BRIN MATHEMATICS
RESEARCH CENTER

# MASON - 7

## Mid-Atlantic Seminar On Numbers

### March 29 - 30, 2025

The "Mid-Atlantic Seminar On Numbers" (MASON) is a regional conference focused on number theory, primarily drawing mathematicians from the Mid-Atlantic region of the United States. The conference primarily attracts mathematicians from the Mid-Atlantic region of the United States, who present their research in a smaller, collaborative setting across various universities in the region.

## PLENARY SPEAKERS

Shabnam Akhtari, Penn State University
Andrew O'Desky, Princeton University
Lillian Pierce , Duke University

## ORGANIZERS

Angel Kumchev, Towson University
Nathan McNew, Towson University
Larry Washington, University of Maryland

BRINMRC.UMD.EDU

CSIC Building, 4th Floor
8169 Paint Branch Drive
University of Maryland
College Park, MD 20742

DEPARTMENT OF
MATHEMATICS

Credit Image: https://mathblog.com/reference/arithmetic/number-theory/
The cover has been designed using assets from Freepik.com

# MASON VII Mid-Atlantic Seminar On Numbers

## **Schedule:** Saturday March 29th 2025

| | **Room A** Toll 2213 | **Room B** Toll 2214 |
|---|---|---|
| **9:00 AM** | **Registration, Coffee and Mingling** Kirwan 3201 | |
| **9:55 AM** | **Opening Remarks -** Kirwan 3206 | |
| **10:00 AM**<br>Kirwan 3206 | **Shabnam Akhtari** Penn State<br>**Monogenic Orders and Classical Diophantine Equations** | |
| **10:50-11:10 AM** | **Break** | |
| **11:10 AM** | **William Craig**<br>United States Naval Academy<br>**Quasimodular forms, $q$-multiple zeta values, and partitions** | **Joshua Harrington**<br>Cedar Crest College<br>**Monogenic trinomials of the form $x^4 + ax^3 + d$ and their Galois groups** |
| **11:40 AM** | **Wissam Ghantous**<br>University of Central Florida<br>**A symmetric symbol for triples of modular forms** | **Chris Bispels**<br>UMBC<br>**Using Integer Covering Systems to find Repdigit and Other Forms of Riesel and Sierpiński Numbers** |
| **12:10-2:00 PM** | **Lunch** | |
| **2:00 PM**<br>Kirwan 3206 | **Andrew O'Desky** Princeton<br>**Algebraic integers of bounded height and given Galois group** | |
| **2:50-3:10 PM** | **Break** | |
| **3:10 PM** | **Charles Samuels**<br>Christopher Newport University<br>**Function spaces on the places of $\overline{\mathbb{Q}}$** | **Travis Morrison**<br>Virginia Tech<br>**The SEA algorithm for endomorphisms of supersingular elliptic curves** |
| **3:40 PM** | **Michael Mossinghoff**<br>CCR<br>**Oscillations in the Goldbach conjecture** | **Maher Mamah**<br>Pennsylvania State University<br>**The Supersingular Isogeny Path and Endomorphism Ring Problems: Unconditional Reductions** |
| **4:10 PM** | **Amita Malik**<br>Pennsylvania State University<br>**Zeros of derivatives of L-functions attached to Maass forms** | **William Mahaney**<br>Virginia Tech<br>**Computing Isogenies At Singular Points of the Modular Polynomial** |
| **4:40 PM** | **Kassie Archer**<br>United States Naval Academy<br>**Egyptian fractions and arithmetical structures on graphs** | **Ian Whitehead**<br>Swarthmore College<br>**The Local-Global Conjecture for Generalized Circle Packings** |
| **5:00 PM** | **Problem Session** | |

