PAlmetto Number Theory Series

December 8-9, 2018

Abstracts

Chen An (Duke University)

Title: *ℓ-torsion in class groups of certain families of D_4-quartic fields*

Scheduled: Saturday, LC 412, 10:30 a.m.

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.

Lea Beneish (Emory University)

Title: *Quasimodular moonshine and arithmetic connections*

Scheduled: Sunday, LC 405, 9:55 a.m.

Abstract: We prove the existence of a module for the largest Mathieu group, whose trace functions are weight two quasimodular forms. Restricting to the subgroup fixing a point, we see that the integrality of these functions is equivalent to certain divisibility conditions on the number of $\mathbb{F}_p$ points on Jacobians of modular curves. Extending such expressions to arbitrary primes, we find trace functions for modules of cyclic groups of prime order with similar connections. Moreover, for cyclic groups, we give an explicit vertex operator algebra construction whose trace functions are given only in terms of weight two Eisenstein series.

Kubra Benli (University of Georgia)

Title: *Small prime power residues modulo p*

Scheduled: Sunday, LC 405, 11:50 a.m.

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 discuss some results on the number of prime k^{th} power residues which are smaller than the bound proved by Elliott.

Bruce Berndt (University of Illinois)

Title: *The final problem: a series identity from the Lost Notebook*

Scheduled: Saturday, LC 412, 1:30 p.m.

Abstract: When Ramanujan's lost notebook was published in 1988, accompanying it were other

unpublished notes and partial manuscripts by Ramanujan. In one of these previously unpublished partial manuscripts, Ramanujan offered two elegant identities, associated, respectively, with the classical *circle* and *divisor problems*. In fact, they are two-variable analogues, but not generalizations, of classical identities associated with these two famous problems. The origin and history of this partial manuscript is unclear. We do know that after Ramanujan died in 1920, the University of Madras on 30 August, 1923 sent to G.H. Hardy a parcel of Ramanujan's unpublished work, probably containing the lost notebook and the previously mentioned fragment. Unfortunately, we do not have any record of what was included in this package. If this fragment was included in the mailing, then it is possible that Ramanujan wrote it at the end of his life in either 1919 or 1920. On the other hand, from Hardy's paper on the *circle problem* published in 1915, it is evident that by early in his stay in England, Ramanujan had developed a strong interest in the *circle* and *divisor problems*, and so the fragment may emanate from this period. In 2013, Alexandru Zaharescu, Sun Kim and the speaker published a proof of the identity from the fragment connected with the *circle problem*. The identity associated with the *divisor problem* was not established until this past summer by Zaharescu, Junxian Li, and the speaker. We think that this is the last identity from the lost notebook and other unpublished papers that was to be proved.

Abbey Bourdon (Wake Forest University)

Title: *Torsion points and isogenies on CM elliptic curves*

Scheduled: Saturday, LC 401, 3:20 p.m.

Abstract: We say an elliptic curve E defined over a number field F has complex multiplication (CM) if $\mathrm{End}_{\overline{F}}(E) \cong \mathcal{O}$, an order in an imaginary quadratic field K. For any positive integer N, we determine the least d in which there exists a number field F of degree d and an $\mathcal{O}$-CM elliptic curve E/F with an F-rational point of order N. The proof relies on several new results concerning rational cyclic isogenies on CM elliptic curves, extending work of Kwon (1999). This is joint work with Pete L. Clark.

Zarathustra (Zeb) Brady (MIT)

Title: *A semidefinite framework for upper bound sieves*

Scheduled: Saturday, LC 412, 3:50 p.m.

Abstract: The standard approach to sieve theory, based on inclusion-exclusion inequalities, can be put into the framework of linear programming: we are trying to find a collection of sieve weights (one for each squarefree number), satisfying a certain collection of linear inequalities, such that a certain linear combination of the sieve weights is minimized (for instance, the beta sieve and the Selberg sieve correspond to particular choices of sieve weights). The Large Sieve does not fall into this framework. In this talk, I'll describe a new framework based on semidefinite programming for proving upper bounds on sifted sets, where instead of trying to find a collection of sieve weights satisfying a collection of linear conditions, we are trying to find a collection of "sifting matrices" (one for each squarefree number) satisfying certain positive semidefiniteness conditions. In this framework, both the Large Sieve and the Larger Sieve will correspond to particular choices of sifting matrices. I'll show that this new framework has several nice properties that the linear programming framework lacks, such as being able to handle the prime 2 correctly, and getting good bounds while only using sifting matrices corresponding to primes instead of all squarefree

numbers. I'll also describe some numerical computations using this framework to get upper bounds for sizes of admissible tuples.

