CTNT 2018 - TITLES AND ABSTRACTS

JUNE 1ST - JUNE 3RD

ABBEY BOURDON (Wake Forest)

Title: Sporadic Points with j-invariant of Bounded Degree

Abstract: Our work is motivated by the following classification problem: For a fixed positive integer d, what finite groups arise as the torsion subgroup of an elliptic curve defined over a number field of degree d? A serious challenge in attempting to extend the classification beyond $d = 1$ or $d = 2$ is the need to identify all groups which arise for only finitely many isomorphism classes of elliptic curves. The known examples of such groups correspond to elliptic curves with a rational point of order N appearing in unusually low degree; that is, they correspond to sporadic points on the modular curve $X_1(N)$. In this talk, I will discuss recent results concerning sporadic points of $X_1(N)$ which arise from elliptic curves with j-invariant in an extension of bounded degree. This is joint work with Özlem Ejder, Yuan Liu, Frances Odumodu, and Bianca Viray.

MICHAEL CHOU (Tufts)

Title: Torsion of CM elliptic curves defined over the maximal abelian extension of $\mathbb{Q}$

Abstract: The first main theorem of complex multiplication relates the field of definition of torsion points of a CM elliptic curve in terms of certain ray class fields. In this talk we show how this idea can be used to give a partial classification of the possible torsion structures that can arise for CM elliptic curve defined over the maximal abelian extension of $\mathbb{Q}$. This is joint work with Pete Clark and Marko Milosevic.

ALINA COJOCARU (UIC)

Title: Primes, elliptic curves and cyclic groups

Abstract: Inspired by the similarities between the group of units of the finite field with p elements, $\mathbb{F}_p$, and the group of $\mathbb{F}_p$-rational points of an elliptic curve, I will give an overview of results pertaining to the cyclicity of the groups defined by the reductions modulo primes of an elliptic curve over $\mathbb{Q}$.

HARRIS DANIELS (Amherst College)

Title: Groups of generalized G-type and applications to torsion subgroups of rational elliptic curves over infinite extensions of $\mathbb{Q}$

Abstract: Recently there has been much interest in studying the torsion subgroups of elliptic curves base-extended to infinite extensions of $\mathbb{Q}$. In this talk we study what happens with the torsion of an elliptic curve E over $\mathbb{Q}$ when changing base to the compositum of all number fields with Galois group G for a fixed group G. We start with a survey of what is known and then continue studying the problem by giving a group theoretic condition called generalized G-type, which is a necessary condition for a number field with Galois group H to be contained in that compositum. In general,

group theory allows one to reduce the original problem to the question of finding rational points on finitely many modular curves. To illustrate this method we completely determine which torsion structures occur for elliptic curves defined over $\mathbb{Q}$ and base-changed to the compositum of all fields whose Galois group is of generalized A_4-type. This is joint work with Maarten Derickx and Jeffrey Hatley.

TAYLOR DUPUY (UVM)

Title: How do we use Mochizuki's Inequality?

Abstract: I will attempt to shed some light on Mochizuki's inequality from a user's perspective. I would like to discuss applications, inputs required, where it comes from, and places where his Szpiro bounds can be tinkered with. This may end up being a talk about the p-adic logarithm and some adelic volume computations. We'll see what happens. This is joint work with Anton Hilado.

JORGE FLOREZ (CUNY)

Title: Eisenstein cocycles for $\mathrm{GL}(n)$ and values of L-functions in imaginary quadratic extensions

Abstract: We generalize Sczech's Eisenstein cocycle for $\mathrm{GL}(n)$ over totally real extensions of $\mathbb{Q}$ to finite extensions of imaginary quadratic fields. By evaluating the cocyle on certain cycles, we parametrize complex values of Hecke L-functions previously considered by Colmez, giving a cohomological interpretation of his algebraicity result on special values of the L-functions.

