Study of positive solutions of nonlinear elliptic partial differential equations

Abraham Abebe

UNCG Summer School in Computational Number Theory 2013

May 20, 2013

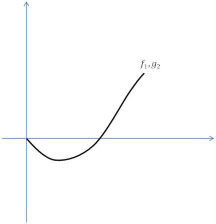
Introduction

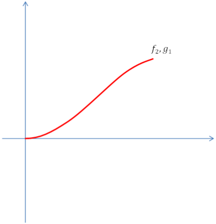
Consider the elliptic system

$$\left.\begin{array}{rlll} -\Delta u = & \lambda_1 f_1(u) + \mu_1 g_1(v) & \text{in} & \Omega; \\ -\Delta v = & \lambda_2 f_2(u) + \mu_2 g_2(v) & \text{in} & \Omega; \\ & u = v = 0 & \text{on} & \partial\Omega, \end{array}\right\} \quad (1)$$

- $\lambda_i, \mu_i > 0$ are parameters
- $\Omega \subset \mathbb{R}^N$ is a smooth bounded domain
- $f_1, g_2 : [0,\infty) \to \mathbb{R}$ are C^1, $f_2, g_1 : [0,\infty) \to [0,\infty]$ are C^1 nondecreasing
- $f_i(0) = 0 = g_i(0)$, $f_1'(0) \le 0$, $g_2'(0) \le 0$
- $f_2'(0) = 0 = g_1'(0)$
- $\lim_{s\to\infty} \frac{f_i(s)}{s} = 0 = \lim_{s\to\infty} \frac{g_i(s)}{s}$

The system (1) has two positive solutions when λ_1 and μ_2 are large.





Three solution theorem

Sub-super solution

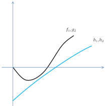
A pair $(\underline{u},\underline{v})((\overline{u},\overline{v}))$ is a subsolution(supersolution) to (1) if it satisfies $\leq$ ($\geq$) in (1). Strict sub or super-solution if not a solution.

Three solution theorem (Shivaji, 1987) [3]

Suppose there exist a sub-solution ψ_1, a strict super-solution ϕ_1, a strict sub-solution ψ_2 and a super-solution ϕ_2 for a system $-\Delta u = f(u) \;\; in\ \Omega; \quad u = 0 \;\; on\ \partial\Omega$ such that $\psi_1 < \phi_1 < \phi_2$, $\psi_1 < \psi_1 < \phi_2$ and $\psi_2 \not< \phi_1$. Then the system has at least three solutions u_1, u_2, u_3 such that $\psi_1 \leq u_1 < u_2 < u_3 \leq \phi_2$.

Remark: The above result works for any cooperative system, which is the case in our system (1) since $\frac{\partial g_1}{\partial v} > 0$ and $\frac{\partial f_2}{\partial u} > 0$

1. **sub-solution:** $(\underline{u},\underline{v}) = (0,0)$
2. **strict sub-solution:** $(\underline{u},\underline{v}) = (w_1, w_2)$ (not so trivial) but with help of [2] where w_1,w_2 are respectively solutions to
   $-\Delta w = h_1(w) \;\; in\ \Omega; \quad w = 0 \;\; on\ \partial\Omega$ and
   $-\Delta w = h_2(w) \;\; in\ \Omega; \quad w = 0 \;\; on\ \partial\Omega$



THE UNIVERSITY of NORTH CAROLINA GREENSBORO

Conclusion

1. **strict super-solution:** $(\overline{u}, \overline{v}) = (\epsilon\phi, \epsilon\phi)$ (for $\epsilon > 0$) and ϕ is the fist eigenfunction corresponding to the first eigenvalue of the operator $-\Delta$ (see [1]).
2. **super-solution:** $(\overline{u}, \overline{v}) = (Me, Me)$ (for large M) and the function e is the unique solution to the problem $-\Delta u = 1 \;\; in\ \Omega; \quad u = 0 \;\; on\ \partial\Omega.$

Work on progress

- Extension to p-Laplacian systems; $\Delta_p u := (\mathrm{div}(|\nabla u|^{p-2}u))$
- Simulation

R. Shivaji C. Maya, *Multiple positive solutions for a class of semilinear boundary value probems*, NonLinear Analysis,Elsevier Science **38** (1999), 497–504.

A. Castro J. B. Garner and R. Shivaji, *Existence results for classes of sublinear semipositone problems*, Results in Mathematics **23** (1993), 214–220.

R. Shivaji, *A remark on the existence of three solutions via sub-super solutions, in: Lakshmikantham, v. (ed.)*, Lecture Notes in Pure and Applied Mathematics Springer, Berlin **109** (1987), 561–566.

THE UNIVERSITY of NORTH CAROLINA GREENSBORO

My (possible, potential) Mathematical Interests

Or at least, an example of one

Rebecca Black

University of Maryland

May 17, 2013

Confession

I do not have a thesis problem yet, and indeed do not yet know very precisely what my research interests are.

Confession

I do not have a thesis problem yet, and indeed do not yet know very precisely what my research interests are.

Instead of trying to summarize everything I might end up studying, let me focus on one specific example of a problem.

Confession

I do not have a thesis problem yet, and indeed do not yet know very precisely what my research interests are.

Instead of trying to summarize everything I might end up studying, let me focus on one specific example of a problem.

Definition

A central simple algebra of degree n over a field k is called cyclic if it has a presentation $\langle x, y : x^n = a, y^n = b, xy = \zeta_n yx \rangle$ for some $a, b, \zeta_n \in k$, ζ_n a primitive nth root of unity.

Confession

I do not have a thesis problem yet, and indeed do not yet know very precisely what my research interests are.

Instead of trying to summarize everything I might end up studying, let me focus on one specific example of a problem.

Definition

A central simple algebra of degree n over a field k is called cyclic if it has a presentation $\langle x, y : x^n = a, y^n = b, xy = \zeta_n yx \rangle$ for some $a, b, \zeta_n \in k$, ζ_n a primitive nth root of unity.

Conjecture (Albert)

Every central division algebra of prime degree p is cyclic.

