Number **T**heory **S**eries in **L**os **A**ngeles

SCHEDULE OF ACTIVITIES

Saturday, October 26, 2019

9:00-9:30 Hall outside Fowler 302: Coffee and other refreshments

9:30-9:50 Fowler 202: **Hanson Smith** (University of Colorado Boulder), *The Monogeneity of Kummer Extensions and Radical Extensions*
Fowler 302: **Harry Smit** (Utrecht University), *L-functions and isogenies of abelian varieties*

10:00 - 10:20 Fowler 202: **Joe Kramer-Miller** (University of California - Irvine), *p-adic estimates for exponential sums on curves*
Fowler 302: **Liubomir Chiriac** (Portland State University), *Summing Fourier coefficients over polynomials values*

10:30-10:50 Fowler 202: **Alia Hamieh** (University of Northern British Columbia), *Additive Twists of Fourier Coefficients of Hilbert Modular Forms*
Fowler 302: **Yong Suk Moon** (University of Arizona), *Barsotti-Tate deformation ring in the relative case*

11:00 - 11:20 Fowler 202: **Sarah Fujimori, Ethan Yang, and Jonathan Sy** (Euler Math Circle), *S-universal quadratic forms*
Fowler 302: **Biao Wang** (SUNY at Buffalo), *An analogue of a formula for Chebotarev Densities*

11:20 - 11:40 Break

11:40 - 12:40 Fowler 202: **Beth Malmskog** (Colorado College), *Locally Recoverable Codes with Many Recovery Sets from Curves over Finite Fields*

12:40 - 2:30 Lunch

The organizer thanks the National Science Foundation, the National Security Agency, and Occidental College for their support.

2:30 - 3:20 Fowler 202: **Soumya Sankar** (University of Wisconsin - Madison), *Proportion of ordinary curves in some families*

3:30 - 3:50 Fowler 202: **Sarah Arpin** (University of Colorado - Boulder), *Adventures in Supersingularland: An Exploration of Supersingular Elliptic Curve Isogeny Graphs*
Fowler 302: **Vlad Matei** (University of California - Irvine), *Average size of the automorphism group of smooth projective hypersurfaces*

4:00 - 4:20 Fowler 202: **Nathan Green** (University of California - San Diego), *A Galois Equivariant Class Number Formula for Drinfeld L-functions*
Fowler 302: **Evangelos Nastas** (Syracuse University), Cancelled ~~*On a generalization of the Ramanujan-Nagell equation*~~

4:45 - 5:45 Fowler 302: **Panel Discussion: Jesse Elliot (CSU-CI), Edray Goins (Pomona College), and Nathan Kaplan (UC-Irvine)**, *Job application process*

5:45 DINNER (No organized dinner.)

Sunday, October 27, 2019

9:00-9:30 Hall outside Fowler 302: Coffee and other refreshments

9:30-9:50 Fowler 202: **Maksym Radziwill** (Caltech) *The distribution of lattice points on the sphere*
Fowler 302: **Siddesh Wagh** (University of Wisconsin - Madison), *Maass space for lifts to GL(2) over a division quaternion algebra*

10:00 - 10:20 Fowler 202: **Andrei Shubin** (Caltech) *On the variance of number of lattice points on the surface of the sphere*
Fowler 302: **Huixi Li** (University of Nevada - Reno), *On a Variant of the Elliott-Halberstam Conjecture and the Goldbach Conjecture*

10:30-10:50 Fowler 202: **Steven Jin** (University of Maryland - College Park), *Linnik's Large Sieve and the L^1 Norm of Exponential Sums*
Fowler 302: **Kelly Isham** (University of California - Irvine), *Power sequences in* $(\mathbb{Z}/m\mathbb{Z}, \cdot)$

11:00 - 11:20 Fowler 202: **Liyang Yang** (Caltech), *Fourier Coefficients of Symmetric Power Representations with Applications*
Fowler 302: **Jesse Elliot** (California State University - Channel Islands), *Asymptotic expansions of the prime counting function*

11:20 - 11:40 Break

11:40 - 12:40 Fowler 202: **Eric Urban** (Columbia University), *Bernouilli numbers, Eisenstein series and cyclotomic units*

