Some problems in analytic number theory for polynomials over a finite field

Zeev Rudnick [*]

Abstract.
   The lecture explores several problems of analytic number theory in the context of function fields over a finite field, where they can be approached by methods different than those of traditional analytic number theory. The resulting theorems can be used to check existing conjectures over the integers, and to generate new ones. Among the problems discussed are: Counting primes in short intervals and in arithmetic progressions; Chowla's conjecture on the autocorrelation of the Möbius function; and the additive divisor problem.

Mathematics Subject Classification (2010). Primary 11T55; Secondary 11N05, 11N13.

Keywords. Function fields over a finite field, Chowla's conjecture, the additive divisor problem, primes in short intervals.

1. Introduction

The goal of this lecture is to explore traditional problems of analytic number theory in the context of function fields over a finite field. Several such problems which are currently viewed as intractable over the integers, have recently been addressed in the function field context with vastly different tools than those of traditional analytic number theory, and the resulting theorems can be used to check existing conjectures over the integers, and to generate new ones. The problems that I will address concern

- Counting primes in short intervals and in arithmetic progressions

- Chowla's conjecture on the autocorrelation of the Möbius function

- The twin prime conjecture

- The additive divisor problem

- The variance of sums of arithmetic functions in short intervals and arithmetic progressions.

Before describing the problems, I will briefly survey some quantitative aspects of the arithmetic of the ring of polynomials over a finite field.

2. Background on arithmetic in $\mathbb{F}_q[x]$

2.1. The Prime Polynomial Theorem. Let $\mathbb{F}_q$ be a finite field of q elements, and $\mathbb{F}_q[x]$ the ring of polynomials with coefficients in $\mathbb{F}_q$. The polynomial ring $\mathbb{F}_q[x]$ shares several qualitative properties with the ring of integers $\mathbb{Z}$, for instance having a Euclidean algorithm, hence unique factorization into irreducibles. There are also several common quantitative aspects. To set these up, I review some basics.

The units of the ring of integers are ± 1, and every nonzero integer is a multiple by a unit of a positive integer. Analogously, the units of $\mathbb{F}_q[x]$ are the nonzero scalars $\mathbb{F}_q^\times$, and every nonzero polynomial is is a multiple by a unit of a monic polynomial. The analogue of a (positive) prime is a monic irreducible polynomial. To investigate arithmetic properties of "typical" integers, one samples them uniformly in the dyadic interval $[X, 2X]$ with $X \to \infty$; likewise to investigate arithmetic properties of "typical" polynomials, one samples them uniformly from the monic polynomials $\mathcal{M}_n$ of degree n, with $\#\mathcal{M}_n = q^n \to \infty$.

The Prime Number Theorem (PNT) states that the number $\pi(x)$ of primes $p \leq x$ is asymptotically equal to

$$\pi(x) \sim \mathrm{Li}(x) := \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x} \ , \quad x \to \infty \ . \tag{2.1}$$

The Riemann Hypothesis is equivalent to the assertion that

$$\pi(x) = \mathrm{Li}(x) + O\left(x^{1/2 + o(1)}\right) . \tag{2.2}$$

The Prime Polynomial Theorem asserts that the number $\pi_q(n)$ of monic irreducible polynomials of degree n is

$$\pi_q(n) = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right) , \tag{2.3}$$

the implied constant absolute. This corresponds to the PNT (and to the Riemann Hypothesis) if we map $x \leftrightarrow q^n$, recalling that x is the number of positive integers up to x and q^n is the number of monic polynomials of degree n. Note that (2.3) gives an asymptotic result whenever $q^n \to \infty$; in comparison, the results described below will usually be valid only in the large finite field limit, that is n fixed and $q \to \infty$.

2.2. Cycle structure. For $f \in \mathbb{F}_q[x]$ of positive degree n, we say its cycle structure is $\lambda(f) = (\lambda_1, \ldots, \lambda_n)$ if in the prime decomposition $f = \prod_\alpha P_\alpha$ (we allow repetition), we have $\#\{\alpha : \deg P_\alpha = j\} = \lambda_j$. In particular $\deg f = \sum_j j\lambda_j$. Thus we get a partition of $\deg f$, which we denote by $\lambda(f)$. For instance, $\lambda_1(f)$ is the number of roots of f in $\mathbb{F}_q$, and f is totally split in $\mathbb{F}_q[x]$ - that is $f(x) = \prod_{j=1}^n (x - a_j)$, $a_j \in \mathbb{F}_q$- if and only if $\lambda(f) = (n, 0, \ldots, 0)$. Moreover f is prime if and only if $\lambda(f) = (0, 0, \ldots, 0, 1)$.