# MASON VII Mid-Atlantic Seminar On Numbers

## **Schedule:** Sunday March 30th 2025

| | **Room A** Toll 2213 | **Room B** Toll 2214 |
|---|---|---|
| **8-9 AM** | **Registration, Coffee and Mingling** Kirwan 3201 | |
| **9:00 AM**<br>Kirwan 3206 | **Lillian Pierce** Duke<br>**Superorthogonality** | |
| **9:50-10:10 AM** | **Break** | |
| **10:10 AM** | **Russell Jay Hendel**<br>Towson University<br>**Proof of a Conjecture on the Growth of the Maximal Resistance Distance in a Linear 3–Tree** | **Foivos Chnaras**<br>University of Maryland<br>**On the cyclotomic Iwasawa invariants of Elliptic Curves of rank 1** |
| **10:40 AM** | **Wing Hong Tony Wong**<br>Kutztown University of Pennsylvania<br>**Digital sums and variations** | |
| **11:10 AM** | **Max Alekseyev**<br>George Washington University<br>**On computing solutions to** $2^n \equiv 3 \pmod{n}$ **and beyond** | **Michael Wills**<br>University of Virginia<br>**Non-trivial local-to-global principles for 0-cycles on products of elliptic curves** |
| **11:40 AM** | **Steven J. Miller**<br>Williams College<br>**From Sperner's Lemma to Spurring Research** | |

Shabnam Akhtari, Pennsylvania State University
Monogenic Orders and Classical Diophantine Equations

An order $O$ in a number field is called monogenic if it can be generated by one element over the integers, that is $O = \mathbb{Z}[\alpha]$. In this case we call $\alpha$ a monogenizer of $O$. Since $\mathbb{Z}[\alpha] = \mathbb{Z}[\pm\alpha + c]$, for any integer $c$, we call two algebraic integers $\alpha$ and $\alpha'$ equivalent if $\alpha + \alpha'$ or $\alpha - \alpha'$ is a rational integer. By a monogenization of $O$, we mean an equivalence class of monogenizers of $O$. Győry has shown that there are finitely many monogenizations for a given order. An interesting (and open) problem is to count the number of monogenizations of a given monogenic order. First we will observe, for a given order $O$, that $O = \mathbb{Z}[\alpha]$ in $\alpha$, is indeed a Diophantine equation, namely an index form equation. Then we will modify some algorithmic approaches, due to Gaál, Pethő and Pohst for finding solutions of index form equations in quartic number fields to obtain new and improved upper bounds for the number of monogenizations of a quartic order.

Max Alekseyev, George Washington University
On computing solutions to $2^n \equiv 3(modn)$ and beyond

Solving a congruence $b^n \equiv c \pmod{n}$ with respect to $n$ for given integers $b$ and $c$ in most cases is a hard problem with no or just a few known solutions. We present a number of computational techniques that can help to find all solutions or to prove their absence below a given bound. In particular, we discuss a folklore problem of solving $2^n \equiv 3 \pmod{n}$, for which we discovered a new solution $n = 3468371109448915$ and now know all solutions below $10^{18}$. We further discuss applications of the presented methods to related problems such as finding Carmichael numbers with a prescribed divisor.

Kassie Archer, United States Naval Academy
Egyptian fractions and arithmetical structures on graphs

An arithmetical structure on a connected graph is a labeling of the vertices of the graph with positive integers so that the label at a given vertex divides the sum of the labels of all its neighbors, and so that the gcd of all the labels is equal to 1. In this talk, we see that in studying the arithmetical structures of star graphs and complete graphs, Egyptian fractions play a large role. In particular, there is an abelian group associated to each arithmetical structure called the critical group; we use Egyptian fractions to partially determine what critical groups can be realized by these graphs. We also discuss some open questions.

Chris Bispels, University of Maryland, Baltimore County
Using Integer Covering Systems to find Repdigit and Other Forms of Riesel and Sierpiński Numbers

A Riesel number $k$ is an odd integer such that $k2^n - 1$ is composite for all $n$, the first of which was found in 1956 by Hans Riesel. Four years later, Wacław Sierpiński defined a similar number using addition in place of subtraction, called Sierpiński numbers. In this paper, we prove we prove the existence of repunit, repdigit, and repnumber Sierpiński and Riesel numbers in different infinite patterns of bases. Additionally, we generalize a previous result on appending a digit repeatedly to an existing Sierpiński number in base 10 to obtain a new Sierpiński number to an infinite number of bases.

