MASON: Mid Atlantic Seminar On Numbers

October 29, 2016

Abstracts

Saikat Biswas, Arizona State University

Capitulation, unit groups, and the cohomology of S-idèle classes

Let L/K be a finite, cyclic extension of number fields with Galois group G, and suppose that S is a finite set of primes of K that includes all the infinite primes. Two arithmetic problems can be considered in this setting. First, the extension of ideals from K to L induces the S-capitulation map, the kernel of which classifies S-ideal classes in K that become principal in L, and the cokernel of which classifies the ambiguous S-ideal classes in L that do not arise from the corresponding ideals in K. Secondly, there is a canonical action of G on the group of S-units of L and the corresponding cohomology groups encode important arithmetic information. In this talk, we study the S-idèle classes of L and relate it to the S-capitulation map described above as well as to the G-cohomology of the S-units of L.

Abbey Bourdon, University of Georgia

Torsion in Isogeny Classes of CM Elliptic Curves

Let F be a number field and let $E_{/F}$ be an elliptic curve with complex multiplication (CM). That is, we assume the ring of endomorphisms of E defined over the algebraic closure of F is isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field K. We wish to understand the structure of the group of rational torsion points of E, denoted $E(F)[\text{tors}]$, in the case where F contains K. If $\mathcal{O} = \mathcal{O}_K$, the full ring of integers in K, one may avoid the technical complications associated with the study of non-maximal orders, so it is desirable to understand to what extent one may "reduce to the maximal order." In this talk, we will show that $\#E(F)[\text{tors}]$ is bounded by $\#E'(F)[\text{tors}]$, where $E'_{/F}$ is an $\mathcal{O}_K$-CM elliptic curve isogenous to E. This is joint work with Pete L. Clark.

Greg Dresden, Washington and Lee University

When is $a^n + 1$ the sum of two squares?

Using Fermat's two squares theorem and properties of cyclotomic polynomials, we prove assertions about when numbers of the form a^n+1 can be expressed as the sum of two integer squares. We prove that a^n+1 is the sum of two squares for all $n \in \mathbb{N}$ if and only if a is a perfect square. We also prove that for $a \equiv 0, 1, 2 \pmod 4$, if a^n+1 is the sum of two squares, then $a^\delta+1$ is the sum of two squares for all $\delta | n,\ \delta > 1$. Using Aurifeuillian factorization, we show that if a is a prime and $a \equiv 1 \pmod 4$, then there are either zero or infinitely many odd n such that $a^n + 1$ is the sum of two squares. When $a \equiv 3 \pmod 4$, we define m to be the least positive integer such that $\frac{a+1}{m}$ is the sum of two squares, and prove that if $a^n + 1$ is the sum of two squares for any odd integer n, then $m|n$, and both $a^m + 1$ and $\frac{n}{m}$ are sums of two squares.

Note: Joint work with Prof. Jeremy Rouse of Wake Forest University and six undergraduates (Yue, Islam, and Schmitt from W&L; and Hess, Stamm, and Warren from WF)

Eva Goedhart, Lebanon Valley College

On the Family of Diophantine Equations of the Form $X^{2N} + 2^{2\alpha}5^{2\beta}p^{2\gamma} = Z^5$

I will briefly present my most recent work with Helen G. Grundman (AMS Director of Education and Diversity). We prove that no equation of the form $X^{2N} + 2^{2\alpha}5^{2\beta}p^{2\gamma} = Z^5$ has integral solutions with $N > 1$ and $\gcd(X, Z) = 1$. Drawing inspiration from Bennett's work in which he proves that the equation $x^2n+y^2n = z^5$ has no solutions with $n > 1$ and $\gcd(x, y) = 1$, we use the modular approach, as developed by Bennett and Skinner, along with more elementary divisibility arguments.

