SouthEastern Regional Meeting On Numbers XXIX

Saturday and Sunday, April 2–3, 2016

Abstracts

Genesis Alberto, James Madison University / Howard University

---

Title: The division polynomials for the Holm curve and their properties

Abstract: Let p be a prime number and $\mathbb{K} = \mathbb{F}_p$ be the finite field with p elements, and $\lambda \in \mathbb{K}$ such that $\lambda \neq 0, \pm 1$. In this work we will study the division polynomials of the Holm elliptic curve in its original form,

$$H_\lambda : y^3 - y = \lambda(x^3 - x)$$

and a remodeled form,

$$H'_\lambda : (u - \lambda)v^2 = u^3 - \lambda.$$

We will explicitly state their group structures together with the bi-rational correspondence to their Weierstrass models. Using these mappings, we will derive the multi-variable division polynomials and the single variable division polynomials, then investigate their properties.

Max Alekseyev, George Washington University

Title: A computational method for solving exponential-polynomial Diophantine equations

Abstract: We propose a computational method for solving some Diophantine equations of the form $KQ^n = f(m)$, where K and Q are fixed positive integers and $f(m)$ is a second-degree polynomial with integer coefficients. Our method involves solving generalized Pell-Fermat equations and computing zeros of the solution modulo some powers of Q. We illustrate our method on the equation $3^n = 2m^2 + 1$ and show that its only solutions are $(m, n) = (0, 0), (\pm 1, 1), (\pm 2, 2),$ and $(\pm 11, 5)$.

Darren Glass, Gettysburg College

Title: Counting arithmetical structures on graphs

Abstract: For any finite graph, Lorenzini defined the notion of an arithmetical structure on the graph; one formulation of this definition is a labelling of the vertices of a graph with positive integers so that the label of each vertex is a divisor of the sum of the labels of all adjacent vertices. These structures are of interest for a number of reasons, but in this talk, I will emphasize the number theoretic questions they lead to and discuss recent work with various co-authors counting the number of structures on graphs in various families.

Robert Grizzard, University of Wisconsin–Madison

Title: Counting units of bounded degree and height

Abstract: We'll show that the number of algebraic units of degree d and height at most T is asymptotic to $c_d T^{d(d-1)}$, where c_d is an explicit constant. This is a special case of an asymptotic formula for the number of algebraic integers of bounded degree and height having any given norm, any given trace, any given norm and trace, and beyond! Our results build on work of Chern-Vaaler and Sinclair on counting polynomials with bounded Mahler measure. This is joint work in progress with Joseph Gunther (CUNY).

Anne M. Ho, Coastal Carolina University

Title: Counting Artin-Schreier curves over finite fields

Abstract: A number of authors have considered the weighted sum of various types of curves with a certain genus g over a finite field $k := \mathbb{F}_q$ of a specific characteristic. These include elliptic curves (Howe), hyperelliptic curves (Van der Geer, Van der Vlught), and Artin-Schreier curves (Cardona, Nart, Pujols, Sadornil). We extend the work of these authors by considering a related weighted sum for Artin-Schreier curves with a given genus g over fields of any characteristic p. We will discuss our results and methods of counting, which include looking at ramification divisors, finding associated rational models $y^p - y = u(x)$, and examining the actions of $\mathrm{PGL}_2(k)$ on the models. In addition, we will discuss the geometric connections to the moduli space of Artin-Schreier curves.

Bob Hough, Institute of Advanced Study

Title: The minimum modulus problem for covering systems

Abstract: A distinct covering system of congruences is a finite collection of arithmetic progressions to distinct moduli

$$a_i \bmod m_i, \qquad 1 < m_1 < m_2 < \cdots < m_k$$

whose union is the integers. Answering a question of Erdős, I have shown that the least modulus m_1 of a distinct covering system of congruences is at most 10^{16}. I will describe aspects of the proof, which involves the theory of smooth numbers and a relative form of the Lovász local lemma.

Angel Kumchev, Towson University

Title: Recent progress in the Waring-Goldbach problem

Abstract: Recent progress on Vinogradov's mean-value theorem has resulted in improved estimates for exponential sums of Weyl type. In recent joint work with T.D. Wooley, we apply

these new estimates to obtain sharper bounds for the function $H(k)$ in the Waring-Goldbach problem. We obtain new results for all exponents $k \geq 7$; in particular, we establish that $H(k) \leq (4k-2)\log k - (2\log 2 - 1)k - 3$ when k is large. The latter bound represents the first improvement on a classical result of Hua from the 1940s.

