NUMBER FIELDS AND FUNCTION FIELDS: COALESCENCES, CONTRASTS AND EMERGING APPLICATIONS

J.P. KEATING, Z. RUDNICK AND T.D. WOOLEY

Abstract. The similarity between the density of the primes and the density of irreducible polynomials defined over a finite field of q elements was first observed by Gauss. Since then, many other analogies have been uncovered between arithmetic in number fields and in function fields defined over a finite field. Although an active area of interaction for the past half century at least, the language and techniques used in analytic number theory and in the function field setting are quite different, and this has frustrated interchanges between the two areas. This situation is currently changing and there has been substantial progress on a number of problems stimulated by bringing together ideas from each field. We here introduce the papers published in this Theme Issue, where some of the recent developments are explained.

1. Introduction

The similarity between the density of the primes and the density of irreducible polynomials defined over a finite field of q elements was first observed by Gauss as early as 1797. Since then, many other analogies have been uncovered between arithmetic in number fields and in function fields defined over a finite field. In several cases, problems in the function field setting have proved easier to solve; for example, Weil, in the 1940's, and Deligne, in the 1970's, established function-field analogues of the Riemann Hypothesis.

Although an active area of interaction for the past half century at least (see, for example, the excellent textbook [10], detailing the connections), the language and techniques used in analytic number theory and in the function

Date: January 26, 2015.

We thank the Royal Society for the support of the Theo Murphy international scientific meeting on *Number fields and function fields: coalescences, contrasts and emerging applications*, held at the Kavli Royal Society International Centre for the Advancement of Science at Chicheley Hall, 29–30 May 2014, which was the origin of this Theme Issue.

JPK gratefully acknowledges support under EPSRC Programme Grant EP/K034383/1 LMF: L-Functions and Modular Forms, a grant from Leverhulme Trust, a Royal Society Wolfson Merit Award, a Royal Society Leverhulme Senior Research Fellowship, and by the Air Force Office of Scientific Research, Air Force Material Command, USAF, under grant number FA8655-10-1-3088. ZR is similarly grateful for support from the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013) / ERC grant agreement n° 320755, and from the Israel Science Foundation (grant No. 925/14).

field setting are quite different, and this has frustrated interchanges between the two areas. In the past 20 years, the work of Katz and Sarnak [9] on the statistical distribution of the zeros of L-functions in function fields and number fields has proved a major stimulus to strengthening links. This move to find and exploit common ground has accelerated in recent years, leading to considerable progress on a number of problems.

This Theme Issue focuses on some of the areas where connections between ideas from analytic number theory and function fields are currently proving fruitful and interesting. Our aim here is to introduce the papers that follow, in which these recent developments are explored in more detail.

2. Arithmetic Statistics

Two papers, [2] and [4], address a recurrent theme, that of correlations between values of arithmetic functions, obtaining results in the function field case to lend support to conjectures made over the integers.

The paper [2] by Andrade, Bary Soroker and Rudnick studies analogues of some classical problems in analytic number theory, concerning the autocorrelations of divisor functions, in the setting of the ring of polynomials $\mathbb{F}_q[t]$ over a finite field of q elements. Denoting by $d_k(f)$ the number of representations of a monic polynomial $f \in \mathbb{F}_q[t]$ as a product of k monic polynomials, they study the asymptotic behaviour of autocorrelation functions such as

$$q^{-n} \sum_{\deg f = n} d_k(f) d_k(f+1),$$

where f runs over all monic polynomials of degree n. In the limit $q \to \infty$, it is shown that these autocorrelation sums behave as though $d_k(f)$ and $d_k(f+1)$ were independent. The corresponding problems over the integers for $k \geq 3$ are currently open.

A key ingredient behind the results is that the cycle structure of f and its shift $f+1$ are independent: for $f \in \mathbb{F}_q[t]$ of positive degree n, we say its cycle structure is $\lambda(f) = (\lambda_1, \dots, \lambda_n)$ if in the prime decomposition of f there are exactly λ_j primes of degree j. Thus we get a partition of n. The independence result is the statement that for fixed n, given partitions λ_1, λ_2 of n, then as $q \to \infty$ we have

$$q^{-n} \#\{f \in \mathcal{M}_n : \lambda(f) = \lambda_1, \lambda(f+1) = \lambda_2\} = p(\lambda_1)p(\lambda_2) + O\left(q^{-\frac{1}{2}}\right), \tag{1}$$

where $p(\lambda)$ is the probability that a random permutation on n letters has cycle structure λ. For q even, the proof of (1) requires the results of the paper by Carmon [4] in this volume, which deals with autocorrelation of the Möbius function in $\mathbb{F}_q[t]$, and especially deals with the even characteristic case, which is exceptional in this context. The results obtained are analogues of a conjecture of Chowla over the integers, which is widely viewed as inaccessible by current techniques and ideas.

