UNCG 125
Celebrating 125 Years of Opportunity & Excellence

Summer School in Computational Number Theory

NSF

Algorithms for Extensions of Large Degree

May 28 to June 1, 2018

Speakers

- **Peter Bruin** (Universiteit Leiden)
- **Claus Fieker** (Technische Universität Kaiserslautern)
- **Jordi Guàrdia** (Universitat Politècnica de Catalunya)

Organized by the number theory group at UNCG

www.uncg.edu/mat/numbertheory/summerschool

Introduction and Research Interests

Vishal Arul

MIT

Research Interests

- Interested in studying computational aspects of jacobians of superelliptic curves
  - A superelliptic curve $\mathcal{C}$ is the projective normalization of the affine $\mathbf{A}^2$-curve cut out by the equation $y^n = f(x)$. When $n = 2$, it is called a hyperelliptic curve.
  - The curve $\mathcal{C}$ embeds into $J = \mathrm{Pic}^g\ \mathcal{C}$, a g-dimensional abelian variety.
- Previous work: helped write a program in Sage (which will be included in future versions of Sage) that uses p-adic methods to compute the characteristic polynomial of Frobenius for a superelliptic curve over $\mathbf{F}_{p^n}$. Joint with A. Best, E. Costa, R. Magner, N. Triantafillou.
  - Main accomplishment is that it runs in $O(p^{1/2+o(1)})$ time, allowing it to be of use when p is large.

Research Interests

- Suppose we are in the nice case where $d = \deg f$ is coprime to n (meaning there is a unique point at ∞) and f is separable. Then $g = (n-1)(d-1)/2$ and J can be identified with $\mathrm{Pic}^0\, \mathcal{C}$ using the unique point at ∞.
- Current work: working on generalizing a formula of Y. Zarhin about "division by 2" on hyperelliptic curves to the superelliptic case.
  - Since the Jacobian J is an abelian variety, multiplication by 2 gives an endomorphism of J. For every point P of $\mathcal{C}$, there are 2^{2g} points D on J such that $2D = P - \infty$. Zarhin gives formulas for these 2^{2g} such divisors.
  - My work is on the superelliptic generalization. Instead of multiplication by 2, consider the "$1 - \zeta$" map, where ζ is the map on J induced by the map on $\mathcal{C}$ given by $\zeta : (x, y) \mapsto (x, \zeta_n y)$. Goal is to give formulas for the n^{d-1} points D on J satisfying $(1 - \zeta)D = P - \infty$.

Hi! 😀

Alex J. Best

5/28/2018

Boston University

Coleman integration

If $C/\mathbf{R}$ is a curve, $P, Q \in C$, $\omega \in \Omega^1_C$ (e.g. $\frac{x\mathrm{d}x}{y}$), we have a path integral

$$\int_P^Q \omega \in \mathbf{R}.$$

Coleman integration

If $C/\mathbf{R}$ is a curve, $P, Q \in C$, $\omega \in \Omega^1_C$ (e.g. $\frac{x\mathrm{d}x}{y}$), we have a path integral

$$\int_P^Q \omega \in \mathbf{R}.$$

What about if $C/\mathbf{Q}_p$?

Coleman defined

$$\int_P^Q \omega \in \mathbf{Q}_p$$ 

Coleman integration

If $C/\mathbf{R}$ is a curve, $P, Q \in C$, $\omega \in \Omega^1_C$ (e.g. $\frac{x\mathrm{d}x}{y}$), we have a path integral

$$\int_P^Q \omega \in \mathbf{R}.$$

What about if $C/\mathbf{Q}_p$?

Coleman defined

$$\int_P^Q \omega \in \mathbf{Q}_p$$ 

a "path" integral, with cool properties  .

Coleman integration

If $C/\mathbf{R}$ is a curve, $P, Q \in C$, $\omega \in \Omega^1_C$ (e.g. $\frac{x\mathrm{d}x}{y}$), we have a path integral

$$\int_P^Q \omega \in \mathbf{R}.$$

What about if $C/\mathbf{Q}_p$?

Coleman defined

$$\int_P^Q \omega \in \mathbf{Q}_p$$ 

a "path" integral, with cool properties  .

These can be explicitly computed in many cases! 

Applications

Rational points: We can sometimes find ω so that

$$\text{Zeroes}\left(\int_{p_0}^{x} \omega\right) \supseteq C(\mathbf{Q})$$ 

Applications

Rational points: We can sometimes find ω so that

$$\text{Zeroes}\left(\int_{p_0}^{x}\omega\right) \supseteq C(\mathbf{Q})$$ 

Heights:

Coleman-Gross introduced a height pairing on abelian varieties, it be decomposed as a sum of local terms, one of which is

$$h_p(D_1, D_2) = \int_{D_2} \omega_{D_1}$$ 

Applications

Rational points: We can sometimes find ω so that

$$\text{Zeroes}\left(\int_{p_0}^{x}\omega\right) \supseteq C(\mathbf{Q})$$ 

Heights:

Coleman-Gross introduced a height pairing on abelian varieties, it be decomposed as a sum of local terms, one of which is

$$h_p(D_1, D_2) = \int_{D_2} \omega_{D_1}$$ 

p-adic BSD:

Using the above height pairing one can define a p-adic regulator so that for a modular abelian variety $A/\mathbf{Q}$ conjecturally

$$\mathcal{L}^*(A,0) = \epsilon_p(A)\frac{|\text{Ш}(A/\mathbf{Q})|\,\text{Reg}_\gamma(A/\mathbf{Q})\prod_v c_v}{|A(\mathbf{Q})_{\text{tors}}||A^\vee(\mathbf{Q})_{\text{tors}}|}$$ 

Introduction

Benjamin Carrillo

Arizona State University

May 28, 2018

Let L/K be a Galois extension of local fields with Galois group G. Let $\mathcal{O}_L$ be the ring of integers of L over K. For $i \in \mathbb{Z}_{\geq -1}$, let the i^{th} ramification group of L/K be the set:

$$G_i = \{s \in G \mid v_L(s(a) - a) \geq i + 1 \text{ for all } a \in \mathcal{O}_L\}$$

The set of ramification groups gives a filtration of G and provides information on how the discriminant will grow in a chain of subfields of L.

The *Galois slope content* is a vector that encapsulates this filtration. We can determine the Galois slope content of an extension by calculating the discriminant of various subfields.

Unfortunately there does not exist an efficient procedure to compute subfields of the Galois closure of p-adic field extensions, but there are more efficient methods to computing subfields of the Galois closure of number fields.

We introduce the notion of a *global splitting model*. Consider a polynomial $f(x) \in \mathbb{Z}[x]$ and let F be the field generated by a root of $f(x)$ over $\mathbb{Q}$, we say $f(x)$ is a *global splitting model* when $\mathrm{Gal}(\hat{F}/\mathbb{Q}_p) = \mathrm{Gal}(F/\mathbb{Q})$, where $\hat{F}$ is the completion of F with respect to a $\mathfrak{P}$-adic absolute value.

How can we find *global splitting models*?

- Databases
- Composita of other global splitting models
- Class Field Theory
- Generic Polynomials

My Problem

Endrit Fejzullahu

University of Florida

efejzullahu@ufl.edu

May 28, 2018

Let K be a finite extension of $\mathbb{Q}_p$ and let L/K be a totally ramified extension of degree p. Let $\mathfrak{R} \subset \mathcal{O}_K$ be the set Teichmüller representatives of $\mathcal{O}_K/(\pi_K)$. A polynomial

$$f(X) = X^p + a_{p-1}X^p + \cdots + a_1X + a_0 \in \mathcal{O}_K[x]$$

is said to be *Eisenstein* if $v_K(a_i) \geqslant 1$ and $v_K(a_0) = 1$. Let $E(L)$ be the set of Eisenstein polynomials over K that have a root in L. Let e be the ramification degree of K over $\mathbb{Q}_p$, i.e. $v_K(p) = e$. Given a polynomial $f(X) \in E(L)$, we define the type of f as follows:

1. If $\min_{1 \leqslant i \leqslant p-1} v_K(a_i) = m \leqslant e$, let λ be the least integer such that $v_K(a_\lambda) = m$, and take $\omega \in \mathfrak{R}$ such that $a_\lambda \equiv \omega \pi_K^m$. In this case the type of f is $\langle \lambda, m, \omega \rangle$.
2. If $v(a_i) \geqslant e + 1$ for $1 \leqslant i \leqslant p - 1$, we say f is of type $\langle 0 \rangle$.

Theorem

All polynomials in $E(L)$ are of the same type.

Theorem (S. Amano)

There exists a prime element of L that is root of an Eisenstein polynomial of the form

$$X^p - \omega \pi_K^m X^\lambda - \pi_K a$$

if L is of type $\langle \lambda, m, \omega \rangle$, or root of an Eisenstein polynomial of the form

$$X^p - \pi_K a$$

if L is of type $\langle 0 \rangle$.

This theorem shows that every totally ramified extension L/K of degree p is determined by an Eisenstein polynomial with only three nonzero terms. My goal is to do this more generally. That is, understand which totally ramified extensions of a local field K (not necessarily of characteristic 0) correspond to Eisenstein polynomials with only three nonzero terms.

Introduction

Nathan Fontes

Number Theory Summer School 2018 - UNCG

28 May 2018

Definition

Let k and N be integers. Then a *modular form of weight k for $\Gamma_0(N)$* is a holomorphic function $f : \mathcal{H} \to \mathbb{C}$ such that:

(i) $f(g(z)) = (cz + d)^k f(z)$ for all $g \in \Gamma_0(N)$, $z \in \mathcal{H}$.

(ii) f is holomorphic at ∞.

We can write a q-expansion of a modular form f at a point $z \in \mathcal{H}$:

$$f(z) = \sum_{n=0}^{\infty} a_n q^n \text{ for } q = e^{2\pi i z}.$$

The *p^{th} Hecke operator of weight k*, T_p, is a linear transformation on the space of weight k modular forms.

- The eigenvalues of T_p are exactly the p^{th} coefficients, a_p, in the q-expansions of eigenforms.
- Modular forms are linear combinations of such eigenforms.

Past Research

Goal: Compute spaces of modular forms of weight k for $\Gamma_0(N)$.

- Modular symbols (an infinite set of symbols modulo infinite relations) can be identified with modular forms.
- Manin symbols (a finite set of symbols modulo finite relations) can be identified with modular symbols.
- Hecke operators on Manin Symbols give information about Hecke operators on modular forms.
- Eigenforms are computed using Hecke operators on Manin symbols.

Past Research

Goal: Compute spaces of modular forms of weight k for $\Gamma_0(N)$.

- Modular symbols (an infinite set of symbols modulo infinite relations) can be identified with modular forms.
- Manin symbols (a finite set of symbols modulo finite relations) can be identified with modular symbols.
- Hecke operators on Manin Symbols give information about Hecke operators on modular forms.
- Eigenforms are computed using Hecke operators on Manin symbols.

Future Research: I am attending the Ph.D. program in mathematics at Clemson University beginning Fall 2018!

Vector-Valued Modular Forms

Richard Gottesman

University of California, Santa Cruz (grad school)
Queen's University, Ontario, Canada (postdoc)

May 28, 2018

Fun facts about myself and about vector-valued modular forms:

I do improv comedy.

I will be attending workshops and conferences in Budapest and Luxembourg in July.

I like lots of different kinds of mathematics and I hope to get some ideas for new projects during this workshop.

The generalization of a modular form with respect to a character is a vector-valued modular form with respect to a representation.

Vector-valued modular forms are used in number theory, Moonshine, and vertex operator algebras.

My work expresses certain vector-valued modular forms in terms of the Gaussian hypergeometric series evaluated at the inverse of a Hauptmodul.

One of my goals is to make progress towards proving the *unbounded denominator conjecture*:

Modular forms on a noncongruence subgroup have unbounded denominators.