SUMITA GARAI (Penn State)

Title: Endomorphism Rings of Finite Drinfeld Modules and Algorithms

Abstract: The theory of Drinfeld modules runs parallel to the theory of Elliptic curves, and our result was motivated by a similar result for Elliptic curves. Let $A = \mathbb{F}_q[T]$ be the polynomial ring over $\mathbb{F}_q$, and F be the field of fractions of A. Let ϕ be a Drinfeld A-module of rank r over F. For all but finitely many primes $\mathfrak{p} \lhd A$, one can reduce ϕ modulo $\mathfrak{p}$ to obtain a Drinfeld A-module $\phi \otimes \mathbb{F}_\mathfrak{p}$ of rank r over $\mathbb{F}_\mathfrak{p} = A/\mathfrak{p}$. It is known that the endomorphism ring $\mathcal{E}_\mathfrak{p} = \mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\phi \otimes \mathbb{F}_\mathfrak{p})$ is an order in an imaginary field extension K of F of degree r. Let $\mathcal{O}_\mathfrak{p}$ be the integral closure of A in K, and let $\pi_\mathfrak{p} \in \mathcal{E}_\mathfrak{p}$ be the Frobenius endomorphism of $\phi \otimes \mathbb{F}_\mathfrak{p}$. Then we have the inclusion of orders $A[\pi_\mathfrak{p}] \subset \mathcal{E}_\mathfrak{p} \subset \mathcal{O}_\mathfrak{p}$ in K. In a joint work with my advisor, Mihran Papikian, we showed that if ϕ is a Drinfeld Module without complex multiplication, then for arbitrary non-zero ideals $\mathfrak{n}, \mathfrak{m}$ of A, there are infinitely many $\mathfrak{p}$ such that $\mathfrak{n}$ divides the index $\chi(\mathcal{E}_\mathfrak{p}/A[\pi_\mathfrak{p}])$ and $\mathfrak{m}$ divides the index $\chi(\mathcal{O}_\mathfrak{p}/\mathcal{E}_\mathfrak{p})$. We also give an algorithm to compute $\mathcal{E}_\mathfrak{p}$ in the rank-2 case.

JEFFREY HATLEY (Union College)

Title: Comparing Selmer Groups of Positive Corank

Abstract: Given two elliptic curves which are congruent mod p, one can often use arithmetic information about one curve to deduce information about the other. In particular, the structures of their p-Selmer groups are often closely related, a fact which was first proved by Greenberg and Vatsal to establish some cases of the Iwasawa main conjecture. More recently, these sorts of results have been used to deduce parity relations between the analytic ranks of congruent elliptic curves.

Such results have always required the Selmer groups to satisfy a certain finiteness condition, but this condition is known to fail in many interesting cases. We will discuss a method of getting around this non-finiteness issue in the anticyclotomic setting. (This work is joint with Antonio Lei.)

CIHAN KARABULUT (William Paterson U.)

Title: Sums of Hermitian forms and the special values of Dedekind zeta function of an imaginary quadratic field.

Abstract: In one of his papers, D. Zagier studies a certain family of functions defined in a very simple way as sums of powers of quadratic polynomials with integer coefficients and discovers that these functions have several surprising properties and are related to many other subjects, including Diophantine approximation, special values of zeta functions and modular forms. Following Zagier, we study a similar family of functions defined using binary Hermitian forms and show that this family of functions also have similar properties. In particular, we obtain Cohen-Zagier type formulas for special values of Dedekind zeta function of an imaginary quadratic field.

KRZYSZTOF KLOSIN (CUNY)

Title: The Paramodular Conjecture for abelian surfaces with rational torsion.

Abstract: The Paramodular Conjecture can be viewed as an analogue of the Taniyama-Shimura Conjecture for abelian varieties of dimension 2 where the role of classical modular forms is assumed by Siegel modular forms. We will report on recent progress towards the conjecture for abelian surfaces which possess rational p-torsion. In such case this p-torsion gives rise to a reducible Galois representation of a particular shape and we will discuss properties of the universal deformation ring of such representations. We will explain how these results allow us in particular to prove new cases of the conjecture.This is joint work with T. Berger.

