Saturday, September 15, 2018

8:30 - 9:00 Coffee and a few refreshements in Manchester 017

9:00 - 10:00 **David Zywina** (Cornell University), Computing ℓ-adic monodromy groups

10:10 - 10:30 **Andrew Kobin** (University of Virginia), Wild Stacky Curves

10:40 - 11:00 **James Phillips** (University of Virginia), Good reduction of covers of elliptic curves

11:00 - 11:20 Coffee break in Manchester 017

11:20 - 11:40 **Chung-Ru Lee** (Duke University), Rational Points in Regular Orbits attached to Infinitesimal Symmetric Spaces

11:50 - 12:10 **Dan Yasaki** (UNC-Greensboro), On the growth of torsion in the cohomology of arithmetic groups

12:10 - 1:40 Lunch

1:40 - 2:30 **Aaron Landesman** (Stanford University), The average size of Selmer groups over function fields

2:40 - 3:00 **Lori Watson** (University of Georgia), Hasse Principle Violations of Quadratic Twists of Hyperelliptic Curves

3:00 - 3:20 Coffee break in Manchester 017

3:20 - 3:40 **Chad Awtrey** (Elon University), On Galois groups of doubly even octic polynomials

3:50 - 4:10 **Harsh Mehta** (University of South Carolina), Malle's conjecture on Frobenius groups and semi direct products

4:20 - 4:30 Break

4:30 - 4:50 **Carrie Finch-Smith** (Washington & Lee University), Prescribed gaps in sequences of Sierpiński numbers

5:00 - 5:20 **Arindam Roy** (UNC Charlotte), Zeros of partial sums of L-functions

Sunday, September 16, 2018

8:15 - 8:45	Coffee and a few other refreshments in Manchester 017
8:45 - 9:35	**Anastassia Etropolski** (Rice University), Chabauty-Coleman Experiements for Genus 3 Hyperelliptic Curves
9:45 - 10:05	**Michael Cerchia** (Wake Forest University), Determining the image of the Arboreal Galois representation
10:15 - 10:35	**Noah Lebowitz-Lockard** (University of Georgia), Irreducible Quadratic Polynomials and Euler's Function
10:35 - 10:55	Coffee break in Manchester 017
10:55 - 11:15	**Kübra Benli** (University of Georgia), Small prime power residues
11:25 - 11:45	**Chen An** (Duke University), ℓ-torsion in class groups of certain families of D_4-quartic fields
11:55 - 12:55	**Lillian Pierce** (Duke University), Counting

All talks will take place in Manchester Hall, room 016. This room is either in the basement, or on ground level, depending on which side of the building you enter from.

The organizers wish to thank the National Science Foundation, the National Security Agency, and the Wake Forest University Department of Mathematics and Statistics for their support.

Abstracts

David Zywina (Cornell University),*Computing ℓ-adic monodromy groups*

Abstract: Fix a prime ℓ and an abelian variety A over a number field. The Galois action on the torsion points of A can be described by an ℓ-adic Galois representation. The Zariski closure G of its image is called the ℓ-adic monodromy group of A. The group G encodes a lot of the arithmetic/geometry of A. For example, the Sato-Tate distribution of A can conjecturally be determined from G. We will discuss approaches to studying and computing these monodromy groups.

Andrew Kobin (University of Virginia),*Wild Stacky Curves*

Abstract: In their paper "The canonical ring of a stacky curve," Voight and Zureick-Brown give a combinatorial description of the canonical ring of a tame stacky curve (similar to the notion of an orbifold curve) using the root stack construction, which encodes Kummer theory in the language of stacks. To allow wild ramification, one must replace root stacks with something analogous in characteristic $p > 0$. In this talk, I introduce such a construction, call a "universal Artin-Schreier root stack," and show how it can be used to describe covers of stacky curves in the $\mathbb{Z}/p\mathbb{Z}$-case.

James Phillips (University of Virginia), *Good reduction of covers of elliptic curves*

Abstract: Covers of an algebraic curve correspond to extensions of its field of rational functions. Studying its fundamental group then allows us to gain information about the Galois theory of its function field. This is considerably easier, however, in characteristic zero than it is in positive characteristic, due to results such as Riemann's Existence Theorem. Given a cover in characteristic zero, we can use its reduction to positive characteristic to bridge this gap, so long as the reduced cover is "as nice" as the original. To this end, we will give some criteria for determining when this happens in the case of covers of elliptic curves branched over one point, extending results of Raynaud and Obus.