Indroduction and Interests

Cole Love

UNCG

May 26, 2018

About Me

- Current second year PhD student at UNCG
- B.S. in Applied Mathematics and Computer Science at UW-Stout
- Research Interests: Additive Number Theory and Algorithmic Complexity

Waring's Problem over Finite Fields

- Waring's problem asks whether there exists some positive integer s such that every natural number can be expressed as the sum of at most s k-th powers.
- We consider the problem of representing an arbitrary polynomial as a sum of k-th powers over a field of positive characteristic.
- Let v(p,k) denote the smallest natural s such that every polynomal in $\overline{\mathbb{F}}_p[t]$ can be written as the sum of at most s k-th powers.
- Under certain conditions, we can relate v(p,k) to the sum of the digits in the base-q expansion of k.

Galois Groups of Eisenstein Polynomials over Local Fields

Jonathan Milstead

May 28, 2018

Ramification Polygons

1. Definition: Newton polygon of $\dfrac{\varphi(\alpha x + \alpha)}{\alpha^n}$.

2. One Segment (Greve): $\mathrm{Gal}(\varphi) = G_1 \rtimes H$

   $\{t_{A,v} : (\mathbb{F}_p)^m \to (\mathbb{F}_p)^m : x \mapsto Ax + v \mid A \in H' \leq \mathrm{GL}(m,p),\ v \in (\mathbb{F}_p)^m\}$

3. Max Tame Subextension (Greve)

$$T = I\left(\sqrt[e_1 e_0]{(-1)^{v_1}\gamma_1^{b_1 n}\varphi_0}, \ldots, \sqrt[e_\ell e_0]{(-1)^{v_\ell}\gamma_\ell^{b_\ell n}\varphi_0} \right)$$

Blocks

1. Greve

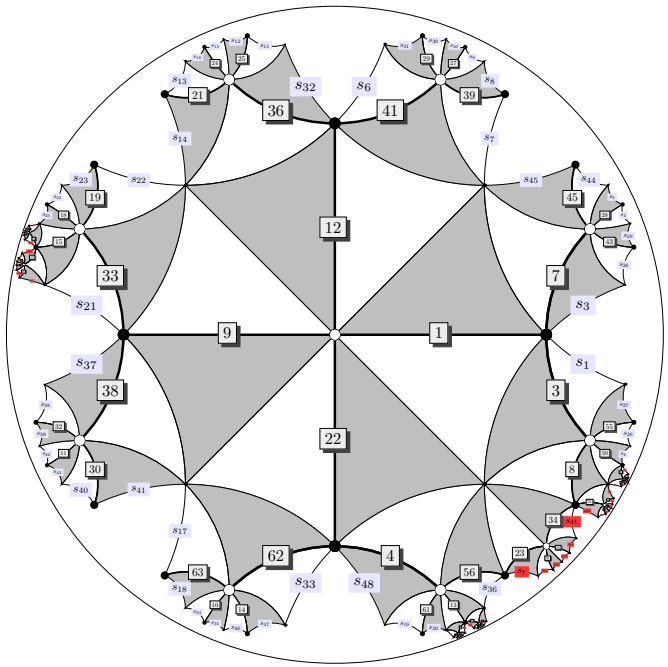
$$\Delta_i = \{\alpha' \in \overline{K} \mid \varphi(\alpha') = 0 \text{ and } \nu_L(\alpha' - \alpha_1) \geq m_i + 1\}$$

Corresponds to $K[x]/(\varphi) = L_0 \supset L_1 \supset \ldots \supset L_\ell \supset K$

2. Residual Polynomial Classes (Milstead, Pauli)

$$\left\{ \alpha' : \begin{array}{l} \varphi(\alpha') = 0 \text{ and either} \\ \\ v_L(\alpha' - \alpha_1) > m_i + 1 \text{ or} \\ \\ v_L(\alpha' - \alpha_1) = m_i + 1 \text{ and } \dfrac{-1 + \frac{\alpha'}{\alpha_1}}{\alpha_1^{m_i}} \in \delta\mathbb{F}_p \end{array} \right\}$$

(2-Group) Belyĭ maps

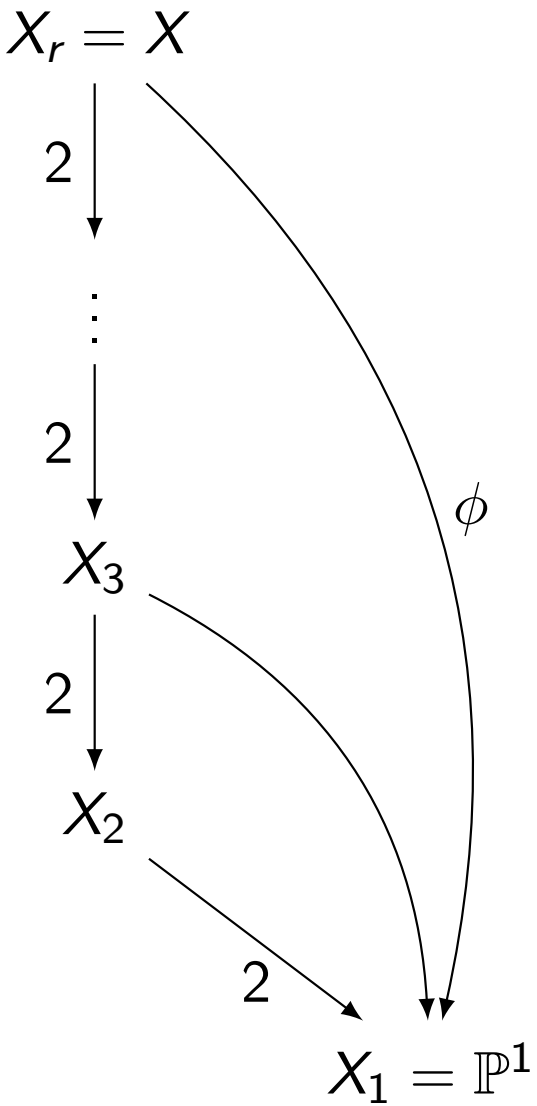


Michael Musty

UNCG Summer School in Computational Number Theory

2018

2-Group (Galois) Belyĭ maps



Nonhyperelliptic example

`128S1-128,32,128-g62` $\to$ `64S1-64,16,64-g30` $\to$
`32S1-32,8,32-g14` $\to$ `16T1-16,4,16-g6` $\to$ `8T1-8,2,8-g2` $\to$
`4T1-4,1,4-g0` $\to$ `2T1-2,1,2-g0`

$$
\begin{aligned}
X \subset \mathbb{A}^6 : & \; x_1^5 - x_1 - x_2^2 \\
& \; x_1 - x_1^3 + x_2 x_4^4 \\
& \; x_1^3 x_3 - x_1 x_3 - x_2 x_4^2 \\
& \; x_1^2 x_4^2 - x_2 x_3 + x_4^2 \\
& \; x_2 x_3 - x_1^2 - 1 \\
& \; x_3 x_4^2 - 1 \\
& \; x_5^2 - x_4 \\
& \; x_6^2 - x_5 \\
\phi : & \; x_3^4 x_2^2 - 2 x_3^2 x_2 + 1
\end{aligned}
$$

`https://math.dartmouth.edu/~mjmusty/32.html`

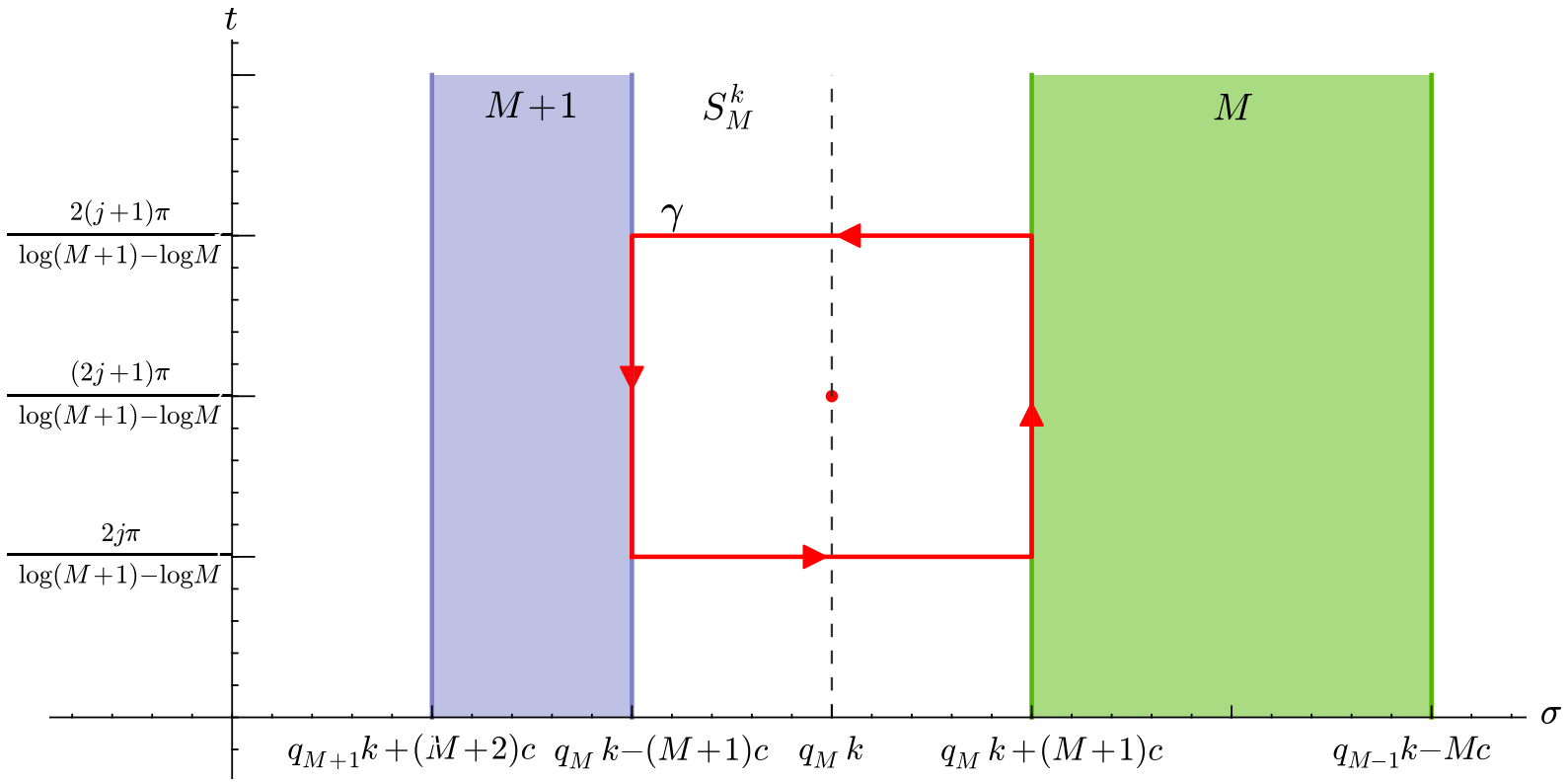
Research Interest:

Algorithms for Local Fields and Zeros of Derivatives of Zeta

Sebastian Pauli

University of North Carolina at Greensboro

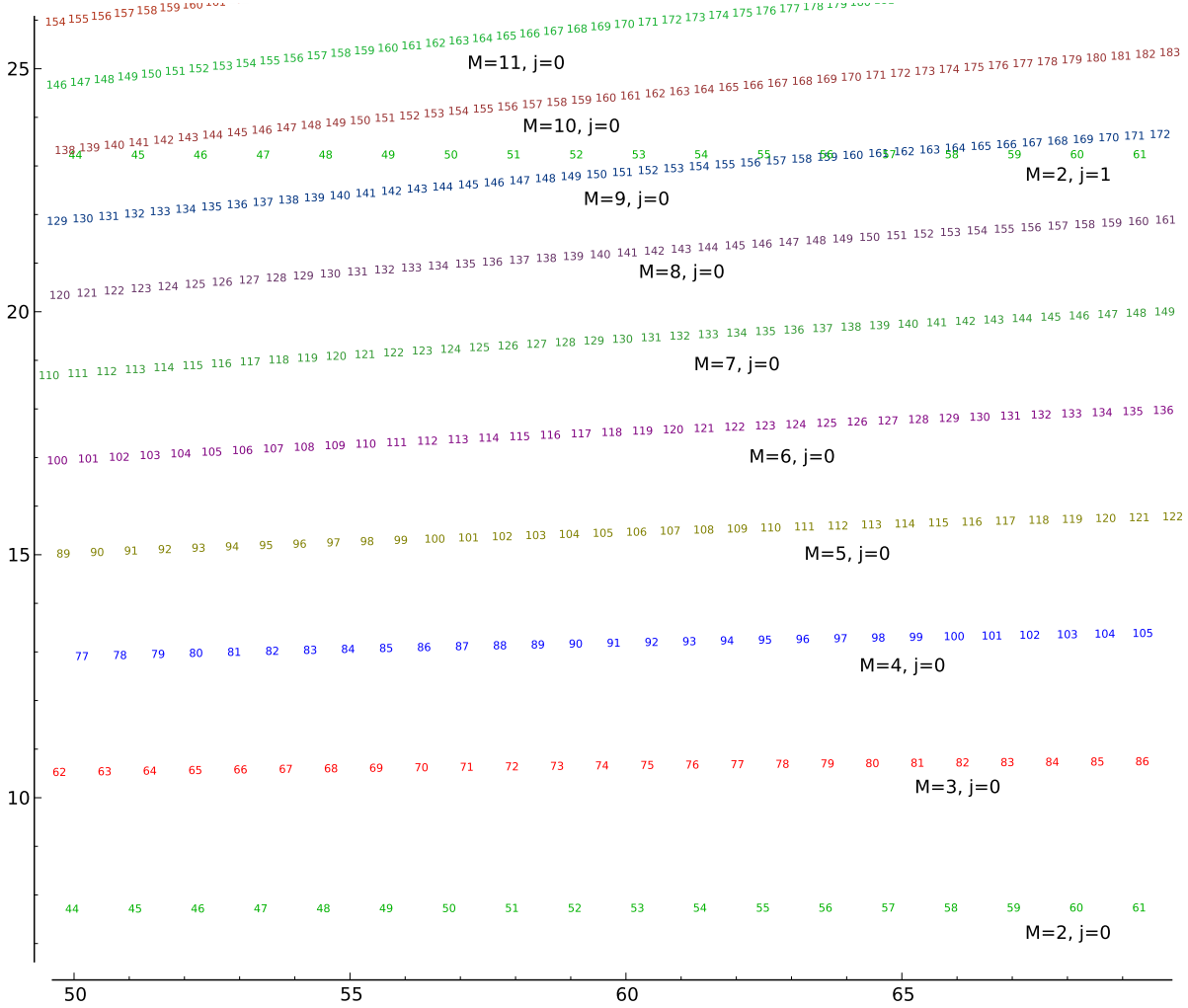
Zeros of Derivatives of ζ – Right Half Plane



Theorem (Binder, P., Saidak)

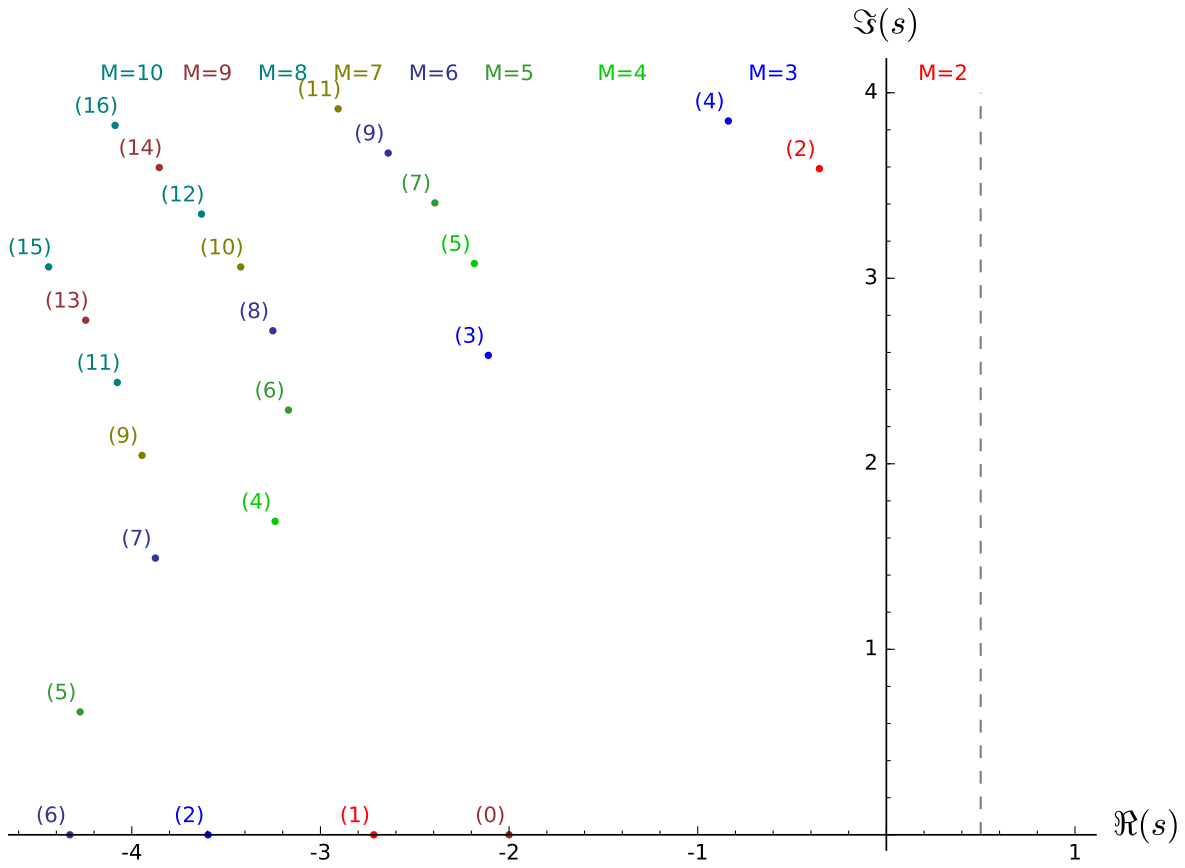
For $M \geq 2$ and $q_M = \dfrac{\log\left(\frac{\log M}{\log M+1}\right)}{\log\left(\frac{M}{M+1}\right)}$ the red box contains one zero of $\zeta^{(k)}(s)$.

Zeros of Derivatives of ζ – Right Half Plane



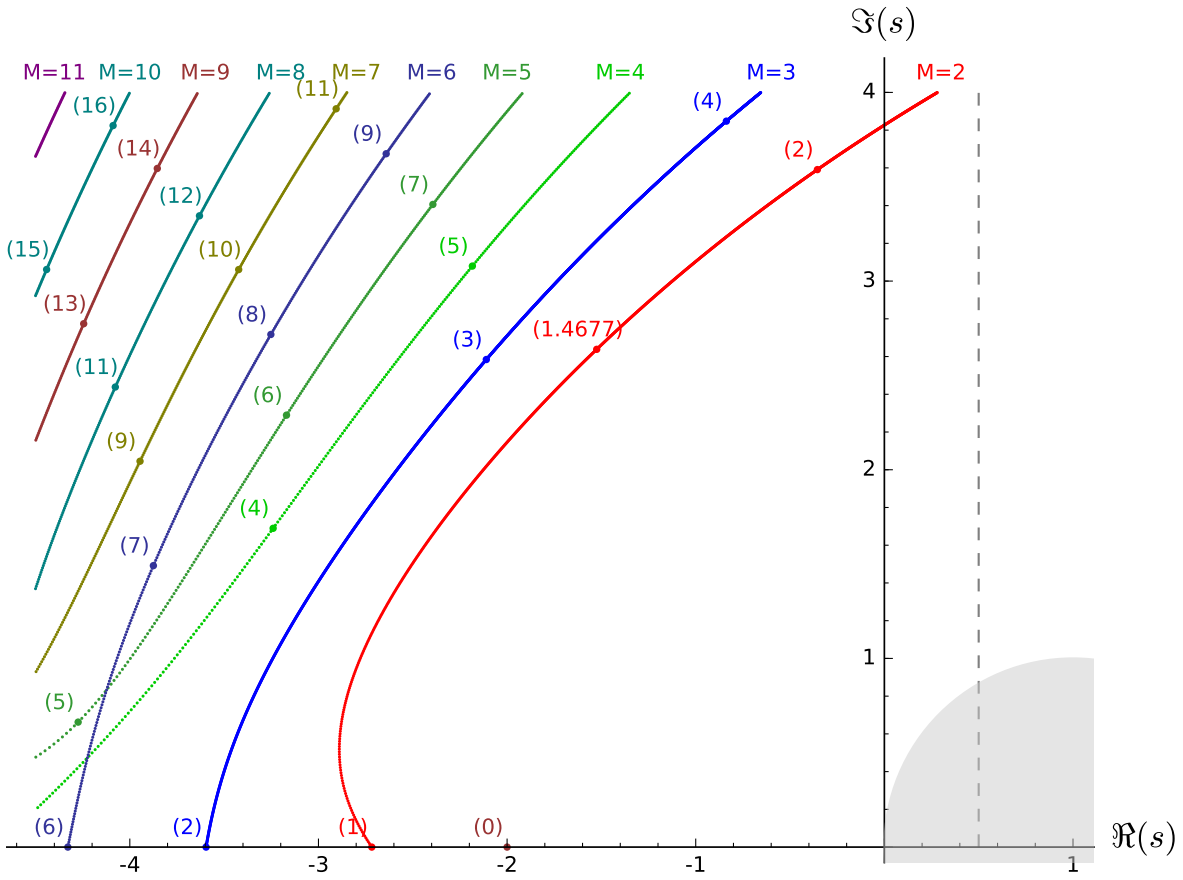
Zeros of Derivatives of ζ – Left Half Plane

with Ricky Farr and Filip Saidak



Zeros of Derivatives of ζ – Left Half Plane

with Ricky Farr and Filip Saidak



Number Theory Summer School

James Rudzinski

University of North Carolina at Greensboro

May 28, 2018

Symmetric Chain Decomposition

Definition (Symmetric chain decomposition)

A symmetric chain decomposition of B_n is a partition of B_n into symmetric chains.

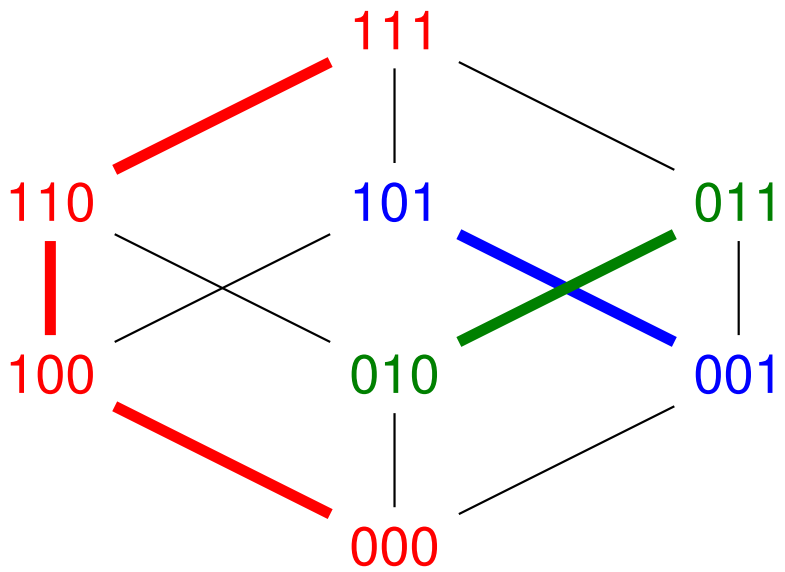


Figure: Symmetric chain decomposition of B_3

Symmetric Chain Decomposition

We were able to organize the initial strings in a tree so that each string could also be attained in an efficient way by only adding ones. We can recursively generate the initial string of each chain along with the indices of the zeros that are to be changed to ones.