NATHAN JONES (UIC)

Title: Never-primitive points on elliptic curves over the rationals

Abstract: Artin's primitive root conjecture states that, given an integer c that is neither equal to -1 nor a perfect square, there are infinitely many primes p for which c is a primitive root modulo p. In the 1970s Lang and Trotter formulated an analogue for an elliptic curve E over the rational numbers: given a rational point Q on E of infinite order, they conjectured a precise density for the number of primes p for which the reduction of Q mod p generates the entire group of $\mathbb{Z}/p\mathbb{Z}$-rational points of E. In this talk we will discuss the following question: under what conditions on E and Q is the predicted density in Lang-Trotter's generalization of Artin's primitive root conjecture equal to zero? (In such a case we call Q a "never-primitive" point on E.) This represents joint work with F. Pappalardi and P. Stevenhagen.

JAMIE JUUL (Amherst College)

Title: Odoni's Conjecture

Abstract: Let K be a field and $f(x) \in K[x]$ be a polynomial of degree $d > 1$. We can consider extensions of K formed by adjoining preimages of any point $x_0 \in K$ under iterates of $f(x)$, $K(f^{-n}(x_0))$. In 1985, Odoni showed that the Galois group $\mathrm{Gal}(K(f^{-n}(x_0))/K)$ can be embedded in

$[S_d]^n$. In the same paper, Odoni conjectured for any $d > 1$ and any number field (or more generally, Hilbertian field) K, there is at least one $f(x) \in K[x]$ of degree d so that $\mathrm{Gal}(K(f^{-n}(0))/K) \cong [S_d]^n$ for all n. We discuss recent progress on this conjecture. This is joint work with Rob Benedetto.

ROBERT LEMKE OLIVER (Tufts)

Title: Selmer groups, Tate-Shafarevich groups, and ranks of abelian varieties in quadratic twist families

Abstract: We determine the average size of the ϕ-Selmer group in any quadratic twist family of abelian varieties having an isogeny ϕ of degree 3 over any number field. This has several applications towards the rank statistics in such families of quadratic twists. For example, it yields the first known quadratic twist families of absolutely simple abelian varieties over $\mathbb{Q}$, of dimension greater than one, for which the average rank is bounded; in fact, we obtain such twist families in arbitrarily large dimension. In the case that E/F is an elliptic curve admitting a 3-isogeny, we prove that the average rank of its quadratic twists is bounded; if F is totally real, we moreover show that a positive proportion of these twists have rank 0 and a positive proportion have 3-Selmer rank 1. We also obtain consequences for Tate-Shafarevich groups of quadratic twists of a given elliptic curve. This is joint work with Manjul Bhargava, Zev Klagsbrun, and Ari Shnidman.

WANLIN LI (Wisconsin)

Title: Effective Bounds on the Dimensions of Jacobians Covering Abelian Varieties (joint work with Juliette Bruce)

Abstract: We show that any polarized abelian variety over a finite field is covered by a Jacobian whose dimension is bounded by an explicit constant. We do this by first proving an effective version of Poonen's Bertini theorem over finite fields, which allows us to show the existence of smooth curves arising as hypersurface sections of bounded degree and genus. Additionally, we show that for simple abelian varieties a better bound is possible. As an application of these results we show that if E is an elliptic curve over a finite field then for any n there exist smooth curves of bounded genus whose Jacobians have a factor isogenous to E^n.

YUAN LIU (Wisconsin)

Title: The realizability problem with inertia conditions

Abstract: We consider the inverse Galois problem with described inertia behavior. For a finite group G, one of its subgroups I and a prime p, we ask whether or not G and I can be realized as the Galois group and inertia subgroup at p of an extension of $\mathbb{Q}$. We discuss the results when $|G|$ is odd and when $G = GL_2(\mathbb{F}_p)$. Finally, we provide an example arising from Grunwald-Wang's counterexample for which the local-global principle of our realizability problem fails.

