Γ acts on $\mathbb{H} \cup \mathbb{R} \cup \{\infty\}$ by linear fractional transformations. Elements in Γ may be classified as parabolic, elliptic or hyperbolic according to their types of fixed points: parabolic elements have one real fixed point, hyperbolic two real fixed points. Let k be a positive even integer and $f : H \longrightarrow \mathbb{C}$ a holomorphic function. We define the slash operator, $|_k$ by

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

f is a weight k modular form if

1. $(f|_k\gamma)(z) = f(z)$ for all $\gamma \in \Gamma$;
2. f is bounded at infinity.

Modular Forms

Let $f \in S_k(\Gamma)$, $\Gamma = SL(2, \mathbb{Z})$ and η, η' be a hyperbolic pair.

Modular Forms

Let $f \in S_k(\Gamma)$, $\Gamma = SL(2,\mathbb{Z})$ and η, η' be a hyperbolic pair. Set $\Gamma_\eta = \{\gamma \in SL(2,\mathbb{Z}) : \gamma\eta = \eta \text{ and } \gamma\eta' = \eta'\}$, with $\Gamma_\eta =< \pm\gamma_\eta >$.

Modular Forms

Let $f \in S_k(\Gamma)$, $\Gamma = SL(2, \mathbb{Z})$ and η, η' be a hyperbolic pair. Set $\Gamma_\eta = \{\gamma \in SL(2, \mathbb{Z}) : \gamma\eta = \eta$ and $\gamma\eta' = \eta'\}$, with $\Gamma_\eta = < \pm\gamma_\eta >$. Let $\sigma_\eta \in SL(2, \mathbb{R})$ satisfy

$$\gamma_\eta \sigma_\eta = \sigma_\eta A.$$

Modular Forms

Let $f \in S_k(\Gamma)$, $\Gamma = SL(2,\mathbb{Z})$ and η, η' be a hyperbolic pair. Set $\Gamma_\eta = \{\gamma \in SL(2,\mathbb{Z}) : \gamma\eta = \eta \text{ and } \gamma\eta' = \eta'\}$, with $\Gamma_\eta =< \pm\gamma_\eta >$. Let $\sigma_\eta \in SL(2,\mathbb{R})$ satisfy

$$\gamma_\eta \sigma_\eta = \sigma_\eta A.$$

Then the hyperbolic fourier expansion of f at the hyperbolic pair η, η' is

$$(f|_k \sigma_\eta)(w) = \sum_{n=-\infty}^{\infty} a_n w^{-\frac{k}{2} + \frac{2\pi i n}{\lambda_\eta}}.$$

We assume $\eta = \sqrt{m}$, m squarefree. Let $\gamma_\eta = \left(\begin{smallmatrix} a_0 & mc_0 \\ c_0 & a_0 \end{smallmatrix}\right)$ where (a_0, c_0) is the fundamental solution of Pell's equation: $x^2 - my^2 = 1$.

We assume $\eta = \sqrt{m}$, m squarefree. Let $\gamma_\eta = \left(\begin{smallmatrix} a_0 & mc_0 \\ c_0 & a_0 \end{smallmatrix}\right)$ where (a_0, c_0) is the fundamental solution of Pell's equation: $x^2 - my^2 = 1$. $\quad \Gamma_\eta = < \pm\gamma_\eta >$

We assume $\eta = \sqrt{m}$, m squarefree. Let $\gamma_\eta = \left(\begin{smallmatrix} a_0 & mc_0 \\ c_0 & a_0 \end{smallmatrix}\right)$ where (a_0, c_0) is the fundamental solution of Pell's equation: $x^2 - my^2 = 1$. $\Gamma_\eta =< \pm\gamma_\eta >$ Let σ_η be the diagonalizing matrix for γ_η that is

$$\gamma_\eta \sigma_\eta = \sigma_\eta A,$$

where $A = \begin{pmatrix} \epsilon_m & 0 \\ 0 & {\epsilon_m}^{-1} \end{pmatrix}$.