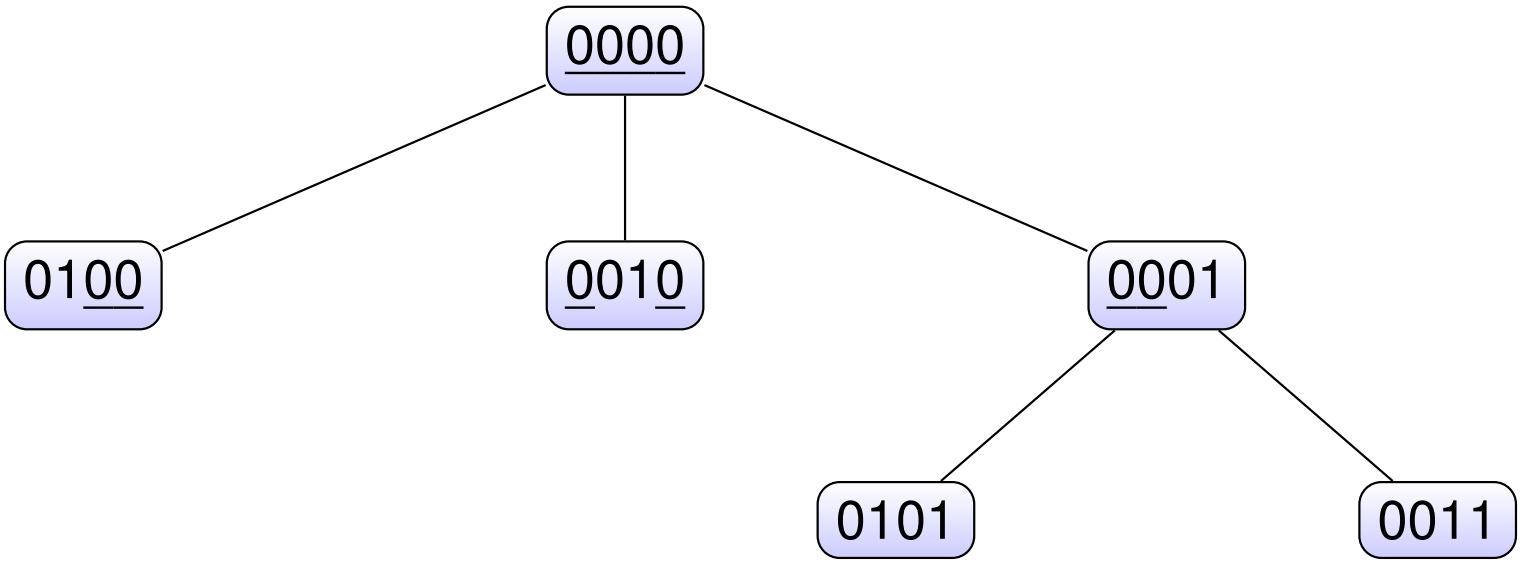


Figure: Tree of inital strings for the symmetric chain decomposition of B_4.

Introduction

Sandi Rudzinski

Department of Mathematics and Statistics
University of North Carolina at Greensboro

UNCG Number Theory Summer School

About Me and Math Interests

About Me

- I just finished my first year of being a Ph.D. student and my third year at UNCG.
- I have two daughters, ages 8 and 12.
- My undergraduate degree is in computer science, but I was also a music major. I play piano, oboe, organ, and a few others.

Math Interests / Past Research

- I love algebra and all things algebraic, and I really enjoy teaching.
- Undergraduate Project: An adaptive learning program using belief networks
- Master's Thesis: Symbolic Computation of Resolvents with Dr. Sebastian Pauli

Filip SAIDAK

Department of Mathematics

UNC Greensboro

RESEARCH INTERESTS

Analytic, Probabilistic and Elementary Number Theory

1. **Prime numbers**
   - general distribution
   - special forms
2. **Riemann ζ-function**
   - properties of zeros
   - non-vanishing
   - higher derivatives
   - monotonicity
   - Dirichlet L-functions
3. **Arithmetic functions**
   - probabilistic results
   - special values

Visible Lattice and Ammann-Beenker Points

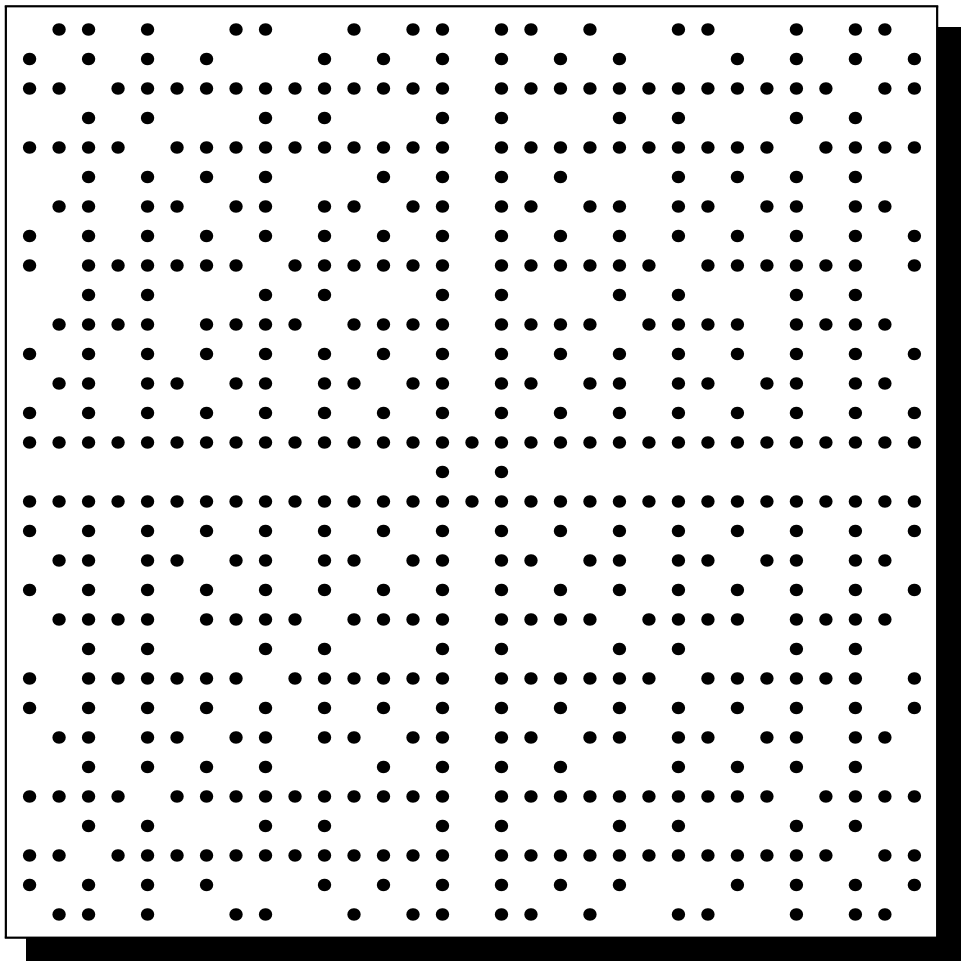
Bernd Sing

UWI, Barbados

UNC Greensboro, 28 May 2018

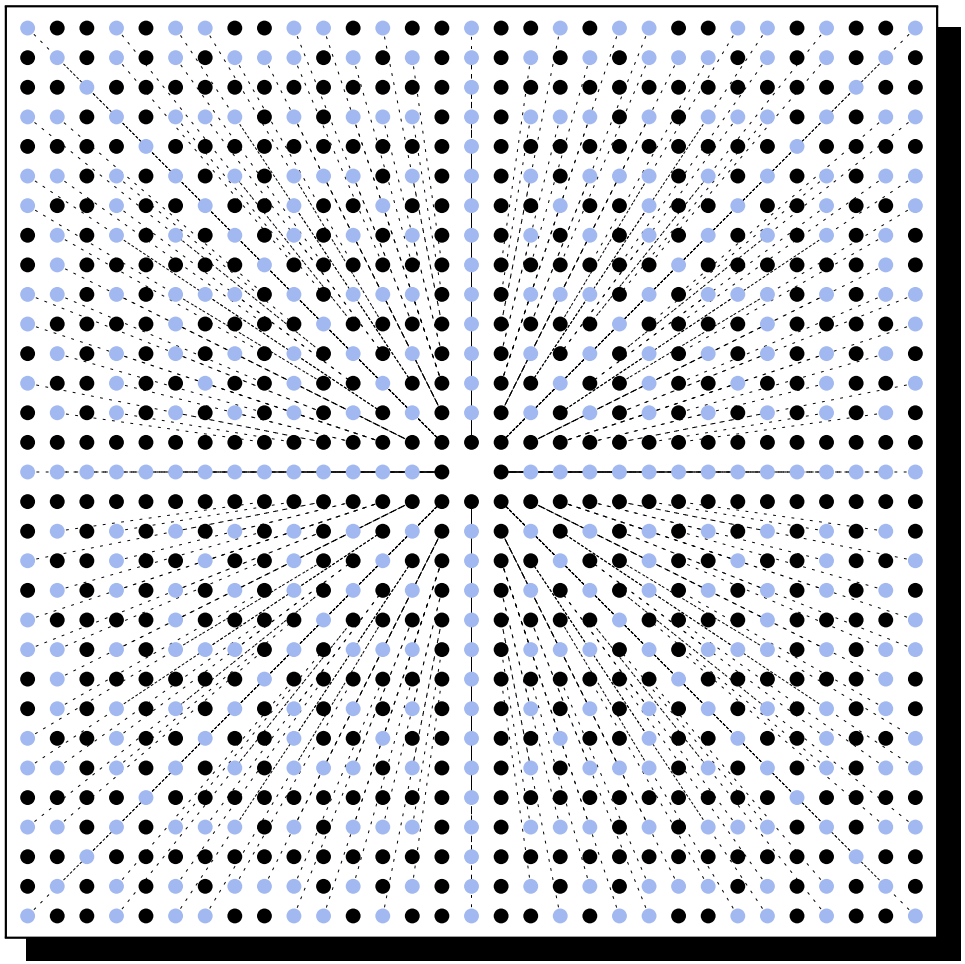
Visible Lattice Points

The *visible lattice points* V_{lat} are the points $(m, n) \in \mathbb{Z}^2$ with $\gcd(m, n) = 1$.