CHRISTOPHER RASMUSSEN (Wesleyan)

Title: Cyclic Covers and Ihara's Question

Abstract: Let ℓ be a rational prime and k a number field. Given a superelliptic curve C/k of ℓ-power degree, we describe the field generated by the ℓ-power torsion of the Jacobian variety, in terms of the branch set and reduction type of C (and hence, in terms of data determined by a suitable

affine model). If the Jacobian possesses good reduction away from ℓ, and the branch set is rational over a pro-ℓ extension of $k(\mu_{\ell^\infty})$ unramified away from ℓ, then the ℓ-power torsion of the Jacobian is rational over the maximal such extension.

The result is a natural extension of earlier work by Anderson and Ihara, who demonstrated that a stricter condition on the branch locus guarantees the ℓ-power torsion of the Jacobian is rational over the fixed field of the kernel of the canonical pro-ℓ outer Galois representation attached to an open subset of $\mathbb{P}^1$.

DAVID ROHRLICH (Boston University)

Title: Arithmetic statistics of Artin representations

Abstract: An irreducible two-dimensional representation ρ of a finite group is said to be *dihedral* if its image is a dihedral group, and by analogy we call ρ *quaternionic* if its image is a generalized quaternion group. In the case of dihedral Artin representations, there are at least a few precise statements of a statistical nature. For example, let $\vartheta^{\mathrm{di}}(x)$ be the number of isomorphism classes of dihedral Artin representations of $\mathbb{Q}$ of conductor $\leqslant x$. Then as a corollary to Siegel's famous formulas for averages of class numbers of binary quadratic forms, one knows that

$$\vartheta^{\mathrm{di}}(x) \sim \frac{\pi}{36\zeta(3)^2} x^{3/2}. \tag{1}$$

Or if we write $\vartheta^{D_4}(x)$ for the number of such isomorphism classes with image equal to the dihedral group of order 8, then a very recent theorem of Altuğ, Shankar, Varma, and Wilson gives

$$\vartheta^{D_4}(x) \sim cx \log x \tag{2}$$

with a constant $c > 0$ (their result is actually considerably more precise than this). On the other hand, analogues of results like (1) and (2) for quaternionic Artin representations appear to be lacking. We shall comment on some of the difficulties.

KOJI SHIMIZU (Harvard)

Title: Constancy of generalized Hodge-Tate weights of a p-adic local system

Abstract: An étale p-adic local system on a rigid analytic variety can be regarded as a family of p-adic Galois representations of p-adic fields parametrized by the variety, and such objects have been studied in the relative p-adic Hodge theory. Sen attached to each p-adic Galois representation a multiset of numbers called generalized Hodge-Tate weights. In this talk, we show that the multiset of generalized Hodge-Tate weights of a p-adic local system is constant.

HANSON SMITH (U. of Colorado)

Title: Ramification in the Division Fields of Supersingular Elliptic Curves and Sporadic Points on Modular Curves

Abstract: Consider an elliptic curve E over a number field K. Write d for $[K : \mathbb{Q}]$ and $E(K)_{\mathrm{tors}}$ for the torsion subgroup of E over K. The problem of understanding $E(K)_{\mathrm{tors}}$ and the relation between d and $|E(K)_{\mathrm{tors}}|$ has been and continues to be an area of interest and innovation. We will briefly survey the history of this problem including recent developments towards improved uniform bounds on $|E(K)_{\mathrm{tors}}|$ and the classification of $E(K)_{\mathrm{tors}}$ when $[K : \mathbb{Q}] = 3$.

