Summer School on Galois Theory and Number Theory
Konstanz, July 18-24, 2015

STATISTICAL NUMBER THEORY IN FUNCTION FIELDS

Lior Bary-Soroker

School of Mathematical Sciences

Tel Aviv University

Contents

1 Survey of Mini-Course

The polynomial ring $\mathbb{F}_q[T]$ over a finite field $\mathbb{F}_q$ shares several properties with the ring of integers; for instance a qualitative aspect is that it has unique factorization into irreducibles. A quantitative aspect is an analogue of the Prime Number Theorem (PNT), namely the Prime Polynomial Theorem (PPT). Recall that if $\pi(x)$ denotes the number of primes up to x, then the PNT asserts that

$$\pi(x) \sim \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x}, \qquad x \to \infty. \tag{1}$$

Analogously, let $\pi_q(n)$ be the number of monic irreducible polynomials in $\mathbb{F}_q[T]$ of degree n. Then the PPT asserts that

$$\pi_q(n) = \frac{q^n}{n} + O(q^{n/2}/n), \tag{2}$$

where the implied constant is absolute. Here x corresponds to q^n and $\log x$ to n; so the analogy becomes apparent.

This mini-course concerns further quantitative analogues that were obtained recently.

One problem that the mini-course will address and provide a proof of a function field analogue is the Hardy-Littlewood prime tuple conjecture: Given an arithmetic function $f\colon \mathbb{Z} \to \mathbb{C}$ we defined its mean value to be the asymptotic value of

$$\langle f(n) \rangle_{n \le x} := \frac{1}{x} \sum_{n \le x} f(n).$$

Let $\lambda\colon \mathbb{Z} \to \mathbb{C}$ be the prime characteristic function; i.e. $\lambda(n) = 1$ if n is a prime number and $\lambda(n) = 0$ otherwise. Then the PNT can be rephrased as the following statement on the mean value of λ:

$$\langle \lambda(n) \rangle_{n \le x} \sim \frac{1}{\log x}, \qquad x \to \infty. \tag{3}$$

In this point of view, a natural problem is to compute the autocorrelations of λ. The Hardy-Littlewood prime tuple conjecture says that for an r-tuple $(a_1, \ldots, a_r)$ of distinct integers one has

$$\langle \lambda(n + a_1) \cdots \lambda(n + a_r) \rangle \sim \mathfrak{S}(a_1, \ldots, a_r) \frac{1}{(\log x)^r}, \qquad x \to \infty. \tag{4}$$

Here

$$\mathfrak{S}(a_1, \ldots, a_r) = \prod_p \left(\frac{1 - \nu(p) p^{-1}}{(1 - p)^{-r}} \right)$$

where $\nu(p)$ is the number of residues classes mod p that $a_1, \ldots, a_r$ cover. In other words, the events that the $n + a_i$ are simultaneously prime are independent up to the factor $\mathfrak{S}$.

We note that if $a_1, \ldots, a_r$ cover all residues modulo some prime p, i.e. $\nu(p) = p$, then $\mathfrak{S} = 0$. In this case, the left hand side in (4) also tends to zero (since $\lambda(n + a_1) \cdots \lambda(n + a_r) \neq 0$ for only finitely many n's). We consider these cases as trivial. In the nontrivial case; i.e., when $\nu(p) < p$ for all p, one may show that $\mathfrak{S}$ converges to a positive number.

Some special cases:

- When $r = 1$, (4) is the same as PNT. This is the only nontrivial case of (4) that is known.
- The simplest nontrivial case is when $r = 2$ and $(a_1, a_2) = (0, 2)$. If the conjecture was true, then in particular we would get infinitely many n's with $\lambda(n)\lambda(n+2) \neq 0$. But this would then imply that both n and $n+2$ are prime for infinitely many n's, which is the content of the twin prime conjecture.