Visible Lattice Points

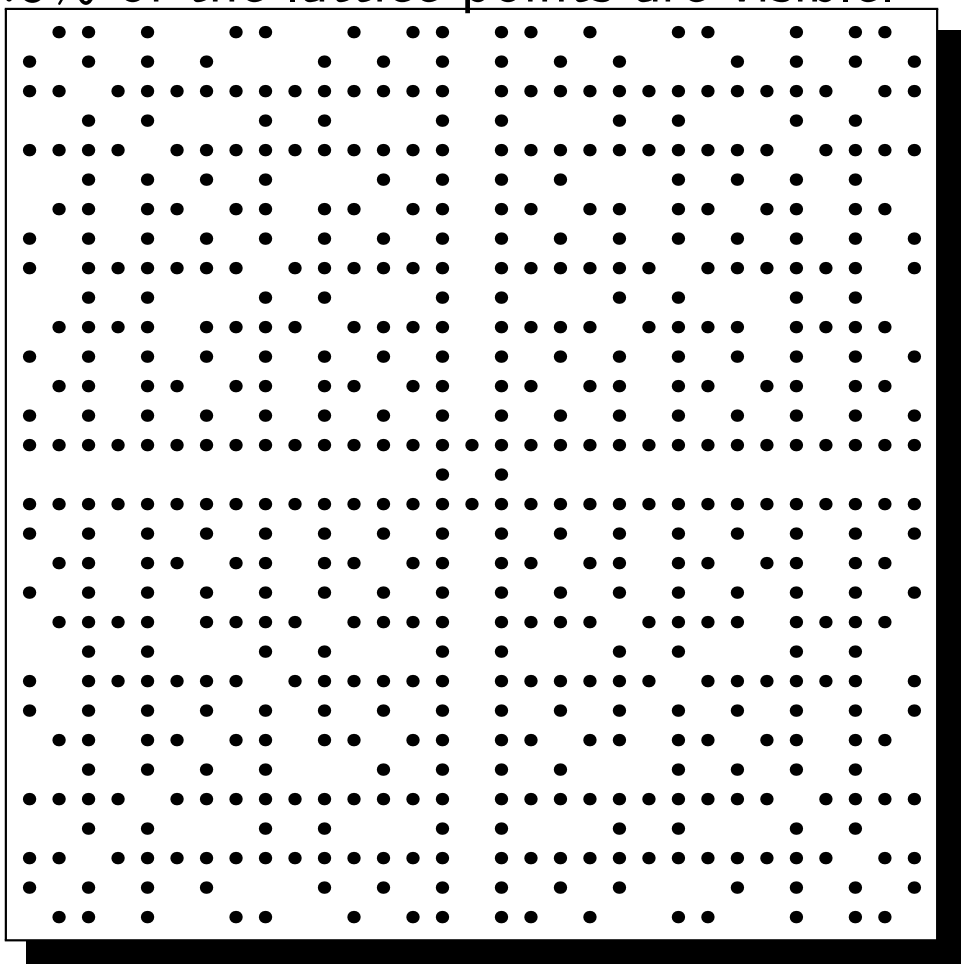
The *visible lattice points* V_{lat} are the points $(m, n) \in \mathbb{Z}^2$ with $\gcd(m, n) = 1$.



Visible Lattice Points

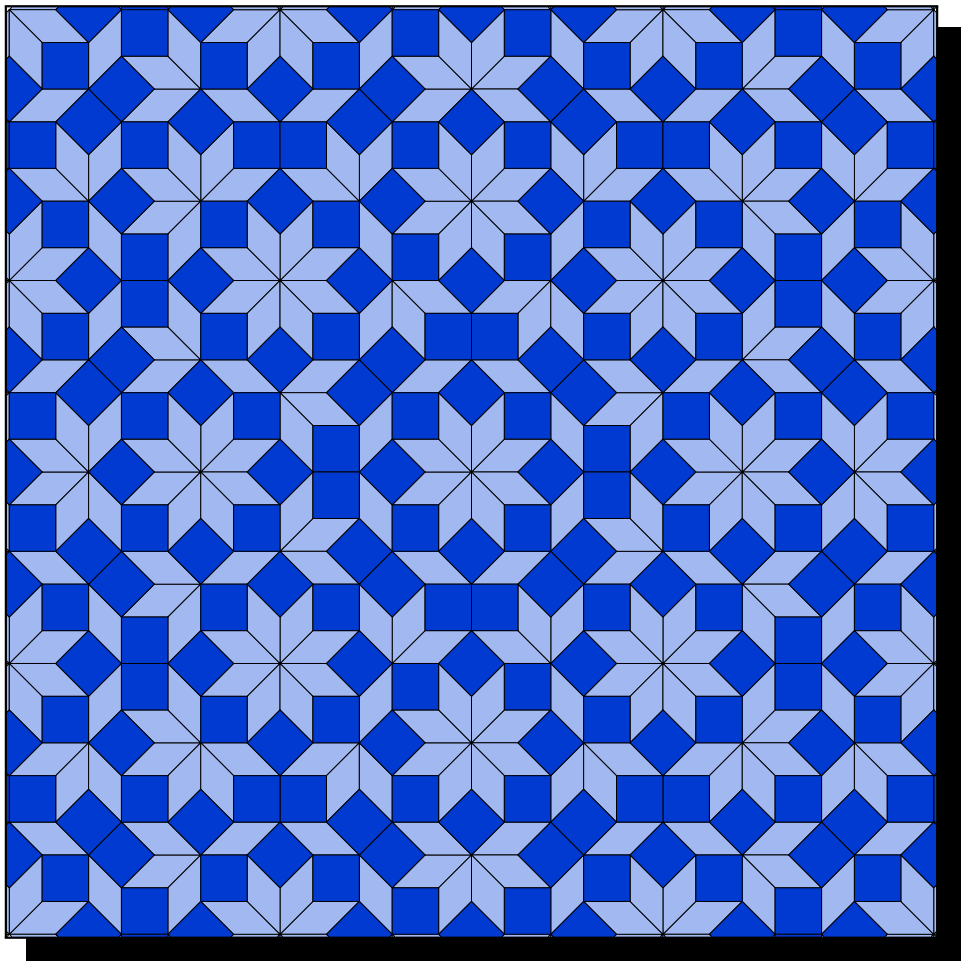
One can show dens $V_{\text{lat}} = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^2}\right) = \frac{1}{\zeta(2)} = \frac{6}{\pi^2} \approx 0.6079,$

i.e., around 60.8% of the lattice points are visible.



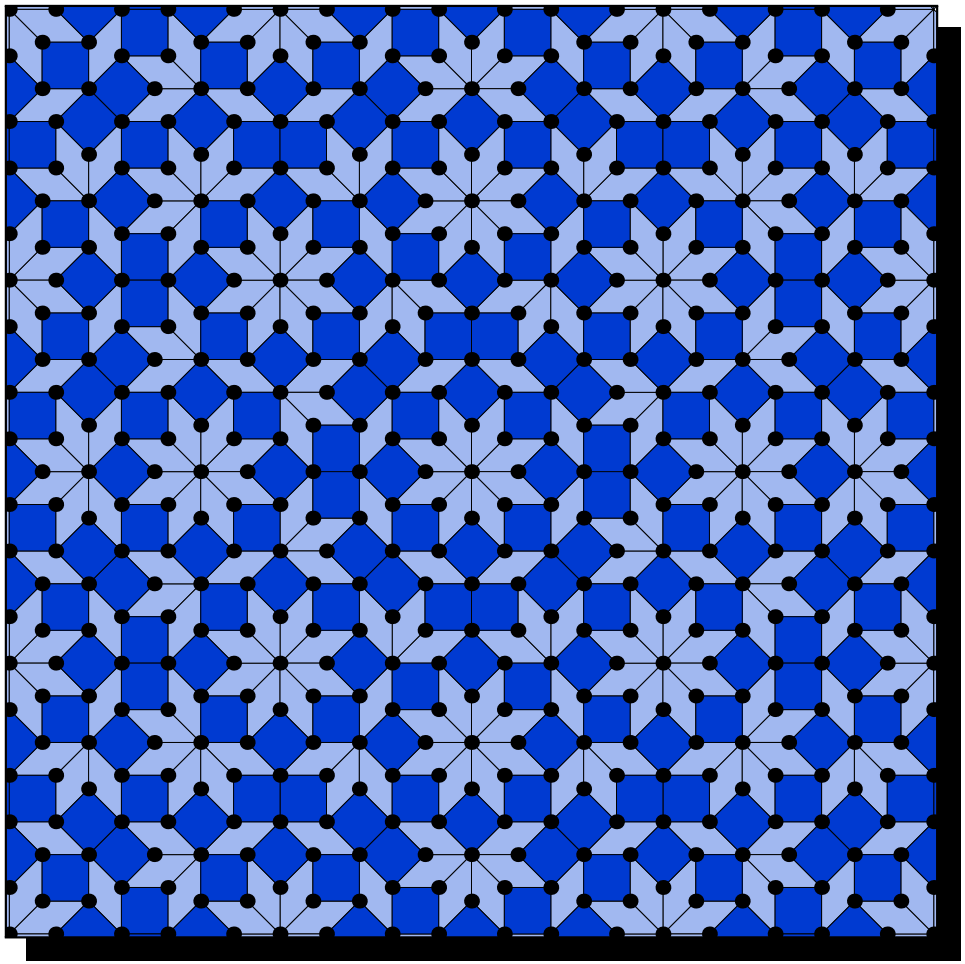
Visible Ammann-Beenker Points

The prototiles of the *Ammann-Beenker tiling* are a square and a rhomb (of sidelength 1).



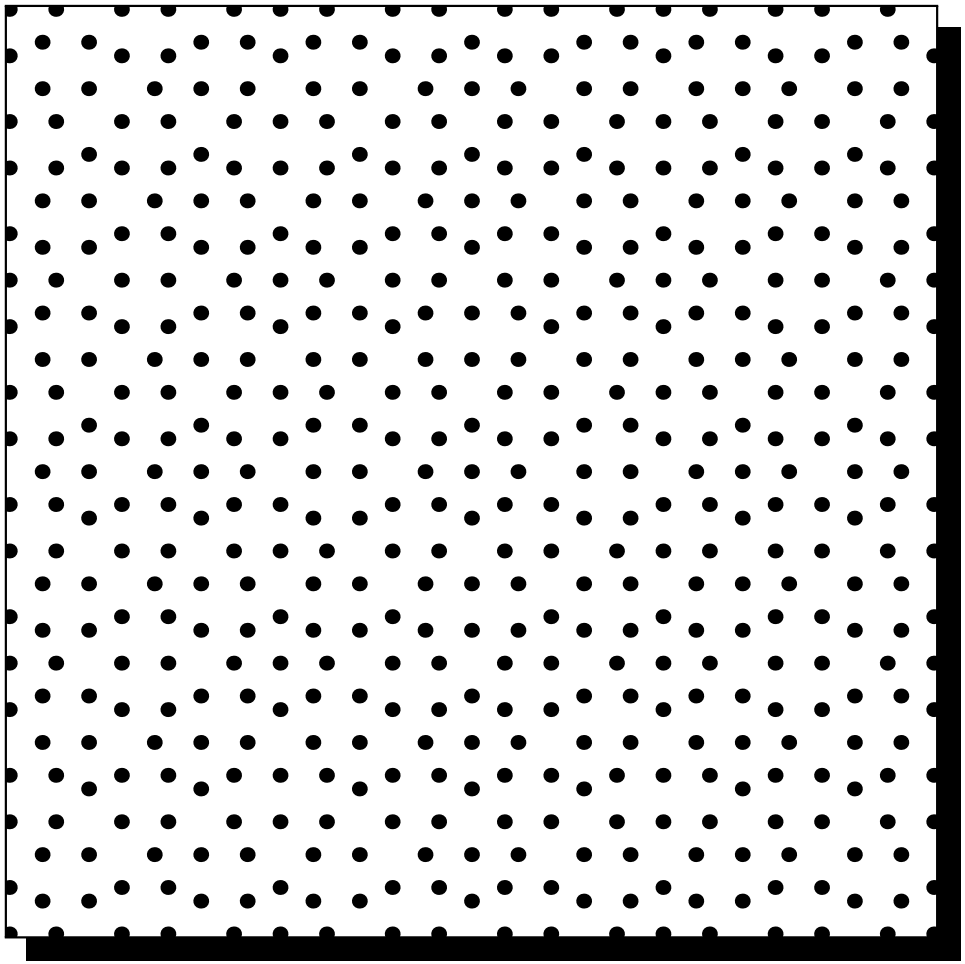
Visible Ammann-Beenker Points

The vertices of the Ammann-Beenker tiling form a relatively dense and uniformly discrete point set.