Jaclyn Lang, University of California–Los Angeles

Title: Images of Galois representations

Abstract: Galois representations are a major topic of study in modern number theory. They provide a way to access information about the absolute Galois group of the rational numbers. One usually wants to prove that the images of such representations are "as large as possible". We will discuss what this means and what is known for certain types of Galois representations coming from modular forms and p-adic families of modular forms. The talk should be accessible to a general number theory audience.

Codie Lewis, James Madison University

Title: Numerical data regarding the Cohen-Lenstra heuristics for class groups of real quadratic fields

Abstract: We performed a numerical investigation into predictions made by the Cohen-Lenstra heuristics. Data was obtained up to a discriminant bound of 4 million for the purpose of establishing a baseline from which more complete studies may be performed. The particular heuristic of concern to us predicts that the percentage of class groups of real quadratic fields with square-free discriminant which contain a p-part in their torsion asymptotically approaches $1-\prod_{k\geq 2}(1-p^{-k})$ as the bound on the discriminant is taken to infinity. As it has been suggested that there exits a discrepancy between the conjectured probabilities and the data, we calculated the statistics for $p = 3, 5, 7$ and used curve fitting to explore secondary terms of the form CX^s for each p.

Nathan McNew, Towson University

Title: Numbers divisible by a large shifted prime

Abstract: In 1980 Erdös and Wagstaff showed that most positive integers are not divisible by any "large" shifted primes. We improve upon this result by obtaining precise estimates for the count of integers up to x divisible a shifted prime $p - 1 > y$ in essentially the full range of x and y. In particular, we show that as x and y tend to infinity this count is at most $x/(\log y)^{(b+o(1))}$ where $b = 1 - (1 + \log\log 2)/\log 2$ is the Erdös-Ford-Tenenbaum constant, and that this bound is optimal for a large range of y. We also mention applications of this result to arithmetic statistics of elliptic curves.

Michael Mossinghoff, Davidson College

Title: Thunder over Liouville

Abstract: *Thunder over Louisville* is the largest annual pyrotechnic display on the continent, occurring each April in another southeastern state. We discuss some rhetorical thunder over the Liouville function, the completely multiplicative arithmetic function $\lambda(n)$ defined by setting $\lambda(p) = -1$ for each prime p. We discuss some rumblings over the last century in number theory concerning this function and its connection to the Riemann Hypothesis and other problems, including bolts of insight by Pólya and Turán, a reverberating theorem of Ingham's, and a blast from Grosswald and others. In particular, we look at questions involving the magnitude of oscillations in certain sums involving this function, and some recent efforts quantifying these variations. This is joint work with T. Trudgian.

Andrew Obus, University of Virginia

Title: The local lifting problem for A_4

Abstract: Let k be an algebraically closed field of characteristic p and G a finite group. The local lifting problem asks whether a G-Galois extension $k[[z]]/k[[t]]$ lifts to a characteristic zero G-Galois extension $R[[Z]]/R[[T]]$. The speaker has recently solved the local lifting problem for $G = A_4$ and $p = 2$. The talk will motivate the local lifting problem, discuss why A_4 is an interesting case, and shed some light on the proof.

Kevin Sheng, Emory University

Title: The Cohen-Lenstra heuristics and Soundararajan's thesis

Abstract: We give an exposition of Kannan Soundararajan's Princeton Ph.D. thesis. His main theorem gives lower bounds on the number of torsion elements of the ideal class group $\mathrm{CL}(K)$ for imaginary quadratic fields $K = \mathbb{Q}(\sqrt{-d})$. The proof relies on counting the number of square free d satisfying certain Diophantine conditions. These conditions are shown to be sufficient for the existence of elements of order g. Proofs of certain classical results from algebraic number theory, such as the finiteness of $\mathrm{CL}(K)$, are also included.