Michael Cerchia (Wake Forest University)

Title: *Classifying the images of the Arboreal Galois representation*

Scheduled: Saturday, LC 401, 2:50 p.m.

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 $p \leq x$ for which $E/\mathbb{F}_p$ is non-singular and $\alpha \in \mathbb{F}_p^2$ 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 $p \leq x$, and $\pi(x)$ is the total number of primes $p \leq x$. 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.

Huy Dang (University of Virginia)

Title: *Deformations of Artin-Schreier covers and the connectedness of the moduli space of Artin-Schreier curves*

Scheduled: Saturday, LC 405, 3:20 p.m.

Abstract: In this talk, I will discuss the deformations of Z/p-covers and the connectedness of the moduli space of Z/p-covers of fixed genus. Let R be a complete discrete valuation ring of equal characteristic and k be its residue field (for example R=k[[t]]). Given an order p-automorphism of a formal disc over R, the dual graph of its semi-stable model along with the associated degeneration data give rise to a combinatorial object called a Hurwitz tree. We are able to show that the existence of such a tree along with some combinatorial conditions on its structure is equivalent to the existence of a deformation of Z/p-covers over k with ramification data encoded in that tree. That helps us show that the moduli space of Z/p-covers of fixed genus is connected when the genus is sufficiently large.

Jeff Hoffstein (Brown University)

Title: *An overview of the theory and applications of multiple Dirichlet series*

Scheduled: Saturday, LC 412, 5:10 p.m.

Abstract: The first multiple Dirichlet series was written down by Siegel in the 1950's. In the 1980's Dorian Goldfeld and I wrote down the first application: a mean value theorem for values of quadratic Dirichlet L-series evaluated at the center of the critical strip. Over the next several decades I, Bump, Brubaker, Chinta, Diaconu, Friedberg, Goldfeld, Gunnells and others have continued to develop and exploit this subject. I will describe the origins and main accomplishments of the theory of multiple Dirichlet series and some recent new developments. My aim is to make this talk accessible to as wide an audience as possible.

Pin Hung Kao (Flagler College)

Title: *Polynomials and products of polynomials at prime arguments*

Scheduled: Sunday, LC 401, 9:55 a.m.

Abstract: We adopt A. J. Irving's double-sieve method to study the almost-prime values produced by irreducible polynomials and products of irreducible polynomials evaluated at prime arguments. For the first part of the talk, we present a refinement of the double-sieve method and the improvements on Irving's results. We will show, in the second part of the talk, that the double-sieve method, combined with the estimates involving the upper and lower DHR sifting functions, improve upon the results cited in Diamond–Halberstam for both small and large values of g, where g is the degree of the polynomial in question. (The results from the second part of the talk is a joint work with C. Franze.)

Daniel Keliher (Tufts University)

Title: *Comparing the number of D_4 and S_4 extensions of a number field*

Scheduled: Sunday, LC 412, 11:50 a.m.

Abstract: When ordered by discriminant, about 83% of quartic fields over $\mathbb{Q}$ have associated Galois group S_4, while only 17% have Galois group D_4. We study this disparity over a general number field by studying the ratio between the number of D_4 and the number of S_4 degree 4 extensions of a number field. Conditional on GRH, we give a lower bound for a typical quadratic field and for arbitrary number fields. In doing so, we find (unconditionally) that there are fields over which the proportion of quartic extensions that are D_4 can be arbitrarily close to 1. This is joint work with Matthew Friedrichsen.

Aaron Landesman (Stanford University)

Title: *The geometric average size of Selmer groups over function fields*

Scheduled: Sunday, LC 412, 9:00 a.m.

Abstract: We explain why, as q tends to infinity, 100% of elliptic curves of a given height over $F_q(t)$ have rank 0 or 1. We deduce this from a computation of the average size of n-Selmer groups of elliptic curves of fixed height over $F_q(t)$ in the large q limit. In joint work with Tony Feng, we also compute the higher moments of these n-Selmer groups and verify analogs of predictions of Poonen and Rains. Our proof reveals an alternate heuristic for Selmer group distributions: the moments are the number of orbits of certain orthogonal group actions.

