MidAtlantic Seminar On Numbers III

Saturday and Sunday, February 23-24, 2019

James Madison University

Abstracts (★ indicates plenary speakers)

Max Alekseyev, George Washington University

Title: On Zeckendorf and Bunder Representations of Integers

Abstract: Zeckendorf's theorem states that every nonnegative integer has a unique representation (*Zeckendorf representation*) as the sum of distinct Fibonacci numbers $\{F_n \mid n \geq 2\}$ that does not include any two consecutive Fibonacci numbers. Bunder's theorem states that there also exits a unique representation (*Bunder representation*) as the sum of distinct Fibonacci numbers with alternating signs $\{(-1)^{n-1}F_n \mid n \geq 1\}$ that again does not include any two consecutive Fibonacci numbers. We show how one can obtain Bunder representation from Zeckendorf one. We further reveal the connection between Bunder representations and the positional numeral system base the golden ratio reciprocal.

★ Abbey Bourdon, Wake Forest University

Title: Sporadic Points on Modular Curves

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? In 1977, Mazur answered this question for elliptic curves over the rational numbers, and the classification for elliptic curves over quadratic fields was completed in 1992 through a series of papers by Kamienny, Kenku, and Momose. A few years later, Merel proved his celebrated Uniform Boundedness Theorem, which implies that if we fix d, then there are only finitely many groups that arise as the torsion subgroup of an elliptic curve defined over a number field of degree d. However, the complete list of the groups that arise is unknown for any $d > 2$.

A serious challenge in attempting to extend the classification is the need to identify all groups which arise for only finitely many isomorphism classes of elliptic curves–a phenomenon that does not occur for $d = 1$ or $d = 2$. The known examples 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 of bounded degree. This is joint work with Ozlem Ejder, Yuan Liu, Frances Odumodu, and Bianca Viray.

René Christensen, Aalborg University, Denmark

Title: On nested code pairs from the Hermitian curve

Abstract: Secret sharing allows a secret to be split into 'shares' such that a small number of shares reveal nothing, but a sufficiently large number of shares enable reconstruction. The parameters of interest are (1) the secret size compared to the shares, (2) the privacy parameter t, and (3) the reconstruction parameter r. That is, any t shares reveal nothing, and any r shares allow reconstruction. Secret sharing schemes can be described using pairs of nested linear codes, and the exact parameters of the scheme can be determined from the nested codes. In this talk, I will give an overview of the connection between secret sharing and nested codes, and discuss recent work with Olav Geil studying nested codes from improved Hermitian codes.

Huy Dang, University of Virginia

Title: The refined local lifting problem for curves

Abstract: As the name suggests, the goal of a lifting problem is to construct some objects in characteristic 0 which "lift" the given ones in characteristic p. Grothendieck proved that all smooth, projective, connected curve over an algebraically closed field of positive characteristic lift. Thus, it is natural to ask whether one can lift a Galois cover of curves to characteristic zero. Obus, Wewers, and Pop showed that the answer is always positive when the Galois group is cyclic. I will discuss the refined local lifting problem, which concerns whether cyclic Galois covers are liftable "in towers", our approach to tackle the problem, and some partial results.

Jonathan Gerhard, University of Michigan

Title: The interesting worlds of core partitions and numerical semigroups

Abstract: This talk will be a purely expository account of a very interesting connection between core partitions and numerical semigroups. A partition is called n-core if none of the hook-lengths in its Young diagram are divisible by n. A subset of the natural numbers that is closed under addition is called a numerical semigroup.

These two objects seem fairly different at first, but can be connected using the theory of lattice paths! They also have further interesting connections to the study of monomial curves, the modular representation theory of the symmetric group, and the chicken nugget problem.

Eva Goedhart, Lebanon Valley College

Title: An Application of Continued Fractions to Solving Diophantine Equations

Abstract: After a quick review of some continued fraction results, I will present an application to the following joint work with H.G. Grundman. For positive integers a, b, c, k with $k \geq 7$, the family of Diophantine equations $(a^2cX^k - 1)(b^2cY^k - 1) = (abcZ^k - 1)^2$ has no integer solutions x, y, $z > 1$ with $a^2x^k \neq b^2y^k$. While my focus will be on the application of continued fractions, the proof also uses a Diophantine approximation theorem.