Foivos Chnaras, University of Maryland

On the cyclotomic Iwasawa invariants of Elliptic Curves of rank 1

For elliptic curves of rank 1 over $\mathbb{Q}$, we provide a numerical criterion that determines whether the Iwasawa invariants at a prime $p$ of good reduction attain their minimum possible value.

William Craig, United States Naval Academy

Quasimodular forms, $q$-multiple zeta values, and partitions

In recent years, MacMahon's generalized sum-of-divisor functions have seen a resurgence of study stemming from two sources: they are quasimodular forms due to work of Andrews and Rose, and they fit into the algebraic framework of $q$-multiple zeta values as formulated, for instance, by Bachmann and Kühn. In this talk, we discuss the theory of $q$-multiple zeta values from a $q$-series perspective with a focus on quasimodular forms. In particular, we show how any quasimodular form (of any level) of weight at least two can be produced as a linear (not algebraic) combination of partition functions of MacMahon's type. We also demonstrate how to calculate these "linearized" formulas for quasimodular forms using the more classical representations in terms of Eisenstein series.

Wissam Ghantous, University of Central Florida

A symmetric symbol for triples of modular forms

We introduce a new $p$-adic triple symbol based on the Garrett-Rankin $p$-adic $L$-function and show that it satisfies symmetry relations, when permuting the three input modular forms. We also provide computational examples illustrating this symmetry property. To do so, we develop algorithms to compute ordinary projections of nearly overconvergent modular forms as well as certain projections over spaces of non-zero slope. Our work also gives an efficient method to calculate certain Poincare pairings in higher weight, which may be of independent interest.

Joshua Harrington, Cedar Crest College

Monogenic trinomials of the form $x^4 + ax^3 + d$ and their Galois groups

In this talk, we will show that all but two monogenic trinomials of the form $f(x) = x^4 + ax^3 + d$ have Galois group in $\{S_4, A_4\}$. We further further show that the Galois group $f(x)$ is $A_4$ if and only if $f(x) = x^4 + 4kx^3 + 27k^4 + 1$ for some integer $k$ with $27k^4 + 1$ squarefree.

Russell Jay Hendel, Towson University

Proof of a Conjecture on the Growth of the Maximal Resistance Distance in a Linear 3–Tree

Barret, Evans and Francis conjectured that if $G$ is the straight linear 3-tree with $n$ vertices and $H$ is the straight linear 3-tree with $n+1$ vertices then

$$\lim_{n\to\infty} r_H(1,n+1) - r_G(1,n) = \frac{1}{14},$$

where $r_G(u,v)$ and $r_H(u,v)$ are the resistance distance between vertices $u$ and $v$ in graphs $G$ and $H$ respectively. In this paper we prove the conjecture by looking at the determinants of deleted Laplacian matrices. The proof uses a Laplace expansion method on a family of determinants to determine the underlying recursion this family satisfies and then uses routine linear algebra methods to obtain an exact Binet formula for the $n$-th term.

David Hubbard, Retired

Computing the $p$-part of Class Groups

The class group of a number field has been an important invariant since the 1800s. We present here some techniques for computing the $p$-Sylow subgroup of class groups in the case of a cyclic degree-$p$ extension of number fields. The remarkable thing is that almost all the computations take place in the base field. This may make these class group computations possible for larger number fields. Currently though, a possibly large search is needed at each step.

