TITLES AND ABSTRACTS

49TH BARRETT LECTURES

Relative K-Groups and Rings of Integers

Adebisi Agboola (UCSB)

Abstract: Suppose that F is a number field and G is a finite group. I shall discuss a conjecture in relative algebraic K-theory (in essence, a conjectural Hasse principle applied to certain relative algebraic K-groups) that implies an affirmative answer to both the inverse Galois problem for F and G and to an analogous problem concerning the Galois module structure of rings of integers in tame extensions of F. It also implies the weak Malle conjecture on counting tame G-extensions of F according to discriminant. The K-theoretic conjecture can be proved in many cases (subject to mild technical conditions), e.g. when G is of odd order, giving a partial analogue of a classical theorem of Shafarevich in this setting. While this approach does not, as yet, resolve any new cases of the inverse Galois problem, it does yield substantial new results concerning both the Galois module structure of rings of integers and the weak Malle conjecture.

Much of what we shall discuss is joint work with Leon McCulloh.

On Graphs of Hecke Operators

Roberto Alvarenga (USP and UC Irvine)

Abstract: Some of recent development in number theory is related to Hecke operators and automorphic forms (e.g., Langlands correspondence). In Bombay 1979, Don Zagier observes that if the kernel of certain operators on automorphic forms turns out to be an unitarizable representation, over the field of rational numbers $\mathbb{Q}$, a formula of Hecke implies the Riemann hypothesis. Zagier calls the elements of this kernel toroidal automorphic forms. Moreover, Zagier asks what happens if $\mathbb{Q}$ is replaced by a global function field and remarks that the space of unramified toroidal automorphic forms can be expected to be finite dimensional. Motivated these questions, Oliver Lorscheid introduces, in 2012, the *graphs of Hecke operators* for global function fields. This theory allowed him to prove, among other things, that the space of unramified toroidal automorphic forms for a global function field is indeed, finite dimensional. The graphs of Hecke operators introduced by Lorscheid encode the action of Hecke operators on automorphic forms.

On the other hand, Ringel (1990), Kapranov (1997), Schiffmann (2012) et al. have been developing the theory of *Hall algebra* of coherent sheaves over a smooth geometric irreducible projective curve over a finite field (in general for a finitary category).

For this talk we discuss the connection between graphs of Hecke operators and Hall algebras. In the elliptic case, Atiyah's work on vector bundles (1957) allow us to describe (explicitly) these graphs.

Rational Points on the Cursed Curve

Jennifer Balakrishnan (Boston University)

Abstract: The split Cartan modular curve of level 13, also known as the "cursed curve," is a genus 3 curve defined over the rationals. By Faltings' proof of Mordell's conjecture, we know that it has finitely many rational points. However, Faltings' proof does not give an algorithm for finding these points. We discuss how to determine rational points on this curve using "quadratic Chabauty," part of Kim's nonabelian Chabauty program. This is joint work with Netan Dogra, Steffen Mueller, Jan Tuitman, and Jan Vonk.

---

a-Numbers of Curves in Artin-Schreier Covers

Jeremy Booher (University of Arizona)

Abstract: Let $\pi : Y \to X$ be a branched $\mathbf{Z}/p\mathbf{Z}$-cover of smooth, projective, geometrically connected curves over a perfect field of characteristic $p > 0$. We investigate the relationship between the a-numbers of Y and X and the ramification of the map π. This is analogous to the relationship between the genus (respectively p-rank) of Y and X given the Riemann-Hurwitz (respectively Deuring-Shafarevich) formula. Except in special situations, the a-number of Y is not determined by the a-number of X and the ramification of the cover, so we instead give bounds on the a-number of Y. We provide examples showing our bounds are sharp. The bounds come from a detailed analysis of the kernel of the Cartier operator. This is joint work with Bryden Cais.

Arithmetic Levi-Civita Connection

Alexandru Buium (University of New Mexico)

Abstract: We present existence and uniqueness results for certain remarkable Frobenius lifts on the p-adic completions of the general linear group over the integers; these Frobenius lifts will be attached to a given symmetric matrix with integer coefficients. We will then consider the problem of defining and computing commutators of the Frobenius lifts corresponding to various primes p. From a conceptual viewpoint, the above collection of Frobenius lifts attached to a symmetric integral matrix may be viewed as an arithmetic analogue, for the spectrum of the integers, of the Levi-Civita connection attached to a metric on a manifold; the collection of commutators of these Frobenius lifts can then be viewed as an arithmetic analogue of Riemannian curvature. We will show that this arithmetic Riemannian curvature satisfies congruences that are analogous to the symmetries of the classical Riemannian tensor. We will also explain how, in order for these analogies to operate, one needs to revisit some of the main concepts of classical Riemannian geometry.

