Saturday, September 15, 2012

9:00 - 9:30 Coffee and other refreshments outside Manchester 016

9:30 - 10:20 **Noam Elkies** (Harvard University), *How many points can a curve have?*

10:30 - 10:50 **Larry Rolen** (Emory University), *Counting number fields by discriminant and point counting on varieties.*

10:50 - 11:05 Coffee break (thank the WFU math department for the coffee)

11:05 - 11:25 **Joshua Harrington** (University of South Carolina), *The factorization of* $f(x)x^n + g(x)$ *when* $\deg f \leq 2$.

11:35 - 11:55 **Jon Grantham** (IDA/CCS), *Repeatedly appending digits and only finding composites.*

11:55 - 1:20 Lunch

1:20 - 2:10 **Sol Friedberg** (Boston College), *Higher theta functions.*

2:20 - 2:40 **Dan Yasaki** (University of North Carolina Greensboro), *Some explicit* $\delta = 1, 2$ *computations.*

2:50 - 3:10 **Jesse Thorner** (Wake Forest University), *Explicit bounds on densities pertaining to Lehmer-type questions.*

3:10 - 3:25 Coffee break (thank the WFU math department for the coffee)

3:25 - 3:45 **Rowland Carlson** (Wake Forest University), *Infinite families of infinite families of congruences for k-regular partitions.*

3:55 - 4:15 **Marie Jameson** (Emory University), *A problem of Zagier on quadratic polynomials and continued fractions.*

4:25 - 4:45 **Marvin Jones** (University of South Carolina), *Solutions of the cubic Fermat equation in quadratic fields.*

4:55 - 5:15 **Kate Thompson** (University of Georgia), *Geometry of numbers and representations by quadratic forms, part I.*

5:25 - 5:45 **Jacob Hicks** (University of Georgia), *Geometry of numbers and representations by quadratic forms, part II.*

Sunday, September 16, 2012

8:15 - 8:30	Coffee and other refreshments outside Manchester 016
8:30 - 9:20	**Zev Klagsbrun** (University of Wisconsin-Madison), *New results concerning the distribution of 2-Selmer ranks within the quadratic twist family of an elliptic curve.*
9:30 - 9:50	**David Zureick-Brown** (Emory University), *The Cohen-Lenstra conjectures and random Dieudonné modules.*
10:00 - 10:20	**Cassie Williams** (James Madison University), *Conjugacy classes in GSp_4 and an application to the enumeration of abelian surfaces.*
10:20 - 10:35	Coffee break (thank the WFU math department for the coffee)
10:35 - 10:55	**Peter Fletcher** (Virginia Tech), *Properties of safe primes.*
11:05 - 11:25	**Nicolas Smoot** (Armstrong Atlantic State University), *The distribution of consecutive octic residues and possible generalization.*
11:35 - 11:55	**Thomas Wright** (Wofford College), *Carmichael numbers in arithmetic progressions.*
11:55 - 1:20	Lunch
1:20 - 2:10	**Ian Petrow**, (Stanford University), *Moments of L-functions and their derivatives.*
2:20 - 2:40	**Caroline Turnage-Butterbaugh**, (University of Mississippi), *Large gaps between zeros of Dedekind zeta-functions of quadratic number fields.*
2:50 - 3:10	**Robert Lemke Oliver**, (Emory University), *Multiplicative functions dictated by Artin symbols.*

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 Mathematics Department for their support.

Abstracts

Noam Elkies, Harvard University, *How many points can a curve have?*

Diophantine equations, one of the oldest topics of mathematical research, remain the object of intense and fruitful study. A rational solution to a system of algebraic equations is tantamount to a point with rational coordinates (briefly, a "rational point") on the corresponding algebraic variety V. Already for V of dimension 1 (an "algebraic curve"), many natural theoretical and computational questions remain open, especially when the genus g of V exceeds 1. (The genus is a natural measure of the complexity of V; for example, if P is a nonconstant polynomial without repeated roots then the equation $y^2 = P(x)$ gives a curve of genus g iff P has degree $2g + 1$ or $2g + 2$.) Faltings famously proved that if $g > 1$ then the set of rational points is finite (Mordell's conjecture), but left open the question of how its size can vary with V, even for fixed g. Already for $g = 2$ there are curves with literally hundreds of points; is the number unbounded?