The cycle structure of a permutation σ of n letters is $\lambda(\sigma) = (\lambda_1, \ldots, \lambda_n)$ if in the decomposition of σ as a product of disjoint cycles, there are λ_j cycles of length j. For instance, $\lambda_1(\sigma)$ is the number of fixed points of σ, and $\sigma = I$ is the identity if and only if $\lambda(\sigma) = (n, 0, \ldots)$. Moreover $\sigma \in S_n$ is an n-cycle if and only if $\lambda(\sigma) = (0, 0, \ldots, 0, 1)$.

For each partition $\lambda \vdash n$, denote by $p(\lambda)$ the probability that a random permutation on n letters has cycle structure λ:

$$p(\lambda) = \frac{\#\{\sigma \in S_n : \lambda(\sigma) = \lambda\}}{\# S_n} . \tag{2.4}$$

Cauchy's formula for $p(\lambda)$ is

$$p(\lambda) = \prod_{j=1}^n \frac{1}{j^{\lambda_j} \cdot \lambda_j!} \tag{2.5}$$

In particular, the proportion of n-cycles in the symmetric group S_n is $1/n$.

The connection between cycle structures of polynomials and of permutations is by means of the following observation, a straight-forward consequence of the Prime Polynomial Theorem (2.3): Given a partition $\lambda \vdash n$, the probability that a random monic polynomial f of degree n has cycle structure λ is asymptotic, as $q \to \infty$, to the probability $p(\lambda)$ that a random permutation of n letters has that cycle structure:

$$\frac{1}{q^n} \#\{f \text{ monic}, \deg f = n : \lambda(f) = \lambda\} = p(\lambda) + O\left(\frac{1}{q}\right) . \tag{2.6}$$

Note that unlike the Prime Polynomial Theorem (2.3), this result (2.6) gives an asymptotic only in the large finite field limit $q \to \infty$, n fixed.

Having set up the preliminaries, I turn to discussing new results on quantitative aspects of arithmetic in $\mathbb{F}_q[x]$.

3. Asymptotics in short intervals and arithmetic progressions

3.1. Primes in short intervals. Some of the most important problems in prime number theory concern the distribution of primes in short intervals and in arithmetic progressions. According to the Prime Number Theorem, the density

of primes near x is $1/\log x$. Thus one wants to know what is the number $\pi(x, H)$ of primes in an interval of length $H = H(x) \ll x$ around x:

$$\pi(x, H) := \#\{x < p \le x + H : p \text{ prime}\} . \tag{3.1}$$

We expect that for H sufficiently large,

$$\pi(x, H) \sim \frac{H}{\log x} . \tag{3.2}$$

The PNT implies that (3.2) holds for $H \approx x$, and the Riemann Hypothesis gives (3.2) for all $H > x^{1/2+o(1)}$. In 1930, Hoheisel gave an unconditional proof that (3.2) holds for all $H > x^{1-\delta}$ for any positive $\delta < 1/33,000$; this has since been improved, currently to $H > x^{7/12-o(1)}$ (Heath Brown 1988). It is believed that the result should hold for all $H > x^{\epsilon}$, for any $\epsilon > 0$, though Maier [30] showed that it does not hold for $H = (\log x)^N$ for any N; see Granville and Soundararajan [15] for a general framework for such results on irregularities of distribution and for sharper results. Selberg (1943) showed, assuming the Riemann Hypothesis, that (3.2) holds for *almost all x* provided $H/(\log x)^2 \to \infty$.