Central simple algebras of degree p that split over an extension K/k are classified by the Galois cohomology set $H^1(K, PGL_p)$.

Central simple algebras of degree p that split over an extension K/k are classified by the Galois cohomology set $H^1(K, PGL_p)$.

Vague, heuristic definition

The essential dimension of a group G is the minimal transcendence degree over the base field necessary to define classes of $H^1(K, G)$ for extensions K/k.

Central simple algebras of degree p that split over an extension K/k are classified by the Galois cohomology set $H^1(K, PGL_p)$.

Vague, heuristic definition

The essential dimension of a group G is the minimal transcendence degree over the base field necessary to define classes of $H^1(K, G)$ for extensions K/k.

Cyclic algebras are always defined over $k(x, y)$ which has transcendence degree at most two, so the conjecture would imply $ed(PGL_p) = 2$ for all primes p. This is an open question!

Research Interests - Nonabelian generalizations of class groups

Michael Bush
Washington and Lee University

May 20, 2013

Let K be a number field and $Cl(K)$ be the class group of K. Class groups can be thought of as Galois groups.

Theorem (from class field theory)

$$Cl(K) \cong \mathrm{Gal}(H/K)$$

where H is the maximal unramified abelian extension of K (also called the *Hilbert class field of K*).

Let K be a number field and $Cl(K)$ be the class group of K. Class groups can be thought of as Galois groups.

Theorem (from class field theory)

$$Cl(K) \cong \mathrm{Gal}(H/K)$$

where H is the maximal unramified abelian extension of K (also called the *Hilbert class field of K*).

Replacing H with the maximal unramified extension of K or some other maximal extension with restricted ramification, one can consider the associated Galois group.

These groups are often nonabelian and may be finite/infinite. They arise naturally in various parts of number theory. eg. the embedding problem for $\mathcal{O}_K$.

Let G be one of these Galois groups. Questions I like to think about:

(i) How can one determine if G is finite/infinite?

(ii) What sort of groups arise in this way?

(iii) Can one compute/describe G when finite (or certain special finite quotients if infinite)?

(iv) If one fixes a group, can one say anything about how often this particular group occurs as the Galois group as one varies K over some family of fields?

Let G be one of these Galois groups. Questions I like to think about:

(i) How can one determine if G is finite/infinite?

(ii) What sort of groups arise in this way?

(iii) Can one compute/describe G when finite (or certain special finite quotients if infinite)?

(iv) If one fixes a group, can one say anything about how often this particular group occurs as the Galois group as one varies K over some family of fields?

Things I'd like to get out of the workshop:

(i) A better understanding of some of the basic algorithms in CNT (particularly in relation to class groups and Galois groups).

(ii) Perhaps some understanding of the main factors governing running times and how one might come up with reasonable estimates ahead of time.

Zeros of the Derivatives of the Riemann Zeta Function in the Left Half Plane

Ricky E. Farr

UNCG

April 17, 2013

Zeros of $\zeta^{(k)}$ on the left half plane

Levinson and Montgomery 1974

The Riemann hypothesis implies that $\zeta^{(k)}$ has at most finitely many non-real zeros with $\sigma < \frac{1}{2}$.

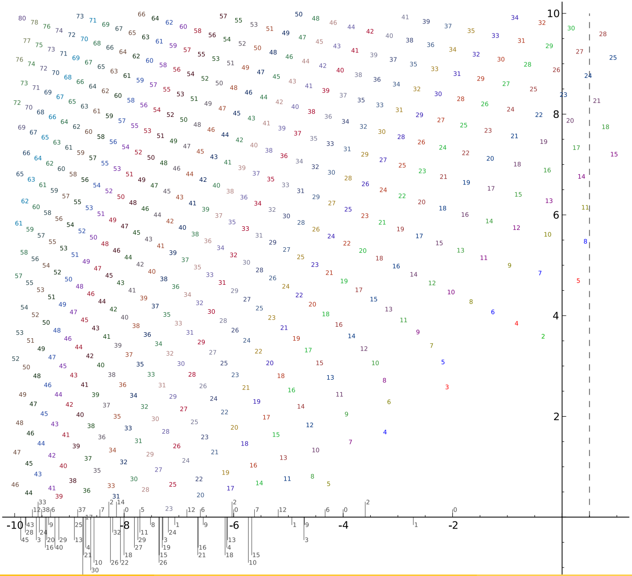
Levinson and Montgomery 1974

- For $n \geq 2$ there is a unique zero of ζ' in the interval $(-2n, -2n+2)$
- ζ' has no non-real zeros with $\sigma < 0$

Yildirim 1996

- ζ'' has only one pair of non-real zeros with $\sigma < 0$
- ζ''' has only one pair of non-real zeros with $\sigma < 0$

Zeros of $\zeta^{(k)}$ on the left half plane



Chebyshev Radical Extensions

Alden Gassert

University of Massachusetts, Amherst

Sumer School at UNCG

May 20-24, 2013

Chebyshev Polynomials

Arithmetic Dynamics is the study of number theoretic properties of dynamical systems.

Chebyshev Polynomials

Arithmetic Dynamics is the study of number theoretic properties of dynamical systems.

The Chebyshev polynomials are a unique family of polynomials defined by a trigonometric relation.

$$T_d(2\cos(\theta)) = 2\cos(d\theta)$$

$$T_0(x) = 2 \qquad T_1(x) = x$$

$$T_2(x) = x^2 - 2 \qquad T_3(x) = x^3 - 3x$$

$$T_4(x) = x^4 - 4x^2 + 2 \qquad T_5(x) = x^5 - 5x^3 + 5x$$

$$T_{d+1}(x) = x \cdot T_d(x) - T_{d-1}(x)$$

$$T_d(T_e(x)) = T_e(T_d(x)) = T_{de}(x)$$

Chebyshev Polynomials

Arithmetic Dynamics is the study of number theoretic properties of dynamical systems.

