UNCG Summer School in Computational Number Theory

FUNCTION FIELDS

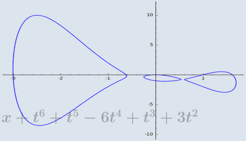
May 30 to June 3, 2016

Speakers

- **Florian Hess**
  Oldenburg
- **Mike Jacobson**
  Calgary
- **Renate Scheidler**
  Calgary

$$\begin{tikzcd}[arrows=dash]
 & KE \arrow[dl] \arrow[ddr] & \\
K = F(t)[x]/(f) \arrow[d] & & \\
F(t) \arrow[dr] & & E = F(\alpha) \arrow[dl] \\
 & F &
\end{tikzcd}$$

$$f(t,x) = x^2 + (t+1)x + t^6 + t^5 - 6t^4 + t^3 + 3t^2$$



organized by the number theory group at UNCG

www.uncg.edu/numbertheory/summerschool

Introductory talk

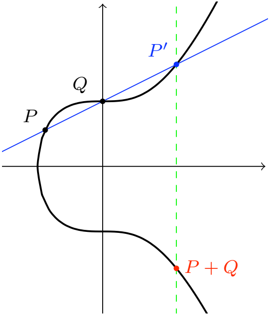
Optimal representations of Trace-zero subgroups

Giulia Bianco (PhD student)

Research area: Elliptic curve cryptography
Advisor : Prof. Dr. Elisa Gorla
University of Neuchatel, Switzerland

Monday, May 30th 2016

UNCG Summer School in Computational Number Theory 2016
University of North Carolina at Greensboro



- E : elliptic curve defined over $\mathbb{F}_q$ finite field, $+$: addition law on E.

- n odd prime number, $(E(\mathbb{F}_{q^n}),+)$ group of points of E with coordinates in $\mathbb{F}_{q^n}$.

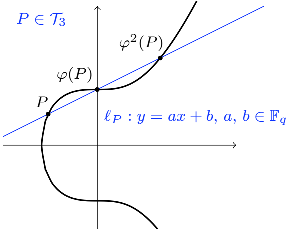
- Frobenius endomorphism $\varphi : E(\mathbb{F}_{q^n}) \longrightarrow E(\mathbb{F}_{q^n})$, $(X,Y) \mapsto (X^q, Y^q)$, $P_\infty \mapsto P_\infty$.

Trace-zero subgroup of $E(\mathbb{F}_{q^n})$

$$\mathcal{T}_n = \{P \in E(\mathbb{F}_{q^n}) \,:\, P + \varphi(P) + \cdots \varphi^{n-1}(P) = P_\infty\}$$

Trace-zero subgroups are interesting for cryptographic applications

Aims

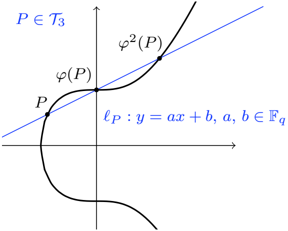


- Optimal representations of points of $\mathcal{T}_n$: represent $P \in \mathcal{T}_n$ with the least possible number of $\mathbb{F}_q$-coordinates.

- Find algorithms for scalar multiplication in the optimal representation.

$$\{P, \varphi(P), \varphi^2(P)\} \qquad \longleftrightarrow \qquad (a, b) \in \mathbb{F}_q^2$$ representation of P

Aims



- Optimal representations of points of $\mathcal{T}_n$: represent $P \in \mathcal{T}_n$ with the least possible number of $\mathbb{F}_q$-coordinates.

- Find algorithms for scalar multiplication in the optimal representation.

$$\begin{tikzcd}
\{P, \varphi(P), \varphi^2(P)\} \arrow[d, "\text{scalar multiplication of points}"] & (a, b) \in \mathbb{F}_q^2 \arrow[l] \arrow[d, "\text{scalar multiplications of lines?}"] & \text{representation of } P \\
\{kP, \varphi(kP), \varphi^2(kP)\} \arrow[r] & (a_k, b_k) \in \mathbb{F}_q^2 & \text{representation of } kP
\end{tikzcd}$$

Note : Montgomery's ladder performs scalar multiplication of vertical lines...

Ben Breen

Dartmouth College

UNCG Summer School in Computational Number theory

May 30, 2016

Current interests

- Algebraic Number Theory, Algebraic Geometry, Arithmetic Geometry
- Projects

  1. **Hilbert modular forms**
     Working on developing a fast multiplication algorithm for Hilbert modular forms. Hopefully it will be implemented for both SAGE and Magma
  2. **Heuristics for Narrow Class Groups**
     I'm investigating the narrow class group in quartic fields using Bhargava's parameterization of quartic rings.

Past work

- *Wild ramification in a family of low-degree extensions arising from iteration*
- We looked at wild ramification in a family of iterated extensions. For integer values of c, we consider the splitting field of $(x^2+c)^2+c$, the second iterate of x^2+c. We give complete information on the factorization of the ideal (2) as c varies, and find a surprisingly complicated dependence of this factorization on the parameter c.
- Joint work Rafe Jones, Tommy Occhipiniti, and Michelle Yuen

Introduction and Interests

Marguerite Delcourt

EPFL
UNCG Summer School

May 30, 2016

Research Interests: Number Theory for Cryptography

Worked on several projects including on the hardness of the Learning With Errors problem (LWE) over lattices:

Lattice of dimension n:
$L(\mathbf{b_1},...,\mathbf{b_n}) = \{\sum_{i=1}^{n} x_i \mathbf{b_i} : x_i \in \mathbb{Z} \text{ for } 1 \le i \le n\}$, with n linearly independent vectors $\mathbf{b_1}$,...,$\mathbf{b_n}$ are a *basis* of the lattice.

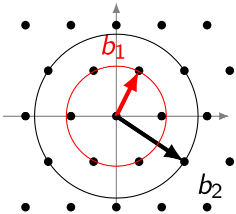
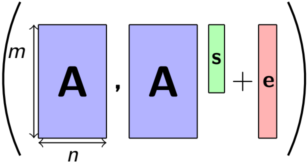


Figure : Lattice of dimension 2, The Shortest Vector Problem

Goal of SVP:
find a non zero vector of length $\lambda(L) = \min(\|\mathbf{b}\|_2 : \mathbf{b} \in L\backslash\{0\})$ from an arbitrary basis
$\|\mathbf{b}\|_2 = \sqrt{\sum_i \mathbf{b_i}^2}$ is the euclidean norm.

The Learning With Errors problem over lattices [Reg05]

- The computational version of LWE: Given $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ and $\mathbf{b} = \mathbf{As} + \mathbf{e}$, find $\mathbf{s} \in \mathbb{Z}_q^n$ with $\mathbf{e}$ gaussian over $\mathbb{Z}_q^n$.
- The decisional version of LWE: Distinguish $(\mathbf{A}, \mathbf{b})$ uniform from $(\mathbf{A}, \mathbf{As} + \mathbf{e} \mod q)$, with $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m \times n})$, $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$ is secret and $\mathbf{e}$ is the gaussian error.



Also worked on other hard problems such as factoring with Coppersmith's modifications to the Number Field Sieve.
I love using mathematics for information security in general.

My Research Interest

Lance Everhart

Department of Mathematics and Statistics
University of North Carolina at Greensboro

May 24, 2016

Let d be a squarefree positive integer and $\mathcal{O}_d$ be the ring of integers of $\mathbb{Q}(\sqrt{d})$.

In my research for my thesis I am working towards computing and tabulating congruence subgroups of

$$\mathrm{PSL}_2(\mathcal{O}_d) = \mathrm{SL}_2(\mathcal{O}_d)/\{\pm 1\}$$

(Hilbert modular group) of level $n \in \mathbb{Z}$ using Magma.

Currently working on ways to compute the representatives of fixed point groups of a general $\mathrm{PSL}_2(\mathcal{O}_d)$ using a fundamental domain.