Chung-Ru Lee (Duke University), *Rational Points in Regular Orbits attached to Infinitesimal Symmetric Spaces*

Abstract: Motivated by problems arising in the relative trace formula and arithmetic invariant theory we prove the existence of rational points on orbits arising from certain infinitesimal symmetric spaces. As an application, we prove analogous results for orbits in certain global reductive symmetric spaces.

Dan Yasaki (UNC-Greensboro), *On the growth of torsion in the cohomology of arithmetic groups*

Abstract: Bergeron and Venkatesh recently gave a precise conjecture about the growth of the order of the torsion subgroup of homology groups over a tower of cocompact congruence

subgroups. We investigate computationally the cohomology of several (non-cocompact) arithmetic groups, including $\mathrm{GL}_n(\mathbb{Z})$ for $n = 3, 4, 5$ and $\mathrm{GL}_2(\mathcal{O})$ for various rings of integers, and observe its growth as a function of level. In all cases where our dataset is sufficiently large, we observe excellent agreement with the same limit as in the predictions of Bergeron-Venkatesh. Our data also prompts us to make two new conjectures on the growth of torsion not covered by the Bergeron-Venkatesh conjecture.

Aaron Landesman (Stanford University), *The average size of Selmer groups over function fields*

Abstract: We explain why, in the large q limit, the average size of the n-Selmer group of an elliptic curve over $\mathbb{F}_q(t)$ is the sum of the divisors of n. More generally, with Tony Feng, we verify predictions of Poonen and Rains for the distributions of Selmer groups over function fields, again in the large q limit. Our proof reveals an alternate heuristic for Selmer group distributions: the moments are the number of orbits of certain orthogonal group actions.

Lori Watson (University of Georgia), *Hasse Principle Violations of Quadratic Twists of Hyperelliptic Curves*

Abstract: A curve $C/\mathbb{Q}$ is said to violate the Hasse Principle if C has points over every completion of $\mathbb{Q}$ but not over $\mathbb{Q}$ itself. Conditionally on the ABC conjecture, we show that if a hyperelliptic curve $C/\mathbb{Q}$ is given by $y^2 = f(x)$, where f is a polynomial of even degree > 6 with integer coefficients and no rational roots, then there are many quadratic twists of C violating the Hasse Principle. This is joint work with Pete L. Clark.

Chad Awtrey (Elon University), *On Galois groups of doubly even octic polynomials*

Abstract: Let $f(x) = x^8 + ax^4 + b$ be an irreducible polynomial with rational coefficients, $g(x) = x^4 + ax^2 + b$, G_f the Galois group of f, and G_g the Galois group of g. We investigate the extent to which knowledge of G_g determines G_f. We show that, in general, knowledge of G_g does not automatically determine G_f, except when G_g is cyclic of order 4. We also show that G_f is completely determined when G_g is dihedral of order 8 and $4b - a^2$ is a perfect square.

Harsh Mehta (University of South Carolina), *Malle's conjecture on Frobenius groups and semi direct products*

Abstract: We let a group G act on the set of d letters, $[d]$, by the induced left multiplication of action of the symmetric group S_d acting on $[d]$. We attain upper bounds for the number of degree d algebraic extensions K/k with Galois group G as the norm of the discriminant $\mathcal{N}_{k/\mathbb{Q}}(d_{K/k})$ is bounded above by $x \to \infty$. We attain upper bounds for the number of such extensions for groups of the form $G = F \rtimes H$ with certain conditions on F and H. Malle made a conjecture about what the asymptotic of this quantity should be as $\mathcal{N}_{k/\mathbb{Q}}(d_{K/k}) \to \infty$. We show that under a conjecture of Cohen and Lenstra, the upper bounds we achieve, match the prediction of Malle.

Carrie Finch-Smith (Washington & Lee University), *Prescribed gaps in sequences of Sierpiński numbers*

Abstract: An odd positive integer k with the property that $k \cdot 2^n + 1$ is composite for all natural numbers n is called a Sierpiński number. In this talk, we discuss sequences of Sierpiński numbers in which consecutive terms differ by powers of 2.