12:40 END OF CONFERENCE

Abstracts

SARAH ARPIN, University of Colorado, *Adventures in Supersingularland: An Exploration of Supersingular Elliptic Curve Isogeny Graphs*
In this work, we study isogeny graphs of supersingular elliptic curves. Supersingular isogeny graphs were introduced as a hard problem into cryptography by Charles, Goren, and Lauter for the construction of cryptographic hash functions (CGL06). These are large expander graphs, and the hard problem is to find an efficient algorithm for routing, or path-finding, between two vertices of the graph. First, we consider two related graphs that help us understand the structure: the 'spine' $\mathcal{S}$, which is the subgraph of $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ given by the j-invariants in $\mathbb{F}_p$, and the graph $\mathcal{G}_\ell(\mathbb{F}_p)$, in which both curves and isogenies must be defined over $\mathbb{F}_p$. We show how to pass from the latter to the former. Next, we study the involution on $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ that is given by the Frobenius of $\mathbb{F}_p$ and give heuristics on how often shortest paths between two conjugate j-invariants are preserved by this involution (mirror paths). This is joint work with Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Travis Scholl, Jana Sotkov arXiv 1909.07779

LIUBOMIR CHIRIAC, Portland State University, *Summing Fourier coefficients over polynomials values*

This talk is concerned with mean values of Fourier coefficients of modular forms over polynomials. While there are many important results in this direction for polynomials of degree at most two, rather little is known beyond that. Here we will present an approach to obtain some bounds for sums involving polynomials of arbitrary degree.

JESSE ELLIOT (California State University - Channel Islands), *Asymptotic expansions of the prime counting function*

We provide several asymptotic expansions of the prime counting function $\pi(x)$. We define an *asymptotic continued fraction expansion* of a complex-valued function of a real or complex variable to be a possibly divergent continued fraction whose approximants provide an asymptotic expansion of the given function. We explain why, for each positive integer n, two well known continued fraction expansions of the exponential integral function $E_n(z)$, in the regions where they diverge, correspondingly yield two asymptotic continued fraction expansions of $\pi(x)/x$. As a corollary we determine all of the best rational function approximations of the function $\pi(e^x)/e^x$.

SARAH FUJIMORI, JONATHAN SY, ETHAN YANG (Euler Math Circle), *S-universal quadratic forms*

A famous theorem of Bhargava and Hanke is that if a positive definite quadratic form with integer coefficients represents all positive integers in a critical list of 29 integers, the largest of which is 290, it represents all positive integers. Following this, DeBenedetto and Rouse proved an analogous theorem for the set of integers coprime to 3. In this talk, we generalize their result to finding a critical list for quadratic forms representing all positive integers coprime to p for each prime p. For each prime p, we also find the minimal nontrivial multiple of p that is represented by every quadratic form which is universal for integers coprime to p.

NATHAN GREEN, University of California - San Diego, *A Galois Equivariant Class Number Formula for Drinfeld L-functions*

Classically, the class number formula relates the residue of the Dedekind zeta function at 1 with the class number and the regulator of a given number field. Recently, Taelman gave an analogue of the class number formula for function fields using the L-function attached to a Drinfeld module. In this setting, however, the class number is replaced by a generator of the Fitting ideal of the "class module" coming from Galois cohomology and the regulator is replaced by the index of two naturally occurring lattices coming from the Drinfeld module structure. In our work, we generalize Taelman's class number formula to the Galois equivariant setting and give a volume interpretation of L-value which can be viewed as a Tamagawa number formula for Drinfeld L-values. Joint work with Joseph Ferrara, Zach Higgins and Cristian Popescu.

ALIA HAMIEH, University of Northern British Columbia, *Additive Twists of Fourier Coefficients of Hilbert Modular Forms*

In this talk, we discuss sums of additively twisted Fourier coefficients of Hilbert modular forms. We obtain upper bounds for such sums that are uniform in the additive character and the weight of the form itself. This is joint work in progress with Naomi Tanabe.

KELLY ISHAM, (University of California - Irvine), *Power sequences in* $(\mathbb{Z}/m\mathbb{Z}, \cdot)$

For each a in $\mathbb{Z}/m\mathbb{Z}$, consider the power sequence $a, a^2, a^3, \cdots$. Eventually, $a^j = a^k$ in $\mathbb{Z}/m\mathbb{Z}$ for some $j \leq k$. The set $\{a^j, a^{j+1}, \ldots, a^{k-1}\}$ is called the cycle of a. If $i \neq 1$, we call $a, a^2, \ldots, a^{j-1}$ the tail of a. Further, by combining any sequences that share elements, we can form components that partition $\mathbb{Z}/m\mathbb{Z}$. Previous work has determined a partial classification of the structure of these power sequences by determining the cycle structure both algebraically and number-theoretically. We complete the classification by proving results about the structure of the tails. Lastly, we define a lattice between the components and provide a homomorphism between comparable components.