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

Thank You

Fractional Derivatives of Hurwitz Zeta Functions

Ricky Farr Joint Work With Sebastian Pauli

University of North Carolina at Greensboro

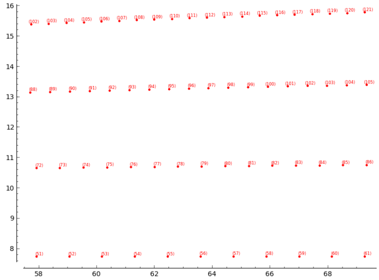
30 May 2016

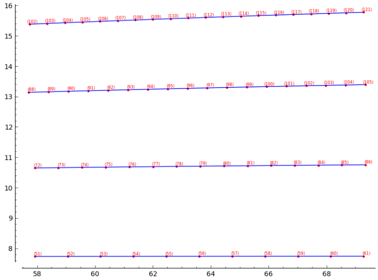
Hurwitz Zeta Functions And Their Derivatives

Fractional Derivative of Hurwitz Zeta Functions

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

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



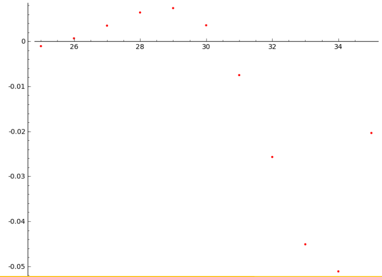


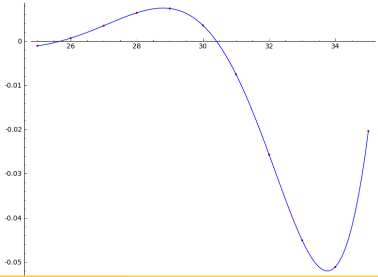
Generalized Non-Integer Stieltjes Constants

Definition

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

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





Research Interests

Jeroen Hanselman

Universität Ulm

jeroen.hanselman@uni-ulm.de

Sunday 29th May, 2016

Bounding the field extension necessary to achieve semistable reduction

Situation

Let C be a curve over $\mathbb{Q}$. After a suitable transformation, we can consider C as a curve over $\mathbb{Z}$. We may be interested in what happens when we consider these equations modulo p.

Example

$C : XY - 2 = 0$

We want to find a curve C' that is isomorphic to C over $\mathbb{Q}$ and has "nice" properties modulo p.
For our example: $C' : X'Y' - 1 = 0$ is smooth for all p.

Semistable reduction theorem (Deligne-Mumford)

Let C be a smooth, projective curve connected curve over K of genus $g \geq 2$. Then there exists a finite field extension $[L : K]$ such that C_L has a semi-stable model over $\mathcal{O}_L$.

Relative version:

Let $f : X \to Y$ be a finite map between curves over a field K. Then there exists a finite field extension $[L : K]$ such that f lifts to a finite morphism $\tilde{f} : \mathcal{X} \to \mathcal{Y}$ between two semistable models of C_L.

My goal:

Finding an explicit bound for this field extension in terms of the original cover. Currently trying to see if it is possible to write this bound purely in terms of the genera of X and Y.

Current research topic (just started):

Finding explicit curves whose endomorphism algebra is isomorphic to a quaternion algebra.

Introduction and Research

Austin Lawson

University of North Carolina at Greensboro

Current Research - Coarse Spaces

Definition

a) The pair $(X, \mathcal{E})$ is a **coarse space** if X is a set and $\mathcal{E}$ is a collection of subsets of $X \times X$, called entourages satisfying,

1) A subset of an entourage is an entourage
2) A finite union of entourages is an entourage
3) The diagonal $\Delta = \{(x,x) \mid x \in x\}$
4) If $E \in \mathcal{E}$, then $E^{-1} = \{(y,x) \mid (x,y) \in E\}$
5) If $E_1, E_2 \in \mathcal{E}$, then $E_1 \circ E_2 = \{(x,z) \mid (x,y) \in E_1 \textit{ and } (y,z) \in E_2\}$

b) Let $(X, \mathcal{E})$ be a coarse space. Let $\mathcal{Y}$ be a family of coarse subspaces of $\mathcal{Y}$. Let $L \in \mathcal{E}$. We say X admits an an L-**decomposition** over $\mathcal{Y}$, denoted $X \xrightarrow{L} \mathcal{Y}$ if

$$X = X^0 \cup X^1 \text{ where } X^i = \sqcup_L X^i_j$$

where $X^i_j \in \mathcal{Y}$ and $X^i_j \neq X^i_{j'}$ implies $X^i_j \times X^i_{j'} \cap L = \emptyset$.

c) A coarse family $\mathcal{Y}$ is **uniformly bounded** if $\cup_{Y \in \mathcal{Y}} Y \times Y$ is an entourage.

Decomposition Complexity

Definition

a) A coarse space X is said to have **straight finite coarse decomposition complexity** (SFCDC) if for any sequence of entourages $L_1 \subset L_2 \subset \cdots$ there exists a finite sequence of families $\mathcal{Y}_0, \mathcal{Y}_1, \cdots, \mathcal{Y}_n$ of subsets of X with $\mathcal{Y}_0 = X, \mathcal{Y}_n$ uniformly bounded and $\mathcal{Y}_{i-1} \xrightarrow{L_i} \mathcal{Y}_i$ for $0 \leq i \leq n-1$.

b) A coarse space $(X, \mathcal{E})$ is said to have **coarse property A** if for each $\varepsilon > 0$ and for each $E \in \mathcal{E}$ there exists a map $a : X \to \ell^1(X), x \mapsto a_x$ such that,

1) $\|a_x\| = 1$ for all $x \in X$
2) $(x, y) \in E$ implies $\|a_x - a_y\|_1 < \varepsilon$
3) There is some $S \in \mathcal{E}$ such that for each $x \in X$ $\text{supp}(a_x) \subset S[x] = \{s \in X \mid (s, x) \in S\}$.

Conjecture

SFCDC $\Rightarrow$ coarse property A.

Research interests

Sumin Leem

Department of Mathematics and Statistics
University of Calgary

May 30 2016

Research Interests

Research Interests

Hyperelliptic curve algorithms and their implementation (arithmetic, discrete logarithm, ...), Cryptography in general.

Hyperelliptic curves

A hyperelliptic curve C of genus g over K (g$\geq$1) is an equation of the form

$$C : v^2 + h(u)v = f(u) \quad in \quad K[u, v]$$

where degrees of monic polynomials $h(u),\ f(u) \in K[u]$ are at most g, 2g+1 respectively, and there are no solutions $(u, v) \in \bar{K} \times \bar{K}$ which simultaneously satisfy the curve equation and two partial derivative equations, $2v + h(u) = 0$ and $h'(u)v - f'(u) = 0$.

Research Interests

Jacobian of a Hyperelliptic curve

Jacobian of a Hyperelliptic curve H is

$$Jac(H) = Div^0(H)/Prin(H)$$

where $Div^0(H)$ is degree zero divisors on H and $Prin(H)$ is principal divisors on H.

NOTE: Jac(H) is an abelian group.

Distribution of Primes

Junxian Li

University of Illinois at Urbana-Champaign

UNCG Summer School
May 30, 2016

Gap Distribution of Primes

Prime Number Theorem

$$\pi(x) \sim \frac{x}{\log x}$$

Average gap $\sim \log x$

I Small Gap

- $\liminf_n (p_{n+1} - p_n)$.
- Hardy-Littlewood prime tuples conjecture.
- $\liminf_n (p_{n+1} - p_n) \leq 70000000$ (Zhang, 2013), $\liminf_n (p_{n+1} - p_n) \leq 600$ (Maynard, 2013).

II Large Gap

- $G(x) = \limsup_{p_{n+1} \leq x} (p_{n+1} - p_n)$.
- Granville conjecture $G(x) \gtrsim 2e^{-\gamma} \log^2 x$.
- $G(x) \gg \frac{\log_3 x}{\log_4 x} \log x$ (Westzynthius, 1931), $G(x) \gg \frac{\log_2 x \log_4 x}{(\log_3 x)^2} \log x$ (Erdös & Rankin, 1938), $G(x) \gg \frac{\log_2 x \log_4 x}{\log_3 x} \log x$ (Ford, Green, Konyagin, Maynard, Tao, 2014).

Gap Distribution of Primes

Prime Number Theorem

$$\pi(x) \sim \frac{x}{\log x}$$

Average gap $\sim \log x$

I Small Gap

- $\liminf_n (p_{n+1} - p_n)$.
- Hardy-Littlewood prime tuples conjecture.
- $\liminf_n (p_{n+1} - p_n) \leq 70000000$ (Zhang, 2013), $\liminf_n (p_{n+1} - p_n) \leq 600$ (Maynard, 2013).