Arindam Roy (UNC Charlotte), *Zeros of partial sums of L-functions*

Abstract: Let $f(n)$ be a multiplicative function taken from a suitable class of multiplicative functions and let $F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ for Re $(s) > 1$. We give an estimate for $\sum_{n \le x} \frac{f(n)}{n}$ in term of $|F(1 + 1/\log x)|$. As a consequence, we obtain a non-trivial zero-free region for the partial sums of most of the L-functions. We also discuss some results regarding the distribution of zeros of partial sums of Dedekind zeta functions. This is a joint work with Akshaa Vatwani.

Anastassia Etropolski (Rice University), *Chabauty-Coleman Experiments for Genus 3 Hyperelliptic Curves*

Abstract: Given a curve of genus at least 2, it was proven in 1983 by Faltings that it has only finitely many rational points. Unfortunately, this result is ineffective, in that it gives no bound on the number of rational points. 40 years earlier, Chabauty proved the same result under the condition that the rank of the Jacobian of the curve is strictly smaller than the genus. While this is obviously a weaker result, the methods behind that proof could be made effective, and this was done by Coleman in 1985. Coleman's work led to a procedure known as the Chabauty-Coleman method, which has shown to be extremely effective at determining the set of rational points exactly, particularly in the case of hyperelliptic curves. In this talk I will discuss how we implement this method using Sage to provably determine the set of rational points on a large set of genus 3, rank 1 hyperelliptic curves, and how these calculations fit into the context of the state of the art conjectures in the field. The subject of this talk is joint work with Jennifer Balakrishnan, Francesca Bianchi, Victoria Cantoral-Farfan, and Mirela Ciperiani.

Michael Cerchia (Wake Forest University), *Determining the image of the Arboreal Galois representation*

Abstract: Suppose $E/\mathbb{Q}$ is an elliptic curve and $\alpha \in E(\mathbb{Q})$ is a point of infinite order. How often is it the case that α has odd order when we reduce E mod p? If we let S be the set of primes $p \le x$ for which $E/\mathbb{F}_p$ is non-singular and $\alpha \in \mathbb{F}_p$ has odd order, then our general goal is to determine

$$\lim_{x \to \infty} \frac{\pi_S(x)}{\pi(x)}$$

where $\pi_S(x)$ is the number of primes p with $p \in S$ and $p \le x$, and $\pi(x)$ is the total number of primes $p \le x$. It turns out that the answer to this question is contingent upon determining all possible images of a particular Galois representation – the Arboreal Galois representation. This talk will explore this connection.

Noah Lebowitz-Lockard (University of Georgia), *Irreducible Quadratic Polynomials and Euler's Function*

Abstract: We investigate the range of Euler's phi-function. In 1929, Pillai proved that almost all numbers lie outside the range of phi. For a given polynomial P, we may ask whether P(n) is almost always outside the range of phi as well. We discuss this problem for irreducible quadratic polynomials and relate it to a few unsolved problems.

Kübra Benli (University of Georgia), *Small prime power residues*

Abstract: Let p be a prime number. For each positive integer k, it is widely believed that the smallest prime that is a kth power residue modulo p should be $O(p^{\epsilon})$, for any $\epsilon > 0$. Elliott has proved that such a prime is at most $p^{\frac{k-1}{4}+\epsilon}$, for each $\epsilon > 0$. In this talk we will see how extended reciprocity laws can lead to a result on number of prime kth power residues which are less than the bound proved by Elliott.

Chen An (Duke University), *ℓ-torsion in class groups of certain families of D_4-quartic fields*

Abstract: In this talk, we will briefly discuss results on ℓ-torsion in class groups of number fields. Some results are obtained by Ellenberg-Pierce-Wood and Pierce-Turnage-Butterbaugh-Wood. Without assuming GRH, they prove nontrivial upper bounds for ℓ-torsion in class groups of almost all number fields in certain families. Notably the methods fail to deal with D_4-quartic fields. I will describe my recent work on ℓ-torsion in class groups of almost all fields in certain families of D_4-quartic fields.

Lillian Pierce (Duke University), *Counting*

Abstract: Many problems in number theory can be phrased in terms of counting: counting primes, counting points, counting elements with certain properties in a group or field, or counting fields themselves. In this talk we will discuss a problem of counting elements of a certain finite order in a particular type of group, and see how this relates in some unexpected ways to other counting problems—in fact, to all the above counting problems.