Arithmetic statistics over finite fields and function fields

organized by
Alina Bucur, Chantal David, and Jordan Ellenberg

Workshop Summary

This workshop was devoted to the study of statistical questions about objects of arithmetic geometry, especially algebraic varieties over function fields and finite fields. The analogy between function fields and number fields has been a rich source of insights throughout the modern history of number theory. In this setting, three active directions of number theory and algebraic geometry meet. The first direction is techniques imported from classical analytic number theory, which often must be modified and improved in the function field setting (sieve methods, Hardy-Littlewood method, etc.) The second direction is the theory of random matrices, which in this setting involves not only the much-studied properties of random complex matrices but those of random ℓ-adic matrices as well. Finally, following Katz-Sarnak, arithmetic statistical questions over function fields can often be phrased as problems of counting $\mathbb{F}_q$-rational points on moduli schemes defined over $\mathbb{Z}$: such problems are deeply connected with the algebraic geometry and algebraic topology of the manifolds formed by the complex points on these moduli spaces.

The workshop was run in the usual AIM style, with two talks in the morning separated by a break and time in the afternoon for working in groups. The first talk was given by Bjorn Poonen and focused on the Bhargava-Kane-Lenstra-Poonen-Rains heuristics giving a model for the distribution of Selmer groups, Tate-Shafarevich groups and rank of elliptic curves in terms of intersections of maximal isotropic subspaces. The second talk, by Melanie Matchett Wood, focused on point count statistics for curves over finite fields. One of the main points discussed was under which conditions can we hope for a distribution given by a sum of independent and identically distributed random variables for the number of points over curves in some family. On Tuesday, the talks were given by Jon Keating and Alexei Entin and took a more analytic approach, concentrating on mean and variance of arithmetical functions over function fields in short intervals, and one-level densities in families of curves over finite fields with application to the number field setting. On Wednesday, the first talk, by Nick Katz, explained the geometry behind the connection between statistics for families of curves of fixed genus over finite fields and random matrix theory that underlines the Katz-Sarnak philosophy. The second talk was given by Jordan Ellenberg who gave an impromptu talk on how to use topology and stable cohomology of moduli spaces to understand arithmetic statistics questions over function fields, focusing on questions which were addressed already in the other talks and discussions, but from a different viewpoint. On Thursday, the talks were given by Paul Pollack (about finite field analogues of classical analytical number theory questions) and by Rachel Pries (about new results for Hurwitz spaces obtained by Pries and Turkelli). By popular demand, Friday morning Poonen explained further the Bhargava-Kane-Lenstra-Poonen-Rains model and the rest of the time was taken by the wrap-up session and research in groups.

Some of the more notable topics discussed in the research groups are listed below.

- *Extensions of the Bhargava-Kane-Lenstra-Poonen-Rains (BKLPR) heuristics*
  The group developed a version of the BKLPR heuristics [bkplr] with $\mathbb{Z}_p$ replaced by $\mathbb{Z}$, counting up to height B. They used the rank 2 case, where other heuristics are known, to calibrate B with the height used when counting elliptic curves, and then use that calibration to make a predictions for the number of curves of rank 3 (and higher rank) in the family of all elliptic curves over $\mathbb{Q}$, and in families of quadratic twists.

- *Geometric Poonen-Rains and Bhargava-Kane-Lenstra-Poonen-Rains statistics.*
  The group discussed analogues of the Poonen-Rains [pr] and BKLPR [bkplr] conjectures over function fields, focusing in particular on the question: given an elliptic curve $E/\mathbb{F}_q(t)$, is there a natural moduli space $X_{E,n}$ over $\mathbb{F}_q$ such that the point count $|X_{E,n}(\mathbb{F}_q)|$ computes the average size of the mod ℓ Selmer group of a random twist of E by a squarefree polynomial of degree n? We were able to show that such a space exists under mild conditions on E; then the "large q limit" of the Poonen-Rains conjecture, by Weil II, comes down to a computation of the connected components of this space, which in turn reduces to a statement about the monodromy in H^2 of certain families of elliptic surfaces. Fortunately, Chris Hall was in attendance at the workshop, and explained to us that the relevant monodromy statements had already been proven by him in a published paper! Some subset of the participants, possibly in collaboration with students, will write this up.

- *Point counting for $\mathbb{Z}/3\mathbb{Z}$-covers of $\mathbb{P}^1$ over a finite $\mathbb{F}_q$ by the whole genus*
  The point count in [bdfl] for cyclic trigonal curves was done by the signature of the cyclic covering map, not the whole genus. The method employed made use of the sums of the cubic characters associated to these covers. The goal of this research group was to use the results about cubic field extensions from [woodabelian] to compute the distribution of the number of points of a $\mathbb{Z}/3\mathbb{Z}$ cover of $\mathbb{P}^1$ of genus g as $g \to \infty$ and compare with the statistics from [bdfl].

- *Bounded gaps over $\mathbb{F}_q(t)$.*
  A group looked at the recent breakthrough paper of Maynard [maynard] proving bounded gaps between k primes, and tried to see if Maynard's sieve can be done over function fields, i.e. proving that there are infinitely many sets of k prime polynomials such the difference of their degrees is absolutely bounded by a constant B_k. The conclusion seems to be that everything can be translated in the function field setting, and that one actually gets also the same quantitative results (the same order of magnitude for the constants B_k).

- *Conjectures about the moments of $L(1/2, \chi_d)$ over function fields.*
  The goal is to gather sufficient numerical data to test the recent conjectures of Andrade and Keating about the moments of special values of L-functions over function

fields. As far as we know, the computer is still running on that.

- *Variance of arithmetic functions sums over short intervals in $q \to \infty$ limit.*

  The focus was made on the special arithmetic functions $d_k(n)$, $\Lambda(n)$, $\mu(n)$. This was studied by two different approaches; using the tools of analytic number theory over function fields, as in a recent paper of Keating and Rudnick [kr], and or with a geometric approach, as sketched by Ellenberg in his Wednesday morning talk. Both groups seem to be confident to get new results.

Other interesting research avenues were proposed, as local statistics for zeros for L-functions of orthogonal type, but were not studied during the workshop because of lack of time. Several of the research groups are continuing to work actively on the projects started at AIM, and are optimistic about getting new results for statistics over finite fields.

Bibliography

[bklpr] M. Bhargava, D. Kane, H.W. Lenstra jr, B. Poonen and E. Rains, *Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves*, preprint, arXiv:1304.3971.

[bdfl] A. Bucur, C. David, B. Feigon and M. Lalín, *Statistics for traces of cyclic trigonal curves over finite fields*, Int. Math. Res. Not. IMRN 2010, no. 5, 932–967.

[kr] J.P. Keating and Z. Rudnick, *The variance of the number of prime polynomials in short intervals and in residue classes*, Int. Math. Res. Not. IMRN 2012; doi: 10.1093/imrn/rns220.

[maynard] J. Maynard, *Small gaps between primes*, preprint, arXiv:1311.4600.

[pr] B. Poonen and E. Rains, *Random maximal isotropic subspaces and Selmer groups*, J. Am. Math. Soc. 25 (2012), no. 1, 245–269.

[woodabelian] M.M. Wood, *On the probabilities of local behaviors in abelian field extensions*, Compos. Math. 146 (2010), no. 1, 102–128.