To set up an analogous problem for the polynomial ring $\mathbb{F}_q[x]$, we first need to define short intervals. For a nonzero polynomial $f \in \mathbb{F}_q[x]$, we define its norm by

$$|f| = \#\mathbb{F}_q[x]/(f) = q^{\deg f} ,$$

in analogy with the norm of a nonzero integer $0 \ne n \in \mathbb{Z}$, which is $|n| = \#\mathbb{Z}/n\mathbb{Z}$. Given a monic polynomial $A \in \mathcal{M}_n$ of degree n, and $h < n$, the "short interval" around A of diameter q^h is the set

$$I(A; h) := \{f \in \mathcal{M}_n : |f - A| \le q^h\} . \tag{3.3}$$

The number of polynomials in this "interval" is

$$H := \#I(A; h) = q^{h+1} . \tag{3.4}$$

We wish to count the number of prime polynomials in the interval $I(A; h)$. In the limit $q \to \infty$, Bank, Bary-Soroker and Rosenzweig [4] give an essentially optimal short interval result:

Theorem 3.1. *Fix $3 \le h < n$. Then for every monic polynomial A of degree n, the number of prime polynomials P in the interval $I(A; h) = \{f : |f - A| \le q^h\}$ about A satisfies*

$$\#\{P \text{ prime}, P \in I(A; h)\} = \frac{H}{n}\left(1 + O_n(q^{-1/2})\right) ,$$

the implied constant depending only on n.

For irregularities of distribution analogous to Maier's theorem in the large degree limit $n \to \infty$ (q fixed), see [36].

For other applications, we will need a version which takes into account the cycle structure:

Theorem 3.2 ([4]). *Fix $n > 1$, $3 \leq h < n$ and a partition $\lambda \vdash n$. Then for any sequence of finite fields $\mathbb{F}_q$, and every monic polynomial A of degree n,*

$$\#\{f \in I(A; h) : \lambda(f) = \lambda\} = p(\lambda)H\left(1 + O_n(q^{-1/2})\right) ,$$

with $p(\lambda)$ as in (2.4), (2.5), the implied constant depending only on n.

3.2. Primes in arithmetic progressions.

Dirichlet's theorem states that any arithmetic progression $n = A \bmod Q$ contains infinitely many primes provided that A and Q are coprime, and the prime number theorem in arithmetic progressions states that for fixed modulus Q, the number of such primes $p \leq x$ is

$$\pi(x; Q, A) \sim \frac{\mathrm{Li}(x)}{\phi(Q)}, \quad x \to \infty , \tag{3.5}$$

where $\phi(Q)$ is Euler's totient function, the number of residues coprime to Q. The Generalized Riemann Hypothesis (GRH) asserts that (3.5) continues to hold for moduli as large as $Q < X^{1/2 - o(1)}$. An unconditional version, for almost all $Q < x^{1/2 - o(1)}$, and all $A \bmod Q$, is given by the Bombieri-Vinogradov theorem. Going beyond the GRH, the Elliott-Halberstam conjecture gives a similar statement for Q as large as $x^{1-\epsilon}$.

For $\mathbb{F}_q[x]$, it is a consequence of the Riemann Hypothesis for curves over a finite field (Weil's theorem) that given a modulus $Q \in \mathbb{F}_q[x]$ of positive degree, and a polynomial A coprime to Q, the number $\pi_q(n; Q, A)$ of primes $P = A \bmod Q$, $P \in \mathcal{M}_n$ satisfies

$$\pi_q(n; Q, A) = \frac{\pi_q(n)}{\Phi(Q)} + O(\deg Q \cdot q^{n/2}) ,$$

where $\Phi(Q)$ is the number of coprime residues modulo Q. For $q \to \infty$, the main term is dominant as long as $\deg Q < n/2$.

Going beyond the Riemann Hypothesis for curves, Bank, Bary-Soroker and Rosenzweig [4] show an individual asymptotic continues to hold for even larger moduli in the limit $q \to \infty$:

Theorem 3.3 ([4]). *If $1 \leq \deg Q \leq n - 3$ then*

$$\pi_q(n; Q, A) = \frac{\pi_q(n)}{\Phi(Q)}\left(1 + O_n(q^{-\frac{1}{2}})\right) .$$

This should be considered as an individual version of the Elliot-Halberstam conjecture. As in the short interval case, they have a stronger result which takes into account the cycle structure.

4. Autocorrelations and twisted convolution

In this section we describe results on the autocorrelation of various classical arithmetic functions in the function field context.