We briefly review the structure of rational points on curves of genus 0 and 1, and then report on relevant work since Faltings on points on curves of given genus $g > 1$.

Larry Rolen, Emory University, *Counting number fields by discriminant and point counting on varieties*

In this talk, we will study the classical problem of counting number fields by discriminant. We relate the problem to one of counting points on varieties. We will discuss progress towards counting D_5 extensions and show a new bound for the number of A_n number fields which beats the previous known bounds for $6 \leq n \leq 84393$.

Joshua Harrington, University of South Carolina, *The factorization of $f(x)x^n + g(x)$ when* $\deg f \leq 2$

In this talk we investigate the factorization of the polynomials $f(x)x^n + g(x) \in \mathbb{Z}[x]$ in the special case where $f(x)$ is a monic quadratic polynomial with negative discriminant. We also mention similar results in the case that $f(x)$ is monic and linear.

Jon Grantham, IDA/CCS, *Repeatedly appending digits and only finding composites*

In this talk, I discuss the question of whether you can append the same digit repeatedly to a starting number and be guaranteed to produce composites.

Sol Friedberg, Boston College, *Higher theta functions*

The classical Jacobi theta function transforms with respect to a multiplier system that includes a quadratic Kronecker symbol $\left(\frac{c}{d}\right)$. Are there theta functions transforming with respect to n-th order residue symbols $\left(\frac{c}{d}\right)_n$ when $n > 2$? Yes, but they are still in many ways mysterious. In this talk I will explain how automorphic forms on covers of $GL(2)$ lead to such functions, and

describe a new conjecture (joint with Gautam Chinta and Jeff Hoffstein) that gives information about the Fourier coefficients of such a higher theta function in one new case. Much still remains to be done!

Dan Yasaki, University of North Carolina Greensboro, *Some explicit $\delta = 1$, 2 computations*

In this talk, I give a preliminary report on some recent computations (joint with Paul Gunnells) of torsion in the integral cohomology for $\Gamma_0(N) \subset GL_2(O_F)$, where F is the complex cubic field of discriminant -23 ($\delta = 1$) and where F is the cyclotomic field of fifth roots of unity ($\delta = 2$). I begin with a discussion Koecher's work, which generalizes work of Voronoi to give a tessellation of the symmetric space associated to these groups. These tessellations give a cell complex which can be used to investigate the torsion. I present the results of these computations, providing computational evidence in support of conjectures of Bergeron-Venkatesh about the growth of torsion with covolume.

Jesse Thorner, Wake Forest University, *Explicit bounds on densities pertaining to Lehmer-type questions*

Given a newform f with squarefree level and trivial character, we will present tools that will help provide explicit lower bounds for the density of Fourier coefficients of f which do not equal zero. In particular, we will prove that

$$\#\{x \leq p \leq 2x : a(p) = 0\} \leq 0.42x^{3/4},$$

for sufficiently large x. This assumes that the symmetric-power L-functions of f are L-functions for which the Generalized Riemann Hypothesis is true.

Rowland Carlson, Wake Forest University, *Infinite families of infinite families of congruences for k-regular partitions*

Let $k \in \{10, 15, 20\}$ and let $b_k(n)$ denote the number of k-regular partitions of n. We prove for half of all primes p and any $t \geq 1$ that there exist $p - 1$ arithmetic progressions modulo p^{2t} such that $b_k(n)$ is a multiple of 5 for each n in one of these progressions.

Marie Jameson, Emory University, *A problem of Zagier on quadratic polynomials and continued fractions*

For any non-square $1 < D \equiv 0, 1 \pmod 4$, Zagier defined

$$A_D(x) := \sum_{\substack{\text{disc}(Q)=D \\ Q(\infty)<0<Q(x)}} Q(x)$$

and proved that $A_D(x)$ is a constant function. For rational x, it turns out that this sum is finite. Here we address the infinitude of the number of quadratic polynomials for nonrational x, and more importantly address some problems posed by Zagier related to characterizing the polynomials which arise in terms of the continued fraction expansion of x. In addition, we study

the divisibility of the constant functions $A_D(x)$ as D varies, by using the Cohen-Eisenstein series and various Hecke-type operators.