Heidi Goodson, Haverford College

Hypergeometric Functions and Arithmetic and Analytic Properties of Dwork Hypersurfaces

In this talk, we investigate the relationship between special functions and arithmetic and analytic properties of algebraic varieties. More specifically, we use Greene's finite field hypergeometric functions to give point count formulas for families of higher dimensional varieties called Dwork hypersurfaces. Furthermore, inspired by a result of Manin for curves, we study the relationship between certain period integrals and the trace of Frobenius of these varieties. We show that these can be expressed in terms of "matching" classical and finite field hypergeometric functions. Through congruences between classical and finite field hypergeometric functions that we prove, we give a connection between arithmetic and analytic properties of Dwork hypersurfaces.

Jon Grantham, IDA/CCS

Parallel Computation of Primes of the Form $x^2 + 1$

It has long been an open question whether or not there are infinitely many primes of the form $x^2 + 1$. Marek Wolf and Robert Gerbeicz recently computed all primes of the for $x^2 + 1$ up to 10^{26}. We extend the list up to 6.25×10^{28} through a parallel implementation.

Spencer Hamblen, McDaniel College

Local Arboreal Representations

Let $f(z) = z^\ell - c$ be a separable polynomial over a field K complete with respect to a discrete valuation v and with residue field of characteristic p. We examine the Galois groups and ramification groups obtained from the extensions of K containing all of the roots of the n-th iterate of $f(z)$ in both the tame ($\ell \neq p$) and wild ($\ell = p$) cases, and show how these groups depend on the valuation $v(c)$.

James Hammer, Cedar Crest College

On the Congruence $x^x \equiv x \pmod{n}$

Solutions to the congruence $x^x \equiv x \pmod{p}$, where p is a prime and $1 \leq x \leq p-1$, have been investigated by several authors. Although Kurlberg, Luca, and Shparlinski have recently shown that a solution exists with $x \neq 1$ for almost all primes, there do exist primes for which the only solution is $x = 1$, and they conjecture that the set of such primes is infinite. In this presentation, we investigate the nature of the solutions to this congruence when the prime modulus is replaced with a composite number. Among the results presented, we show that, unlike the situation when the modulus is a prime, there is always a solution with $x \neq 1$. In addition, we prove several results concerning the structure of these solutions, with special attention given to the algebraic structure. In particular, we show that there exists infinitely many composite numbers n for which the set of all solutions to $x^x \equiv x \pmod{n}$, with $1 \leq x \leq n-1$, is a subgroup of the group of units modulo n.

Mike Knapp, Loyola University

Sextic forms over extensions of $\mathbb{Q}_2$

In this talk, we determine the minimum number of variables needed to guarantee that a homogeneous polynomial of the form $a_1x_1^6 + a_2x_2^6 + \cdots + a_sx_s^6$ has a nontrivial zero in certain quadratic extensions of $\mathbb{Q}_2$.

Patrick Lank, University of Massachusetts Lowell

Arithmetic Combinatorics & Diophantine Equations

This will be a discussion of analytic number theory and its applications to exponential Diophantine equations. In particular, the application of sumsets in regards to additive combinatorics and a class of Diophantine equations (i.e. linear, exponential, etc.). The shared properties in additive combinatorics are called inverse problems. The solutions to such problems over the chosen class of Diophantine equations in the context of sumsets show the shared number theoretic type of equivalence classes and relations between elements within a solution set for a given equation. Lastly, if time allows, there will be a discussion about such inverse problems and their applications to arithmetic geometry. Specifically elliptic curves, torsion points, and algebraic varieties.

Matthew Litman, Penn State University

On Consecutive Primitive nth Roots of Unity Modulo q

Given $n \in \mathbb{N}$, we study the conditions under which a finite field of prime order q will have adjacent elements of multiplicative order n. In particular, we analyze the resultant of the cyclotomic polynomial $\Phi_n(x)$ with $\Phi_n(x+1)$, and exhibit Lucas and Mersenne divisors of this quantity. For each $n \neq 1, 2, 3, 6$, we prove the existence of a prime q_n for which there is an element $\alpha \in \mathbb{Z}_{q_n}$ where α and $\alpha + 1$ both have multiplicative order n. Additionally, we use algebraic norms to set analytic upper bounds on the size and quantity of these primes.