$$T_d(T_e(x)) = T_e(T_d(x)) = T_{de}(x)$$

Consider the polynomials

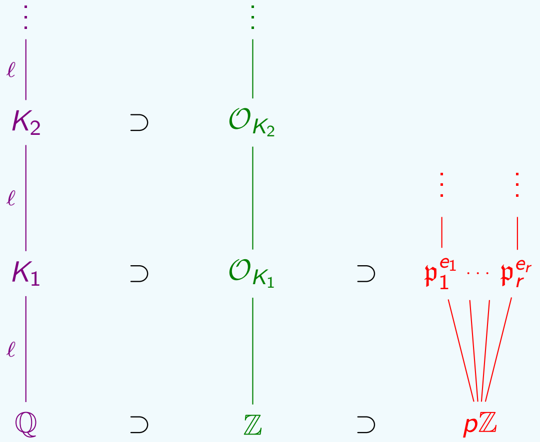
$$T_\ell^n(x) - t := \underbrace{T_\ell \circ \cdots \circ T_\ell}_{n}(x) - t = T_{\ell^n}(x) - t$$

where ℓ is an odd prime, and t is an integer for which every iterate is irreducible.

A Chebyshev radical θ_n is a root of $T_\ell^n(x) - t$.

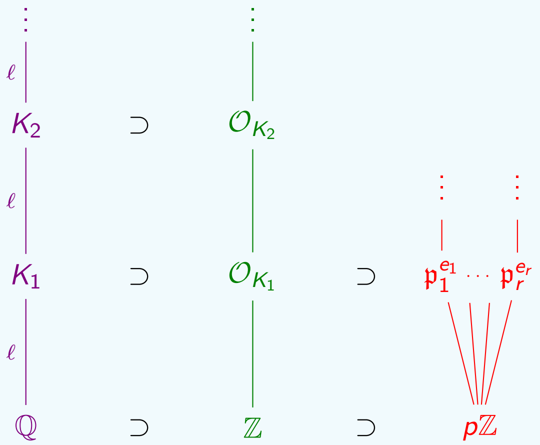
Chebyshev Radical Extensions

A Chebyshev radical θ_n is a root of $T_\ell^n(x) - t$. Consider a sequence of roots: $\{t = \theta_0, \theta_1, \theta_2, \ldots\}$ satisfying $T_\ell(\theta_n) = \theta_{n-1}$. (i.e. θ_n is a root of $T_\ell^n(x) - t$.) Let $K_n = \mathbb{Q}(\theta_n)$.



Chebyshev Radical Extensions

A Chebyshev radical θ_n is a root of $T_\ell^n(x) - t$. Consider a sequence of roots: $\{t = \theta_0, \theta_1, \theta_2, \ldots\}$ satisfying $T_\ell(\theta_n) = \theta_{n-1}$. (i.e. θ_n is a root of $T_\ell^n(x) - t$.) Let $K_n = \mathbb{Q}(\theta_n)$.



– disc(K_n)?

– basis for $\mathcal{O}_{K_n}$?

– decomposition of primes?

Bobby Grizzard

UNCG Summer School 2013

Department of Mathematics
The University of Texas at Austin
rgrizzard@math.utexas.edu

May 21, 2013

Interests

Interests

Things I like:

Interests

Things I like:

- Heights (and Diophantine geometry)

Interests

Things I like:

- Heights (and Diophantine geometry)
- Infinite algebraic extensions of $\mathbb{Q}$

Interests

Things I like:

- Heights (and Diophantine geometry)
- Infinite algebraic extensions of $\mathbb{Q}$
- Applications of group theory to number theory

Interests

Things I like:

- Heights (and Diophantine geometry)
- Infinite algebraic extensions of $\mathbb{Q}$
- Applications of group theory to number theory
- Using computation to gain insight to theoretical problems – Sage, GAP

Interests

Things I like:

- Heights (and Diophantine geometry)
- Infinite algebraic extensions of $\mathbb{Q}$
- Applications of group theory to number theory
- Using computation to gain insight to theoretical problems – Sage, GAP
- Elliptic curves and abelian varieties

Interests

Things I like:

- Heights (and Diophantine geometry)
- Infinite algebraic extensions of $\mathbb{Q}$
- Applications of group theory to number theory
- Using computation to gain insight to theoretical problems – Sage, GAP
- Elliptic curves and abelian varieties
- Unlikely intersections

Problems I have thought about / am thinking about

Problems I have thought about / am thinking about

- If a field extension is generated by polynomials of a given degree d, are all sub extensions generated by polynomials of degree at most d?

Problems I have thought about / am thinking about

- If a field extension is generated by polynomials of a given degree d, are all sub extensions generated by polynomials of degree at most d?
- Are there only finitely many elements of height $\leq T$ in the infinite extension $\mathbb{Q}^{(d)} := \mathbb{Q}(\beta \mid [\mathbb{Q}(\beta) : \mathbb{Q}] \leq d)$? (Northcott Property)

Problems I have thought about / am thinking about

- If a field extension is generated by polynomials of a given degree d, are all sub extensions generated by polynomials of degree at most d?
- Are there only finitely many elements of height $\leq T$ in the infinite extension $\mathbb{Q}^{(d)} := \mathbb{Q}(\beta \mid [\mathbb{Q}(\beta) : \mathbb{Q}] \leq d)$? (Northcott Property)
- If $A/\mathbb{Q}$ is an abelian variety, is there an $\varepsilon > 0$ such that if $\alpha \in \mathbb{Q}(A_{\text{tors}})$, then α has height $\geq \varepsilon$? (Bogomolov Property)

Problems I have thought about / am thinking about

- If a field extension is generated by polynomials of a given degree d, are all sub extensions generated by polynomials of degree at most d?
- Are there only finitely many elements of height $\leq T$ in the infinite extension $\mathbb{Q}^{(d)} := \mathbb{Q}(\beta \mid [\mathbb{Q}(\beta) : \mathbb{Q}] \leq d)$? (Northcott Property)
- If $A/\mathbb{Q}$ is an abelian variety, is there an $\varepsilon > 0$ such that if $\alpha \in \mathbb{Q}(A_{\text{tors}})$, then α has height $\geq \varepsilon$? (Bogomolov Property)
    - Can ε be chosen to depend only on the dimension of A?