II Large Gap

- $G(x) = \limsup_{p_{n+1} \leq x} (p_{n+1} - p_n)$.
- Granville conjecture $G(x) \gtrsim 2e^{-\gamma} \log^2 x$.
- $G(x) \gg \frac{\log_3 x}{\log_4 x} \log x$ (Westzynthius, 1931), $G(x) \gg \frac{\log_2 x \log_4 x}{(\log_3 x)^2} \log x$ (Erdös & Rankin, 1938), $G(x) \gg \frac{\log_2 x \log_4 x}{\log_3 x} \log x$ (Ford, Green, Konyagin, Maynard, Tao, 2014).

Gap Distribution of Primes

Prime Number Theorem

$$\pi(x) \sim \frac{x}{\log x}$$

Average gap $\sim \log x$

I Small Gap

- $\liminf_n (p_{n+1} - p_n)$.
- Hardy-Littlewood prime tuples conjecture.
- $\liminf_n (p_{n+1} - p_n) \leq 70000000$ (Zhang, 2013), $\liminf_n (p_{n+1} - p_n) \leq 600$ (Maynard, 2013).

II Large Gap

- $G(x) = \limsup_{p_{n+1} \leq x} (p_{n+1} - p_n)$.
- Granville conjecture $G(x) \gtrsim 2e^{-\gamma} \log^2 x$.
- $G(x) \gg \frac{\log_3 x}{\log_4 x} \log x$ (Westzynthius, 1931), $G(x) \gg \frac{\log_2 x \log_4 x}{(\log_3 x)^2} \log x$ (Erdös & Rankin, 1938), $G(x) \gg \frac{\log_2 x \log_4 x}{\log_3 x} \log x$ (Ford, Green, Konyagin, Maynard, Tao, 2014).

Gap Distribution of Primes

Prime Number Theorem

$$\pi(x) \sim \frac{x}{\log x}$$

Average gap $\sim \log x$

I Small Gap

- $\liminf_n (p_{n+1} - p_n)$.
- Hardy-Littlewood prime tuples conjecture.
- $\liminf_n (p_{n+1} - p_n) \leq 70000000$ (Zhang, 2013), $\liminf_n (p_{n+1} - p_n) \leq 600$ (Maynard, 2013).

II Large Gap

- $G(x) = \limsup_{p_{n+1} \leq x} (p_{n+1} - p_n)$.
- Granville conjecture $G(x) \gtrsim 2e^{-\gamma} \log^2 x$.
- $G(x) \gg \frac{\log_3 x}{\log_4 x} \log x$ (Westzynthius, 1931), $G(x) \gg \frac{\log_2 x \log_4 x}{(\log_3 x)^2} \log x$ (Erdös & Rankin, 1938), $G(x) \gg \frac{\log_2 x \log_4 x}{\log_3 x} \log x$ (Ford, Green, Konyagin, Maynard, Tao, 2014).

Gap Distribution of Primes

Prime Number Theorem

$$\pi(x) \sim \frac{x}{\log x}$$

Average gap $\sim \log x$

I Small Gap

- $\liminf_n (p_{n+1} - p_n)$.
- Hardy-Littlewood prime tuples conjecture.
- $\liminf_n (p_{n+1} - p_n) \leq 70000000$ (Zhang, 2013), $\liminf_n (p_{n+1} - p_n) \leq 600$ (Maynard, 2013).

II Large Gap

- $G(x) = \limsup_{p_{n+1} \leq x} (p_{n+1} - p_n)$.
- Granville conjecture $G(x) \gtrsim 2e^{-\gamma} \log^2 x$.
- $G(x) \gg \frac{\log_3 x}{\log_4 x} \log x$ (Westzynthius, 1931), $G(x) \gg \frac{\log_2 x \log_4 x}{(\log_3 x)^2} \log x$ (Erdös & Rankin, 1938), $G(x) \gg \frac{\log_2 x \log_4 x}{\log_3 x} \log x$ (Ford, Green, Konyagin, Maynard, Tao, 2014).

Gap Distribution of Primes

Prime Number Theorem

$$\pi(x) \sim \frac{x}{\log x}$$

Average gap $\sim \log x$

I Small Gap

- $\liminf_n (p_{n+1} - p_n)$.
- Hardy-Littlewood prime tuples conjecture.
- $\liminf_n (p_{n+1} - p_n) \leq 70000000$ (Zhang, 2013), $\liminf_n (p_{n+1} - p_n) \leq 600$ (Maynard, 2013).

II Large Gap

- $G(x) = \limsup_{p_{n+1} \leq x} (p_{n+1} - p_n)$.
- Granville conjecture $G(x) \gtrsim 2e^{-\gamma} \log^2 x$.
- $G(x) \gg \frac{\log_3 x}{\log_4 x} \log x$ (Westzynthius, 1931), $G(x) \gg \frac{\log_2 x \log_4 x}{(\log_3 x)^2} \log x$ (Erdös & Rankin, 1938), $G(x) \gg \frac{\log_2 x \log_4 x}{\log_3 x} \log x$ (Ford, Green, Konyagin, Maynard, Tao, 2014).

Gap Distribution of Primes

Prime Number Theorem

$$\pi(x) \sim \frac{x}{\log x}$$

Average gap $\sim \log x$

I Small Gap

- $\liminf_n (p_{n+1} - p_n)$.
- Hardy-Littlewood prime tuples conjecture.
- $\liminf_n (p_{n+1} - p_n) \leq 70000000$ (Zhang, 2013),
  $\liminf_n (p_{n+1} - p_n) \leq 600$ (Maynard, 2013).

II Large Gap

- $G(x) = \limsup_{p_{n+1} \leq x} (p_{n+1} - p_n)$.
- Granville conjecture $G(x) \gtrsim 2e^{-\gamma} \log^2 x$.
- $G(x) \gg \frac{\log_3 x}{\log_4 x} \log x$ (Westzynthius, 1931),
  $G(x) \gg \frac{\log_2 x \log_4 x}{(\log_3 x)^2} \log x$ (Erdös & Rankin, 1938),
  $G(x) \gg \frac{\log_2 x \log_4 x}{\log_3 x} \log x$ (Ford, Green, Konyagin, Maynard, Tao, 2014).

Gap Distribution of Primes

Prime Number Theorem

$$\pi(x) \sim \frac{x}{\log x}$$

Average gap $\sim \log x$

I Small Gap

- $\liminf_n (p_{n+1} - p_n)$.
- Hardy-Littlewood prime tuples conjecture.
- $\liminf_n (p_{n+1} - p_n) \leq 70000000$ (Zhang, 2013), $\liminf_n (p_{n+1} - p_n) \leq 600$ (Maynard, 2013).

II Large Gap

- $G(x) = \limsup_{p_{n+1} \leq x} (p_{n+1} - p_n)$.
- Granville conjecture $G(x) \gtrsim 2e^{-\gamma} \log^2 x$.
- $G(x) \gg \frac{\log_3 x}{\log_4 x} \log x$ (Westzynthius, 1931), $G(x) \gg \frac{\log_2 x \log_4 x}{(\log_3 x)^2} \log x$ (Erdös & Rankin, 1938), $G(x) \gg \frac{\log_2 x \log_4 x}{\log_3 x} \log x$ (Ford, Green, Konyagin, Maynard, Tao, 2014).

Gap Distribution of Primes

Prime Number Theorem

$$\pi(x) \sim \frac{x}{\log x}$$

Average gap $\sim \log x$

I Small Gap

- $\liminf_n (p_{n+1} - p_n)$.
- Hardy-Littlewood prime tuples conjecture.
- $\liminf_n (p_{n+1} - p_n) \le 70000000$ (Zhang, 2013), $\liminf_n (p_{n+1} - p_n) \le 600$ (Maynard, 2013).

II Large Gap

- $G(x) = \limsup_{p_{n+1} \le x} (p_{n+1} - p_n)$.
- Granville conjecture $G(x) \gtrsim 2e^{-\gamma} \log^2 x$.
- $G(x) \gg \frac{\log_3 x}{\log_4 x} \log x$ (Westzynthius, 1931), $G(x) \gg \frac{\log_2 x \log_4 x}{(\log_3 x)^2} \log x$ (Erdös & Rankin, 1938), $G(x) \gg \frac{\log_2 x \log_4 x}{\log_3 x} \log x$ (Ford, Green, Konyagin, Maynard, Tao, 2014).

