Dynamics and Graphs over Finite Fields: Algebraic, Number Theoretic and Algorithmic Aspects

CIRM, Luminy

29 March – 2 April, 2016

ABSTRACTS OF PLENARY TALKS

1. **William Banks**,

   Primes, exponential sums, and L-functions

   Abstract: This talk will survey some recent directions in the study of prime numbers that rely on bounds of exponential sums and advances in sieve theory. I will also describe some new results on the Riemann zeta function and Dirichlet functions, and pose some open problems.

2. **Yuri Bilu and Florian Luca**,

   Diversity in parametric families of number fields

   Abstract: Let $f(x,t) \in \mathbb{Q}[x,t]$ be a polynomial with $\deg f_x = D \geq 2$. For each positive integer n let x_n be a root of $f(x,n)$. Dvornicich and Zannier proved that

   $$\log[\mathbb{Q}[x_1,\ldots,x_N]:\mathbb{Q}] \gg \frac{N}{\log N}.$$

   In particular, putting

   $$\mathcal{F}_f(N) = \{\mathbb{Q}[x_m] : 1 \leq m \leq N\},$$

   it follows that

   $$\#F_f(N) \gg \frac{N}{\log N}.$$

   In this double-talk, we shall first explain the Dvornicich–Zannier argument, then we show how the last conclusion above can be improved to

   $$\#F_N \gg \frac{N}{(\log N)^{1-c}}$$

   where $c := c(D) > 0$ is a positive constant depending on D, but not on f. The main ingredient of the proof of the improvement consists on counting special divisors of values of polynomials with integer coefficients.

3. **Jean-Marc Deshouillers**,

   Sarnak's conjecture and automatic sequences

   Abstract: We present a joint work with Michael Drmota and Clemens Muellner (Vienna). Sarnak's conjecture (in short, concerning some independence between the Möbius function and any other kind of naturally defined sequence) should hold for deterministic sequences, among other the so-called "automatic sequences". We indeed show that this is the case for almost all the automatic sequences, namely those which are produced by a "synchronizing" automaton. We shall also give some results concerning some other cases.

4. **Sergei Konyagin**,

   Number of nontrivial solutions of an equation with reciprocals

   Abstract: I will discuss our joint results with M. A. Korolev on an upper estimate for the number of nontrivial solutions to the equation

   $$\frac{1}{x_1} + \cdots + \frac{1}{x_r} = \frac{1}{y_1} + \cdots + \frac{1}{y_r}$$

   where $x_1, \ldots, x_r, y_1, \ldots, y_r$ are positive integers not exceeding N. A solution is said to be a nontrivial if $(y_1, \ldots, y_r)$ is not a permutation of $(x_1, \ldots, x_r)$.

5. **Par Kurlberg**,

   Missing class groups and class number statistics for imaginary quadratic fields

   Abstract: The number $F(h)$ of imaginary quadratic fields with class number h is of classical interest: Gauss' class number problem asks for a determination of those fields counted by $F(h)$. The unconditional computation of $F(h)$ for $h \leq 100$ was completed by M. Watkins, and K. Soundararajan has more recently made conjectures about the order of magnitude of $F(h)$ as $h \to \infty$ and determined its average order.

   For odd h we refine Soundararajan's conjecture to a conjectural asymptotic formula and also consider the subtler problem of determining the number $F(G)$ of imaginary quadratic fields with class group isomorphic to a given finite abelian group G.

   Using Watkins' tables, one can show that some abelian groups do *not* occur as the class group of any imaginary quadratic field (for instance $(\mathbb{Z}/3\mathbb{Z})^3$ does not). This observation is explained in part by the Cohen-Lenstra heuristics, which have often been used to study the distribution of the *p-part* of an imaginary quadratic class group. We combine the Cohen-Lenstra heuristics with a refinement of Soundararajan's conjecture to make precise predictions about the asymptotic nature of the *entire* imaginary quadratic class group, in particular addressing the above-mentioned phenomenon of "missing" class groups, for families of p-groups as p tends to infinity. For instance, it appears that *no* groups of the form $(\mathbb{Z}/p\mathbb{Z})^3$ and p prime occurs as a class group of a quadratic imaginary field.

   Conditionally on the Generalized Riemann Hypothesis, we extend Watkins' data, tabulating $F(h)$ for odd $h \leq 10^6$ and $F(G)$ for G a p-group of odd order with $|G| \leq 10^6$. (To do this, we examine the class numbers of all negative prime fundamental discriminants $-q$, for $q \leq 1.1881 \cdot 10^{15}$.) The numerical evidence matches quite well with our conjectures.

   This is joint work with S. Holmin, N. Jones, C. McLeman, and K. Petersen.

6. **Winnie Li**,

   Unramified graph covers of finite degree

   Abstract: Given a finite connected undirected graph X, its fundamental group plays the role of the absolute Galois group of X. The familiar Galois theory holds in this setting. In this talk we shall discuss graph theoretical counter parts of several important theorems for number fields. Topics include

   (a) Determination, up to equivalence, of unramified normal covers of X of given degree,

   (b) Criteria for Sunada equivalence,

   (c) Chebotarev density theorem.

   This is a joint work with Hau-Wen Huang.

7. **Christian Mauduit**,

   Digits and pseudo-randomness

   Abstract: In this talk, we will present several recent results and open problems concerning digital representation of some subsequences of natural integers and of polynomials over finite fields.

8. **Pieter Moree**,

   Cyclotomic coefficients: progress and promise

   Abstract: The study of coefficients of cyclotomic polynomials has seen the last 10 years a flurry of activity, predominantly by very young mathematicians. I give a survey of these developments and will mention some promising open problems. Further I discuss a very recent paper (*J. Number Theory* **163** (2016), 211–237) involving also more seasoned mathematicians, namely, F. Luca, the speaker and I. Shparlinski.