William Mahaney, Virginia Tech

Computing Isogenies At Singular Points of the Modular Polynomial

For number fields or finite fields $K$ of characteristic neither 2 nor 3, it is well known that $\overline{K}$-rational points $(j_1, j_2)$ of the $\ell$th modular polynomial $\Phi_\ell(X,Y) \in K[X,Y]$, where $\ell \neq \mathrm{Char}(K)$ is a prime, parametrize pairs of $\ell$-isogenous elliptic curves $E_{j_1}, E_{j_2}$ over $\overline{K}$. In 1995, Schoof published a paper detailing a novel point counting algorithm for elliptic curves over finite fields. Along with contributions of Atkin and Elkies, Schoof also developed a method that takes as input a pair $(j_1, j_2)$ of $\ell$-isogenous $j$-invariants in a finite field $\mathbb{F}_p$ such that $(j_1, j_2)$ is a non-singular point of $\Phi_\ell \in \mathbb{F}_p[X,Y]$ and computes the normalized $\ell$-isogeny $\phi : E_{j_1} \to E_{j_2}$; however, this method fails if $(j_1, j_2)$ is a singular point. In this talk, we present an extension of Schoof's algorithm to handle singular points of $\Phi_\ell$. Given a finite field $K$ of characteristic not 2 or 3, as well as a singular point $(j_1, j_2) \in K$ of multiplicity $m$ with $j_1, j_2 \neq 0, 1728$, our algorithm computes the $m$ pairs $\{(E_{j_1,i}, E_{j_2,i})\}_{i=1}^m$ of elliptic curves with $j$-invariants $j_1, j_2$, respectively, and the normalized $\ell$-isogenies $\phi_i : E_{j_1,i} \to E_{j_2,i}$ between each such pair.

Amita Malik, Pennsylvania State University

Zeros of derivatives of L-functions attached to Maass forms

Motivated by the close connection of the zeros of the derivative of the Riemann zeta function, we study the zeros of higher order derivatives of L-function attached to Maass forms. This is joint work with Rahul Kumar.

Maher Mamah, Pennsylvania State University

The Supersingular Isogeny Path and Endomorphism Ring Problems: Unconditional Reductions

The supersingular isogeny path problem is defined as follows: Given two supersingular elliptic curves defined over $F_{p^2}$, find an isogeny between them. On the other hand, the Endomorphism ring problem asks to compute the ring of endomorphisms of a supersingular elliptic curve. In this paper we study several number theoretic computational problems related to current post-quantum cryptosystems based on isogenies between supersingular elliptic curves which are motivated by the aforementioned problems. In particular we prove that the supersingular isogeny path and endomorphism ring problems are unconditionally equivalent under polynomial time reductions. We show that access to a factoring oracle is sufficient to solve the Quaternion path problem of KLPT and prove that these problems are equivalent, where previous results either assumed heuristics or the generalised Riemann Hypothesis (GRH). Consequently, given Shor's quantum algorithm for factorization, our results yield unconditional quantum polynomial time reductions between the isogeny path and Endomorphism Ring problems. Recently these reductions have become foundational for the security of isogeny-based cryptography.

Steven J. Miller, Fibonacci Association

From Sperner's Lemma to Spurring Research

Fixed point theorems have a long history in pure and applied mathematics. Depending on the system, there are different techniques to prove them. We describe Sperner's lemma, a key ingredient in proving the existence of Nash equilibria. The proof follows from a simple parity argument, and yields a trivial game where one player always wins. We discuss a simple modification, leading to a more challenging situation where the results are not yet known. This problem will be investigated in detail in the 2025 Polymath Junior REU, members of the audience who are interested in helping as mentors or students should reach out to the speaker.

Travis Morrison, Virginia Tech

The SEA algorithm for endomorphisms of supersingular elliptic curves

For an elliptic curve $E$, Elkies' improvement to Schoof's algorithm involves computing the trace of Frobenius modulo primes $\ell$ for which E has a rational $\ell$-isogeny. In practice, this gives a substantial speedup, but heuristics beyond GRH are required to prove that it yields an asymptotic speedup. Computing the trace of an arbitrary endomorphism can be done with a generalization of Schoof's algorithm. When $E$ is supersingular, computing the trace of an endomorphism is an important subroutine in various algorithms for computing the endomorphism ring of $E$. And in the supersingular case, assuming $E$ is defined over the finite field of $p^2$ elements, E always has rational $ell$-isogenies – we leverage this in a generalization of the SEA algorithm for supersingular endomorphisms, yielding an unconditional asymptotic speedup over the generalization of Schoof's algorithm. We gain further speedups in practice: for example, we can compute the trace modulo $p$ (the characteristic) by computing the action on an invariant differential of $E$, and we can leverage knowledge of the number of points of $E$ since $E$ is supersingular to compute the trace modulo primes dividing $p \pm 1$. This is joint work with Lorenz Panny, Jana Sotakova, and Michael Wills.