Problems I have thought about / am thinking about

- If a field extension is generated by polynomials of a given degree d, are all sub extensions generated by polynomials of degree at most d?
- Are there only finitely many elements of height $\leq T$ in the infinite extension $\mathbb{Q}^{(d)} := \mathbb{Q}(\beta \mid [\mathbb{Q}(\beta) : \mathbb{Q}] \leq d)$? (Northcott Property)
- If $A/\mathbb{Q}$ is an abelian variety, is there an $\varepsilon > 0$ such that if $\alpha \in \mathbb{Q}(A_{\text{tors}})$, then α has height $\geq \varepsilon$? (Bogomolov Property)
  - Can ε be chosen to depend only on the dimension of A?
- What is the relationship between properties such at the Bogomolov and Northcott properties, Galois theory, and field arithmetic?

Problems I have thought about / am thinking about

- If a field extension is generated by polynomials of a given degree d, are all sub extensions generated by polynomials of degree at most d?
- Are there only finitely many elements of height $\leq T$ in the infinite extension $\mathbb{Q}^{(d)} := \mathbb{Q}(\beta \mid [\mathbb{Q}(\beta) : \mathbb{Q}] \leq d)$? (Northcott Property)
- If $A/\mathbb{Q}$ is an abelian variety, is there an $\varepsilon > 0$ such that if $\alpha \in \mathbb{Q}(A_{\text{tors}})$, then α has height $\geq \varepsilon$? (Bogomolov Property)
    - Can ε be chosen to depend only on the dimension of A?
- What is the relationship between properties such at the Bogomolov and Northcott properties, Galois theory, and field arithmetic?
- Lehmer's conjecture (the one about Mahler measure)

The representation problem for inhomogeneous quadratic polynomials

Anna Haensch

Wesleyan University

May 20th, 2013

The Representation Problem

Given a polynomial $f(\vec{x})$ in several variables with rational coefficients, and an integer a, we say that f represents a when the diophantine equation

$$f(\vec{x}) = a$$

has a solution over the integers.

The Representation Problem

Given a polynomial $f(\vec{x})$ in several variables with rational coefficients, and an integer a, we say that f represents a when the diophantine equation

$$f(\vec{x}) = a$$

has a solution over the integers.

$$f(x) = Q(x) + \ell(x) + c$$

The Representation Problem

Given a polynomial $f(\vec{x})$ in several variables with rational coefficients, and an integer a, we say that f represents a when the diophantine equation

$$f(\vec{x}) = a$$

has a solution over the integers.

$$f(x) = Q(x) + \ell(x)$$

The Representation Problem

Given a polynomial $f(\vec{x})$ in several variables with rational coefficients, and an integer a, we say that f represents a when the diophantine equation

$$f(\vec{x}) = a$$

has a solution over the integers.

$$f(x) = Q(x) + 2B(v, x)$$

n is represented by $f(x)$

Inhomogeneous Quadratic Polynomial

n is represented by $f(x)$ | Inhomogeneous Quadratic Polynomial

$$\Updownarrow$$

$Q(v) + n$ is represented by $v + N$ | Coset of a Quadratic Lattice

n is represented by $f(x)$ — Inhomogeneous Quadratic Polynomial

$$\Updownarrow$$

$Q(v) + n$ is represented by $v + N$ — Coset of a Quadratic Lattice

$$\Downarrow$$

$Q(v) + n$ is represented by $M := \mathbb{Z}v + N$ — Quadratic Lattice

n is represented by $f(x)$	Inhomogeneous Quadratic Polynomial
$\Updownarrow$	
$Q(v) + n$ is represented by $v + N$	Coset of a Quadratic Lattice
$\Updownarrow$	
$Q(v) + n$ is represented by $M := \mathbb{Z}v + N$	Quadratic Lattice

n is represented by $f(x)$	Inhomogeneous Quadratic Polynomial
$\Updownarrow$	
$Q(v) + n$ is represented by $v + N$	Coset of a Quadratic Lattice
$\Updownarrow$	
$Q(v) + n$ is represented by $M := \mathbb{Z}v + N$	Quadratic Lattice

Finding Equivalence Classes of Positive Definite Quadratic Forms over Totally Real Number Fields

UNCG Summer School in Computational Number Theory 2013

Paula Hamby

Department of Mathematics and Statistics
University of North Carolina at Greensboro

May 17, 2013

Koecher Theory

- Given a totally real field, $\mathbb{F}$ and its ring of integers, $\mathcal{O}_{\mathbb{F}}$, let

$$V = \{f(x,y) = ax^2 + bxy + cy^2 \mid a, b, c \in \mathcal{O}_{\mathbb{F}}\}$$

be the set of positive definite quadratic forms over $\mathbb{F}$ and $C \subset V$ be the set of positive definite forms.

- By Koecher Theory,
  - C can be decomposed into a union of cells parameterized by perfect binary quadratic forms.
  - There are finitely many perfect binary forms up to $GL_2(\mathcal{O}_{\mathbb{F}})$ equivalence, that they can be computed using a generalization of Voronoi's work. He gave a general algorithm for computing equivalence classes of perfect n-ary forms over the rationals.
  - The cones defined by inequivalent perfect forms form a finite cover of a fundamental domain, containing representatives from each equivalence class of quadratic forms.

Finding Equivalence Classes of Binary Quadratic Forms over $\mathbb{F}$

- V is a 6-dimensional rational vector space. For $\mathbb{F} = \mathbb{Q}(\sqrt{2}), \mathcal{O}_{\mathbb{F}} = \mathbb{Z}[\omega]$, where $\omega = \sqrt{2}$, there are 2 classes of perfect forms. One defines a cone over a polytope with 12 vertices, the other defines a cone over a 5-simplex (6 vertices).
- To find an equivalence class, fix the discriminant and find the upper bound for *a* (which is found the same as for the case $\mathbb{F} = \mathbb{Q}$). The upper bound for *a* defines a bounded region for which the coefficients must belong, so loop over this region and test if found positive definite forms for equivalency and inclusion in the cones defined by the perfect forms.

Thank you!