With this context in mind, we will outline our results. Namely, let p^n be a power of an odd prime and define L to be the minimal extension of K such that $E(L)$ has a point of exact order p^n. Suppose E has supersingular reduction at the primes of K lying above p. We show the ramification index of p in L is strictly greater than $\varphi(p^n)$. If p is unramified in K, we are able to strengthen our argument to prove that p has ramification index at least $p^{2n} - p^{2n-2}$ in L. We apply this strengthened bound to show that sporadic points on the modular curve $X_1(p^n)$ cannot correspond to elliptic curves that are supersingular at primes lying above p in a number field in which p is unramified. Our methods generalize to $X_1(N)$ if an elliptic curve has supersingular reduction at sufficiently many primes lying over the primes dividing N.

ANDREW SUTHERLAND (MIT)

Title: Computation in supersingular isogeny graphs

Abstract: Isogeny graphs of supersingular elliptic curves were one of the first concrete examples of families of Ramanujan graphs; these are optimal expanders with many practical and theoretical applications. There has been a recent surge of interest in supersingular isogeny graphs motivated by applications to post-quantum cryptography (see Christelle VincentвЂ™s talk for a lightning-fast survey). This raises a number of interesting computational and theoretical questions. After reviewing the background theory and algorithmic building blocks used to construct and navigate supersingular isogeny graphs, I will discuss some open problems related to their use in cryptographic applications, from both a constructive and destructive perspective.

YUNQING TANG (Princeton)

Title: Cycles in the de Rham cohomology of abelian varieties over number fields

Abstract: In his 1982 paper, Ogus defined a class of cycles in the de Rham cohomology of smooth proper varieties over number fields. In the case of abelian varieties, this class includes all the Hodge cycles by the work of Deligne, Ogus and Blasius. Ogus predicted that all such cycles are Hodge. In this talk, I will first introduce Ogus' conjecture as a crystalline analogue of Mumford–Tate conjecture and explain how a theorem of Bost on algebraic foliation is related. After this, I will discuss the proof of Ogus' conjecture for some families of abelian varieties.

DINESH THAKUR (University of Rochester)

Title: Special values and related structures in function fields

Abstract: We will survey various recent developments in understanding the nature of special values of zeta, multizeta and L-functions by related abelian an non-abelian structures in function fields such as Drinfeld modules, Anderson t-motives, iterated integrals, Galois representations and algebraic groups.

BIANCA THOMPSON (Harvey Mudd College)

Title: Uniform bounds for pre-periodic points in families of twists

Abstract: Let ϕ be a morphism of $\mathbb{P}^N$ defined over a number field K. We prove that there is a bound B depending only on ϕ such that every twist of ϕ has no more than B K-rational preperiodic

points. (This result is analogous to a result of Silverman for abelian varieties.) For two specific families of quadratic rational maps over $\mathbb{Q}$, we find the bound B explicitly.

WEI-LUN TSAI (Texas A & M)

Title: Analytic formulas for Stark units in quadratic extensions of totally real number fields

Abstract: In this talk, we will explain how Stark units in certain quadratic extensions of totally real number fields can be evaluated explicitly in terms of values of the Barnes multiple Gamma function at algebraic arguments. Also, we will show some explicit examples related to our main result. This is joint work with Adrian Barquero-Sanchez and Riad Masri.

ILA VARMA (Columbia)

Title: The average size of 2-torsion elements in ray class groups of cubic fields

Abstract: In 2005, Bhargava computed the average size of the 2-torsion subgroup in the class groups of cubic fields ordered by discriminant by proving asymptotics on nowhere overramified quartic fields. Class field theory gives a relationship between the number of 2-torsion ideal classes of cubic fields and the number of nowhere overramified quartic fields. I will describe a generalization of this correspondence to 2-torsion elements of the ray class groups of cubic fields, which can enumerated using certain pairs of quartic and quadratic fields satisfying explicit ramification conditions. I will illustrate how one can apply Bhargava's asymptotics on the number of quartic fields of bounded discriminant to obtain the mean number of 2-torsion elements in ray class groups with fixed conductor of cubic fields ordered by discriminant.