Marvin Jones, University of South Carolina, *Solutions of the cubic Fermat equation in quadratic fields*

We will examine when there are nontrivial solutions to the equation $x^3 + y^3 = z^3$ in $\mathbb{Q}(\sqrt{d})$ for a squarefree integer d. In this variation of Fermat's Last Theorem, it is possible for nontrivial solutions to exist in $\mathbb{Q}(\sqrt{d})$ for some choices of d, but not for all. Our argument assumes the Birch and Swinnerton-Dyer conjecture and follows a similar argument as Tunnell's solution to the congruent number problem.

Kate Thompson, University of Georgia, *Geometry of numbers and representations by quadratic forms, part I*

The question of what values are represented by a positive-definite integral quadratic form is a problem with centuries of history and interest. A particular measure of the complexity of this question comes in the class number of the quadratic form. Building off work of Kaplansky and Voight, who classified (modulo GRH) the complete list of discriminants for class number 1 positive-definite integral binary quadratic forms, a recent VIGRE group at UGA successfully used Geometry of Numbers (GoN) techniques to show precisely which primes are represented by these 2779 $SL_2(\mathbb{Z})$-equivalence classes of forms. This work was completed by P.L.Clark, J.Hicks, H.Parshall, and K.Thompson.

Jacob Hicks, University of Georgia, *Geometry of numbers and representations by quadratic forms, part II*

The universality of the sum of four squares over the integers is a classical result of Geometry of Numbers. The 290-theorem of Bhargava and Hanke gives a necessary and sufficient criterion for (positive) universality and also determines all 6436 universal quaternary forms. The proof of the 290-theorem relies heavily on ternary form theory and escalators. Using only generalizations of the techniques for the classical four squares theorem and of the computer programs relevant to the previous talk, the universality of approximately 100 (and counting!) of these forms can be shown. The basics ideas have the potential to be applied to other S-integer rings in a straightforward manner. This work was completed by P.L.Clark, J.Hicks, K.Thompson, and N.Walters.

Zev Klagsbrun, University of Wisconsin-Madison, *New results concerning the distribution of 2-Selmer ranks within the quadratic twist family of an elliptic curve*

Given an elliptic curve E defined over a number field K, we can ask what proportion of quadratic twists of E have 2-Selmer rank r for any non-negative integer r. I will present new results obtained by Mazur, Rubin, and myself about this distribution, including some surprising results relating to parity that have implications regarding Goldfeld's conjecture over number fields as well as some of my own results in the special case when $E(\mathbb{Q})[2] = \mathbb{Z}/2$ that conflict

with the conjectured distribution arising from the Delaunay heuristics on the Tate-Shafaravich group.

David Zureick-Brown, Emory University, *The Cohen-Lenstra conjectures and random Dieudonné modules*

Knowledge of the distribution of class groups is elusive - it is not even known if there are infinitely many number fields with trivial class group. Cohen and Lenstra's heuristic models the p-part of a class group by a random finite abelian p-group, correctly predicting many strange experimental observations.

While proof of the Cohen-Lenstra conjectures remains inaccessible, the function field analogue – distribution of class groups of quadratic extensions of $\mathbb{F}_p(t)$ – is more tractable. Friedman and Washington modeled the l-power part (with l not p) of such class groups as random matrices and derived heuristics which agree with experiment. Achter later refined these heuristics, and many cases have been proved (Achter, Ellenberg and Venkatesh).

When $l = p$, the l-power torsion of abelian varieties, and thus the random matrix model, goes haywire. I will explain the correct linear algebraic model – Dieudoneé modules. Our main result is an analogue of the Cohen-Lenstra/Friedman-Washington heuristics – a theorem about the distributions of class numbers of Dieudoneé modules (and other invariants particular to $l = p$). Finally, I'll present experimental evidence supporting our heuristics.