Representation Theorems for Quadratic Forms

Jacob Hicks

University of Georgia

May 20, 2013

Tools

Theorem (Key tool)

Let q be quadratic form over a normed ring R. Let $n \in R$ be squarefree. Then there exists a $k = k(q, R)$ of bounded norm and $\vec{x} \in R^n$ such that

$$q(\vec{x}) = kn$$

Then the problem is simplified to finding reductions for all $k \notin R^\times$. If q represents kn then q represents n.

There are two ingredients to this theorem

1. "Magic Lattice" theorem
2. Minkowski's convex body theorem, Hermite Constants, Pigeon Hole Principal.

Extending the Technique

- The "Magic" lattice theorem imposes restrictions on the types of quadratic forms. Currently it requires them to be 2^n-ary and have square discriminant.
- We are restricted to rings where the Hermite constant is bounded above.
- Currently I am working to extend this by using various transforms to change the ring of the quadratic form.
- I am working on trying to using various generalization of Hermite constants (Adelic Heights, Rankin's)

Current Interests

Avi Kulkarni

May 20, 2013

My recent interests are in the geometry of curves and in computational number theory.

My recent interests are in the geometry of curves and in computational number theory.

Definition

A curve is a smooth projective variety of dimension 1. A divisor of a curve is a formal sum of points on the curve. A principle divisor is one that can be realized as the zeros and poles of a regular function.

My recent interests are in the geometry of curves and in computational number theory.

Definition

A curve is a smooth projective variety of dimension 1. A divisor of a curve is a formal sum of points on the curve. A principle divisor is one that can be realized as the zeros and poles of a regular function.

The Jacobian of a curve C is a geometric object with a group structure we can associate to the curve.

My recent interests are in the geometry of curves and in computational number theory.

Definition

A curve is a smooth projective variety of dimension 1. A divisor of a curve is a formal sum of points on the curve. A principle divisor is one that can be realized as the zeros and poles of a regular function.

The Jacobian of a curve C is a geometric object with a group structure we can associate to the curve.

Question

Given a curve and its Jacobian, describe the family of curves sharing that particular Jacobian.

S-unit equation

$$A_1 x_1 + A_2 x_2 + \ldots + A_n x_n = B$$

$$x_i \in \{p_1^{e_1} \ldots p_s^{e_s}\}$$

S-unit equation

$$A_1 x_1 + A_2 x_2 + \ldots + A_n x_n = B$$

$$x_i \in \{p_1^{e_1} \ldots p_s^{e_s}\}$$

Problem

Determine solutions with no vanishing sub-sum if they exist.

S-unit equation

$$A_1 x_1 + A_2 x_2 + \ldots + A_n x_n = B$$

$$x_i \in \{p_1^{e_1} \ldots p_s^{e_s}\}$$

Problem

Determine solutions with no vanishing sub-sum if they exist.

Approach

Using sieving techniques to confirm there are no solutions in cases where this might be expected.

Mathematical Interests

Jonah Leshin

Brown University

UNCG Summer School in Computational Number Theory

May 20, 2013

Algebraic Number Theory

Class Field Towers

Let $K = K_0$ be a number field and for $i \geq 1$, put $K_i = H_{K_{i-1}}$. Consider the tower $K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots$.

Question: Which families of number fields have infinite class field towers? For example, are there infinitely many primes p for which $\mathbb{Q}(\sqrt[3]{p})$ has infinite class field tower?

Galois Representations

What is the fixed field of the kernel of an abstract representation $\rho : G_{\mathbb{Q}} \to GL_n(F)$ if...$F = \mathbb{C}$? $n = 3$? $\operatorname{Im} \rho$ is solvable?

-Tools: Group theory, Class field theory, Serre's conjecture/ Langlands

Arithmetic Geometry

Torsion Points on Abelian Varities

Given an abelian variety A over a number field K, how does $A(K)_{tor}$ compare to $A'(K)_{tor}$ for K-isogenous A'?

How are the rational points of $A_{\mathfrak{p}}$ over all primes $\mathfrak{p}$ of K related to $A(K)_{tor}$?

Noether's Problem

Given a finite group G and a field K, what does $K(G) := K(x_g : g \in G)^G$ look like? Is it a purely transcendental extension of K? If not, what is the minimal degree d such that there is a purely transcendental extension F of K with $[K(G) : F] = d$? How does the picture change for different groups G and fields K?

Mathematical background and interests

Adam Lizzi

University of Maryland

May 17, 2013

First love: integer factorization problem

Given $n \in \mathbb{Z}$, determine prime numbers $p_1, \cdots, p_r$ so that $n = \prod_{i=1}^{r} p_i$.

Studying approaches to this problem during college convinced me to try to become a professional mathematician.

There are three sophisticated algorithms for factoring: the **quadratic sieve**, the **number field sieve**, and the **elliptic curve method**. The first two attempt to find numbers a and b satisfying $a^2 \equiv b^2 \pmod{n}$. If they succeed, then

$$n \mid a^2 - b^2 = (a-b)(a+b),$$

and potentially the factors of n have spread out among $a-b$ and $a+b$, so that we can detect them.

Largest number I've factored myself (quadratic sieve)

$424531313687724587938508659434054133107159755411 =$
$1112443125761586160 37 \times 381620690403464493177020 2903$

What I enjoy about the factorization problem is trying to bridge the gap between theoretical and practical. I'm drawn to areas like algebraic number theory and arithmetic geometry where questions of this sort abound.

Much like how a number field has objects associated to it (discriminant, regulator, integral basis, ...) that we call upon, algebraic curves have a cast of associated objects. They include the Jacobian, the zeta function, point counts over finite fields, ...

Problem

Let $C : y^2 = f(x)$ be a curve of genus two *(so* $\deg f = 5$*, and* f *satisfies some other condiitons)*. Associated to C is its **Jacobian** J_C, an algebraic surface. Determine polynomials so that J_C is the zero set of those polynomials.

Introductions
UNCG summer school in Computational Number Theory

Christine McMeekin

Previous Work

- Undergraduate thesis

- Computing/programming background

Previous Work

- Undergraduate thesis
  - Proved an upper bound on the rank of elliptic curves.