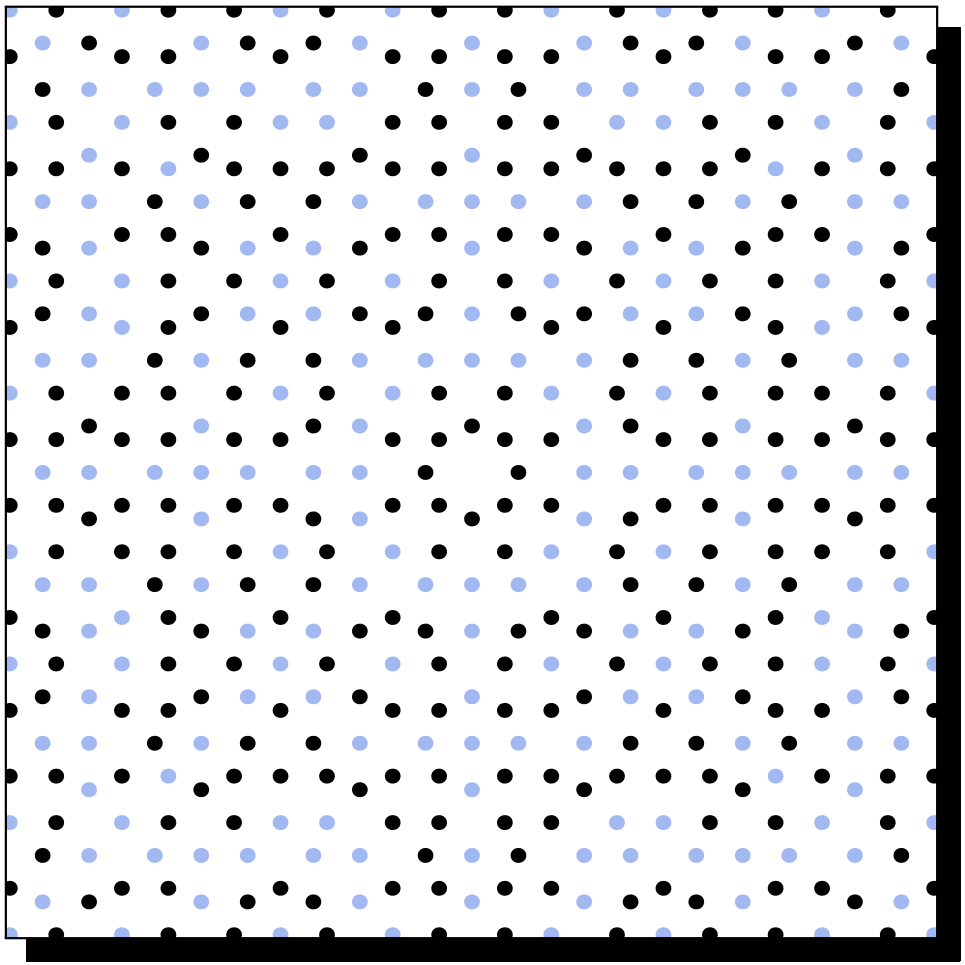
Visible Ammann-Beenker Points

The vertices of the Ammann-Beenker tiling form a relatively dense and uniformly discrete point set.



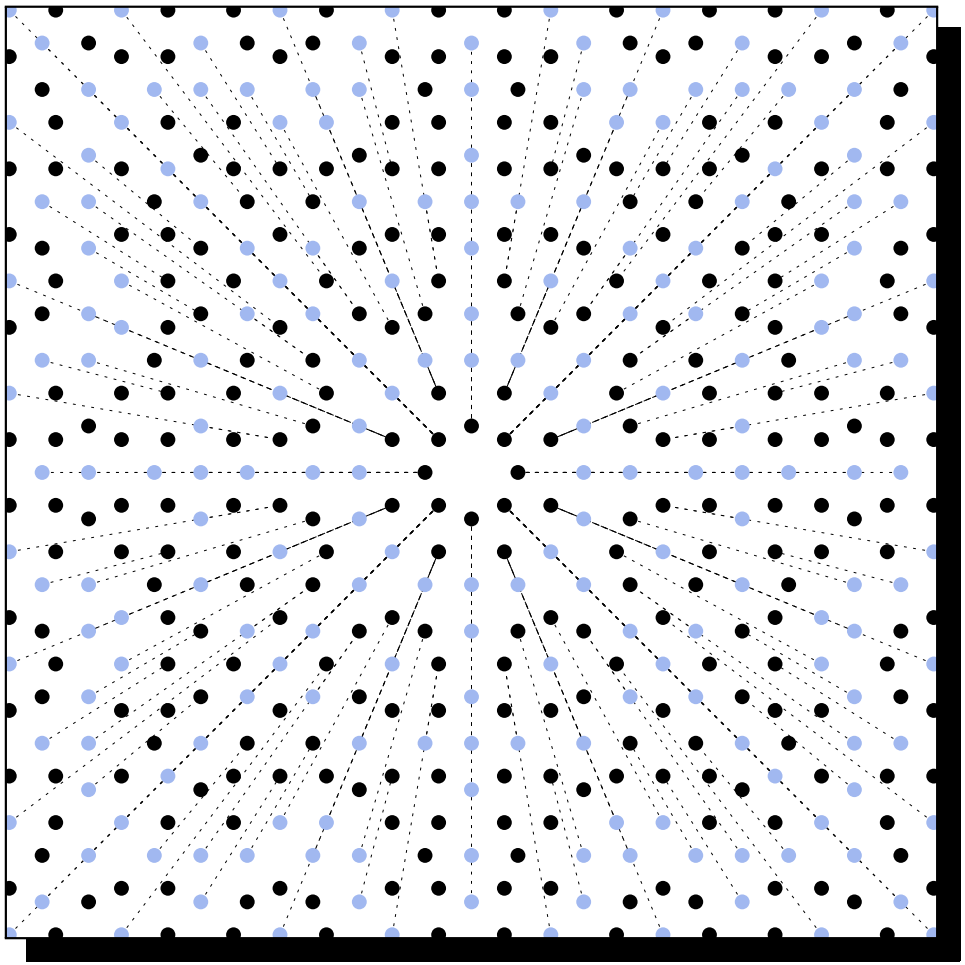
Visible Ammann-Beenker Points

One might ask: Which points are visible here?



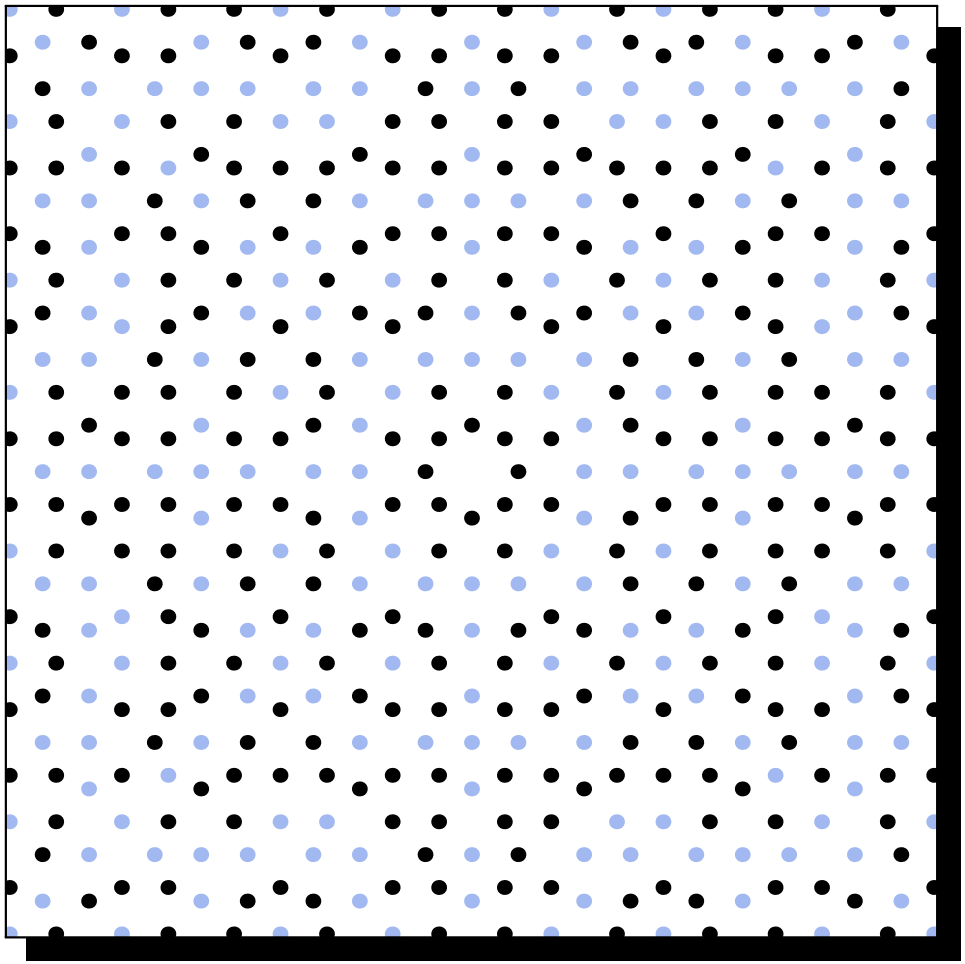
Visible Ammann-Beenker Points

One might ask: Which points are visible here?



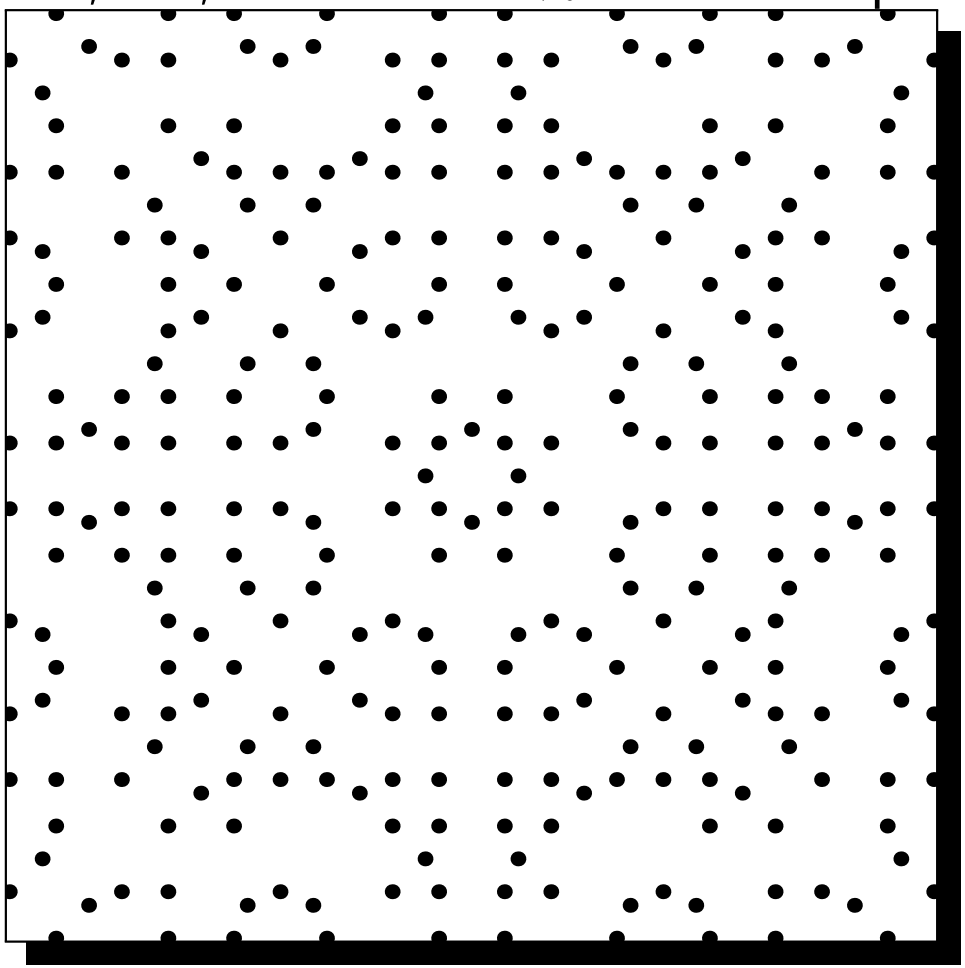
Visible Ammann-Beenker Points

One might ask: Which points are visible here? And what is their density?