Jon Grantham, IDA/CCS

Title: Episode III: German Conjectures, an Italian Poet, and Brazilian Primes
Abstract: I will discuss primes which are values of cyclotomic polynomials.

Hester Graves, IDA/CCS

Title: The Minimal Euclidean Function on the Gaussian Integers
Abstract: In 1949, Motzkin introduced a new tool to study Euclidean domains. As a side effect, it described the minimal Euclidean algorithm for a given domain. He showed that the minimal Euclidean algorithm on the integers is $\phi_{\mathbb{Z}}(x) = \lfloor \log_2 |x| \rfloor$. Lenstra gave an elegant proof of what the minimal Euclidean algorithm on $\mathbb{Z}[i]$. This talk will give a new, elementary proof and an alternate description of said function that allows for fast computation.

Anna Haensch, Duquesne University

Title: Spinor Regular Ternary Quadratic Forms
Abstract: It has long been known that integral quadratic forms fail to satisfy a local-global principle. That is, representation of an integer locally at $\mathbb{Z}_p$ for every prime p does not guarantee a global representation over the integers. The failure of the local-global principle is particularly interesting when the form is in three variables. In this talk we explore the underlying structure of such forms and determine for which forms the local-global principle holds, and for which forms the local-global principle almost holds (and why it eventually fails!).

Spencer Hamblen, McDaniel College

Title: Student research on generalizations of Waring's Problem
Abstract: Over the last 6 summers, undergraduates at McDaniel College have investigated a version of Waring's Problem over quaternion rings and ramified ℓ-adic rings using elementary number theory. I will give a summary of their results and methods, and discuss the process of leading beginning mathematics students through original research.

Russell Hendel, Towson University

Title: Recursive Triangles Embedded in 2nd Order Recursions

Abstract: At West Coast Number Theory 2018 the following result was presented. The k-acci numbers are defined by $\langle F(0), F(1), ..., F(k-1)\rangle = \langle 0, 1, .., 1\rangle$ with every $F(n)$ equal to the sum of the previous k sequence members. Define $G(n) = F(-n)$. Then G when regarded as an infinite word over the monoid of integers has the following subword: $1^{k-1}B_2; 1^{k-2}B_3; \ldots; 1, B_k$, where the exponentiation indicates repeated concatenation and the B_j are blocks of j consecutive integers. The B_j, when arranged as rows, satisfy a triangular recursion: $B(j,p) = 2B(j-1,p) - B(j-1,p-1)$ (over appropriate indices). In this talk we first review the above and then (as time permits) show other examples of recursive triangles embedded in recursive sequences.

Michael Knapp, Loyola University Maryland

Title: Counterexamples to a Conjecture of Norton

Abstract: Let $\Gamma^*(k)$ be the smallest integer s such that the equation

$$a_1x_1^k + \cdots + a_sx_s^k = 0$$

has a nontrivial solution in every p-adic field $\mathbb{Q}_p$, regardless of the values of the (rational integer) coefficients. An old conjecture of Norton was that we should have $\Gamma^*(k) \equiv 1 \pmod{k}$ for all degrees k. This was disproved in 1974 by Bovey, who showed that $\Gamma^*(8) = 39$, but until a few years ago this was the only known counterexample. In this talk, we show that there are infinitely many counterexamples to Norton's conjecture. This is joint work with Hemar Godinho.

Angel Kumchev, Towson University

Title: A hybrid of two theorems of Piatetski-Shapiro

Abstract: I will start with a short history of two classical results of Piatetski-Shapiro: the Piatetski-Shapiro prime number theorem and an additive Diophantine inequality for fractional powers of primes. Then I will present some new results on a hybrid problem. This is joint work with Zhivko Petrov (Sofia).

Lindsey-Kay Lauderdale, Towson University

Title: On the Intersection Numbers of Finite Groups

Abtract: In a popular paper of Cohn, the concept of a covering number of a group was introduced. The *covering number* of a finite group G is the smallest number of proper subgroups of G whose set-theoretic union is G. Covering numbers are the subject of prior research by numerous authors, and in this talk we focus on a dual problem to that of covering numbers of groups, which involves maximal subgroups of finite groups. In addition, we will compare our results to some of the well-known results on covering numbers.