- Computing/programming background

Previous Work

- Undergraduate thesis
  - Proved an upper bound on the rank of elliptic curves.
  - Wrote some programs in SAGE to get an idea of how sharp the bound was in various cases.

- Computing/programming background

Previous Work

- Undergraduate thesis
  - Proved an upper bound on the rank of elliptic curves.
  - Wrote some programs in SAGE to get an idea of how sharp the bound was in various cases.
  - SAGE data lead to the suspicion that the hardest piece of this bound to compute may not be contributing to the bound.
- Computing/programming background

Previous Work

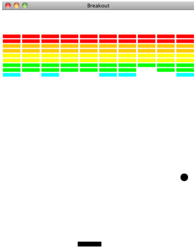
- Undergraduate thesis
  - Proved an upper bound on the rank of elliptic curves.
  - Wrote some programs in SAGE to get an idea of how sharp the bound was in various cases.
  - SAGE data lead to the suspicion that the hardest piece of this bound to compute may not be contributing to the bound.
- Computing/programming background
  - some experience with SAGE

Previous Work

- Undergraduate thesis
  - Proved an upper bound on the rank of elliptic curves.
  - Wrote some programs in SAGE to get an idea of how sharp the bound was in various cases.
  - SAGE data lead to the suspicion that the hardest piece of this bound to compute may not be contributing to the bound.
- Computing/programming background
  - some experience with SAGE
  - took intro to programming in Python

Previous Work

- Undergraduate thesis
  - Proved an upper bound on the rank of elliptic curves.
  - Wrote some programs in SAGE to get an idea of how sharp the bound was in various cases.
  - SAGE data lead to the suspicion that the hardest piece of this bound to compute may not be contributing to the bound.
- Computing/programming background
  - some experience with SAGE
  - took intro to programming in Python
  - and wrote this *totally baller* breakout game... :)



Stuff I'm learning now...

Stuff I'm learning now...

- Want to understand more about computing the Fourier coefficients of the modular invariant $J(\tau)$.

Stuff I'm learning now...

- Want to understand more about computing the Fourier coefficients of the modular invariant $J(\tau)$.
- Given an elliptic curve $E/\mathbb{Q}$ with multiplicative reduction mod some prime p, want to better understand relationships between j-invariant and the $\mathcal{L}$-invariant defined by

$$\mathcal{L}_p(E) = \frac{\log_p(q)}{\mathrm{ord}_p(q)}$$

where $q \in p\mathbb{Z}_p$ is the Tate period for E.

The Computation of Galois Groups over Local Fields

Jonathan Milstead, UNCG

The General Case

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

In all cases, OM Algorithm used to find

Splitting Field of given polynomial

Brute Force Method

First: Let $l = \frac{p^f-1}{e_o}$ and $k = \frac{r(p-1)}{e_o}$. Then Gal($T/\mathbb{Q}_p$) is generated by the maps s,t where s: $\zeta \mapsto \zeta$, $\sqrt[e_o]{\zeta^r p} \mapsto \zeta^l \sqrt[e_o]{\zeta^r p}$
and t: $\zeta \mapsto \zeta^p$, $\sqrt[e_o]{\zeta^r p} \mapsto \zeta^k \sqrt[e_o]{\zeta^r p}$
Second: Continue maps s and t to W. If Defining Polynomial of W has m roots, obtain $2m$ maps.
Third: Use OM Algorithm to find roots of inputted polynomial : $\{\alpha_1, ...\alpha_n\}$.
Fourth: Identify Transitive Subgroup of S_n. Each map corresponds to one generator. Each generator formed by tracking how maps send an α_i to an α_j.

Primitive Prime Divisors in Arithmetic Dynamics

Khoa Nguyen

Department of Mathematics
UC Berkeley

May 2013

Diophantine geometry: studies K-rational points on varieties defined over K where K is arithmetically interesting (e.g.: number fields, function fields,...)

Dynamics: studies a self-map $\phi: S \to S$, and all the iterates ϕ^n for $n \in \mathbb{N}$.

Arithmetic dynamics: when K is arithmetically interesting, S is a variety over K, and ϕ is a K-morphism.

Example: a special case of a joint result with Chad Gratton and Thomas Tucker (to appear Bulletin London Math. Soc.):

Diophantine geometry: studies K-rational points on varieties defined over K where K is arithmetically interesting (e.g.: number fields, function fields,...)

Dynamics: studies a self-map $\phi: S \to S$, and all the iterates ϕ^n for $n \in \mathbb{N}$.

Arithmetic dynamics: when K is arithmetically interesting, S is a variety over K, and ϕ is a K-morphism.

Example: a special case of a joint result with Chad Gratton and Thomas Tucker (to appear Bulletin London Math. Soc.):

Diophantine geometry: studies K-rational points on varieties defined over K where K is arithmetically interesting (e.g.: number fields, function fields,...)

Dynamics: studies a self-map $\phi : S \to S$, and all the iterates ϕ^n for $n \in \mathbb{N}$.

Arithmetic dynamics: when K is arithmetically interesting, S is a variety over K, and ϕ is a K-morphism.

Example: a special case of a joint result with Chad Gratton and Thomas Tucker (to appear Bulletin London Math. Soc.):

Diophantine geometry: studies K-rational points on varieties defined over K where K is arithmetically interesting (e.g.: number fields, function fields,...)

Dynamics: studies a self-map $\phi: \ S \to S$, and all the iterates ϕ^n for $n \in \mathbb{N}$.

Arithmetic dynamics: when K is arithmetically interesting, S is a variety over K, and ϕ is a K-morphism.

Example: a special case of a joint result with Chad Gratton and Thomas Tucker (to appear Bulletin London Math. Soc.):

Theorem

Let $\phi(X) \in \mathbb{Q}[X]$ of degree $d \geq 2$. Let $a \in \mathbb{Q}$ having infinite ϕ-orbit. Assume the ABC conjecture.

(a) Assume that $\phi(X)$ does not have the form uX^d. Then for all $n >> 0$, there is a prime p (depending on n) such that $v_p(\phi^n(a)) > 0$ and $v_p(\phi^m(a)) \leq 0$ for all $1 \leq m < n$.