Gap Distribution of Primes

Prime Number Theorem

$$\pi(x) \sim \frac{x}{\log x}$$

Average gap $\sim \log x$

I. Small Gap
   - $\liminf_n (p_{n+1} - p_n)$.
   - Hardy-Littlewood prime tuples conjecture.
   - $\liminf_n (p_{n+1} - p_n) \leq 70000000$ (Zhang, 2013), $\liminf_n (p_{n+1} - p_n) \leq 600$ (Maynard, 2013).

II. Large Gap
   - $G(x) = \limsup_{p_{n+1} \leq x} (p_{n+1} - p_n)$.
   - Granville conjecture $G(x) \gtrsim 2e^{-\gamma} \log^2 x$.
   - $G(x) \gg \frac{\log_3 x}{\log_4 x} \log x$ (Westzynthius, 1931), $G(x) \gg \frac{\log_2 x \log_4 x}{(\log_3 x)^2} \log x$ (Erdös & Rankin, 1938), $G(x) \gg \frac{\log_2 x \log_4 x}{\log_3 x} \log x$ (Ford, Green, Konyagin, Maynard, Tao, 2014).

Gap Distribution of Primes

Prime Number Theorem

$$\pi(x) \sim \frac{x}{\log x}$$

Average gap $\sim \log x$

I Small Gap

- $\liminf_n (p_{n+1} - p_n)$.
- Hardy-Littlewood prime tuples conjecture.
- $\liminf_n (p_{n+1} - p_n) \leq 70000000$ (Zhang, 2013),
  $\liminf_n (p_{n+1} - p_n) \leq 600$ (Maynard, 2013).

II Large Gap

- $G(x) = \limsup_{p_{n+1} \leq x} (p_{n+1} - p_n)$.
- Granville conjecture $G(x) \gtrsim 2e^{-\gamma} \log^2 x$.
- $G(x) \gg \frac{\log_3 x}{\log_4 x} \log x$ (Westzynthius, 1931),
  $G(x) \gg \frac{\log_2 x \log_4 x}{(\log_3 x)^2} \log x$ (Erdös & Rankin, 1938),
  $G(x) \gg \frac{\log_2 x \log_4 x}{\log_3 x} \log x$ (Ford, Green, Konyagin, Maynard, Tao, 2014).

Gap Distribution of Primes

Prime Number Theorem

$$\pi(x) \sim \frac{x}{\log x}$$

Average gap $\sim \log x$

I Small Gap

- $\liminf_n (p_{n+1} - p_n)$.
- Hardy-Littlewood prime tuples conjecture.
- $\liminf_n (p_{n+1} - p_n) \leq 70000000$ (Zhang, 2013), $\liminf_n (p_{n+1} - p_n) \leq 600$ (Maynard, 2013).

II Large Gap

- $G(x) = \limsup_{p_{n+1} \leq x} (p_{n+1} - p_n)$.
- Granville conjecture $G(x) \gtrsim 2e^{-\gamma} \log^2 x$.
- $G(x) \gg \frac{\log_3 x}{\log_4 x} \log x$ (Westzynthius, 1931), $G(x) \gg \frac{\log_2 x \log_4 x}{(\log_3 x)^2} \log x$ (Erdös & Rankin, 1938), $G(x) \gg \frac{\log_2 x \log_4 x}{\log_3 x} \log x$ (Ford, Green, Konyagin, Maynard, Tao, 2014).

Least Prime in Progression

Fix a positive integer k and let ℓ be coprime to k. Let $p(k,\ell)$ denote the smallest prime equivalent to ℓ modulo k, and define

$$P(k) := \max_{(\ell,k)=1} p(k,\ell).$$

Heuristic: $\liminf_k \frac{P(k)}{\phi(k)\log^2 k} = 1, \quad \limsup_k \frac{P(k)}{\phi(k)\log^2 k} = 2.$

I Upper Bound
- Linnik: $P(k) \ll k^L$, where $L > 0$ is a fixed constant.
- Xylouris: $L \leq 5.18$, following a method of Heath-Brown.

II Lower Bound
- Pomerance :
  $P(k) \geq (e^\gamma + o(1))\phi(k)\log k \log_2 k \frac{\log_4 k}{(\log_3 k)^2}, \forall k \notin Q.$
- Li, Pratt, Shakan :
  $P(k) \gg \phi(k)\log k \log_2 k \log_4 k / \log_3 k, \forall k \notin Q' \supset Q.$

- What happens in number fields and function fields ?

Least Prime in Progression

Fix a positive integer k and let ℓ be coprime to k. Let $p(k, \ell)$ denote the smallest prime equivalent to ℓ modulo k, and define

$$P(k) := \max_{(\ell,k)=1} p(k, \ell).$$

Heuristic: $\liminf_k \frac{P(k)}{\phi(k) \log^2 k} = 1, \quad \limsup_k \frac{P(k)}{\phi(k) \log^2 k} = 2.$

I Upper Bound

- Linnik: $P(k) \ll k^L$, where $L > 0$ is a fixed constant.
- Xylouris: $L \leq 5.18$, following a method of Heath-Brown.

II Lower Bound

- Pomerance :
  $P(k) \geq (e^\gamma + o(1))\phi(k) \log k \log_2 k \frac{\log_4 k}{(\log_3 k)^2}, \forall k \notin Q.$
- Li, Pratt, Shakan :
  $P(k) \gg \phi(k) \log k \log_2 k \log_4 k / \log_3 k, \forall k \notin Q' \supset Q.$

- What happens in number fields and function fields ?

Least Prime in Progression

Fix a positive integer k and let ℓ be coprime to k. Let $p(k, \ell)$ denote the smallest prime equivalent to ℓ modulo k, and define

$$P(k) := \max_{(\ell,k)=1} p(k, \ell).$$

Heuristic: $\liminf_k \frac{P(k)}{\phi(k)\log^2 k} = 1, \quad \limsup_k \frac{P(k)}{\phi(k)\log^2 k} = 2.$

I Upper Bound

- Linnik: $P(k) \ll k^L$, where $L > 0$ is a fixed constant.
- Xylouris: $L \leq 5.18$, following a method of Heath-Brown.

II Lower Bound

- Pomerance :
  $P(k) \geq (e^\gamma + o(1))\phi(k) \log k \log_2 k \frac{\log_4 k}{(\log_3 k)^2}, \forall k \notin Q.$
- Li, Pratt, Shakan :
  $P(k) \gg \phi(k) \log k \log_2 k \log_4 k / \log_3 k, \forall k \notin Q' \supset Q.$

- What happens in number fields and function fields ?

Least Prime in Progression

Fix a positive integer k and let ℓ be coprime to k. Let $p(k,\ell)$ denote the smallest prime equivalent to ℓ modulo k, and define

$$P(k) := \max_{(\ell,k)=1} p(k,\ell).$$

Heuristic: $\liminf_k \frac{P(k)}{\phi(k)\log^2 k} = 1, \quad \limsup_k \frac{P(k)}{\phi(k)\log^2 k} = 2.$

I Upper Bound

- Linnik: $P(k) \ll k^L$, where $L > 0$ is a fixed constant.
- Xylouris: $L \leq 5.18$, following a method of Heath-Brown.

II Lower Bound

- Pomerance : $P(k) \geq (e^\gamma + o(1))\phi(k)\log k \log_2 k \frac{\log_4 k}{(\log_3 k)^2}, \forall k \notin Q.$
- Li, Pratt, Shakan : $P(k) \gg \phi(k)\log k \log_2 k \log_4 k / \log_3 k, \forall k \notin Q' \supset Q.$

- What happens in number fields and function fields ?

Least Prime in Progression

Fix a positive integer k and let ℓ be coprime to k. Let $p(k,\ell)$ denote the smallest prime equivalent to ℓ modulo k, and define

$$P(k) := \max_{(\ell,k)=1} p(k,\ell).$$

Heuristic: $\liminf_k \frac{P(k)}{\phi(k)\log^2 k} = 1, \quad \limsup_k \frac{P(k)}{\phi(k)\log^2 k} = 2.$

I Upper Bound

- Linnik: $P(k) \ll k^L$, where $L > 0$ is a fixed constant.
- Xylouris: $L \leq 5.18$, following a method of Heath-Brown.