CHRISTELLE VINCENT (UVM)

Title: A lightning-fast survey of post-quantum cryptography

Abstract: In this talk we will begin by giving a short introduction to Shor's algorithm, and continue by explaining how to makes some math problems that are "hard" to solve on classical computers "easy" to solve on quantum computers. We then present the main families of algorithms that were presented to NIST in the first round of its post-quantum cryptography challenge, focusing on the "hard" problems on which the cryptosystems rely.

KHOI VO (Cal State Long Beach)

Title: On Densities of Subclasses of the Solitary Numbers

Abstract: The question of the density of the set of solitary numbers has been left open for a long time. It has been conjectured that its value is zero. Recently, in "New families of solitary numbers" by Paul Loomis, the author has brought up new sub-classes of solitary numbers. In this presentation, we will proceed in proving the density of these sub-classes of solitary numbers are indeed all zero. This result helped us one step further in the way of proving the conjecture.

PRESTON WAKE (UCLA)

Title: Mazur's Eisenstein ideal, Part 2: Squarefree level

Abstract: This talk concerns joint work with Carl Wang-Erickson, and follows on his talk on Friday. In his influential paper "Modular curves and the Eisenstein ideal", Mazur studied congruences modulo p between cusp forms and the Eisenstein series of weight 2 and prime level N. In particular, he defined the Eisenstein ideal in the relevant Hecke algebra, and showed that it is locally principal. We'll discuss the analogous situation for certain squarefree levels N, and show that, while the Eisenstein ideal may not be locally principal, we can count the minimal number of generators and explain the arithmetic significance of this number.

ERIK WALLACE (UConn)

Title: Bounds for the MordellвЃ“Weil rank of certain families of jacobians of hyperelliptic curves defined over $\mathbb{Q}$

Abstract: In a recent article written in collaboration with Álvaro Lozano-Robledo and Harris Daniels we extend work of Lehmer, Shanks, and Washington on cyclic extensions, and elliptic curves associated to the simplest cubic fields. In particular, we give families of examples of hyperelliptic curves $C : y^2 = f(x)$ defined over $\mathbb{Q}$, with $f(x)$ of degree p, where p is a Sophie Germain prime, such that the rank of the Mordell–Weil group of the jacobian $J/\mathbb{Q}$ of C is bounded by the genus of C and the 2-rank of the class group of the (cyclic) field defined by $f(x)$, and exhibit examples where this bound is sharp.

CARL WANG-ERICKSON (Imperial College)

Title: Mazur's Eisenstein ideal, Part 1: Prime level

Abstract: This talk concerns joint work with Preston Wake, and will be followed by his talk on Sunday. In his landmark 1976 paper *Modular curves and the Eisenstein ideal*, Mazur studied congruences modulo p between cusp forms and an Eisenstein series of weight 2 and prime level N. He proved a great deal about these congruences, and also posed some questions: how many cusp forms of a given level are congruent to the Eisenstein series? How big is the extension generated by their coefficients? We give an answer to these questions in terms of cup products (and Massey products) in Galois cohomology. The meaning of Mazur's question will be illustrated through explicit examples.

LORI WATSON (UGA)

Title: 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.

BIN ZHAO (UConn)

Title: Slopes of modular forms and the Ghost conjecture

Abstract: In this talk, I will report on an on-going joint work with Ruochuan Liu and Liang Xiao, on the study of the p-adic slopes of modular forms. Bergdall and Pollack constructed an explicit

power series, called the ghost series, and they conjectured that under certain regularity condition, the Newton polygon of the ghost series coincides with the Newton polygon of the characteristic power series of the U_p operator on the p-adic overconvergent modular forms. In this talk, I will give another formulation of this conjecture. If time allows, I will talk about some consequences of this conjecture.