Hyperbolic Poincaré Series

$w^{-\frac{k}{2}+\frac{2\pi in}{\lambda_\eta}}$ gives rise to a Poincaré series ($z = \sigma_\eta w$), as follows:

$$P_{\eta,n}(z) = \sum_{\gamma \in (\Gamma_\eta \backslash \Gamma)} \frac{({\sigma_\eta}^{-1}\gamma z)^{-\frac{k}{2}+\frac{2\pi in}{\lambda_\eta}}}{j({\sigma_\eta}^{-1}\gamma, z)^k}.$$

Explicit Fourier Coefficients

The *nth* (parabolic) fourier coefficient of the (parabolic) Poincaré series, $P_n(z)$, is given by

$$a_\nu(n,k) = (2\pi i)^k \sum_{c=1}^{\infty} \frac{k(n,\nu,c)}{c} \left(\frac{\nu}{n}\right)^{\frac{k-1}{2}} J_{k-1}\left(\frac{4\pi\sqrt{n\nu}}{c}\right).$$

Explicit Fourier Coefficients

The *nth* (parabolic) fourier coefficient of the (parabolic) Poincaré series, $P_n(z)$, is given by

$$a_\nu(n,k) = (2\pi i)^k \sum_{c=1}^{\infty} \frac{k(n,\nu,c)}{c} \left(\frac{\nu}{n}\right)^{\frac{k-1}{2}} J_{k-1}\left(\frac{4\pi\sqrt{n\nu}}{c}\right).$$

(Kloosterman Sum) The sum

$$k(n,\nu,c) = \sum_{\substack{d \mod c \\ gcd(c,d)=1}} e^{\frac{2\pi i(n\bar{d}+\nu d)}{c}} \qquad d\bar{d} \equiv 1 \mod c$$

is called a Kloosterman sum.

Hyperbolic Poincaré series

$$P_{\eta,n}(z) = \sum_{\gamma \in (\Gamma_\eta \backslash \Gamma)} \frac{({\sigma_\eta}^{-1}\gamma z)^{-\frac{k}{2}+\frac{2\pi i n}{\lambda_\eta}}}{j({\sigma_\eta}^{-1}\gamma, z)^k}.$$

$$P_{\eta,n}(z) = \sum_{l=1}^{\infty} a_{n,hyp}(l) e^{2\pi i l z},$$

Theorem

(O'Sullivan & T) For $n \in \mathbb{Z}$, the nth parabolic Fourier coefficient of the hyperbolic Poincaré series $P_{\eta,\nu}$ is given by

$$a_{n,hyp}(l) = \sum_{N \in R_m} \frac{1}{N^{\frac{k}{2}}} S_\eta(n,l;N) I_\eta(n,l,\frac{N}{2\sqrt{m}}).$$

Here $R_m = \{N : N \text{ represented by } x^2 - my^2\}$,

$$S_\eta(n,l;N) = \sum_{\delta\in\mathscr{F}_N} \left(\frac{\delta}{\delta'}\frac{2\sqrt{m}}{N(\delta)}\right)^{\frac{2\pi i n}{\lambda_\eta}} e^{\frac{2\pi i \beta_0{}'}{\delta'}}.$$

$$I_\eta(\nu,n;r) := \int_{-\infty+iy}^{\infty+iy} \frac{\left(r-\frac{1}{t}\right)^{2\pi i\nu/\ell_\eta} e^{-2\pi i n t}}{(t-\frac{1}{r})^{k/2} t^{k/2}}\, dt \qquad (r\in\mathbb{R}_{\neq 0},\ y>0,\ k>$$

We are currently trying to understand the properties of the above functions.

Sums of Quadratic Functions with two discriminants

Ka Lun Wong
UNCG Summer School

May, 2014

For a positive non-square discriminant D and a real number x, let $\mathcal{Q}_D(x)$ be the set of all quadratic functions $Q = Q(x) = ax^2 + bx + c$ which satisfy the following conditions:

Introduction

For a positive non-square discriminant D and a real number x, let $\mathcal{Q}_D(x)$ be the set of all quadratic functions $Q = Q(x) = ax^2 + bx + c$ which satisfy the following conditions:

- The three quantities a, b, and c are integers.
- $a < 0$
- $b^2 - 4ac = D$
- $Q(x) > 0$

Introduction

For a positive non-square discriminant D and a real number x, let $\mathcal{Q}_D(x)$ be the set of all quadratic functions $Q = Q(x) = ax^2 + bx + c$ which satisfy the following conditions:

- The three quantities a, b, and c are integers.
- $a < 0$
- $b^2 - 4ac = D$
- $Q(x) > 0$

For an even integer $k \geq 2$, Zagier (1999) defines a function $F_{k,D} : \mathbb{R} \to \mathbb{R}$,

$$F_{k,D}(x) = \sum_{Q \in \mathcal{Q}_D(x)} Q(x)^{k-1}.$$

Zagier (1999) From quadratic functions to modular functions:

For every fixed even k, the functions $F_{k,D}(x)$ for various D span a space of finite dimension($\left[\frac{k}{6}\right] + 1$).