Another paper deals with arithmetic statistics in families of curves defined over a fixed finite field and growing genus. Achter, Erman, Kedlaya, Wood and Zureick-Brown [1] study how many rational points there are on a random algebraic curve of large genus g over a given finite field $\mathbb{F}_q$. The authors propose a heuristic for this question motivated by a (now proven) conjecture of Mumford on the cohomology of moduli spaces of curves; this heuristic suggests a Poisson distribution with mean $q + 1 + 1/(q - 1)$. The paper establishes a weaker version of this statement in which g and q tend to infinity, with q much larger than g.

3. Square-Root Cancellation

The paper by Fouvry, Kowalski and Michel [7] describes some general situations in analytic number theory in which a square-root cancellation phenomenon for exponential sums over finite fields occurs. In numerous calculations in analytic number theory, obtaining such a cancellation (or even sometimes just any cancellation) is crucial. It is very often the case that in such situations deep algebro-geometric tools come into play. Unfortunately although many books and papers about ℓ-adic sheaves and Deligne's general treatment of exponential sums over finite fields using such sheaves are available, very few of them are written in a language easily accessible to non-experts. The paper presents some of the methods of Deligne, Katz and others to the working analytic number theorist who is not familiar with the subtleties of this intricate algebraic machinery. As a motivation, the authors consider the general question of showing strong orthogonality for the product of several different Kloosterman sums against an additive character.

The paper by Katz [8] also examines the issue of square-root cancellation in remainder terms, dealing with remainders which arise when computing moments of certain exponential/character sums over a large finite field. Examples are presented when such cancellation occurs and when it does not.

4. Moments of zeta functions

In the paper [11], Rubinstein and Wu study moments of zeta functions associated to hyperelliptic curves over finite fields. They provide theoretical and numerical evidence in favour of a recent conjecture by Andrade and Keating [3] about moments of central values of quadratic Dirichlet L-functions over function fields. The authors also are able to compute exact formulas for the moments in some particular cases and to determine the size of the remainder term in the predicted moments.

The paper by Conrey and Keating [6] revisits the long-standing problem of determining the moments of the Riemann zeta function on the critical line, bringing together the conventional approach of analytic number theorists via Dirichlet polynomial approximations to $\zeta(s)$ and $\zeta(s)^k$; and detailed conjectures by Conrey, Farmer, Keating, Rubinstein and Snaith [5]. The Dirichlet polynomial approach completely fails when considering the 10th

or higher moment of $\zeta(s)$ on the critical line: it predicts negative values when the moments are clearly non-negative. The aim here is to illustrate the nature and cause of this failing by an analysis of the second and fourth moments.

References

[1] J. Achter, D. Erman, K. Kedlaya, M. Matchett Wood and D. Zureick-Brown, *A heuristic for the distribution of point counts for random curves over a finite field.*

[2] J. C. Andrade, L. Bary Soroker and Z. Rudnick, *Shifted convolution and the Titch-marsh divisor problem over* $\mathbb{F}_q[t]$.

[3] J. C. Andrade and J.P. Keating *Conjectures for the integral moments and ratios of L-functions over function fields*, J. Number Theory 142, 102–148 (2014).

[4] D. Carmon, *The Autocorrelation of the Möbius Function and Chowla's Conjecture for the Rational Function Field in Characteristic* 2.

[5] J. B. Conrey, D.W. Farmer, J.P. Keating, M.O. Rubinstein and N.C. Snaith, *Integral moments of L-functions*, Proc. London. Math. Soc., 91, 33–104 (2005).

[6] J.B. Conrey and J.P. Keating, *Moments of zeta and correlations of divisor-sums: I.*

[7] É. Fouvry, E. Kowalski and P. Michel, *A study in sums of products.*

[8] N. M. Katz, *On a question of Rudnick: do we have square root cancellation for error terms in moment calculations?*

[9] N. M. Katz and P Sarnak, *Random Matrices, Frobenius Eigenvalues, and Monodromy*, American Mathematical Society, Colloquium Publications 45 (1998).

[10] M. Rosen, *Number Theory in Function Fields*, Graduate Texts in Mathematics 210, Springer-Verlag (2002).

[11] M.O. Rubinstein and K. Wu, *Moments of zeta functions associated to hyperelliptic curves over finite fields.*

School of Mathematics, University of Bristol, Bristol BS8 1TW, UK
E-mail address: j.p.keating@bristol.ac.uk
E-mail address: trevor.wooley@bristol.ac.uk

Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel
E-mail address: rudnick@post.tau.ac.il