II Lower Bound

- Pomerance : $P(k) \geq (e^\gamma + o(1))\phi(k)\log k \log_2 k \frac{\log_4 k}{(\log_3 k)^2}, \forall k \notin Q.$
- Li, Pratt, Shakan : $P(k) \gg \phi(k)\log k \log_2 k \log_4 k / \log_3 k, \forall k \notin Q' \supset Q.$

- What happens in number fields and function fields ?

Least Prime in Progression

Fix a positive integer k and let ℓ be coprime to k. Let $p(k, \ell)$ denote the smallest prime equivalent to ℓ modulo k, and define

$$P(k) := \max_{(\ell,k)=1} p(k, \ell).$$

Heuristic: $\liminf_k \frac{P(k)}{\phi(k)\log^2 k} = 1, \quad \limsup_k \frac{P(k)}{\phi(k)\log^2 k} = 2.$

I Upper Bound

- Linnik: $P(k) \ll k^L$, where $L > 0$ is a fixed constant.
- Xylouris: $L \leq 5.18$, following a method of Heath-Brown.

II Lower Bound

- Pomerance : $P(k) \geq (e^\gamma + o(1))\phi(k)\log k \log_2 k \frac{\log_4 k}{(\log_3 k)^2}, \forall k \notin Q.$
- Li, Pratt, Shakan : $P(k) \gg \phi(k) \log k \log_2 k \log_4 k / \log_3 k, \forall k \notin Q' \supset Q.$

- What happens in number fields and function fields ?

Least Prime in Progression

Fix a positive integer k and let ℓ be coprime to k. Let $p(k,\ell)$ denote the smallest prime equivalent to ℓ modulo k, and define

$$P(k) := \max_{(\ell,k)=1} p(k,\ell).$$

Heuristic: $\liminf_k \frac{P(k)}{\phi(k)\log^2 k} = 1, \quad \limsup_k \frac{P(k)}{\phi(k)\log^2 k} = 2.$

I Upper Bound

- Linnik: $P(k) \ll k^L$, where $L > 0$ is a fixed constant.
- Xylouris: $L \leq 5.18$, following a method of Heath-Brown.

II Lower Bound

- Pomerance : $P(k) \geq (e^\gamma + o(1))\phi(k)\log k \log_2 k \frac{\log_4 k}{(\log_3 k)^2}, \forall k \notin Q.$
- Li, Pratt, Shakan : $P(k) \gg \phi(k)\log k \log_2 k \log_4 k / \log_3 k, \forall k \notin Q' \supset Q.$

- What happens in number fields and function fields ?

Least Prime in Progression

Fix a positive integer k and let ℓ be coprime to k. Let $p(k,\ell)$ denote the smallest prime equivalent to ℓ modulo k, and define

$$P(k) := \max_{(\ell,k)=1} p(k,\ell).$$

Heuristic: $\liminf_k \frac{P(k)}{\phi(k)\log^2 k} = 1, \quad \limsup_k \frac{P(k)}{\phi(k)\log^2 k} = 2.$

I Upper Bound

- Linnik: $P(k) \ll k^L$, where $L > 0$ is a fixed constant.
- Xylouris: $L \leq 5.18$, following a method of Heath-Brown.

II Lower Bound

- Pomerance :
  $P(k) \geq (e^\gamma + o(1))\phi(k)\log k \log_2 k \frac{\log_4 k}{(\log_3 k)^2}, \forall k \notin Q.$
- Li, Pratt, Shakan :
  $P(k) \gg \phi(k)\log k \log_2 k \log_4 k / \log_3 k, \forall k \notin Q' \supset Q.$

- What happens in number fields and function fields ?

Least Prime in Progression

Fix a positive integer k and let ℓ be coprime to k. Let $p(k, \ell)$ denote the smallest prime equivalent to ℓ modulo k, and define

$$P(k) := \max_{(\ell,k)=1} p(k, \ell).$$

Heuristic: $\liminf_k \frac{P(k)}{\phi(k)\log^2 k} = 1, \quad \limsup_k \frac{P(k)}{\phi(k)\log^2 k} = 2.$

I Upper Bound

- Linnik: $P(k) \ll k^L$, where $L > 0$ is a fixed constant.
- Xylouris: $L \leq 5.18$, following a method of Heath-Brown.

II Lower Bound

- Pomerance :
  $P(k) \geq (e^\gamma + o(1))\phi(k) \log k \log_2 k \frac{\log_4 k}{(\log_3 k)^2}, \forall k \notin Q.$
- Li, Pratt, Shakan :
  $P(k) \gg \phi(k) \log k \log_2 k \log_4 k / \log_3 k, \forall k \notin Q' \supset Q.$

- What happens in number fields and function fields ?

Least Prime in Progression

Fix a positive integer k and let ℓ be coprime to k. Let $p(k,\ell)$ denote the smallest prime equivalent to ℓ modulo k, and define

$$P(k) := \max_{(\ell,k)=1} p(k,\ell).$$

Heuristic: $\liminf_k \frac{P(k)}{\phi(k)\log^2 k} = 1, \quad \limsup_k \frac{P(k)}{\phi(k)\log^2 k} = 2.$

I Upper Bound

- Linnik: $P(k) \ll k^L$, where $L > 0$ is a fixed constant.
- Xylouris: $L \leq 5.18$, following a method of Heath-Brown.

II Lower Bound

- Pomerance :
  $P(k) \geq (e^\gamma + o(1))\phi(k)\log k \log_2 k \frac{\log_4 k}{(\log_3 k)^2}, \forall k \notin Q.$
- Li, Pratt, Shakan :
  $P(k) \gg \phi(k)\log k \log_2 k \log_4 k/\log_3 k, \forall k \notin Q' \supset Q.$

- What happens in number fields and function fields ?

Divisor Scalar Multiplication Over Low Genus Hyperelliptic Curves

---

Sebastian Lindner

UNIVERSITY OF CALGARY

Background

SETTING: DIVISOR CLASS GROUP

Let C be a hyperelliptic curve of genus g over a finite field K.

- A **divisor** D is a formal sum of points on C.
- The **Divisor Class Group** of C is an additive abelian group related to divisors. In our setting, the divisor class group is isomorphic to the ideal class group of C.

WHY DO WE CARE: HEC CRYPTOGRAPHY

The most computationally intensive operation in Hyperelliptic Curve Cryptography (HECC) is scalar multiplication of a divisor D,

$$[n]D = D + D + D + \cdots + D, \ (n \text{ times.})$$

Efficient implementation of HECC relies on the ability to efficiently compute $[n]D$.

Research Focus

○ **Scalar Multiplication** (or exponentiation in multiplicative groups)

- We are looking at multibase representations of numbers (base 2 and 3) to speed up scalar multiplication due to the low weight, i.e.:

$$57 = 2^5 + 2^4 + 2^3 + 2^0 \quad \text{vs} \quad 57 = 2^1 3^3 + 2^0 3^1$$

○ **Group Law Operations**

- Group law operations (i.e.: doubles and additions) are expressed in polynomial arithmetic and refined to lower level finite field arithmetic.
- We are working on creating efficient tripling operations to take advantage of mixed representations of scalars.

○ **Special Families of Curves**

- We are looking at families of curves that exhibit efficiently computable multiplication by 3 isogenies, reducing the complexity of a triple.

Introduction and Research Interests

Abel Medina Lourenço
University of Campinas

UNCG Summer School in Computational Number Theory 2016

May 30, 2016

Numerical Semigroups

ımerical semigroup S is a subset of $\mathbb{N} \cup \{0\}$,closed under addition and with finite plement

genus is the cardinality of $\mathbb{N}\backslash S$

$_g$ be the quantity of numerical semigroups of genus g.

g	n_g	$n_{g-1}+n_{g-2}$	$n_{g-1}+n_{g-2}/n_g$	n_g/n_{g-1}
2	2	2	1	2
3	4	3	0.75	2
4	7	6	0.857143	1.75
5	12	11	0.916667	1.71429
6	23	19	0.826087	1.91667
7	39	35	0.897436	1.69565
8	67	62	0.925373	1.71795
9	118	106	0.898305	1.76119
10	204	185	0.906863	1.72881
20	37396	35931	0.960825	1.66471
30	5646773	5528869	0.97912	1.64254
40	774614284	765791252	0.98861	1.63128
50	101090300128	100460533126	0.99377	1.62525

$_{g-1} + \mathrm{n}_{g-2})/n_g = 1$ and $\lim\limits_{g\to\infty} n_g/n_{g-1} = \varphi = (1+\sqrt{5})/2$ (Proved by Alex Zhai 2011)

γ-Hyperelliptic Numerical Semigroups

The motivation to study them comes from Weierstrass semigroups at ramified points of doubl
of curves

Let $\gamma \geq 0$ be an integer.A numerical semigroup H is called γ-hyperelliptic if the following condi

1) H has γ even elements in [2,4γ]

2) The (γ+1)th positive element of H is 4γ+2

Currently we are interested in applying this concept to discover the asymptotic behavior of n(3^k,2),which is the amount of numerical semigroups generated by a pair of coprime positive i
whose genus is a power of 3

Diophantine Approximation

In the future,I would like to investigate problems relating Ergodic Theory and Number Theory
There is a well known result on Continued Fractions that states that for every irrational numbe
a sequence of best rational approximations,which are defined by the continued fraction expan
the number.However for generalized vectors the problem is not well understood yet.