Zagier (1999) From quadratic functions to modular functions:

For every fixed even k, the functions $F_{k,D}(x)$ for various D span a space of finite dimension($\left[\frac{k}{6}\right] + 1$).

The average value of $F_{k,D}(x)$ equals $\frac{\zeta_D(1-k)}{2\zeta(1-2k)}$.

Zagier (1999) From quadratic functions to modular functions:

For every fixed even k, the functions $F_{k,D}(x)$ for various D span a space of finite dimension($\left[\frac{k}{6}\right] + 1$).

The average value of $F_{k,D}(x)$ equals $\frac{\zeta_D(1-k)}{2\zeta(1-2k)}$.

The function $T_x(z) := \sum_D F_{k,D}(x) e^{2\pi i D z}$ is a modular form of weight $k + \frac{1}{2}$ on $\Gamma_0(4)$ for any real number x.

Zagier (1999) From quadratic functions to modular functions:

For every fixed even k, the functions $F_{k,D}(x)$ for various D span a space of finite dimension($\left[\frac{k}{6}\right] + 1$).

The average value of $F_{k,D}(x)$ equals $\frac{\zeta_D(1-k)}{2\zeta(1-2k)}$.

The function $T_x(z) := \sum_D F_{k,D}(x)e^{2\pi i D z}$ is a modular form of weight $k + \frac{1}{2}$ on $\Gamma_0(4)$ for any real number x.

Zagier mentioned a way to generalize this function for both odd and even k. We use a different approach to generalize this function that works for both even and odd k.

Applications of Reduction Theory to Automorphic Forms

Dan Yasaki

The University of North Carolina Greensboro

May 19–23, 2014
UNCG Summer School 2014
Modular forms and Geometry

Modular forms over $\mathbb{Q}$

Cusp forms ($f(z) = \sum a_n q^n$) and Hecke operators can be described cohomologically

$$H^1(\Gamma_0(N)\backslash\mathfrak{h};\mathbb{C}) \simeq S_2(N) \oplus \overline{S}_2(N) \oplus \mathrm{Eis}_2(N).$$

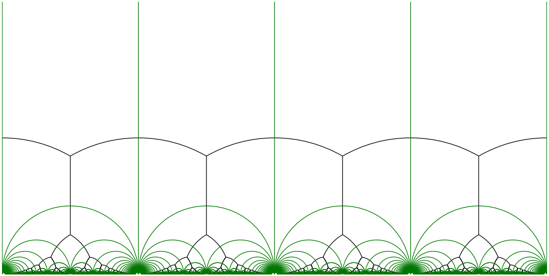


Figure : Upper half plane tessellated by ideal triangles corresponding to *perfect* binary quadratic forms.

Generalization in an example

Many of the ideas and techniques have analogues in the number field setting.

Let F be the cubic field of discriminant -23 with maximal order $\mathcal{O}_F$.

$\mathrm{GL}_2/\mathbb{Q}$	GL_2/F
$\mathbb{Z}$	$\mathcal{O}_F$
subgroup of $\mathrm{GL}_2(\mathbb{Z})$	subgroup of $\mathrm{GL}_2(\mathcal{O}_F)$
$\mathfrak{h}$	$\mathfrak{h} \times \mathfrak{h}_3 \times \mathbb{R}$
one triangle	nine 6-dimensional polytopes
modular symbols	1-sharblies

UNCG Summer School in Computational Number Theory

Modular Forms and Geometry

May 19 to May 23, 2014

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

"Modular Forms are functions on the complex plane that are inordinately symmetric. They satisfy so many internal symmetries that their mere existence seem like accidents. But they do exist."

(Barry Mazur)

Speakers

Avner Ash
(Boston College)
Paul Gunnells
(University of Massachusetts)
Matt Greenberg
(University of Calgary)

Organizers: Brett Tangedal, Dan Yasaki, Filip Saidak, Sebastian Pauli

uncg.edu/mat/numbertheory/summerschool