Visible Ammann-Beenker Points

Here, we get dens $V_{\mathrm{AB}} = \frac{3}{4} \prod_{p \equiv 1,7 \bmod 8} \left(1-\frac{1}{p^2}\right)^2 \prod_{p \equiv 3,5 \bmod 8} \left(1-\frac{1}{p^4}\right) = \frac{1}{\zeta_{\mathbb{Q}(\sqrt{2})}(2)} \approx 0.6969$, i.e., around 69.7% of the AB-points are visible.



Introduction Talk

Carlo Sircana

Summer School: Algorithms for Extensions of Large Degree

28/05/2018, Greensboro

TR 195
SYMBOLIC TOOLS

Master thesis

Factorization of Polynomials over $\mathbb{Z}/n\mathbb{Z}$
Advisor: Prof. Patrizia Gianni
Università di Pisa

PhD Topic

Construction of Number Fields with Solvable Galois Group
Advisor: Prof. Claus Fieker
TU Kaiserslautern

Solvable extensions can be constructed as towers of abelian extensions.
Issues:

- Constructing abelian extensions can be expensive, depending on the type of extension and on the bound on the discriminant.
- The abelian layers usually "don't match".

A C_3-extension of a quadratic field

- may be not normal over $\mathbb{Q}$,
- may have Galois group C_6,
- may have Galois group S_3.

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 28, 2018

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 $\zeta(s, \mathcal{C}) = \sum \mathrm{N}\mathfrak{a}^{-s}$, 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 $\mathrm{Gal}(\mathsf{F}_2/\mathsf{F}) \cong \mathcal{H}_2$. 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.

CLEMSON
COOPERATIVE EXTENSION

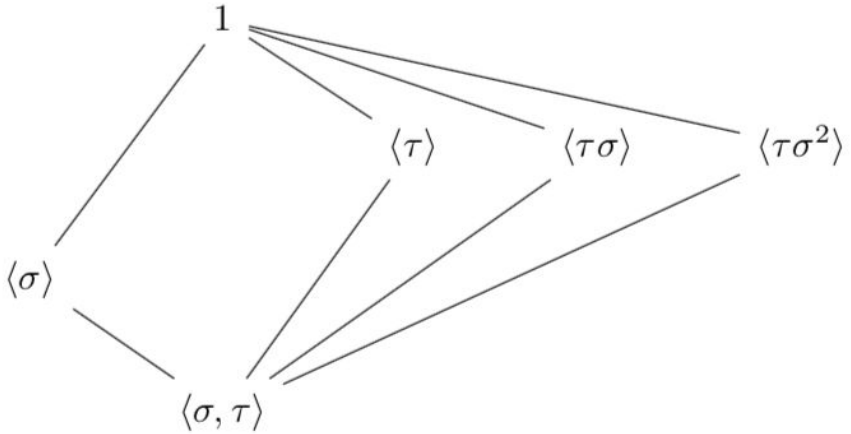
An Example from Ramification Theory

Shuai Wei

Department of Mathematics

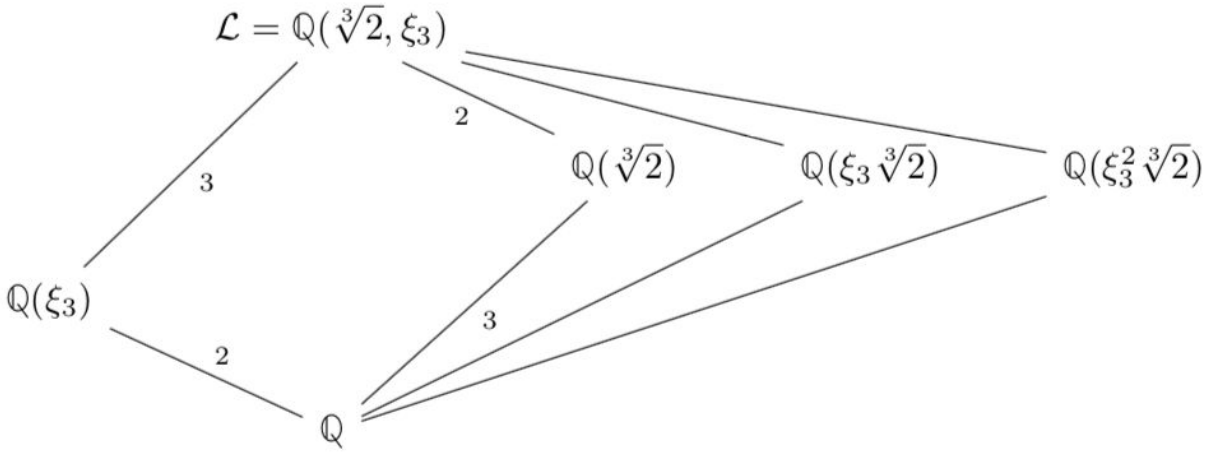
May 28, 2017

$\mathcal{L} = \mathbb{Q}(\sqrt[3]{2}, \xi_3)$ is the splitting field of $x^3 - 2 = (x - \sqrt[3]{2})(x - \xi_3\sqrt[3]{2})(x - \xi_3^2\sqrt[3]{2})$.

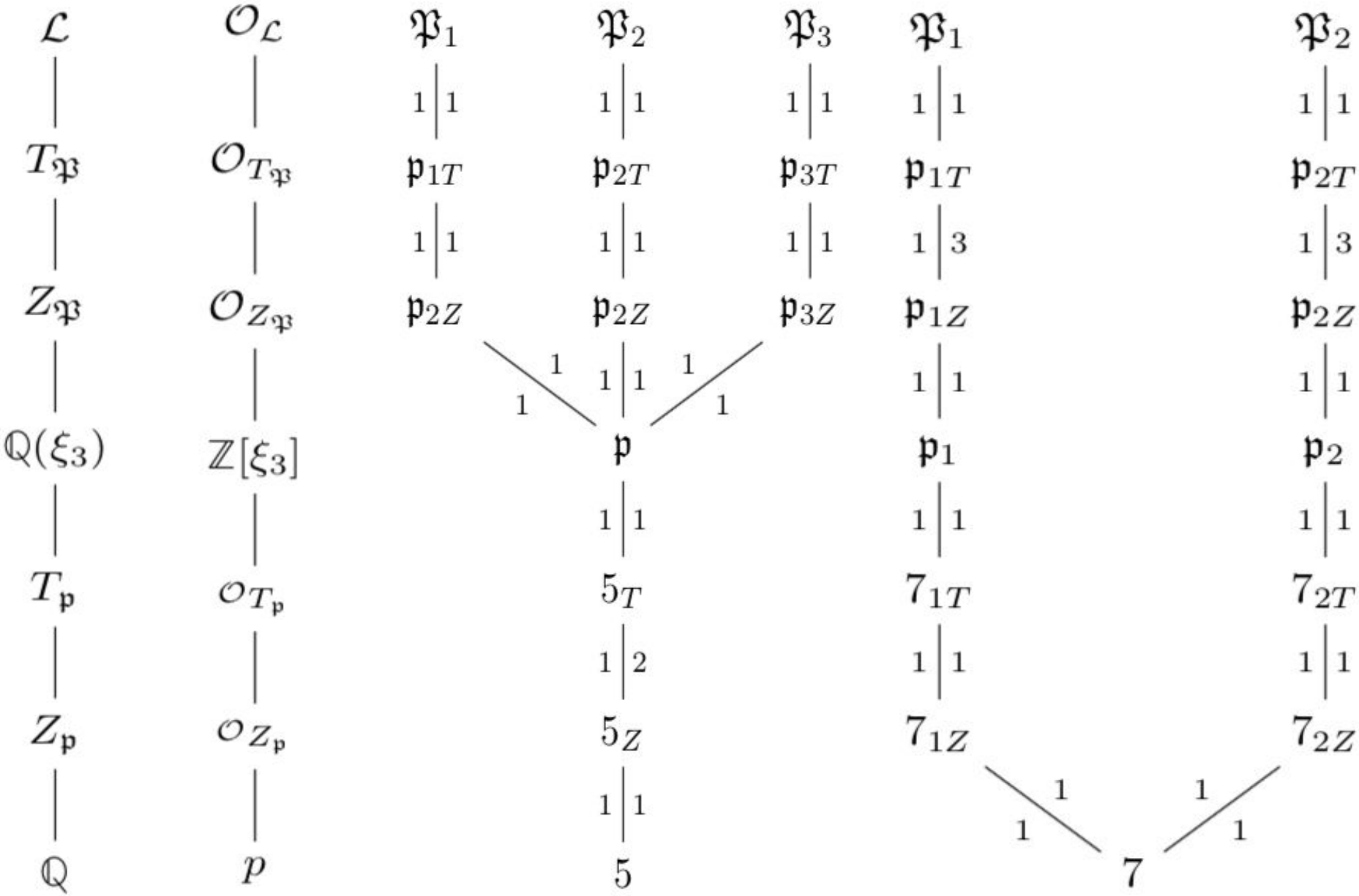


$$\sigma : \begin{cases} \sqrt[3]{2} \mapsto & \xi_3\sqrt[3]{2} \\ \xi_3 \mapsto & \xi_3 \end{cases}$$

$$\tau : \begin{cases} \sqrt[3]{2} \mapsto & \sqrt[3]{2} \\ \xi_3 \mapsto & \xi_3^2 \end{cases}$$



$\mathrm{Gal}(\mathcal{L}/\mathbb{Q}) \cong \langle\sigma,\tau\rangle \cong S_3$ with $|\langle\sigma\rangle| = 3$ and $|\langle\tau\rangle| = 2$.


