On the Limit Points of Certain Geometric Progressions modulo 1

Federico Accossato (Politecnico di Torino)

Abstract: A seminal result by Weyl states that for an irrational number a, the sequence $a, 2a, 3a, \dots$ is equidistributed modulo 1, meaning the proportion of terms $(\{na\})_n$ falling within any subinterval of $[0, 1)$ is equal to the length of that subinterval, where $\{\cdot\}$ denotes the fractional part. Many other sequences are known to be equidistributed in $\mathbb{R}/\mathbb{Z}$. For instance, geometric progressions of the form $(\xi\alpha^n)_n$ are uniformly distributed modulo 1 for a fixed $\xi > 0$ and almost every $\alpha > 1$, or conversely, for a fixed $\alpha > 1$ and almost every $\xi > 0$. When both α and ξ are fixed, the problem becomes significantly more challenging. A theorem by Pisot states that, if α is algebraic, then such a sequence has finitely many limit points if and only if α is a Pisot number and $\xi \in \mathbb{Q}(\alpha)$. A fascinating problem arising from this context is whether, given a Pisot number α, one can find a ξ such that the geometric progression modulo 1 has a prescribed number of limit points. This question is closely related to the problem of identifying linear recurrences with a fixed characteristic polynomial that exhibit a predetermined number of residues modulo an integer. The aim of this talk is to delve deeper into these problems and present some recent findings in this area.

Lucas Atoms: a new definition and their p-adic valuations

Gessica Alecci (Politecnico di Torino)

Abstract: In 2020, Sagan and Tirrell introduced Lucas atoms, which are irreducible factors of Lucas polynomials. The main aim of the authors was to investigate when some combinatorial rational functions are actually polynomials. In this joint work with Piotr Miska, Nadir Murru, and Giuliano Romeo, we introduce them in a more natural and powerful way than the original definition, providing straightforward proofs of their main properties. Moreover, we fully characterize the p-adic valuations of Lucas atoms for any prime p, answering a problem left open by Sagan and Tirrell. Finally, we prove that the sequence of Lucas atoms is not holonomic, in contrast to the Lucas sequence, that is a linear recurrent sequence of order two.

Transcendence in ♠ words: an analogous of a theorem of Bugeaud in the p-adic setting

Laura Capuano (Università Roma Tre)

Abstract: A result of Bugeaud asserts that, whenever a real number α has a continued fraction expansion whose sequence of partial quotients has a "very regular" form (for example, it is an automatic sequence or a sturmian word), then α is either quadratic or transcendental. Bugeaud's proof strongly relies on Schmidt subspace theorem, which is a celebrated result in diophantine approximation that can be seen ad a higher dimensional analogue of Thue-Siegel-Roth theorem. In this talk we will see how similar ideas can be applied to deduce an analogue of Bugeaud's result in the p-adic setting. This Is a joint work in progress with S. Checcoli. M. Mula and L. Terracini.

Cyclo-multiquadratic fields: fast polynomial arithmetic and homomorphic encryption

Iván Blanco Chacón (University of Alcalá - Madrid)

Abstract: In this talk we discuss cyclo-multiquadratic number fields, which are extensions of cyclotomic fields by quadratic roots of certain primes. In recent joint work with Pedrouzo-Ulloa, Barbero and Njah, we have introduced these fields to obtain a homomorphic encryption scheme which offers a reasonable theoretical security while keeping the complexity provided by the Number Theoretical Transform (NTT). In particular, the Polynomial Learning with Errors (PLWE) and Ring Learning with Errors (RLWE) problems are equivalent for this family of field and swapping between NTT and coefficient representations can be achieved at least twice faster than for the usual cyclotomic family. We will sketch these facts and discuss our ongoing research.

p-Adic periods in Chabauty-Kim theory

Ishai Dan-Cohen (Ben-Gurion University of the Negev)

Abstract: For X a smooth scheme over an arithmetic base and p a prime of good reduction, Chabauty-Kim theory uses various unipotent completions of the fundamental group to construct certain locally analytic functions on the space of p-adic points of X. These functions, known as "Kim functions", are typically presented as linear combinations of p-adic iterated integrals over the p-adic numbers. The iterated integrals themselves are in a certain sense rationally defined, while the coefficients tend to be highly transcendental.

Kim functions are particularly well understood in the mixed Tate setting, due, in large part, to the availability of a theory of p-adic periods of mixed Tate motives. In ongoing joint work with David Corwin, we extend aspects of this theory beyond the mixed Tate setting, with particular emphasis on the "mixed elliptic" case. As an application worked out by Corwin, we obtain new information on Kim functions for certain punctured elliptic curves. Their coefficients have yet to be understood.