(b) Assume that $\phi^n(X)$ has a square-free factor in $\bar{\mathbb{Q}}[X]$ for every n. Then for all $n >> 0$, there is a prime p (depending on n) such that $v_p(\phi^n(a)) = 1$ and $v_p(\phi^m(a)) \leq 0$ for all $1 \leq m < n$.

THANK YOU.

Theorem

Let $\phi(X) \in \mathbb{Q}[X]$ of degree $d \geq 2$. Let $a \in \mathbb{Q}$ having infinite ϕ-orbit. Assume the ABC conjecture.

(a) Assume that $\phi(X)$ does not have the form uX^d. Then for all $n >> 0$, there is a prime p (depending on n) such that $v_p(\phi^n(a)) > 0$ and $v_p(\phi^m(a)) \leq 0$ for all $1 \leq m < n$.

(b) Assume that $\phi^n(X)$ has a square-free factor in $\bar{\mathbb{Q}}[X]$ for every n. Then for all $n >> 0$, there is a prime p (depending on n) such that $v_p(\phi^n(a)) = 1$ and $v_p(\phi^m(a)) \leq 0$ for all $1 \leq m < n$.

THANK YOU.

Theorem

Let $\phi(X) \in \mathbb{Q}[X]$ of degree $d \geq 2$. Let $a \in \mathbb{Q}$ having infinite ϕ-orbit. Assume the ABC conjecture.

(a) Assume that $\phi(X)$ does not have the form uX^d. Then for all $n >> 0$, there is a prime p (depending on n) such that $v_p(\phi^n(a)) > 0$ and $v_p(\phi^m(a)) \leq 0$ for all $1 \leq m < n$.

(b) Assume that $\phi^n(X)$ has a square-free factor in $\bar{\mathbb{Q}}[X]$ for every n. Then for all $n >> 0$, there is a prime p (depending on n) such that $v_p(\phi^n(a)) = 1$ and $v_p(\phi^m(a)) \leq 0$ for all $1 \leq m < n$.

THANK YOU.

Theorem

Let $\phi(X) \in \mathbb{Q}[X]$ of degree $d \geq 2$. Let $a \in \mathbb{Q}$ having infinite ϕ-orbit. Assume the ABC conjecture.

(a) Assume that $\phi(X)$ does not have the form uX^d. Then for all $n >> 0$, there is a prime p (depending on n) such that $v_p(\phi^n(a)) > 0$ and $v_p(\phi^m(a)) \leq 0$ for all $1 \leq m < n$.

(b) Assume that $\phi^n(X)$ has a square-free factor in $\bar{\mathbb{Q}}[X]$ for every n. Then for all $n >> 0$, there is a prime p (depending on n) such that $v_p(\phi^n(a)) = 1$ and $v_p(\phi^m(a)) \leq 0$ for all $1 \leq m < n$.

THANK YOU.

On Generalizations and Applications of OM Algorithms

Brian Sinclair

April 17, 2013

OM Algorithms have been described by several mathematicians including Mac Lane, Ford, Okutsu, Cantor-Gordon, Montes, and Pauli, to answer questions related to:

- Computing integral bases (both local and global)
- Factoring polynomials over local fields
- Ideal decomposition in global fields
- Computing valuations
- Computing completions of global fields

OM Algorithms

OM Algorithms have been described by several mathematicians including Mac Lane, Ford, Okutsu, Cantor-Gordon, Montes, and Pauli, to answer questions related to:

- Computing integral bases (both local and global)
- Factoring polynomials over local fields
- Ideal decomposition in global fields
- Computing valuations
- Computing completions of global fields

These algorithms construct a sequence of polynomials with strictly increasing (and known) degrees and valuations that encode strong arithmetic invariants about ramification, inertia, and more. These are called *Okutsu invariants*.

Applications and Generalizations

With papers being regularly published in the ongoing study of OM algorithms, there is future work to be done. My work will include:

With papers being regularly published in the ongoing study of OM algorithms, there is future work to be done. My work will include:

- OM implementation in SAGE

Applications and Generalizations

With papers being regularly published in the ongoing study of OM algorithms, there is future work to be done. My work will include:

- OM implementation in SAGE
- Polynomials with given Okutsu invariants

With papers being regularly published in the ongoing study of OM algorithms, there is future work to be done. My work will include:

- OM implementation in SAGE
- Polynomials with given Okutsu invariants
- A clear guide to OM algorithms and known applications

Applications and Generalizations

With papers being regularly published in the ongoing study of OM algorithms, there is future work to be done. My work will include:

- OM implementation in SAGE
- Polynomials with given Okutsu invariants
- A clear guide to OM algorithms and known applications
- How Okutsu invariants classify polynomials and their extensions

With papers being regularly published in the ongoing study of OM algorithms, there is future work to be done. My work will include:

- OM implementation in SAGE
- Polynomials with given Okutsu invariants
- A clear guide to OM algorithms and known applications
- How Okutsu invariants classify polynomials and their extensions
- Maximal Tamely Ramified Subextensions and Splitting Fields

Applications and Generalizations

With papers being regularly published in the ongoing study of OM algorithms, there is future work to be done. My work will include:

- OM implementation in SAGE
- Polynomials with given Okutsu invariants
- A clear guide to OM algorithms and known applications
- How Okutsu invariants classify polynomials and their extensions
- Maximal Tamely Ramified Subextensions and Splitting Fields
- The three "discriminants": classical, reduced, Okutsu

Applications and Generalizations

With papers being regularly published in the ongoing study of OM algorithms, there is future work to be done. My work will include:

- OM implementation in SAGE
- Polynomials with given Okutsu invariants
- A clear guide to OM algorithms and known applications
- How Okutsu invariants classify polynomials and their extensions
- Maximal Tamely Ramified Subextensions and Splitting Fields
- The three "discriminants": classical, reduced, Okutsu
- Further ideas: Multivariate polynomials, characteristic polynomials

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 20, 2013

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

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_2 x^2 + a_1 x + 1 \in \mathbb{Z}[x].$$

For this reason, $e^{-2\zeta'(0,\mathcal{C})}$ is called a "Stark unit". By class field theory, there exists a ray class field $\mathsf{F}_2 := \mathsf{F}(\mathfrak{m}\mathfrak{p}_\infty^{(2)})$ with the following special property: F_2 is an abelian extension of F with 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.

