PA lmetto N umber T heory S eries

SCHEDULE OF ACTIVITIES

Refreshments are in the Wyman Williams Room, next to room 412 in LeConte.
Saturday morning talks are in room 405 in LeConte.
All other talks are in room 412 in LeConte.

SATURDAY, DECEMBER 13, 2008

9:30 COFFEE AND OTHER REFRESHMENTS

10:00 **Morley Davidson** (Kent State), *Cyclotomic reductions of partition polynomials*

10:25 **Mike Mossinghoff** (Davidson College), *Barker sequences and Wieferich cycles*

10:50 **Joshua Harrington** (Shippensburg University), *On the Iteration of a Function Related to Euler's ϕ-Function*

11:15 **Lenny Jones** (Shippensburg University), *Concerning a question on the reducibility of polynomials*

11:40 **Tom Binder** (Universitaet Luebeck), *Zero-free regions of derivatives of the Riemann zeta function*

12:00 LUNCH (a list of restaurants in the area will be made available)

1:30 **Jeff Vaaler** (University of Texas at Austin), *Recent work on the Weil height*

2:30 COFFEE BREAK

2:50 **Carl Pomerance** (Dartmouth College), *Order and chaos*

3:55 **Dan Baczkowski** (University of South Carolina), *Maximum number of $\mathbb{F}_q$-rational points on curves of small genus over the finite field $\mathbb{F}_q$*

The organizers thank the National Science Foundation, the National Security Agency and the Mathematics Department at the University of South Carolina for their support.

4:20 **Dan Yasaki** (University of North Carolina at Greensboro), *Hecke eigenforms and elliptic curves over* $\mathbb{Q}(\zeta_5)$

4:40 COFFEE BREAK

5:00 **Alina Cojocaru** (University of Illinois at Chicago), *Twin prime questions for elliptic curves*

6:00 DINNER (a list of restaurants in the area will be made available)

SUNDAY, DECEMBER 14, 2008

8:30 COFFEE AND OTHER REFRESHMENTS

9:00 **Nigel Boston** (University College Dublin, Ireland, and University of Wisconsin), *Random groups in Number Theory and Topology*

10:05 **Luis Finotti** (University of Tennessee), *Computations with Witt vectors of length* 3

10:25 COFFEE BREAK

10:45 **Amanda Folsom** (University of Wisconsin), *A classical problem of Rademacher on the partition function and related problems in analytic number theory*

11:50 **Tim Flowers** (Clemson University), *Asymptotics of Bernoulli, Euler, and Strodt polynomials*

12:10 END OF CONFERENCE

ABSTRACTS

DAN BACZKOWSKI, University of South Carolina, *Maximum number of $\mathbb{F}_q$-rational points on curves of small genus over $\mathbb{F}_q$*

Let q be a prime raised to an odd power, say $q = p^{2k+1}$. Let $N(Q)$ denote the number of $q \leq Q$ such that $p \mid \lfloor 2q^{1/2} \rfloor$. J.-P. Serre ascertained that the largest number of $\mathbb{F}_q$-rational points on curves of small genus over the finite field $\mathbb{F}_q$ depends on the aforementioned divisibility property. F. Luca and I. Shparlinski have obtained the bound $N(Q) \ll Q^{17/140}$. O. Trifonov and I have obtained improvements which will be discussed.

Saturday, 3:55-4:15

TOM BINDER, Universitaet Luebeck, *Zero-free regions of derivatives of the Riemann zeta function*

We study zeros of derivatives of the Riemann zeta function on the right-hand side of the line $s = 1$ of the complex plane, where s denotes the real part of the argument. It is shown that a previously known zero-free region depending only on s and the degree k of the derivative constitutes the first element of an infinite series of wedge-shaped zero-free regions. These zero-free regions are separated by narrow strips. By developing ways for numerical evaluation of derivatives with high degree, we show that these strips indeed contain zeros. Therefore, one cannot expect to extend the zero-free regions such that they connect to each other.

Saturday, 11:40-12:00

NIGEL BOSTON, University College Dublin, Ireland, and University of Wisconsin, *Random groups in Number Theory and Topology*

In a recent Inventiones paper Dunfield and Thurston compared fundamental groups of random 3-mainfolds and random discrete groups. Analogously, we develop a theory comparing certain random Galois groups and random p-groups. This leads to some mysterious mass formulae, some infinite groups that arise with nonzero probability, and applications to number theory.

Sunday, 9:00-10:00

ALINA COJOCARU, University of Illinois at Chicago, *Twin prime questions for elliptic curves*

For an elliptic curve E over $\mathbb{Q}$ and for a prime p, we let E_p denote the reduction of E modulo p. In 1988, Neal Koblitz asked for the number of primes $p < x$ for which $E_p(\mathbb{F}_p)$ forms a group of prime order. In many ways, this question may be viewed as an analogue of the classical twin prime conjecture. In my talk, I will discuss an average version of Koblitz's question. This is joint work with Antal Balog and Chantal David.

Saturday, 5:00-6:00

MORLEY DAVIDSON, Kent State University, *Cyclotomic reductions of partition polynomials*

The polynomials referred to in the title are characteristic polynomials of Euler's well-known recurrence for $p(n)$ involving pentagonal numbers. Motivated by Hardy and Ramanujan's asymptotic treatment, we consider the value of these polynomials at roots of unity, where we discovered that a surprising reduction property holds. In this talk, the proof of this property (joint work with George Andrews) will be developed by retracing the computer experimentation that led to its discovery. Along the way we will mention some allied results and conjectures regarding the zeros and rational factors of these polynomials.