STEVEN JIN, University of Maryland - College Park, *Linnik's Large Sieve and the* L^1 *Norm of Exponential Sums*

(Joint work with Emily Eckels, Andrew Ledoan, and Brian Tobin) The large sieve of Linnik is used to investigate the behavior of the L^1 norm of various classes of exponential sums. In particular, we produce a refinement of Balog and Ruzsa's lower bound for the L^1 norm of the exponential sum with Mobius μ function coefficients, and we also present an elementary proof of Vaughan's lower bound for the case of von Mangoldt Λ function coefficients.

JOE KRAMER-MILLER, University of California - Irvine, *p-adic estimates for exponential sums on curves*

Let X be a smooth proper curve over a finite field $\mathbb{F}_q$ of characteristic $p \geq 5$ and let $V \subset X$ be an affine curve. For a regular function $\overline{f}$ on V, we may form the L-function $L(\overline{f}, V, s)$ associated to the exponential sums of $\overline{f}$. We prove a lower bound on the Newton polygon of $L(\overline{f}, V, s)$, depending on local monodromy invariants. This lower bound is precisely the irregular Hodge filtration associated to a twisted de Rham complex. In particular, we confirm Deligne's hope that the irregular Hodge filtration forces bounds on p-adic valuations of Frobenius eigenvalues.

HUIXI LI, University of Nevada - Reno, *On a Variant of the Elliott-Halberstam Conjecture and the Goldbach Conjecture*

In this presentation we show that the binary Goldbach conjecture for sufficiently large even integers would follow under the assumptions of both the Elliott-Halberstam conjecture and a variant of the Elliott-Halberstam conjecture twisted by the Möbius function, provided that the sum of their level of distributions exceeds 1. This continues the work of Pan. An analogous result for the twin prime conjecture is obtained by Ram Murty and Vatwani.

BETH MALMSKOG, Colorado College, *Locally Recoverable Codes with Many Recovery Sets from Curves over Finite Fields*

Error correcting codes are systems for incorporating redundancy into stored or transmitted data, so that errors can be identified and even corrected. A good error correcting code is efficient and can correct many errors relative to its efficiency. These codes are ubiquitous in the digital age, and many excellent codes arise from algebraic constructions. The increasing importance of cloud computing and storage has created a need for codes that protect against server failure in large computing facilities. One way of approaching this problem is to ask for local recovery. An error correcting code is said to be locally recoverable if any symbol in a code word can be recovered by accessing a subset of the other symbols. This subset is known as the helper or recovery set for the given symbol. It may be desirable to have many disjoint recovery sets for each symbol, in case of multiple server failures or to provide many options for recovery. This talk describes how geometry and number theory can be powerful tools for creating such codes, including a construction using fiber products of curves to generate arbitrarily many recovery sets.

VLAD MATEI, University of California - Irvine, *Average size of the automorphism group of smooth projective hypersurfaces*

We show that the average size of the automorphism group over $\mathbb{F}_q$ of a smooth degree d hypersurface in $\mathbb{P}^n_{\mathbb{F}_q}$ is equal to 1 except for the tuples $(n, d) = (2, 3), (3, 4)$. We also discuss some consequences of this result for the moduli space of smooth degree d hypersurfaces in $\mathbb{P}^n$.

EVANGELOS NASTAS, Syracuse University, Cancelled
~~*On a generalization of the Ramanujan-Nagell equation*~~

~~The main reason for this project is to shed light on the following equation $x^2 + p = 2^n$, where $p = 2^? - 1$, and $k \in \mathbb{N}^+$. For $k = 3$ the aforementioned equation takes the form $x^2 + 7 = 2^n$, which has already been solved by Nagell proving Ramanujan's conjecture that its only solutions are: $x = \pm1, \pm3, \pm5, \pm12, \pm181$, $n = 3, 4, 5, 7, 15$. Now by using Nagell's proof and by generalizing it we are looking for the solutions of $x^2 + p = 2^n$.~~

MAKSYM RADZIWILL, Caltech, *The distribution of lattice points on the sphere*

In 1968 Linnik showed using his "ergodic method" that lattice points on the surface of a three dimensional sphere equidistribute, strengthening previous work of Gauss. In 2017 Bourgain Rudnick and Sarnak posited that these lattice points behave like points thrown at random. To quantify this they conjectured (among other things) an asymptotic for the variance of the number of lattice points in a thin randomly rotated cap or annuli lying on the surface of the sphere. I will discuss joint work with Peter Humphries in which we settle this conjecture of Bourgain Rudnick Sarnak for thin annuli with large outer radius. I will also explain the challenges that prevent us from establishing this conjecture for thin caps.