Manin-Mumford Problem and homotheties in l-adic representations

Aurélien Galateau (Cergy Paris Université)

Abstract: I will explain how classical estimates on the group of homotheties in the l-adic representation associated to the torsion of an abelian variety translate into a uniform bound on the torsion locus of a subvariety. I will also say a word about the distribution of small points.

Multivariate cryptography and the hardness of polynomial system solving

Elisa Gorla (Universities of Neuchatel)

Abstract: Multivariate cryptography belongs to post-quantum cryptography, which is the branch of cryptography which remains secure even in the presence of a quantum computer. After introducing motivating the need for post-quantum cryptography, I will discuss the role played by commutative algebra techniques in multivariate cryptography. The security of multivariate cryptographic primitives relies on the hardness of computing the solutions of multivariate polynomial systems over finite fields. Since we can compute the solutions of a polynomial system from its Groebner basis, bounds on the complexity of Groebner bases computations provide bounds on the security of the corresponding multivariate cryptographic primitives. In this talk, I will introduce and discuss some algebraic invariants which play a role in these security estimates and motivate their importance in this applied setting.

Lifting problem for universal quadratic forms

Vítězslav Kala (Charles University - Prague)

Abstract: A quadratic form is universal if it represents all the positive integers; the most well-known example being the sum of four squares over the integers $\mathbb{Z}$. In my talk, I'll start with a brief overview of universal quadratic forms over number fields. Then I'll mostly focus on the lifting problem for universal forms, ie, on the question "when can a quadratic form with coefficients from a given number field be universal over a larger field?" (Based on joint works with Daejun Kim, Seok Hyeong Lee, and Pavlo Yatsyna.)

Rational angles in plane lattices

Davide Lombardo (Università di Pisa)

A lattice is a discrete subgroup of $\mathbb{R}^2$ isomorphic to $\mathbb{Z}^2$. It is a natural question to investigate all 'nice' configurations of points that can be found in a lattice, such as regular polygons with all their vertices on lattice points. In joint work with Roberto Dvornicich, Francesco Veneziano and Umberto Zannier, we classify more generally all plane lattices whose points form three or more (genuinely distinct) angles with amplitude a rational multiple of π. The underlying number-theoretic problem is a Diophantine equation in several unknowns, some of which are constrained to be rational numbers, while others are roots of unity. To solve this equation, we combine the general theory of vanishing sums of roots of unity, a Galois-theoretic technique to reduce the resulting bounds, and a direct study of rational points on several curves of genus up to 5.

Zeta and L-functions in function field arithmetic

Federico Pellarin (Università di Roma La Sapienza)

Abstract: This talk deals with analytic functions interpolating zeta and L-values, fundamental in number theory. In the years 1980 David Goss introduced a class of zeta and L-values in function field arithmetic. They can be associated to eg. representations of the absolute Galois group of a global field of positive characteristic through the torsion of a Drinfeld module, and generalize the variants of zeta values previously introduced by Carlitz in the years 1930. Along with this class of zeta values, Goss also introduced some sort of recipe to construct analytic interpolation. In this talk we are going to discuss another way to interpolate these values, by constructing certain rigid analytic functions over curves defined over finite fields and we will explain how certain arithmetic properties emerge from the study of these functions

Rational distances from given points in the plane

Amos Turchet (Università Roma Tre)

Abstract: We consider sets of points in the plane with rational distances from a prescribed finite set of n rational points. These sets are closely related to papers of Anning and Erdös in the 40s and motivated the well-known and still open Erdös-Ulam problem. In our setting we show that for $n \leq 3$, the points are dense in the real topology. On the other hand, for $n \geq 4$, we show that they correspond to rational points in a surface of general type, hence conjecturally degenerate. This is joint work with Pietro Corvaja and Umberto Zannier.

Diagonal classes, Yoshida lifts, and rational points on elliptic curves

Rodolfo Venerucci (Università di Milano)

Abstract: I will report on joint ongoing work with Andreatta, Bertolini and Seveso, addressing the equivariant Birch and Swinnerton-Dyer conjecture for a rational elliptic curve over the number fields cut out by certain self-dual Artin representations of dimension at most 4. Our key tool is the Yoshida endoscopic lift for $GSp(4)$, which associates genus-two Siegel modular forms with appropriate pairs of elliptic modular forms.

Averages of the Liouville and Möbius functions

Alessandro Zaccagnini (Università di Parma)

Abstract: I will talk of various types of averages of arithmetical functions. In particular, I will apply a technique introduced in a recent joint paper with Marco Cantarini and Alessandro Gambini to the functions mentioned in the title.