My Research Interests

Tianyi Mao

CUNY Graduate Center

tmao@gradcenter.cuny.edu

May 20, 2016

Introduction

Research Experience

- Undergraduate: Algebraic codes
  - Mixed Codes
  - Quantum Codes
- Current: Analytic number theory
  - Distribution of integers in number fields
  - Bounded height problem
  - Multiple Dirichlet series

Today: Mixed codes (Joint with Feng)

Mixed Codes

Definition

Let $A_i (1 \leq i \leq s)$ be finite abelian groups. $A = A_1 \oplus A_2 \oplus \ldots \oplus A_s$. A **mixed code** C over A is a subset of A with size $K = |C| \geq 2$.

Note: When all $A_i (1 \leq i \leq s)$ are the same finite group or finite field, this is just the classical code. One have all analog of definitions and bounds (minimal distance, Hamming bounds (perfect codes) and Singleton bounds (MDS codes), dual codes, etc.)

My Work

Calculate $d(C^{\perp})$ for certain mixed codes coming from a partition of finite fields.

Application

Construct asymmetric inhomogenous quantum codes (AIQC)

Galois Groups of Eisenstein Polynomials over Local Fields

Jonathan Milstead

May 30, 2016

Ramification Polygons

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

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

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

3. Max Tame Subextension (Greve)

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

Blocks

1. Greve

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

2. Starting Group (Ex. 3 segments)

   $$\mathrm{Gal}(\varphi) \leq \mathrm{Gal}(\mathsf{L}_1/\mathsf{L}_2) \wr (\mathrm{Gal}(\mathsf{L}_2/\mathsf{L}_3) \wr \mathrm{Gal}(\mathsf{L}_3/\mathbb{Q}_p))$$

3. Residual Polynomial Classes (Milstead,Pauli)

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

Mathematical Interests

Michael Musty
Dartmouth College
math.dartmouth.edu/~mjmusty

UNCG Summer School in Computational Number Theory
May 30, 2016

Iwasawa theory

Let p be prime. A $\mathbb{Z}_p$-**extension** of a number field K is a tower of extensions

$$K = K_0 \subset K_1 \subset \cdots \subset K_n \subset \cdots \subset K_\infty$$

with $\mathrm{Gal}(K_\infty/K)$ isomorphic to the (additive) group $\mathbb{Z}_p$. Let

$$\begin{aligned} h(K_n) &= \text{class number of } K_n \\ e_n &= \text{highest power of } p \text{ dividing } h(K_n). \end{aligned}$$

Iwasawa proved there exist integer constants μ, λ, ν (depending only on p and the $\mathbb{Z}_p$-extension) such that

$$e_n = \mu \cdot p^n + \lambda \cdot n + \nu$$

for all n sufficiently large. Computing λ for $K = \mathbb{Q}(\zeta)$ and p odd was the subject of my MS thesis at the University of Vermont.

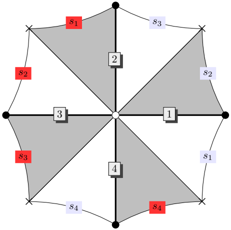
Belyĭ maps

A **Belyĭ map** is a morphism $f : X \to \mathbb{P}^1$ of (compact, connected) Riemann surfaces unramified away from $0, 1, \infty$.

Theorem (Belyĭ 1979)

A curve $X/\mathbb{C}$ can be defined over $\overline{\mathbb{Q}}$ $\iff$ X admits a Belyĭ map.

Belyĭ maps can be described combinatorially by **dessins d'enfants**.



Could a database of Belyĭ maps help us understand $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$?

Enumerating extensions of p-adic fields with given invariants

Sebastian Pauli

(joint work with Brian Sinclair)

University of North Carolina Greensboro

Generating Polynomials of Extensions of $\mathbb{Q}_3$ of degree 9

1. Totally ramified, thus Eisenstein 5085 Extensions

	x^0	x^1	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
3^3	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	0
3^2	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	0
3^1	$\neq 0$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	0
3^0	0	0	0	0	0	0	0	0	0	1

Generating Polynomials of Extensions of $\mathbb{Q}_3$ of degree 9

1. Totally ramified, thus Eisenstein 5085 Extensions
2. Valuation of Discriminant: 15 162 Extensions

	x^0	x^1	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
3^3	0	0	0	0	0	0	0	0	0	0
3^2	*	*	*	*	*	*	*	*	*	0
3^1	$\neq 0$	0	0	*	0	0	*	$\neq 0$	*	0
3^0	0	0	0	0	0	0	0	0	0	1

$3^{12} \cdot 2^2 = 2\,125\,764$ Polynomials

Generating Polynomials of Extensions of $\mathbb{Q}_3$ of degree 9

1. Totally ramified, thus Eisenstein 5085 Extensions
2. Valuation of Discriminant: 15 162 Extensions
3. Ramification polygon: $\{(1,7),(3,3),(9,0)\}$ 108 Extensions

	x^0	x^1	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
3^3	0	0	0	0	0	0	0	0	0	0
3^2	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$	0
3^1	$\neq 0$	0	0	$\neq 0$	0	0	$*$	$\neq 0$	$*$	0
3^0	0	0	0	0	0	0	0	0	0	1

$3^{11} \cdot 2^3 = 1\,417\,176$ Polynomials

Generating Polynomials of Extensions of $\mathbb{Q}_3$ of degree 9

1. Totally ramified, thus Eisenstein	5085 Extensions
2. Valuation of Discriminant: 15	162 Extensions
3. Ramification polygon: $\{(1,7),(3,3),(9,0)\}$	108 Extensions
4. Residual polynomials: $(2+z^2, 1+z^3)$	27 Extensions

	x^0	x^1	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9
	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
3^3	0	0	0	0	0	0	0	0	0	0
3^2	*	0	0	0	0	0	0	0	0	0
3^1	1	0	0	1	0	0	0	2	*	0
3^0	0	0	0	0	0	0	0	0	0	1

$3^2 = 9$ Polynomials

Generating Polynomials of Extensions of $\mathbb{Q}_3$ of degree 9

1. Totally ramified
2. Valuation of Discriminant: 15
3. Ramification polygon: $\{(1,7),(3,3),(9,0)\}$, slopes -2,$-1/3$
4. Residual polynomials: $(2+z^2, 1+z^3)$

Each of the 27 extensions of $\mathbb{Q}_3$ with these invariants is generated by exactly one of the polynomials:

$$\begin{array}{ccc}
x^9+6x^7+3x^3+3 & x^9+3x^8+6x^7+3x^3+3 & x^9+6x^8+6x^7+3x^3+3 \\
x^9+6x^7+3x^3+12 & x^9+3x^8+6x^7+3x^3+12 & x^9+6x^8+6x^7+3x^3+12 \\
x^9+6x^7+3x^3+21 & x^9+3x^8+6x^7+3x^3+21 & x^9+6x^8+6x^7+3x^3+21
\end{array}$$

Each polynomial generates 3 distinct extensions.