9. **Daniel Panario**,

   Periods of iterations of mappings over finite fields with indegrees restricted to $\{0, k\}$

   Abstract: The study of iterations of functions over a finite field and the corresponding functional graphs is a growing area of research with connections to cryptography. The behaviour of such iterations is frequently approximated by what is known as the Brent-Pollard heuristic, where one treats functions as random mappings. This idea was considered by Pollard; he conjectured that quadratic polynomials behave like random mappings with respect to their average rho length. However, the class of $\{0, 2\}$-mappings where the indegree are 0 or 2, could provide a better model for quadratic polynomials due to the similarities between the indegree distribution of these classes. The class of $\{0, k\}$-mappings provides not only a good heuristic model for quadratic polynomials (when $k = 2$) but also for polynomials of the form $x^k + a \in \mathbb{F}_p[x]$ with $p \equiv 1 \pmod{k}$. We aim at understanding Brent-Pollard heuristic for the period of $\{0, k\}$-polynomials.

   We consider the period $\mathbf{T}(f)$ of the sequence of compositions of a mapping f on n nodes. The parameter $\mathbf{T}(f)$ equals the order of the permutation obtained by restricting the mapping f to its cyclic vertices. If φ is a mapping, then $\mathbf{T}(\varphi)$ is the least common multiple of the length of the cycles of φ. Harris (1973) proved that, when properly normalized, the distribution of $\log \mathbf{T}$ converges to the Gaussian distribution. Schmutz (2011) gives an asymptotic estimate for the expected value of $\mathbf{T}$ over all mappings on n nodes.

   In this talk we show that similar estimates to the ones in Schmutz hold when we restrict to the classes of $\{0, k\}$-mappings, for some $k \geq 2$. More precisely we show, for $k_0 \approx 3.36$, that

   $$\log \mathbb{E}_n^{\{0,k\}}[\mathbf{T}] \sim k_0 \cdot \sqrt[3]{\frac{n}{k-1}} \cdot \frac{1}{\log^{2/3} n}.$$

   We also consider the associated parameter $\mathbf{B}$ defined as follows: if φ is a mapping, then $\mathbf{B}(\varphi)$ is the product of the length of the cycles of φ. We show that in this case

   $$\log \mathbb{E}_n^{\{0,k\}}[\mathbf{B}] \sim \frac{3}{2} \cdot \sqrt[3]{\frac{n}{k-1}}.$$

   We provide experimental results about the parameters $\mathbf{T}$ and $\mathbf{B}$ for $\{0, k\}$-polynomials.

   Joint work with Rodrigo S. V. Martins, Claudio Qureshi and Eric Schmutz.

10. **John Roberts**,

    Arithmetic aspects of piecewise linear dynamics

    Abstract: On both the planar rational lattice and on the toral rational lattice with prime denominator, we consider dynamics induced by the action of a word in two matrices that is generated by a piecewise dynamics. We describes results and conjectures concerning:

(i) the growth of rational orbits in the planar case, as described by arithmetic exponents;

(ii) the periods of the dynamics on the prime toral lattice; and

(iii) the divisibility of rational orbits, i.e. the appearance and recurrence of certain primes in the coordinates.

11. **Ilya Shkredov**,

    On multiplicative properties of difference sets

    Abstract: We prove that for any finite set $A \subset \mathbb{R}$ its difference set $D := A - A$ has large product set and quotient set, namely, $|DD|, |D/D| \gg |D|^{1+c}$, where $c > 0$ is an absolute constant. Similar result has place in the prime field $\mathbb{F}_p$ for sufficiently small D. Also we discuss some connected questions of representations of multiplicative subgroups as sumsets/difference sets. Our method gives, in particular, that multiplicative subgroups of the size less than $p^{4/5-\varepsilon}$ cannot be represented in the form $A - A$ for any $A \subset \mathbb{F}_p$.

12. **Christopher Smyth**,

    Describing integer sequences multiplicatively

    Abstract: I describe a recently-developed method for specifying the elements of an infinite increasing sequence of positive integers. While all such sequences can be described by this method, it works particularly well for those having a nice multiplicative structure. I illustrate the method with families of sequences related to Lucas sequences. I also discuss work of Shparlinski et al., where the authors give upper and lower estimates for the density of these sequences.

13. **Cameron Stewart**,

    Polynomial congruences and trees

    Abstract: In this talk we shall discuss joint work with W. Schmidt on trees which are associated with solving polynomial congruences modulo powers of primes.

14. **Franco Vivaldi**,

    Hamiltonian stability over discrete spaces

    Abstract: Dynamical stability in two-dimensional Hamiltonian systems (smooth area-preserving maps) hinges on the existence of invariant circles, which confine orbits in phase space. This is the content of KAM theory, developed some decades ago. Since then, Hamiltonian systems over discrete spaces have been investigated by many researchers, and for many different reasons. Here invariant circles are seldom relevant, and the stability problem must be re-considered from scratch. At present we don't have a coherent body of knowledge on this class of phenomena. I will survey some constructs, few results, and many open questions.

15. **Felipe Voloch**,

    Generators of elliptic curves over finite fields

    Abstract: We will discuss some problems and results connected with finding generators for the group of rational points of elliptic curves over finite fields and connect this with the analogue for elliptic curves over function fields of Artin's conjecture for primitive roots.

16. **Thomas Ward**,

    Two classes of dynamically defined integer sequences

    Abstract: I will give a brief overview of some of the arithmetic, functorial, and analytic questions that come up in trying to understand the collection of integer sequences that arise as periodic point counts for iteration of maps and of compact group automorphisms. In particular I will describe a (conjectural) Polya-Carlson dichotomy in this setting.