Howard Skogman, State University of New York at Brockport

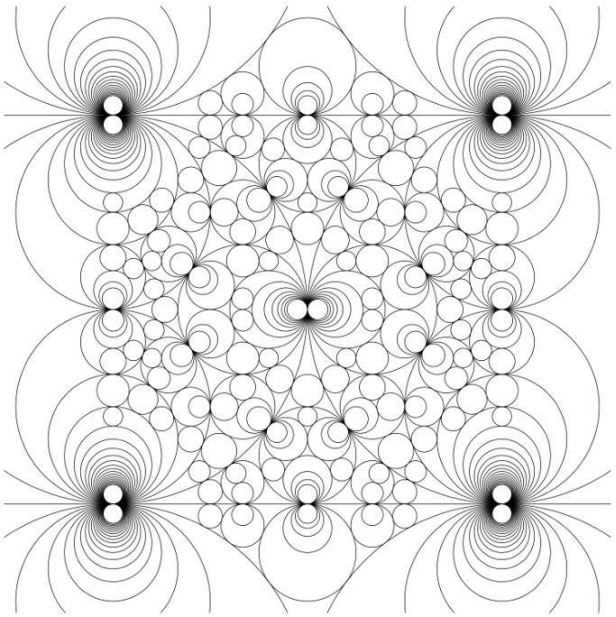
Title: Ramanujan graphs arising as weighted covering graphs

Abstract: We give a new construction of (finite) families of Ramanujan graphs arising as a new type of covering graph called a weighted covering graph. This new type of covering graph generalizes standard covering graphs, and we define a subclass of Galois covers that allow for easier spectral analysis. While our construction is very specialized, the analysis reveals conditions for potential base graphs with Ramanujan covers.

Kate Stange, University of Colorado–Boulder

Title: Visualising the arithmetic of imaginary quadratic fields

Abtract: Let K be an imaginary quadratic field with ring of integers O_K. The Schmidt arrangement of K is the orbit of the extended real line in the extended complex plane under the Mobius transformation action of the Bianchi group $\mathrm{PSL}(2, O_K)$. The arrangement takes the form of a dense collection of intricately nested circles. Aspects of the number theory of O_K can be characterised by properties of this picture: for example, the arrangement is connected if and only if O_K is Euclidean. I'll explore this structure and its connection to Apollonian circle packings. Specifically, the Schmidt arrangement for the Gaussian integers is a disjoint union of all primitive integral Apollonian circle packings. Generalizing this relationship to all imaginary quadratic K, the geometry naturally defines some new circle packings and thin groups of arithmetic interest.



Cindy Tsang, University of California–Santa Barbara

Title: Galois module structure of the square root of the inverse different in Abelian extensions

Abstract: Let K be a number field with ring of integers $\mathcal{O}_K$ and let L/K be a finite Galois extension with group G. A classical problem in number theory is to study the structure of the ring of integers $\mathcal{O}_L$ in L as an $\mathcal{O}_K G$-module. More recently, people have also considered the $\mathcal{O}_K G$-module structure of the so-called square root of the inverse different of L/K. I will briefly talk about the background of this problem and then state a few results that I have proved in the case that G is Abelian.

Hui Xue, Clemson University

Title: When can products of two eigenforms equal?

Abstract: Let f_1, f_2, g_1 and g_2 be Hecke eigenforms of level 1. A natural question is: when can $f_1 \cdot f_2 = g_1 \cdot g_2$ happen? We will give some partial answer to it.

David Zureick-Brown, Emory University

Title: Sporadic torsion on elliptic curves

Abstract: In Mazur's celebrated 1978 Inventiones paper, he classifies the torsion subgroups which can occur in the Mordell-Weil group of an elliptic curve over $\mathbb{Q}$. His result was extended to elliptic curves over quadratic number fields by Kamienny, Kenku, and Momose, with the full classification being completed in 1992. What both of these cases have in common is that each subgroup in the classification occurs for infinitely many elliptic curves, but this no longer holds for cubic number fields. In 2012, Najman showed that there exists an elliptic curve whose torsion subgroup over a particular cubic field is $\mathbb{Z}/(21)$. This was the first sporadic example, because the modular curve $X_1(21)$ classifying such elliptic curves has only finitely many cubic points, therefore there can only be finitely many such curves. In this talk, we will recall what is known so far and introduce new results about sporadic points on the modular curves $X_1(N)$ and $X_1(M, N)$.

This is joint with Anastassia Etropolski and Jackson Morrow.