Iwasawa Theory for Function Fields

Bryden Cais (University of Arizona)

Abstract: Let $\{X_n\}$ be a $\mathbf{Z}_p$-tower of smooth projective curves over a perfect field k of characteristic p that totally ramifies over a finite, nonempty set of points of X_0 and is unramified elsewhere. In analogy with the case of number fields, Mazur and Wiles studied the growth of the p-parts of the class groups $\mathrm{Jac}(X_n)[p^\infty](\overline{k})$ as n-varies, and proved that these naturally fit together to yield a module that is finite and free over the Iwasawa algebra. We introduce a novel perspective by proposing to study growth of the full p-divisible group $G_n := \mathrm{Jac}(X_n)[p^\infty]$, which may be thought of as the p-primary part of the *motivic class group* $\mathrm{Jac}(X_n)$. One has a canonical decomposition $G_n = G_n^{et} x G_n^m x G_n^{ll}$ of G into its etale, multiplicative, and local-local components, as well as an equality $G_n(\overline{k}) = G_n^{et}(\overline{k})$. Thus, the work of Mazur and Wiles captures the etale part of G_n, so also (since Jacobians are principally polarized) the multiplicative part: both of these p-divisible subgroups satisfy the expected structural and control theorems in the limit. In contrast, the local-local components G_n^{ll} are far more mysterious (they can not be captured by $\overline{k}$-points), and indeed the tower they form has no analogue in the number field setting. This talk will survey this circle of ideas, and will present new results and conjectures on the behavior of the local-local part of the tower $\{G_n\}$.

Solutions of the Hurwitz-Markoff Equation over Polynomial Rings

Ricardo Conceição (Gettysburg College)

Abstract: Let A and n be positive integers. The structure of the set of integral solutions of the equation

$$x_1^2 + \cdots + x_n^2 = A x_1 \cdots x_n \tag{1}$$

was first studied by Hurwitz, as a generalization of Markoff's equation (the case $n = A = 3$). Hurwitz showed that all integral solutions can be generated by the action of certain automorphisms of the hypersurface defined by (1) on finitely many solutions. Ever since, several authors have extended Hurwitz's work to the study of solutions of (1) over finite fields and number fields. Our goal is to discuss some progress made in understanding the solutions of (1) over the polynomial ring $k[t]$, where k is a field.

Variation of Néron-Severi Ranks of Reductions of Algebraic Surfaces

Edgar Costa (MIT)

Abstract: We study the behavior of geometric Picard rank of a $K3$ surface over $\mathbb{Q}$ under reduction modulo primes. We compute these ranks for reductions of representative examples, investigate the resulting statistics and discuss the implications.

A User's Guide to Mochizuki's Inequality

Taylor Dupuy (University of Vermont)

Abstract: The aim of this talk is to give just the statement of Mochizuki's inequality. We hope to make the statement of Corollary 3.12 accessible and the ideas behind its application to Szpiro-like inequalities accessible to analytic number theorist. This is joint work with Anton Hilado.

Using Supersingular Elliptic Curves for Cryptography

Kirsten Eisentraeger (Pennsylvania State University)

Abstract: Cryptosystems based on supersingular isogenies have been proposed recently for use in post-quantum cryptography. Three problems have emerged related to their hardness: computing an isogeny between two supersingular elliptic curves, computing the endomorphism ring of a supersingular elliptic curve, and computing a maximal order associated to it. We give reductions between these problems, describe the cryptosystems and discuss their security.

The Unipotent Albanese Map and Rational Points on Varieties

Daniel Hast (Rice University)

Abstract: Given a curve of genus at least 2 over a number field, Faltings' theorem tells us that its set of rational points is finite. Provably computing the set of rational points is a major open problem, as is the question of whether the number of rational points can be uniformly bounded. We will survey some recent progress and ongoing work using the Chabauty–Kim method, which uses the fundamental group to construct p-adic analytic functions that vanish on the set of rational points. In particular, we present a new proof of Faltings' theorem for superelliptic curves over the rational numbers (due to joint work with Jordan Ellenberg), and a conditional generalization of the Chabauty–Kim method to number fields and higher dimensions.

The Mean Value of Cubic L-Functions over Function Fields

Matilde Lalín (Université de Montréal)

Abstract: We present results about the first moment of L-functions associated to cubic characters over $\mathbb{F}_q(T)$ when q is congruent to 1 modulo 3. The case of number fields was considered in previous work, but never for the full family of cubic twists over a field containing the third roots of unity. We will explain how to obtain an asymptotic formula with a main term, which relies on using results from the theory of metaplectic Eisenstein series about cancellation in averages of cubic Gauss sums over functions fields. We will also discuss the case q congruent to 2 modulo 3.