James Rudzinski
UNCG

May 30, 2016

UNCG Number Theory Summer School

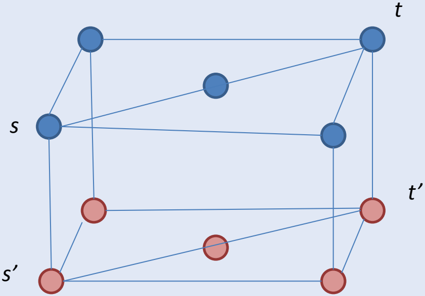
THE UNIVERSITY of NORTH CAROLINA
GREENSBORO

Some Areas of Interest

- Graph Theory
  - Graph Coloring
  - Bunk Bed Graphs
    - Percolation, Connectivity
- Game Theory
  - Combinatorial Games
    - Nim, Dynamic Nim

Current Research

Bunk Bed Conjecture – Given a bunk bed graph with a probability function defined on the edges, the probability that *s* is connected to *t* is greater than the probability that *s* is connected to *t'*.



THE UNIVERSITY *of* NORTH CAROLINA
GREENSBORO

Introduction

Sandi Rudzinski

Department of Mathematics and Statistics
University of North Carolina at Greensboro

May 30, 2016

About Me

- I just finished my first year of graduate school here at UNCG.
- My undergraduate degree is in computer science, but I also used to be a music major.
- My husband is a graduate student here as well, and we have two little girls, ages 6 and 10.
- I really enjoy math, but I am still trying to find a specific research topic.
- Dr. Pauli has kindly agreed to be my adviser and help me find a thesis topic.
- My current areas of possible interest include algebra, topology and logic.

Things I did a long time ago

As a computer science major, I wrote a music theory learning and testing program that used belief networks stored in a database to assess a user's level of readiness to progress through the subject matter based on their performance in particular areas of a test.

I also assisted with a paper involving user-modelling for search recommendations. I helped design and implement the XML-based user model and assisted with implementing the program that would create, read, and edit the user model.

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

Research Interests

Sam Schiavone

Dartmouth College

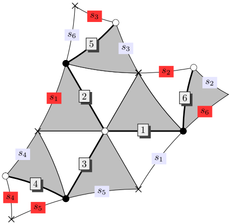
UNCG Summer School in Computational Number Theory
May 30, 2016

Belyĭ Maps

A **Belyĭ map** is a nonconstant morphism $\phi : X \to \mathbb{P}^1$ of algebraic curves unramified outside of $\{0, 1, \infty\}$.

Belyĭ maps can be described combinatorially by bicolored graphs, called **dessins d'enfants**.

In *Esquisse d'un Programme*,
Grothendieck describes an action of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the set of dessins d'enfants.



Numerical calculation of three-point branched covers of the projective line,
M. Klug, M. Musty, S. Schiavone, J. Voight.

Hilbert Modular Forms

A classical modular form $f : \mathcal{H} \to \mathbb{C}$ has a Fourier or q-expansion $f(z) = \sum_{n=0}^{\infty} a_n q^n$ where $q = e^{2\pi i z}$.

Let F be a totally real quadratic number field with ring of integers $\mathcal{O}_F$, e.g., $F = \mathbb{Q}(\sqrt{5})$, $\mathcal{O}_F = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. A Hilbert modular form $F : \mathcal{H}^2 \to \mathbb{C}$ also has a q-expansion $F(z_1, z_2) = \sum_{\nu \in \mathcal{O}_{F,\geq 0}} a_\nu q_1^{\nu_1} q_2^{\nu_2}$ where ν_1, ν_2 are the two embeddings of ν in $\mathbb{R}$ and $(q_1, q_2) = (e^{2\pi i z_1}, e^{2\pi i z_2})$.

We (joint work with B. Breen, J. Voight) are working on developing an algorithm to quickly multiply q-expansions of Hilbert modular forms.

UNCG Summer School

Nicolas Smoot

Georgia Southern University
Advised by Andrew Sills

29 May to 3 June, 2016

Introduction

- I'm a graduate student at Georgia Southern University. I just finished my M.S. in Mathematics.
- As a thesis topic, I studied the application of the circle method to problems in partition theory.

Definition

Fix a to be 1 or 3. Let $n \in \mathbb{N}$. A partition of n is associated with the Göllnitz–Gordon identities if each part is $4, \pm a \pmod 8$. The number of such partitions of n is denoted $g_a(n)$.

For $a = 1$ and $n = 10$, $g_a(n) = g_1(10) = 5$:

- $9+1$
- $7+1+1+1$
- $4+4+1+1$
- $4+1+1+1+1+1+1$
- $1+1+1+1+1+1+1+1+1+1$

Result and Future Interests

Theorem

Let $g_a(n)$ be the number of type-a Göllnitz–Gordon partitions of n. Then

$$
\begin{aligned}
g_a(n) = \frac{\pi\sqrt{2}}{4\sqrt{16n+4a-5}} \sum_{(k,8)=1} \left|\csc\left(\frac{\pi a k}{8}\right)\right| \frac{A_{a,1}(n,k)}{k} I_1\left(\frac{\pi\sqrt{16n+4a-5}}{8k}\right) \\
+ \frac{\pi\sqrt{2}}{\sqrt{16n+4a-5}} \sum_{(k,8)=4} \frac{A_{a,4}(n,k)}{k} I_1\left(\frac{\pi\sqrt{16n+4a-5}}{4k}\right) \\
+ \frac{2\pi}{\sqrt{16n+4a-5}} \sum_{(k,8)=8} \frac{A_{a,8}(n,k)}{k} I_1\left(\frac{\pi\sqrt{16n+4a-5}}{4k}\right)
\end{aligned}
$$

with $A_{a,d}(n,k)$ sums of specific roots of unity.

- The formula above, when truncated for $1 \leq k \leq 3\sqrt{n}$, gives a numerical result which differs from the correct answer by less than ± 0.33 for $1 \leq n \leq 200$.
- Interests include the theory of modular forms, the circle method, the Goldbach and Waring problems.
- Smoot, Nicolas A., "A Partition Function Connected with the Göllnitz–Gordon Identities" (2016). Electronic Theses And Dissertations. Paper 1389. `http://digitalcommons.georgiasouthern.edu/etd/1389`.

My math interests

Jana Sotáková

ALGANT, Universität Regensburg, Universiteit Leiden

UNCG Summer school, May 30 2016

About me

- Got interested in number theory at high school,

About me

- Got interested in number theory at high school,
- undergraduate studies at Masaryk Univerity, Brno, bachelor thesis "**The Number Field Sieve Method**",

About me

- Got interested in number theory at high school,
- undergraduate studies at Masaryk Univerity, Brno, bachelor thesis "**The Number Field Sieve Method**",
- currently studying masters with focus on algebra, geometry and number theory (ALGANT).

About me

- Got interested in number theory at high school,
- undergraduate studies at Masaryk Univerity, Brno, bachelor thesis "**The Number Field Sieve Method**",
- currently studying masters with focus on algebra, geometry and number theory (ALGANT).

Mathematical interests

algebraic number theory $\cap$ computational mathematics $\cap$ arithmetic/algebraic geometry $\cap$ cryptography

About me

- Got interested in number theory at high school,
- undergraduate studies at Masaryk Univerity, Brno, bachelor thesis "**The Number Field Sieve Method**",
- currently studying masters with focus on algebra, geometry and number theory (ALGANT).

Mathematical interests

algebraic number theory $\cap$ computational mathematics $\cap$ arithmetic/algebraic geometry $\cap$ cryptography $\approx$ **(elliptic) curves**

Things I like to think about

1. How to construct elliptic curves over finite fields with a prescribed number of points?

Things I like to think about

1. How to construct elliptic curves over finite fields with a prescribed number of points?
   Connections to algebraic number theory and complex multiplication theory.