Research Interests

Caroline L. Turnage-Butterbaugh

Advisor: Micah B. Milinovich

Department of Mathematics
University of Mississippi

Research Interests

Analytic number theory, in particular the Riemann zeta-function and its generalizations, called L-functions.

Research Interests

Analytic number theory, in particular the Riemann zeta-function and its generalizations, called L-functions.

Moments of the Riemann zeta-function:

$$I_k(T) := \int_0^T \left|\zeta(\tfrac{1}{2}+it)\right|^{2k} dt$$

Research Interests

Analytic number theory, in particular the Riemann zeta-function and its generalizations, called L-functions.

Moments of the Riemann zeta-function:

$$I_k(T) := \int_0^T \left|\zeta(\tfrac{1}{2}+it)\right|^{2k} dt$$

Moments can be used to study:

- the growth of a function on average
- the behavior of zeros of the function
  - the zeros of $\zeta(s)$ $\longleftrightarrow$ the prime numbers

Research Interests

Analytic number theory, in particular the Riemann zeta-function and its generalizations, called L-functions.

Moments of the Riemann zeta-function:

$$I_k(T) := \int_0^T \left|\zeta(\tfrac{1}{2}+it)\right|^{2k} dt$$

Moments can be used to study:

- the growth of a function on average
- the behavior of zeros of the function
  - the zeros of $\zeta(s)$ $\longleftrightarrow$ the prime numbers

Moments are also intriguing objects of study in their own right!

L-functions (generalizations of the Riemann zeta-function)

L-functions (generalizations of the Riemann zeta-function)

Some examples:

- $L(s, \chi)$ Dirichlet L-function of a primitive character χ

L-functions (generalizations of the Riemann zeta-function)

Some examples:

- $L(s, \chi)$ Dirichlet L-function of a primitive character χ
- $\zeta_K(s)$ Dedekind zeta-function of a number field K

L-functions (generalizations of the Riemann zeta-function)

Some examples:

- $L(s, \chi)$ Dirichlet L-function of a primitive character χ
- $\zeta_K(s)$ Dedekind zeta-function of a number field K
- $L(s, E)$ L-function of an elliptic curve E over $\mathbb{Q}$

L-functions (generalizations of the Riemann zeta-function)

Some examples:

- $L(s, \chi)$ Dirichlet L-function of a primitive character χ
- $\zeta_K(s)$ Dedekind zeta-function of a number field K
- $L(s, E)$ L-function of an elliptic curve E over $\mathbb{Q}$

Moments of products of automorphic L-functions:

$$\int_0^T \left|L(\tfrac{1}{2}+it, \pi_1)\right|^{2k_1} \cdots \left|L(\tfrac{1}{2}+it, \pi_r)\right|^{2k_r} dt$$

L-functions (generalizations of the Riemann zeta-function)

Some examples:

- $L(s,\chi)$ Dirichlet L-function of a primitive character χ
- $\zeta_K(s)$ Dedekind zeta-function of a number field K
- $L(s,E)$ L-function of an elliptic curve E over $\mathbb{Q}$

Moments of products of automorphic L-functions:

$$\int_0^T \left|L(\tfrac{1}{2}+it,\pi_1)\right|^{2k_1}\cdots\left|L(\tfrac{1}{2}+it,\pi_r)\right|^{2k_r}\,dt$$

Moments in families:

$$\sum_{|d|\le X} L(\tfrac{1}{2},\pi_1\otimes\chi_d)^{k_1}\cdots L(\tfrac{1}{2},\pi_r\otimes\chi_d)^{k_r}$$

Modular Forms Over Number Fields

Dan Yasaki

The University of North Carolina Greensboro

May 20, 2013
UNCG Summer School 2013
Computational Algebraic Number Theory

Modular forms over $\mathbb{Q}$

A holomorphic function $f\colon \mathfrak{h} \to \mathbb{C}$ is a *weight 2 modular form of level N* if

- $f(\gamma \cdot z) = (cz+d)^2 f(z)$ for every $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N)$, and
- f satisfies certain growth conditions.

$$f(q) = \sum_{n \geq 0} a_n q^n, \quad q = e^{2\pi i z}.$$

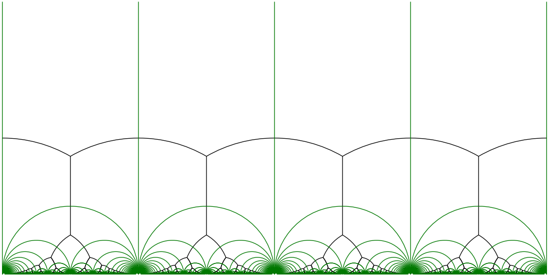
- There is a link between elliptic curves and certain cusp forms
$$a_p(f) = p + 1 - \#E(\mathbb{F}_p).$$
- The a_p are eigenvalues of Hecke operators.

UNCG

Tessellation of $\mathfrak{h}$

Cusp forms and Hecke operators can be described cohomologically

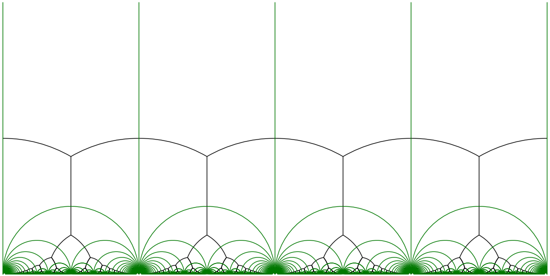
$$H^1(\Gamma_0(N)\backslash\mathfrak{h};\mathbb{C}) \simeq S_2(N) \oplus \overline{S}_2(N) \oplus \mathrm{Eis}_2(N).$$



Tessellation of $\mathfrak{h}$

Cusp forms and Hecke operators can be described cohomologically

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



Generalize...