Noah Lebowitz-Lockard, University of Georgia

Title: Irreducible quadratic polynomials and Euler's function

Abstract: Let $V(x)$ be the number of $n \leq x$ for which $\phi(m) = n$ for some n, where ϕ is Eulers totient function. In 1929, Pillai proved that $V(x) = o(x)$, i.e. that almost all numbers lie outside the range of the totient function. We discuss a generalization of this result, specifically that for a given irreducible quadratic polynomial $P(x)$, almost all numbers of the form $P(n)$ lie outside the range of the totient function as well. We put bounds on the number of $n \leq x$ with this property and show how we can improve them assuming the abc and Bateman-Horn Conjectures.

★ Michelle Manes, University of Hawaii / NSF

Title: "Complex Multiplication" in Arithmetic Dynamics

Abstract: "Arithmetic dynamics" is the study of number theoretic properties of iterated functions. The field draws inspiration from dynamical analogues of theorems and conjectures in classical arithmetic geometry. In this talk, I will describe some of theses analogues with a focus on attempts to develop a "dynamical" theory of complex multiplication.

Gretchen Matthews, Virginia Tech

Title: Algebraic function fields and code-based cryptography

Abstract: Code-based cryptography was introduced in 1978 by McEliece when he described a cryptosystem which depends on linear error-correcting codes. There is renewed interest in code-based cryptography, because unlike many public-key systems used today (including RSA and elliptic curve cryptography) it is believed to be resilient in the face of quantum algorithms. The McEliece cryptosystem relies on Goppa codes, but its large public key size prompts the study of other codes in the McEliece cryptosystem. For the most part, other codes have led to systems which are susceptible to structural attacks. In this talk, we discuss the use of algebraic function fields and related codes in code-based cryptosystems.

Nathan McNew, Towson University

Title: Primitive and geometric-progression-free sets without large gaps

Abstract: We prove the existence of primitive sets (sets of integers in which no element divides another) in which the gap between any two consecutive terms is substantially smaller than the best known upper bound for the gaps in the sequence of prime numbers. The proof uses the probabilistic method. Using the same techniques we improve the bounds obtained by He for gaps in geometric-progression-free sets.

Jae Yong Park, Hofstra University

Title: On Second Order Linear Recurrences of Composite Numbers

Abstract: We present a new proof of the following result of Somer and Dubickas, Novikas, and Šiurys:

Let $(a, b) \in \mathbb{Z}^2$ and let $(x_n)_{n\geq 0}$ be the sequence defined by some initial values x_0 and x_1 and the second order linear recurrence

$$x_{n+1} = ax_n + bx_{n-1}$$

for $n \geq 1$. Suppose that $b \neq 0$ and $(a, b) \neq (2, -1), (-2, -1)$. Then there exist two relatively prime positive integers x_0, x_1 such that $|x_n|$ is a composite integer for all $n \in \mathbb{N}$.

This extends a result of Graham who solved the problem in the particular case $(a, b) = (1, 1)$.

Charles Samuels, Christopher Newport University

Title: The Completion of the Direct Limit of Adèle Rings

Abstract: If K and L are global fields with $K \subseteq L$, then there is a natural injection from the adéle ring $\mathbb{A}_K$ to $\mathbb{A}_L$. Given a fixed global field F and possibly infinite Galois extension E/F, we examine the direct limit $\mathbb{A}_E := \varinjlim \mathbb{A}_K$ taken over the index set$\{K \subseteq E : K/F$ finite Galois$\}$. We investigate several of the basic topological and algebraic properties of $\mathbb{A}_E$, establishing, in particular, its lack of completeness precisely when E/F is infinite. As part of this process, we show that the completion of $\mathbb{A}_E$ may be interpreted as a certain space of continuous functions which equals the classical adèle ring of E when E/F is finite.

★ Jesse Thorner, Stanford University

Title: A new approach to bounding L-functions

Abstract: An L-function is a type of generating function with multiplicative structure which arises from either an arithmetic-geometric object (like a number field, elliptic curve, abelian variety) or an automorphic form. The Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ is the prototypical example of an L-function. While L-functions might appear to be an esoteric and special topic in number theory, time and again it has turned out that the crux of a problem lies in the theory of these functions. Many equidistribution problems in number theory rely on one's ability to accurately bound the size of L-functions; optimal bounds arise from the (unproven!) Riemann Hypothesis for $\zeta(s)$ and its extensions to other L-functions. I will discuss some motivating equidistribution problems along with recent work (joint with K. Soundararajan) which produces new bounds for L-functions by proving a suitable "statistical approximation" to the (extended) Riemann Hypothesis.