Newton Polygon Stratification of the Torelli Locus in PEL-type Shimura Varieties

Wanlin Li (University of Wisconsin-Madison)

Abstract: A fundamental problem in arithmetic geometry is to determine which abelian varieties arise as Jacobians of (smooth) curves. In positive characteristic p, we study this problem from the moduli perspective by asking which Newton strata intersect the Torelli locus in the moduli of abelian varieties. In this talk, I will introduce a general picture where we try to answer his question by replacing $\mathcal{A}_g$ with a Shimura variety of PEL-type, and $\mathcal{M}_g$ with a Hurwitz space of cyclic covers of $\mathbb{P}^1$. Using an inductive method, when $p = 2 \pmod 3$, for all g, we prove the existence of a smooth curve of genus g whose Newton polygon has about $2g/3$ slopes of $1/2$. This work is joint with Mantovan, Pries and Tang.

Complex Moments and the Distribution of Values of $L(1, \chi_D)$ over Function Fields with Applications to Class Numbers

Allysa Lumley (York University)

Abstract: In 1992, Hoffstein and Rosen proved a function field analogue to Gauß' conjecture (proven by Siegel) regarding the class number, h_D, of a discriminant D by averaging over all polynomials with a fixed degree. In this case $h_D = |\mathrm{Pic}(\mathcal{O}_D)|$, where $\mathrm{Pic}(\mathcal{O}_D)$ is the Picard group of $\mathcal{O}_D$. Andrade later considered the average value of h_D, where D is monic, squarefree and its degree $2g+1$ varies. He achieved these results by calculating the first moment of $L(1, \chi_D)$ in combination with Artin's formula relating $L(1, \chi_D)$ and h_D. Later, Jung averaged $L(1, \chi_D)$ over monic, squarefree polynomials with degree $2g + 2$ varying. Making use of the second case of Artin's formula he gives results about $h_D R_D$, where R_D is the regulator of $\mathcal{O}_D$.

For this talk we discuss the complex moments of $L(1, \chi_D)$, with D monic, squarefree and degree n varying. Using this information we can describe the distribution of values of $L(1, \chi_D)$ and after specializing to $n = 2g + 1$ we give results about h_D and specializing to $n = 2g + 2$ we give results about $h_D R_D$.

If time permits, we will discuss similar results for $L(\sigma, \chi_D)$ with $1/2 < \sigma < 1$.

Isogeny Graphs in Cryptography

Travis Morrison (University of Waterloo)

Abstract: A large enough quantum computer will be able to break RSA and elliptic curve cryptography, so several "post-quantum" cryptosystems are under consideration for standardization in a process run by NIST. One submission, SIKE, uses isogenies of supersingular elliptic curves in a public key cryptosystem. Private keys are paths in isogeny graphs. In this talk, I will discuss the structure of these graphs, how they are used in cryptography, and how they might be used to compute endomorphism rings of supersingular elliptic curves.

Non-Archimedean Hyperbolicity and Applications

Jackson Morrow (Emory University)

Abstract: The conjectures of Green-Griffiths-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-Griffiths-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-Griffiths-Lang conjecture. This is joint work with Ariyan Javanpeykar (Mainz) and Alberto Vezzani (Paris 13.)

The Proportion of a Certain Family of Everywhere Locally Soluble Genus 1 Curves

Jennifer Park (Ohio State University)

Abstract: Poonen and Voloch proved that the Hasse principle holds for either 100% or 0% of most families of hypersurfaces (specified by degrees and the number of variables). In this joint work with Tom Fisher and Wei Ho, we study one of the special families of hypersurfaces not accounted for by Poonen and Voloch, and we show that the explicit proportion of everywhere locally soluble $(1,1)$-curves in $P^1 \times P^1$ is about 87.4%.

Conductors and Minimal Discriminants of Hyperelliptic Curves in Odd Residue Characteristic

Padmavathi Srinivasan (Georgia Tech)

Abstract: Conductors and minimal discriminants are two measures of degeneracy in a family of hyperelliptic curves. We will outline recent progress in extending Liu's inequality in genus 2 relating these two invariants to hyperelliptic curves of arbitrary genus when the residue characteristic is odd.

Low Degree Points on Curves

Isabel Vogt (MIT and Stanford University)

Abstract: In this talk we will discuss an arithmetic analogue of the gonality of a curve over a number field: the smallest positive integer e such that the points of residue degree bounded by e are infinite. By work of Faltings, Harris-Silverman and Abramovich-Harris, it is well-understood when this invariant is 1, 2, or 3; by work of Debarre-Fahlaoui these criteria do not generalize to e at least 4. We will study this invariant using the auxiliary geometry of a surface containing the curve and devote particular attention to scenarios under which we can guarantee that this invariant is actually equal to the gonality. This is joint work with Geoffrey Smith.

Hearing Algebraic Curves and Factoring Polynomials

Felipe Voloch (University of Canterbury)

Abstract: The possibility of telling apart algebraic curves over a finite field by their zeta function is a problem analogous to the classical question of hearing the shape of a drum. Just like drums, this is not always possible but often is. We discuss this problem and approaches to telling algebraic curves apart by looking at zeta functions of their étale covers. This problem has a surprising connection with the question of factoring polynomials over finite fields in deterministic polynomial time. We will also discuss this connection and a conjectural resolution.