Cassie Williams, James Madison University, *Conjugacy classes in GSp_4 and an application to the enumeration of abelian surfaces*

The Frobenius endomorphism of an abelian variety $A/\mathbb{F}_q$ acts as a symplectic similitude on the torsion subgroups $A[\ell^n](\overline{\mathbb{F}}_q)$. In 2003, Gekeler considered the distribution of these endomorphisms for elliptic curves in the groups $\mathrm{GL}_2(\mathbb{Z}/\ell^r)$ and found a relationship, via isogeny and the class number, to the Euler factors of the L-function of a quadratic imaginary field. We have extended Gekeler's heuristic for the distribution of Frobenius elements from elliptic curves to abelian surfaces by identifying conjugacy classes in $\mathrm{GSp}_4(\mathbb{Z}/\ell^r)$ and relating their sizes to a ratio of class numbers via complex multiplication.

Peter Fletcher, Virginia Tech, *Properties of safe primes*

Let p be a prime greater than 3 such that $p-1$ is square free. We call a congruence class in the multiplicative group of units of $\mathbb{Z}/(p)$ divisor provided it contains a divisor of $p-1$. We let L denote the least common multiple of the orders of all the divisors and consider the set S of primes p for which there is at most one divisor whose order is L. The set S comprises all safe primes, but fewer than 400 primes less than 100,000,000,000. Of these others, only 31, 43 and 112643 have a divisor whose order is L. All the known primes p in S have the property that $L = p - 1$.

Nicolas Smoot, Armstrong Atlantic State University, *The distribution of consecutive octic residues and possible generalization*

The distribution of power residues of $\mathbb{F}_p$, for a fixed prime p, is a deep and beautiful problem in number theory. In particular, we wish to discuss the occurrence of pairs of consecutive power residues. It is trivial to determine the formula for the number of pairs of consecutive quadratic residues, but similar formulas for higher powers are more difficult. The formula for consecutive quartic residues was discussed in a recent paper entitled *Enumeration of Triangles in Quartic Residue Graphs*. Here, we wish to extend their ideas to develop a formula for consecutive octic residues. We will then compare the formulas for pairs of consecutive quadratic, quartic, and octic residues, and consider the possibility of a generalization that will describe the number of pairs of consecutive 2^n residues.

Thomas Wright, Wofford College, *Carmichael numbers in arithmetic progressions*

In this talk, we prove that for any a and M with $(a, M) = 1$, there are infinitely many Carmichael numbers congruent to a mod M.

Ian Petrow, Stanford University, *Moments of L-functions and their derivatives*

It has been a general principle of modern mathematics that to study some inaccessible object, one deforms it into a family of objects which is more accessible. I will discuss moments of L-functions and moments of their derivatives as a way to study the structure of families of L-functions. Naturally, this leads us to consider trace formulae and the random matrix models. I will present some new results on moments of derivatives, on both the L-function and random matrix sides.

Caroline Turnage-Butterbaugh, University of Mississippi, *Large gaps between zeros of Dedekind zeta-functions of quadratic number fields*

Let K be a quadratic number field with discriminant d. The Dedekind zeta-function attached to K can be expressed by $\zeta_K(s) = \zeta(s)L(s, \chi_d)$ for $s \neq 1$, where $\zeta(s)$ is the Riemann zeta-function, the character χ_d is the Kronecker symbol associated to d, and $L(s, \chi_d)$ is the corresponding Dirichlet L-function. Using the mixed second moments of $\zeta_K(\frac{1}{2} + it)$ and its derivatives, we prove the existence of gaps between consecutive zeros of $\zeta_K(s)$ on the critical line which are much larger than the average spacing. We also conjecture a more precise main term for these moments using a modification of the recipe of Conrey, Farmer, Keating, Rubenstein, and Snaith combined with ideas of Hughes and Young.

Robert Lemke Oliver, Emory University, *Multiplicative functions dictated by Artin symbols*

Granville and Soundararajan have recently put forward the notion that generic multiplicative functions deserve greater study in the area of analytic number theory. Here we study such functions which arise from the arithmetic of number fields. For each finite Galois extension K/Q, we construct a natural class $\mathcal{S}_K$ of completely multiplicative functions whose values are

dictated by Artin symbols, and we show that the only functions in $\mathcal{S}_K$ whose partial sums exhibit greater than expected cancellation are Dirichlet characters.