Tianyi Mao, CUNY Graduate Center

The Distribution of Integers in a Totally Real Cubic Field

Hecke studies the distribution of fractional parts of quadratic irrationals with Fourier expansion of Dirichlet series. This method is generalized by Behnke and Ash-Friedberg, to study the distribution of the number of totally positive integers of given trace in a general totally real number field of any degree. When the field is cubic, we show that the asymptotic behavior of a weighted Diophantine sum is related to the structure of the unit group. The main term can be expressed in terms of Grössencharacter L-functions.

John Miller, Johns Hopkins

Lower Bounds for Counting Low-Lying Zeros

Using the Weil explicit formula and certain test functions, we find an unconditional lower bound for the number of low-lying zeros of general L-functions that satisfy the Ramanujan-Petersson conjecture. The results improve upon what can be achieved using the best known q-aspect subconvexity bounds.

Tristan Phillips, Shippensburg University

New Primitive Covering Numbers and Their Properties

A *covering number* is a positive integer L such that a covering system of the integers can be constructed with distinct moduli that are divisors $d > 1$ of L. If no proper divisor of L is a covering number, then L is called *primitive*. In 2007, Zhi-Wei Sun gave sufficient conditions for the existence of infinitely many covering numbers, and he conjectured that these conditions were also necessary for a covering number to be primitive. Recently Jones and White have shown that Sun's conjecture is false by finding infinitely many counterexamples. In this article, we give necessary and sufficient conditions for certain positive integers to be primitive covering numbers. We use these results to answer a question of Sun, and to prove the existence of infinitely many previously-unknown primitive covering numbers. We also show, for each of these new primitive covering numbers L, that a covering can be constructed with distinct moduli using only a proper subset of the divisors $d > 1$ of L as moduli.

Charles Samuels, Christopher Newport University

A Connection Between Fibonacci Numbers and Metric Heights

The metric Mahler measure was introduced by Dubickas and Smyth in 2001 as a means of rephrasing Lehmer's conjecture in topological language. Through various generalizations of their construction, it has been discovered that the Fibonacci sequence is closely connected to the behavior of the metric Mahler measure. We formulate a conjecture which purports to describe this connection and show how to resolve this conjecture in several new special cases.

Robert Vaughan, Penn State University

The density of positive diagonal binary quadratic forms

I will describe some famous questions on sums of squares and discuss some recent work with Brandon Hanson which is concerned with showing that a positive proportion of n can be represented by some form $x^2 + zy^2 = n$ with z generally quite small compared with the with the size of n.

Jiayuan Wang, George Washington University

A Computational Method for Solving Exponential-Polynomial Diophantine Equations

We propose a novel computational method for solving some Diophantine equations of the form $\mathcal{K} \cdot Q^n = f(m)$, where $\mathcal{K}$ and Q are fixed positive integers and $f(m)$ is a second degree polynomial with integer coefficients. Our method involves solving generalized Pell–Fermat equations and computing zeros of the solution modulo some powers of Q. We illustrate our method with the equation $3^n = 2m^2 + 1$ and show that its only solutions are $(m, n) = (0, 0)$, $(\pm 1, 1)$, $(\pm 2, 2)$, and $(\pm 11, 5)$.

Cassie Williams, James Madison University

Numerical secondary terms for a conjecture of Cohen and Lenstra

In 1984, Cohen and Lenstra published their classic paper describing a heuristic to explain the observed frequency with which finite abelian groups occur as the class group of a quadratic number field and applied their theoretical framework to make several conjectures about such class groups. Thirty years of improvements in computing and algorithms have made it easy to obtain large data sets against which to test the Cohen-Lenstra conjectures, and discrepancies between their predictions and reality have been noted by several authors. Analytic approaches to determining secondary terms only work for some of the conjectures, and so we instead turn to a numerical approach. We used Sage to perform a numerical investigation of the discrepancy between one of the Cohen-Lenstra conjectures for real quadratic fields and reality. We will share our results, including secondary terms for various small primes, the error in our new estimates, and some interesting patterns.