Saturday, 10:00-10:20

LUIS FINOTTI, University of Tennessee, *Computations with Witt vectors of length 3*

The j-invariant of the canonical lifting of an ordinary elliptic curve can be given as a Witt vector of functions on the j-invariant of the curve in positive characteristic. Mazur and Tate asked about the nature of these functions. A complete description can be given for the function appearing on the second coordinate, but computational difficulties arise when trying to form a proper conjecture on the third coordinate. In this talk we will discuss methods that allow us to overcome these difficulties and apply them to get a proper conjecture.

Sunday, 10:05-10:25

TIM FLOWERS, Clemson University, *Asymptotics of Bernoulli, Euler, and Strodt polynomials*

It is well known that both Bernoulli polynomials and Euler polynomials on a fixed interval are asymptotically sinusoidal. A recent paper by Borwein, Calkin, and Manna uses an idea of Strodt to generalize Bernoulli and Euler polynomials and view them as members of a family of polynomials. We used these ideas to study the asymptotics of non-uniform Strodt polynomials. We will describe the experimental process which led to several conjectures. In addition, we will show how experiments suggested the methods used to prove some of these results.

Sunday, 11:50-12:10

AMANDA FOLSOM, University of Wisconsin, *A classical problem of Rademacher on the partition function and related problems in analytic number theory*

In this talk we will address a classical problem of Rademacher as well as related problems in analytic number theory. In the late 1930s by way of the "circle method", Rademacher obtained an exact analytic formula for $p(n)$, the number of partitions of a positive integer n. The exact formula is an infinite series which may be truncated to approximate $p(n)$ with a certain error term. Here, we study the asymptotic distrbution of $p(n)$ using the equidistribution of Heegner points. We obtain an asymptotic formula for $p(n)$ with an effective error term which significantly sharpens the error bounds obtained by Rademacher and D.H. Lehmer. Using similar methods, we study the asymptotic distribution of traces of a class of Maass-Poincare series that generalizes the modular j-function. This is joint work with Riad Masri.

Sunday, 10:45-11:45

JOSHUA HARRINGTON, Shippensburg University, *On the Iteration of a Function Related to Euler's ϕ-Function*

A unit x in a commutative ring R with identity is called *exceptional* if $1 - x$ is also a unit in R. For any integer $n \geq 2$, define $\phi_e(n)$ to be the number of exceptional units in the ring of integers modulo n. Following work of Shapiro, Mills, Catlin and Noe on iterations of Euler's ϕ-function, we develop analogous results on iterations of the function ϕ_e, when restricted to a particular subset of the positive integers.

Saturday, 10:50-11:10

LENNY JONES, Shippensburg University, *Concerning a question on the reducibility of polynomials*

Filaseta asked the following question:

> For what positive integers d does there exist $f(x) \in \mathbb{Z}[x]$ with $f(1) \neq -d$ such that $f(x)x^n + d$ is reducible over the rationals for all $n \geq 0$?

Extending work of Schinzel, Filaseta has shown that such a polynomial exists when $d \equiv 0 \pmod 4$. The concept of a covering not only plays a crucial role in the proof of this result, but Filaseta has also proven that if such a polynomial exists for any odd d, then an odd covering of the integers exists, which generalizes another theorem of Schinzel. In this presentation we discuss some open questions and results involving coverings, including some recent work of the presenter concerning the above question of Filaseta.

Saturday, 11:15-11:35

MICHAEL MOSSINGHOFF, Davidson College, *Barker sequences and Wieferich cycles*

A Barker sequence is a finite sequence of integers $a_0, \ldots, a_{n-1}$, each ± 1, for which $|\sum_j a_j a_{j+k}| \leq 1$ for $k \neq 0$. It is widely conjectured that no Barker sequences exist with length $n > 13$. A number of quite restrictive conditions are known on the length n of a long Barker sequence, so restrictive in fact that no permissible value of $n > 13$ was even known, though prior work had established that $n > 10^{22}$. We describe a large computational effort aimed at identifying the smallest permissible values of n. Much of the computation consists of an extensive search for certain prime pairs (q, p) that satisfy a Wieferich condition, where $q^{p-1} \equiv 1 \bmod p^2$.

Saturday, 10:25-10:45

CARL POMERANCE, Dartmouth College, *Order and chaos*

One can consider the function $l_a(n)$, when a, n are coprime, which is the order of a in the multiplicative group mod n. Locally this function appears fairly chaotic, for example $l_2(49) = 21$, $l_2(51) = 8$, $l_2(53) = 52$. In fact recently the Russian mathematician V. I. Arnold has conjectured that the order function is connected with a chaotic dynamical system. One might think that averaging would take care of local chaos, but we shall see that a certain amount of chaos persists.

Saturday, 2:50-3:50

JEFF VAALER, University of Texas at Austin, *Recent work on the Weil height*

This will be a mostly expository talk about open problems and recent results on the Weil height of algebraic numbers. In particular we will discuss the Lehmer conjecture and related inequalities, estimates for the number of algebraic numbers with bounded degree and bounded height, and the complete metric space determined by the Weil height.

Saturday, 1:30-2:30

DAN YASAKI, Univ. of North Carolina at Greensboro, *Hecke eigenforms and elliptic curves over* $\mathbb{Q}(\zeta_5)$

Let ζ be a primitive fifth root of unity, and let F be the cyclotomic field $F = \mathbb{Q}(\zeta)$. Hecke eigenforms over F are found for a range of prime levels. For each form, a corresponding elliptic curve over F is found.

Saturday, 4:20-4:40