Noah Lebowitz-Lockard (University of Georgia)

Title: *Irreducible quadratic polynomials and Euler's function*

Scheduled: Sunday, LC 405, 12:20 p.m.

Abstract: Let $V(x)$ be the number of $n \leq x$ for which $\varphi(m) = n$ for some m, where φ is Euler's totient function. In 1929, Pillai proved that $V(x) = o(x)$, i.e. that almost all numbers lie outside the range of the totient function. We discuss some improvements and variants of this result, such as the fact that for any irreducible quadratic polynomial $P(x)$, almost all numbers of the form $P(n)$

lie outside the range of the totient function as well. We put bounds on the number of $n \leq x$ with this property and show how we can improve them assuming the abc Conjecture.

Robert Lemke-Oliver (Tufts University)

Title: *Rank growth of elliptic curves in nonabelian extensions*

Scheduled: Saturday, LC 412, 10:00 a.m.

Abstract: Given an elliptic curve $E/\mathbb{Q}$, it is a conjecture of Goldfeld that asymptotically half of its quadratic twists will have rank zero and half will have rank one. Nevertheless, higher rank twists do occur: subject to the parity conjecture, Gouvêa and Mazur constructed $X^{1/2-\epsilon}$ twists by discriminants up to X with rank at least two. For any $d \geq 3$, we build on their work to consider twists by degree d S_d-extensions of $\mathbb{Q}$ with discriminant up to X. We prove that there are at least $X^{c_d-\epsilon}$ such twists with positive rank, where c_d is a positive constant that tends to $1/4$ as $d \to \infty$. Moreover, subject to a suitable parity conjecture, we obtain the same result for twists with rank at least two. This is joint work with Frank Thorne.

Jackson Morrow (Emory University)

Title: *Non-archimedean hyperbolicity and applications*

Scheduled: Sunday, LC 401, 11:50 a.m.

Abstract: The conjectures of Green, Griffths and Lang predict the precise interplay between different notions of hyperbolicity: Brody hyperbolic, arithmetically hyperbolic, Kobayashi hyperbolic, algebraically hyperbolic, groupless, and more. In his thesis (1993), W. Cherry defined a notion of non-Archimedean hyperbolicity; however, his definition does not seem to be the "'correct' version, as it does not mirror complex hyperbolicity. In recent work, A. Javanpeykar and A. Vezzani introduced a new non-Archimedean notion of hyperbolicity, which ameliorates this issue, and also stated a non-Archimedean variant of the Green-Griffths-Lang conjecture. In this talk, I will discuss complex and non-Archimedean notions of hyperbolicity as well as some recent progress on the non-Archimedean Green-Griffths-Lang conjecture. This is joint work with Ariyan Javanpeykar (Mainz) and Alberto Vezzani (Paris 13).

Arindam Roy (UNC-Charlotte)

Title: *Zeros of partial sums of L-functions*

Scheduled: Saturday, LC 405, 10:30 a.m.

Abstract: Let $f(n)$ be a multiplicative function taken from a suitable class of functions and let $F(s)$ be the corresponding Dirichlet series. We give a non-trivial bound for logarithmic mean values of functions $f(n)$ in terms of $|F(s)|$ when s is near 1 and $\mathrm{Re}(s) > 1$. 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.

Robert Schneider (University of Georgia)

Title: *Multiplicative theory of (additive) partitions*

Scheduled: Saturday, LC 412, 3:20 p.m.

Abstract: Much like the positive integers $\mathbb{Z}^+$, the set $\mathcal{P}$ of integer partitions ripples with interesting patterns and relations. Now, the prime decompositions of integers are in bijective correspondence with the set of partitions into prime parts, if we associate 1 to the empty partition. One wonders: might some number-theoretic theorems arise as images in $\mathbb{Z}^+$ (i.e. in prime partitions) of greater algebraic and set-theoretic structures in $\mathcal{P}$?

We show that many well-known objects from elementary and analytic number theory are in fact special cases of phenomena in partition theory: a multiplicative arithmetic of partitions that generalizes classical theorems; a class of "partition zeta functions" containing the Riemann zeta function and other Dirichlet series (as well as exotic non-classical cases); and other phenomena at the intersection of the additive and multiplicative branches of number theory.

Jeremiah Southwick (University of South Carolina)

Title: *A result with Newton polygons*

Scheduled: Saturday, LC 405, 10:00 a.m.