Things I like to think about

1. How to construct elliptic curves over finite fields with a prescribed number of points?
   Connections to algebraic number theory and complex multiplication theory.
2. Computatational questions:

Things I like to think about

1. How to construct elliptic curves over finite fields with a prescribed number of points?
   Connections to algebraic number theory and complex multiplication theory.
2. Computatational questions:
   - *How to compute the Hilbert polynomial, how to compute the Hilbert class field of a given number field?*

Things I like to think about

1. How to construct elliptic curves over finite fields with a prescribed number of points?
   Connections to algebraic number theory and complex multiplication theory.
2. Computatational questions:
   - *How to compute the Hilbert polynomial, how to compute the Hilbert class field of a given number field?*
   - *How to determine the endomorphism ring of a given elliptic curve?*

Things I like to think about

1. How to construct elliptic curves over finite fields with a prescribed number of points?
   Connections to algebraic number theory and complex multiplication theory.
2. Computatational questions:
   - *How to compute the Hilbert polynomial, how to compute the Hilbert class field of a given number field?*
   - *How to determine the endomorphism ring of a given elliptic curve?*
   - *Counting points on curves,...*

Things I like to think about

1. How to construct elliptic curves over finite fields with a prescribed number of points?
   Connections to algebraic number theory and complex multiplication theory.
2. Computatational questions:
   - *How to compute the Hilbert polynomial, how to compute the Hilbert class field of a given number field?*
   - *How to determine the endomorphism ring of a given elliptic curve?*
   - *Counting points on curves,...*
3. Specific topics I am learning:

Things I like to think about

1. How to construct elliptic curves over finite fields with a prescribed number of points?
   Connections to algebraic number theory and complex multiplication theory.
2. Computatational questions:
   - *How to compute the Hilbert polynomial, how to compute the Hilbert class field of a given number field?*
   - *How to determine the endomorphism ring of a given elliptic curve?*
   - *Counting points on curves,...*
3. Specific topics I am learning: *isogeny volcanoes*,

Things I like to think about

1. How to construct elliptic curves over finite fields with a prescribed number of points?
   Connections to algebraic number theory and complex multiplication theory.
2. Computatational questions:
   - *How to compute the Hilbert polynomial, how to compute the Hilbert class field of a given number field?*
   - *How to determine the endomorphism ring of a given elliptic curve?*
   - *Counting points on curves,...*
3. Specific topics I am learning: *isogeny volcanoes*, *modular forms and theta functions*,

Things I like to think about

1. How to construct elliptic curves over finite fields with a prescribed number of points?
   Connections to algebraic number theory and complex multiplication theory.
2. Computatational questions:
   - *How to compute the Hilbert polynomial, how to compute the Hilbert class field of a given number field?*
   - *How to determine the endomorphism ring of a given elliptic curve?*
   - *Counting points on curves,...*
3. Specific topics I am learning: *isogeny volcanoes*, *modular forms and theta functions*, *pairings*,

Things I like to think about

1. How to construct elliptic curves over finite fields with a prescribed number of points?
   Connections to algebraic number theory and complex multiplication theory.
2. Computatational questions:
   - *How to compute the Hilbert polynomial, how to compute the Hilbert class field of a given number field?*
   - *How to determine the endomorphism ring of a given elliptic curve?*
   - *Counting points on curves,...*
3. Specific topics I am learning: *isogeny volcanoes*, *modular forms and theta functions*, *pairings*, *arithmetic on (Jacobians of) hyperelliptic curves*, ...

Introduction

Emerald Stacy
Oregon State University

- 4th year graduate student
- Research Area: Arithmetic Dynamics
- Advisor: Clayton Petsche
- Graduate Certificate in College and University Teaching
- Minor in Women, Gender and Sexuality Studies

Totally p-adic Numbers

Definition

If α is an algebraic number over $\mathbb{Q}$ with a minimal polynomial that splits completely over $\mathbb{Q}_p$, then we say α is **totally p-adic***.*

Definition

Given a prime p and a positive integer d, we define $\tau_{d,p}$ to the minimal height among all totally p-adic non zero, non-root of unity, algebraic numbers.

Research Questions

Theorem (S.)

Given a prime p,

$$\tau_{2,p} = \begin{cases} \frac{1}{2}\log\left(\frac{1+\sqrt{5}}{2}\right) & \textit{if } p \equiv 1, 4 \pmod 5 \\ \frac{1}{2}\log 2 & \textit{otherwise} \end{cases}$$

Future Questions:

- Is there a congruence condition on p which will completely categorize $\tau_{3,p}$?
- What is the smallest totally 3-adic algebraic number, not a root of unity?
- What is the smallest totally p-adic algebraic number, not a root of unity?

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 30, 2016

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 $\mathsf{F}_2 := \mathsf{F}(\mathfrak{m}\mathfrak{p}_\infty^{(2)})$ 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.

Analytic Semigroups and the Abstract Cauchy Problem

Keller VandeBogert

Georgia Southern University

UNCG Summer School, 2016

Quick intro

1. C_0 and Analytic semigroups, at their core (in relation to evolution equations), are a rigorous foundation to the challenge of defining the exponential of an operator.
2. The Abstract Cauchy problem is an abstract evolution-type equation with initial conditions, ie:

$$\frac{du}{dt}+A(t)u = f(t)$$
$$u(0) = u_0$$

3. Well, in the homogeneous case, you could say that $u(t) = e^{-At}$. This of course seems absurd (recall that A is an arbitrary operator), but, it turns out it isn't.

Some Interesting Results

Theorem (Hille-Yosida Theorem)

A necessary and sufficient condition that a closed linear operator A with dense domain D_A be the infinitesimal generator of a C_0 semigroup is that there exist real numbers M and ω such that for every real $\lambda > \omega$, $\lambda \in \rho(A)$, and:

$$||R(\lambda; A)^n|| \leq \frac{M}{(\lambda - \omega)^n}$$

1. The theory of Analytic Semigroups can be used to solve the Abstract Cauchy Problem under a set of conditions by means of constructing a fundamental solution and convolving with our "forcing function" f.
2. Proving that an operator is the infinitesimal generator of an Analytic Semigroup is an even stronger condition than C_0 semigroups, and this automatically implies better regularity of solutions.
3. The language of semigroups allows for a rather natural way to define the fractional power of an operator: $A^{-\alpha} = \frac{1}{\Gamma(\alpha)} \int_0^\infty e^{-sA} s^{\alpha - 1} ds$

Research Interests:

Algorithms for Galois groups, number fields, and p-adic fields

Chad Awtrey

Elon University (NC)

Computing Galois Groups

NOTATION:

F, $\overline{F}$	field, fixed algebraic closure
$f(x) \in F[x]$	irreducible of degree n
$a_1, \ldots, a_n$	roots of f in $\overline{F}$
$K = F(a_1)$	stem field of f
$K^g = F(a_1, \ldots, a_n)$	splitting field of f
$\mathrm{Aut}(K/F)$	automorphism group of K/F
$\mathrm{Gal}(f) = \mathrm{Aut}(K^g/F)$	transitive subgroup of S_n

QUESTION: How can we compute $\mathrm{Gal}(f)$?

ANSWER: Eliminate all candidates except one using invariants of $\mathrm{Gal}(f)$.

A Family of Invariants

For $1 \leq k \leq n$, let $T_k = a_1 + \cdots + a_k$. (recall: a_i are roots of f)

- Let $H = \mathrm{Sym}(\{1, \ldots, k\}) \times \mathrm{Sym}(\{k+1, \ldots, n\})$. So $H \simeq S_k \times S_{n-k}$.
- Let $R_k(x) = \prod_{g \in S_n/H}(x - T_k^g)$. So $\mathrm{Degree}(R_k(x)) = \binom{n}{k}$.
- $R_k(x)$ can be computed via resultants.

Theorem

Suppose $R_k(x)$ is squarefree. Then K/F has m subfields of index k if and only if $R_k(x)$ has m irreducible factors of degree n/k if and only if $Gal(f)$ has m block systems consisting of n/k blocks of size k.

EXAMPLE:

- Over $\mathbb{Q}$, let $f(x) = x^4 - 4x^3 + 8x^2 - 4x + 1$.
- Then $R_2(f) = (x^2 - 4x + 2)(x^2 - 4x + 6)(x^2 - 4x + 8)$.
- So $\mathrm{Gal}(f) \simeq V_4$.

UNCG Summer School in Computational Number Theory

FUNCTION FIELDS

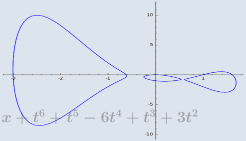
May 30 to June 3, 2016

Speakers

- **Florian Hess**
  Oldenburg
- **Mike Jacobson**
  Calgary
- **Renate Scheidler**
  Calgary

$$\begin{tikzcd}
 & KE \arrow[dl, dash] \arrow[ddr, dash] & \\
K = F(t)[x]/(f) \arrow[d, dash] & & \\
F(t) \arrow[dr, dash] & & E = F(\alpha) \arrow[dl, dash] \\
 & F &
\end{tikzcd}$$

$$f(t,x) = x^2 + (t+1)x + t^6 + t^5 - 6t^4 + t^3 + 3t^2$$



organized by the number theory group at UNCG

www.uncg.edu/numbertheory/summerschool