$\mathcal{L}$
$\mathcal{O}_{\mathcal{L}}$
$T_{\mathfrak{P}}$
$\mathcal{O}_{T_{\mathfrak{P}}}$
$Z_{\mathfrak{P}}$
$\mathcal{O}_{Z_{\mathfrak{P}}}$
$\mathbb{Q}(\xi_3)$
$\mathbb{Z}[\xi_3]$
$T_{\mathfrak{p}}$
$\mathcal{O}_{T_{\mathfrak{p}}}$
$Z_{\mathfrak{p}}$
$\mathcal{O}_{Z_{\mathfrak{p}}}$
$\mathbb{Q}$
p
$\mathfrak{P}_1$ $\mathfrak{P}_2$ $\mathfrak{P}_3$
$\mathfrak{p}_{1T}$ $\mathfrak{p}_{2T}$ $\mathfrak{p}_{3T}$
$\mathfrak{p}_{2Z}$ $\mathfrak{p}_{2Z}$ $\mathfrak{p}_{3Z}$
$\mathfrak{p}$
5_T
5_Z
5
$\mathfrak{P}_1$ $\mathfrak{P}_2$
$\mathfrak{p}_{1T}$ $\mathfrak{p}_{2T}$
$\mathfrak{p}_{1Z}$ $\mathfrak{p}_{2Z}$
$\mathfrak{p}_1$ $\mathfrak{p}_2$
7_{1T} 7_{2T}
7_{1Z} 7_{2Z}
7

Applications of Voronoi to Automorphic Forms

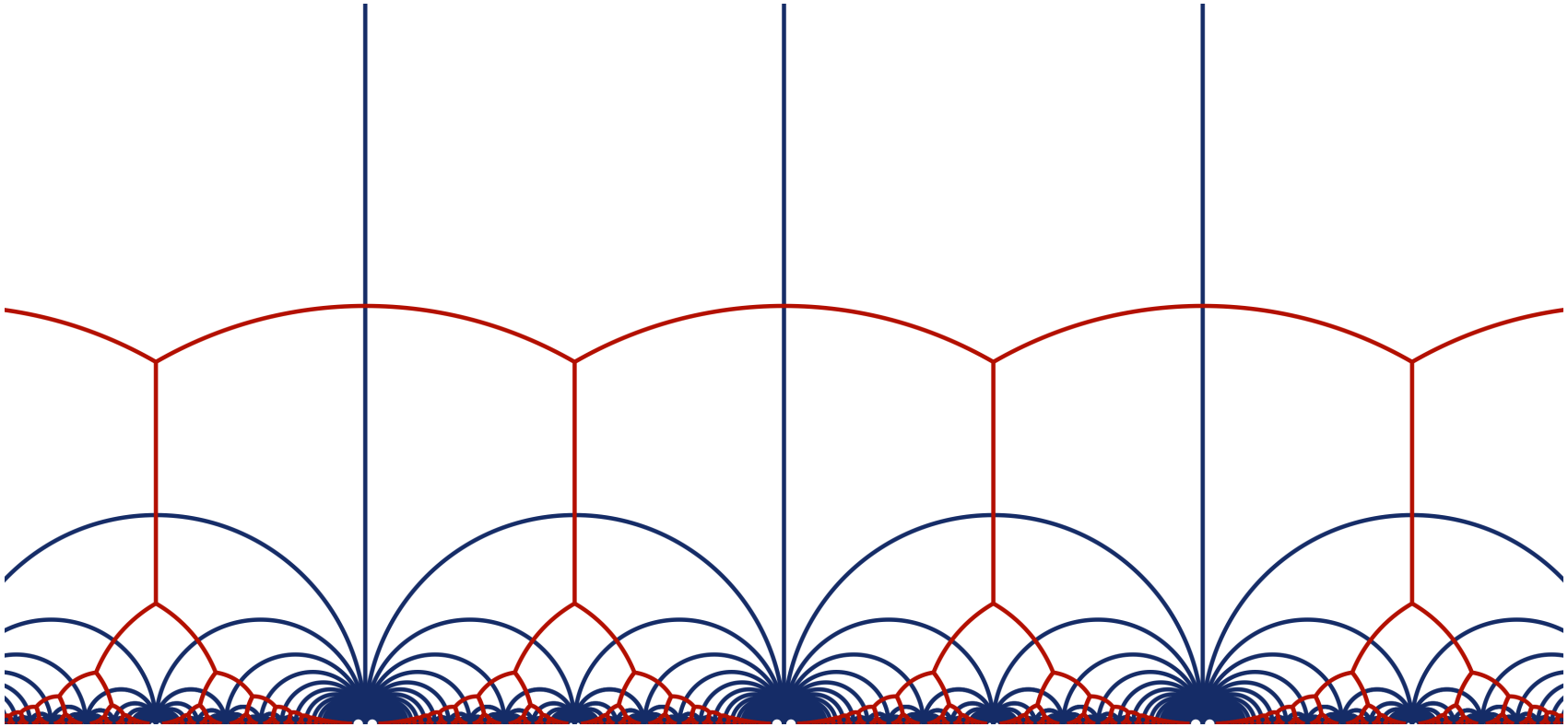
Dan Yasaki

UNC Greensboro

UNCG Summer School in Computational Number Theory
Algorithms for Extensions of Large Degree
(May 28–June 1, 2018)

Perfect forms and tessellations: $\mathbf{G} = \mathrm{SL}_2/\mathbb{Q}$

$$\phi(x,y) = x^2 - xy + y^2, \quad M(\phi) = \left\{ \pm \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \pm \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \pm \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}$$



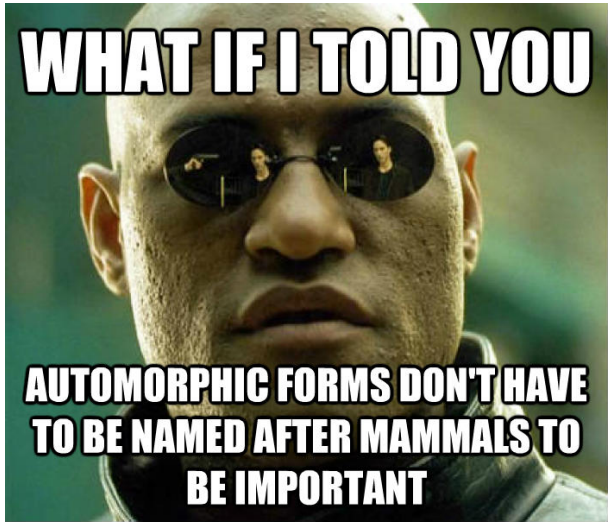
UNC GREENSBORO

Applications

Bianchi
Hilbert
Siegel
⋮

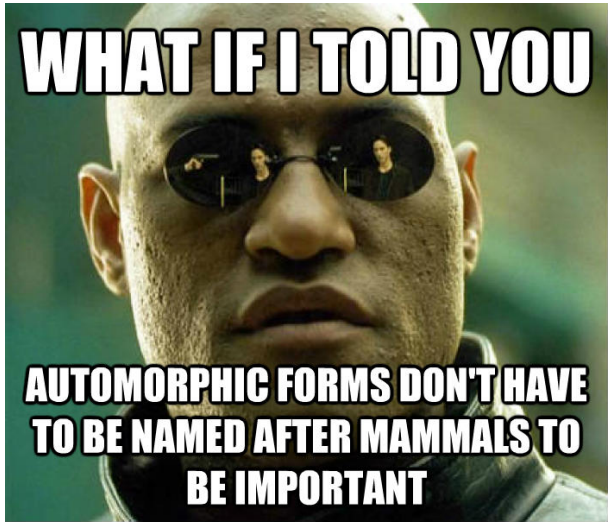
Applications

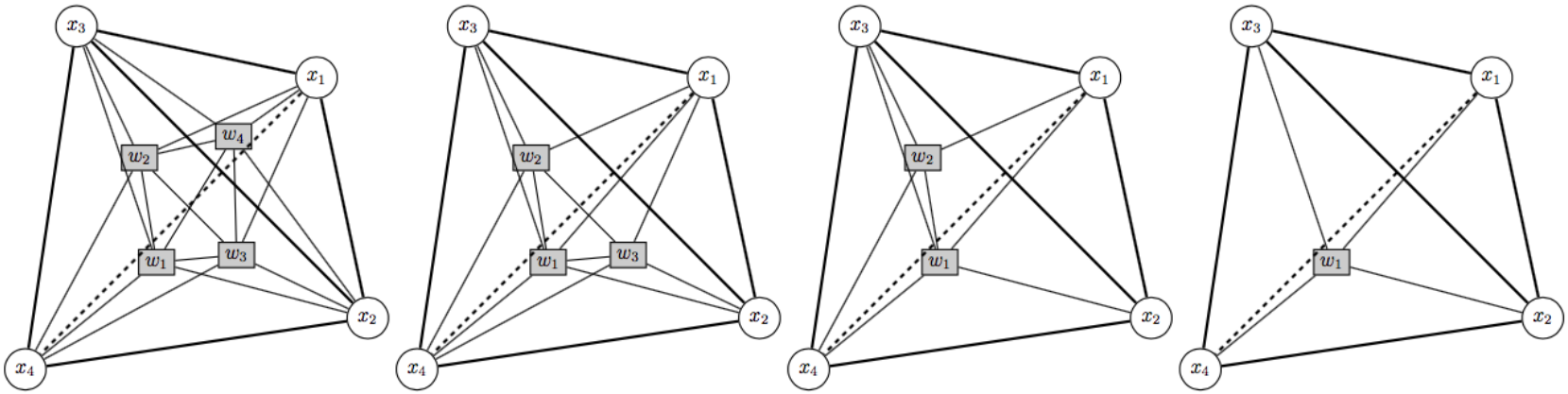
Bianchi
Hilbert
Siegel
⋮



Applications

Bianchi
Hilbert
Siegel
⋮





Introduction and Research Interests

Will Youmans

University of South Florida

May 28, 2018

Research Interests

- My interests are in computational algebraic number theory and its applications in cryptography.
- Cryptographic schemes base their security on the hardness of underlying problems such as the principal ideal problem (PIP) and the short principal ideal problem (SPIP), the shortest vector problem (SVP) and it's variant γ-SVP, among others.
- The nice structure of the fields involved in these schemes often allows for practical and asymptotic improvements to algorithms for computing class groups, unit groups, and more.
- We can use these improvements to tackle the PIP, SPIP, SVP, and others.

My Work So Far

Computing the class group of the maximal real subfield of power-of-2 cyclotomic fields (commonly denoted $\mathbb{Q}(\zeta_{2^n})^+$):

- Computed $Cl(\mathcal{O}_K)$ for $K = \mathbb{Q}(\zeta_{512})^+$ in approximately 7 hours.
- This field appears in cryptographic schemes of Smart and Vercauteren, as well as Garg, Gentry, and Halevi.
- The method can be used to solve the PIP and gives a practical attack on the security of these schemes.

Currently working on computing class groups and unit groups of multiquadratic fields $\mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n})$.

Introduction and Research Interests

Anthi Zervou

University of Paderborn

UNCG Summer School in Computational Number Theory
May 28th, 2018

Introduction

So far I have acquired a bachelor and a master degree in Mathematics at University of Crete.

Introduction

So far I have acquired a bachelor and a master degree in Mathematics at University of Crete.
After that I moved to the University of Paderborn where I recently started my PhD studies under the supervision of Prof. Dr. Jürgen Klüners.

Research Interests

I am interested in

- Algebra
- Computer Algebra
- Galois Theory
- Number Theory and Algebraic Number Theory

Research Interests

I am interested in

- Algebra
- Computer Algebra
- Galois Theory
- Number Theory and Algebraic Number Theory

In my opinion computer algebra is very interesting because we can study and develop algorithms and software for deeply theoretical accomplishments in mathematics.

Research Interests

I am interested in

- Algebra
- Computer Algebra
- Galois Theory
- Number Theory and Algebraic Number Theory

In my opinion computer algebra is very interesting because we can study and develop algorithms and software for deeply theoretical accomplishments in mathematics.
In particular my research topic is the computation of Galois groups of local function fields.

Research Interests

I am interested in

- Algebra
- Computer Algebra
- Galois Theory
- Number Theory and Algebraic Number Theory

In my opinion computer algebra is very interesting because we can study and develop algorithms and software for deeply theoretical accomplishments in mathematics.
In particular my research topic is the computation of Galois groups of local function fields. So far I have studied the ramification polygon and tamely ramified extensions.

Introduction and Research Interest

Dena Zhu

dzion@math.duke.edu

May 28, 2018

Research Interest

Modular Forms, Elliptic Curves, and Modular Curves

- Congruence subgroups
- Complex tori as elliptic curves
- Modular curves and moduli spaces

Modular Curves as Riemann Surfaces

- Charts
- Elliptic points
- Cusps

Dimension Formulas

- Automorphic forms
- Meromorphic differentials
- Divisors and the Riemann-Roch Theorem

References


Fred Diamond and Jerry Shurman (2000)
A First Course in Modular Forms