SOUMYA SANKAR, University of Wisconsin - Madison, *Proportion of ordinary curves in some families*

We say that an abelian variety A over a field k of characteristic p is ordinary if $A[p](\bar{k})$ is the largest possible. A curve C is called ordinary if its Jacobian is ordinary. One can ask: what is the probability that a curve over a finite field is ordinary? The general answer to this question is not known. We answer it for some special families of curves, namely Artin-Schreier and superelliptic curves. This work is motivated by conjectures of Cais, Ellenberg and Zureick-Brown that predict asymptotics for Dieudonne modules of abelian varieties. In my talk, I will talk about these conjectures, why they are hard to prove and why these special families are more tractable than others.

ANDREI SHUBIN, Caltech, *On the variance of number of lattice points on the surface of the sphere*
?
In this talk we will describe how one can get the upper bound of the? conjectured order of the variance of number of points inside a small cup on the surface of 3-sphere? assuming GRH.

HARRY SMIT, Utrecht University, *L-functions and isogenies of abelian varieties*

Faltings's isogeny theorem states that two abelian varieties over a number field are isogenous precisely when the characteristic polynomials of all reductions of the abelian varieties are equal. This implies that two abelian varieties defined over the rational numbers with the same L-function are necessarily isogenous, but this is false over a general number field. One can extract more information from the L-function by "twisting"; a twist of an L-function is the L-function of the tensor of the underlying representation with a character. We show that abelian varieties over a general number field are characterized by their L-function twisted by Dirichlet characters of the underlying number field.

HANSON SMITH, University of Colorado Boulder, *The Monogeneity of Kummer Extensions and Radical Extensions*

This talk will outline recent results establishing necessary and sufficient conditions for a radical extension of an arbitrary number field L to have a relative power integral basis generated by the radical. That is, we give necessary and sufficient conditions for $\mathcal{O}_{L(\sqrt[n]{\alpha})}$ to be $\mathcal{O}_L[\sqrt[n]{\alpha}]$. In the process we will meet a generalization of the Wieferich condition initially used to study Fermat's Last Theorem. Our main tool will be a seemingly new criterion relating ramification and relative monogeneity. The work outlined in this talk can be found in arXiv 1909.07184.

YONG SUK MOON (University of Arizona), *Barsotti-Tate deformation ring in the relative case*

Let K be a finite extension of $\mathbb{Q}_p$, and denote by G_K its absolute Galois group. Fix an absolutely irreducible residual representation ρ of G_K. By the work of Kisin and Liu, for positive integer r, the locus of crystalline representations of G_K with Hodge-Tate weights in $[0, r]$ deforming ρ cuts out a closed subspace of the universal deformation space of ρ. We will discuss some generalization of this result to geometric families of Galois representations in the case $r = 1$.

ERIC URBAN, Columbia University, *Bernouilli numbers, Eisenstein series and cyclotomic units*

I will recall what are the objects of the title and explain how one can combine them in a new way to explain a deep Theorem of Mazur and Wiles (proving a conjecture of Iwasawa) that gives a formula for the cardinality of the p-part of the class groups of cyclotomic fields in terms of Bernouilli numbers.

SIDDESH WAGH, University of Wisconsin - Madison, *Maass space for lifts to GL(2) over a division quaternion algebra*

Muto, Narita and Pitale construct counterexamples to the Generalized Ramanujan Conjecture for GL2(B) over the division quaternion algebra B with discriminant two via a lift from SL2. In this talk I will talk about identifying the image of this lift via a combination of classical methods as well as Jacquet-Langlands correspondence. I will also talk about my current work about finding the Supremum norm for this lift via methods of Theta Lift.

BIAO WANG, SUNY at Buffalo, *An analogue of a formula for Chebotarev Densities*

In this talk, we will introduce an analogue of Dawsey's formula on Chebotarev densities for finite Galois extensions of $\mathbb{Q}$ with respect to the Riemann zeta function $\zeta(ms), m \geq 2$. Her formula may be viewed as the limit version of our formula as $m \to \infty$. In the proof, we mainly use the duality of a prime factor which is close to the largest prime factor of an integer.

LIYANG YANG, Caltech, *Fourier Coefficients of Symmetric Power Representations with Applications*

In this talk, we give nontrivial upper bounds for average of absolute values of Fourier coefficients associated to $\mathrm{Sym}^k \pi$, where π is a non-dihedral cuspidal representation of $\mathrm{GL}(2, \mathbb{A}_{\mathbb{Q}})$ and $1 \leq k \leq 3$. These bounds generalize known results in holomorphic case to Maass forms, without assuming Ramanujan-Petersson conjecture. Also, some applications will be discussed.