Michael Mossinghoff, Center for Communications Research, Princeton
Oscillations in the Goldbach conjecture
Let $R(n) = \sum_{a+b=n} \Lambda(a)\Lambda(b)$, where $\Lambda(\cdot)$ is the von Mangoldt function. This function is often studied in connection with Goldbach's conjecture. It is known on the Riemann Hypothesis (RH) that $\sum_{n \leq x} R(n) = x^2/2 - 4x^{3/2}G(x) + O(x^{1+\epsilon})$, where $G(x) = \Re \sum_{\gamma>0} \frac{x^{i\gamma}}{(\frac{1}{2}+i\gamma)(\frac{3}{2}+i\gamma)}$ oscillates in $x$, and the sum is over the ordinates of the nontrivial zeros of the Riemann zeta function in the upper half-plane. In 1991, Fujii established some bounds on the values of $G(x)$ under RH plus the assumption of linear independence of the ordinates of certain zeros of the zeta function, and remarked that this assumption could be removed with additional work. We revisit this method, and establish improved (and nearly optimal) bounds on the values attained by $G(x)$, without any linear independence assumptions.

Andy O'Desky, Princeton University
Title: Algebraic integers of bounded height and given Galois group
Abstract: How many algebraic integers of bounded height have a minimal polynomial with a given Galois group? One approach to this problem is via Malle's conjecture. In this talk we will discuss an alternative approach using a construction with the Galois group's group algebra which has proven fruitful in recent years. We will explain how this construction lets one apply tools from harmonic analysis and the theory of toric varieties. Applications include a Malle-free determination of the asymptotic count for cyclic Galois groups. Time permitting, we will also explain how this construction gives a new perspective on cubic abelian polynomials.

Charles Samuels, Christopher Newport University
Function Spaces on the Places of $\overline{\mathbb{Q}}$
A 2009 article of Allcock and Vaaler showed how to interpret each point in $\overline{\mathbb{Q}}$ as a function on the space $Y$ places of $\overline{\mathbb{Q}}$. These observations opened a pathway to studying number theoretic objects, such as the Weil height, using methods of functional analysis. In this talk, we study various duals of function spaces on $Y$. By constructing a certain type of measure called a *consistent map*, we describe a collection of Riesz-type representation theorems for these function spaces. Unlike the more classical Riesz Representation Theorem, our results apply to both algebraic and continuous duals.

Michael Wills, University of Virginia
Non-trivial local-to-global principles for 0-cycles on products of elliptic curves
Let $X$ be a smooth projective variety over a number field $K$. A conjecture first stated by Colliot-Thélène and Sansuc in the 1980's predicts that $\mathrm{CH}_0(X)$,

the Chow group of 0-cycles of $X$, obeys a local-to-global principle. This conjecture remains widely open, in part due to its high sensitivity to the base field and the difficulty of explicitly computing $\mathrm{CH}_0(X)$. In this talk, we describe some surfaces $X$ given as self-products of elliptic curves for which a weaker version of this conjecture holds for an infinite family of base changes $L/K$. These examples are further interesting in that we can construct explicit non-trivial global lifts of local information.

Wing Hong Tony Wong, Kutztown University of Pennsylvania

Digital sums and variations

A positive integer $n$ is called a $b$-Niven number if $n$ is divisible by the sum of its digits in base-$b$ representation. It is known that the longest sequence of consecutive $b$-Niven numbers has length $2b$. Our project investigates $b$-Niven numbers within various arithmetic progressions. We further explore variations such as when $n$ is divisible by the product of its nonzero digits. This presentation is inspired by Helen Grundman's plenary talk at MASON IV, and several of the results to be presented in this talk are the product of a collaboration with her.