Abstract: We study a family of polynomials arising from a generating function corresponding to the vanishing properties of the Dedekind-eta function. We use Newton polygons to show the family is irreducible.

Padmavathi Srinivasan (Georgia Tech University)

Title: *Conductors and minimal discriminants of hyperelliptic curves: a comparison in the tame case*

Scheduled: Sunday, LC 412, 10:40 a.m.

Abstract: Conductors and minimal discriminants are two measures of degeneracy of the singular fiber in a family of hyperelliptic curves. In genus one, the Ogg–Saito formula shows that these two invariants are equal, and in genus two, Qing Liu showed that they are related by an inequality. In this talk, we will show that Liu's inequality extends to hyperelliptic curves of arbitrary genus in the absence of wild ramification phenomena. The key ingredients in this proof are an explicit analysis of regular models arising from Jung's method of resolving surface singularities, and an understanding of the behaviour of associated metric trees under a natural inductive process.

Doug Ulmer (University of Arizona)

Title: *An analogue of the Brauer-Siegel theorem for abelian varieties*

Scheduled: Saturday, LC 412, 11:00 a.m.

Abstract: Given a sequence of number fields K of bounded degree, the classical Brauer-Siegel theorem says that the product of h_K (the class number of K) and R_K (the unit regulator of K), grows like the square root of D_K (the discriminant of K). More precisely,

$$\frac{\log(h_K R_k)}{(1/2)\log(D_K)} \longrightarrow 1.$$

Recently, Hindry proposed an analogue for abelian varieties: One considers abelian varieties A of fixed dimension over a fixed global field K and compares the product of the order of $Ш_A$, (the

conjecturally finite Tate-Shafarevich group of A) and R_A (the Neron-Tate regulator of A) with H_A (the exponential differential height of A). Naive analogy suggests that

$$\frac{\log(|\text{Ш}_A|R_A)}{\log(H_A)} \xrightarrow{?} 1.$$

I will introduce the players and explain what is known and expected about this question. In the case where K is a global function field, interesting results may be obtained both analytically and algebraically.

Jiuya Wang (Duke University)

Title: *Malle's conjecture for compositum of number fields*

Scheduled: Saturday, LC 405, 2:50 p.m.

Abstract: Malle's conjecture is a conjecture on the asymptotic distribution of number fields with bounded discriminant. We propose a general framework to prove Malle's conjecture for compositum of number fields based on known examples of Malle's conjecture and good uniformity estimates. By this method, we prove Malle's conjecture for $S_n \times A$ number fields for $n = 3, 4, 5$ and A in an infinite family of abelian groups. As a corollary, we show that Malle's conjecture is true for $C_3 \wr C_2$ in its S_9 representation, whereas its S_6 representation is the first counter example of Malle's conjecture given by Klüners. By a sieve method, we further prove the secondary term for $S_3 \times A$ extensions for infinitely many odd abelian groups A over $\mathbb{Q}$.

Lori Watson (University of Georgia)

Title: *Hasse principle violations of quadratic twists of hyperelliptic curves*

Scheduled: Sunday, LC 412, 9:55 a.m.

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.

Maggie Wieczorek (University of Tennessee)

Title: *Congruence results for $c\phi_k(n)$*

Scheduled: Saturday, LC 412, 2:50 p.m.

Abstract: The partition function is known to exhibit beautiful congruences that are often proved using the theory of modular forms. In this talk, I discuss the extent to which these congruence results apply to generalized Frobenius partitions found through joint work with Marie Jameson. In particular I give a result guaranteeing infinitely many congruences for $c\phi_k(n)$ and prove results regarding the parity of $\overline{c\phi_2}(n)/4$.

Dan Yasaki (University of North Carolina at Greensboro)

Title: *On the growth of torsion in the cohomology of arithmetic groups*

Scheduled: Sunday, LC 412, 12:20 p.m.

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 $GL_n(\mathbb{Z})$ for $n = 3, 4, 5$ and $GL_2(O)$ 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.

Shaoyun Yi (University of Oklahoma)

Title: *Klingen p^2 vectors for $GSp(4, F)$*

Scheduled: Saturday, LC 401, 10:30 a.m.

Abstract: We calculate the dimensions of the spaces of the Klingen p^2-invariant vectors for all irreducible admissible representations of $GSp(4, F)$, where F is a p-adic field.