Let us move to the ring $\mathbb{F}_q[T]$. Let $\mathcal{M}_{n,q} \subseteq \mathbb{F}_q[T]$ be the set of degree n monic polynomials, so $\#\mathcal{M}_{n,q} = q^n$. For an arithmetic function $\phi \colon \mathbb{F}_q[T] \to \mathbb{C}$ one defines the mean value as the asymptotic value of

$$\langle \phi(f) \rangle_{f \in \mathcal{M}_{n,q}} := \frac{1}{q^n} \sum_{f \in \mathcal{M}_{n,q}} \phi(f),$$

as $q^n \to \infty$. However, unlike for the ring $\mathbb{Z}$, here q^n may tend to infinity in various ways:

- large degree — $n \to \infty$
- large characteristic — $p = \mathrm{Char}(\mathbb{F}_q) \to \infty$
- fixed characteristic large finite field — $q = p^\nu$ and $\nu \to \infty$
- large finite field — $q \to \infty$
- mixed...

For the specific analogue of (4) nothing is known in the large degree limit (other than the PPT), however the large finite field limit was completely resolved in a series of works by Bary-Soroker, Bender-Pollack, and Carmon:

Theorem 1.1. *Let $n > 2$ be a fixed integer. Then*

$$\langle \lambda(f + a_1) \cdots \lambda(f + a_r) \rangle_{f \in \mathcal{M}_{n,q}} \sim \frac{1}{n^r}, \qquad q \to \infty$$

uniformly on all distinct $a_1, \dots, a_r \in \mathbb{F}_q[T]$ of degrees $\deg(a_i) < n$.

Bender and Pollack proved this theorem for $r = 2$ and q odd, Bary-Soroker used a different approach to prove the theorem under the assumption that q is odd, and Carmon dealt with the difficulties of the even characteristic case.

The principal goal of the mini-course is to explain the method used to prove this theorem, and used to resolve other function field analogues of other classical problems in number theory. This method is based on irreducible specialization theory (explicit Chebotarev theorem for function fields) and on Galois theory (calculation of monodromy groups).

1.1 References

The following references contain some introductory material that will be used/discussed in the mini-course

1. Rosen's *Number Theory in Function Fields*, Chapters 1-3
2. Serre's *Topics in Galois Theory*, Chapter 4
3. Appendix of *Shifted convolution and the Titchmarsh divisor problem over* $\mathbb{F}_q[t]$ by J. C. Andrade, L. Bary-Soroker, and Z. Rudnick

We will discussed the results and proofs of a (small) subset of the following papers:

1. J. C. Andrade, L. Bary-Soroker, and Z. Rudnick, Shifted convolution and the Titchmarsh divisor problem over $\mathbb{F}_q[t]$, to appear in Phil. Trans. of the Royal Society A.
2. E. Bank and L. Bary-Soroker, Prime polynomial values of linear functions in short intervals, arXiv:1410.1283, to appear in J. Numb. Theo.
3. E. Bank, L. Bary-Soroker, and L. Rosenzweig, Prime polynomials in short intervals over large finite fields, Duke Math. J., Volume 164, Number 2 (2015), 277-295
4. L. Bary-Soroker, Irreducible values of polynomials, Adv. Math., 229 (2), 854-874 (2012)
5. L. Bary-Soroker, Hardy-Littlewood tuple conjecture over large finite fields, Int. Math. Res. Not., 2012, Art. ID rns 249, 8 pp. (2012)
6. Andreas O. Bender, Paul Pollack, On quantitative analogues of the Goldbach and twin prime conjectures over $F_q[t]$, arXiv:0912.1702
7. D. Carmon, The autocorrelation of the Möbius function and Chowla's conjecture for the rational function field in characteristic 2, arXiv:1409.3694
8. Carmon, Dan; Rudnick, Zeev The autocorrelation of the Möbius function and Chowla's conjecture for the rational function field. Q. J. Math. 65 (2014), no. 1, 53–61.
9. A. Entin, On the Bateman-Horn conjecture for polynomials over large finite fields, arXiv:1409.0846