4.1. Autocorrelations of the Möbius function and Chowla's conjecture.

Equivalent formulations of the PNT and the Riemann Hypothesis can be given in terms of growth of partial sums of the Möbius function, defined by $\mu(n) = (-1)^k$ if n is a product of k distinct primes, and $\mu(n) = 0$ otherwise: The PNT is equivalent to nontrivial cancellation $\sum_{n \leq x} \mu(n) = o(x)$, and the RH is equivalent to square-root cancellation: $\sum_{n \leq x} \mu(n) = O(x^{1/2 + o(1)})$.

A conjecture of Chowla on the auto-correlation of the Möbius function, asserts that given an r-tuple of distinct integers $\alpha_1, \ldots, \alpha_r$ and $\epsilon_i \in \{1, 2\}$, not all even, then

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n \leq N} \mu(n + \alpha_1)^{\epsilon_1} \cdot \cdots \cdot \mu(n + \alpha_r)^{\epsilon_r} = 0 \ . \tag{4.1}$$

Note that the number of nonzero summands here, that is the number of $n \leq N$ for which $n + \alpha_1, \ldots n + \alpha_r$ are all square-free, is asymptotically $\mathfrak{S}(\alpha)N$, where $\mathfrak{S}(\alpha) > 0$ if the numbers $\alpha_1, \ldots, \alpha_r$ do not contain a complete system of residues modulo p^2 for every prime p, so that Chowla's conjecture (4.1) addresses non-trivial cancellation in the sum. At this time, the only known case of Chowla's conjecture (4.1) is $r = 1$ where it is equivalent with the Prime Number Theorem.

Sarnak [35] showed that Chowla's conjecture implies that $\mu(n)$ does not correlate with any "deterministic" (i. e., zero entropy) sequence. For recent studies on the correlation between $\mu(n)$ and several sequences of arithmetic functions, see [16, 8, 5, 29].

In joint work with Dan Carmon [6], we have resolved a version of Chowla's conjecture for $\mathbb{F}_q[x]$ in the limit $q \to \infty$. To formulate it, one defines the Möbius function of a nonzero polynomial $F \in \mathbb{F}_q[x]$ to be $\mu(F) = (-1)^r$ if $F = cP_1 \ldots P_r$ with $0 \neq c \in \mathbb{F}_q$ and $P_1, \ldots, P_r$ are distinct monic irreducible polynomials, and $\mu(F) = 0$ otherwise.

Theorem 4.1. *Fix $r > 1$ and assume that $n > 1$ and q is odd. Then for any choice of distinct polynomials $\alpha_1, \ldots, \alpha_r \in \mathbb{F}_q[x]$, with $\max \deg \alpha_j < n$, and $\epsilon_i \in \{1, 2\}$, not all even,*

$$| \sum_{F \in \mathcal{M}_n} \mu(F + \alpha_1)^{\epsilon_1} \ldots \mu(F + \alpha_r)^{\epsilon_r} | \ll_{r,n} q^{n - \frac{1}{2}} \ . \tag{4.2}$$

Thus for fixed $r, n > 1$,

$$\lim_{q \to \infty} \frac{1}{\#\mathcal{M}_n} \sum_{F \in \mathcal{M}_n} \mu(F + \alpha_1)^{\epsilon_1} \ldots \mu(F + \alpha_r)^{\epsilon_r} = 0 \tag{4.3}$$

under the assumption of Theorem 4.1, giving an analogue of Chowla's conjecture (4.1).

Note that the number of square-free monic polynomials of degree n is, for $n > 1$, equal to $q^n - q^{n-1}$. Hence, given r distinct polynomials $\alpha_1, \ldots, \alpha_r \in \mathbb{F}_q[x]$, with $\deg \alpha_j < n$, the number of $F \in \mathcal{M}_n$ for which all of $F(x) + \alpha_j(x)$ are square-free is $q^n + O(rq^{n-1})$ as $q \to \infty$. Thus indeed we display cancellation.

The starting point in our argument is Pellet's formula, which asserts that for the polynomial ring $\mathbb{F}_q[x]$ with q odd, the Möbius function $\mu(F)$ can be computed in terms of the discriminant $\mathrm{disc}(F)$ of $F(x)$ as

$$\mu(F) = (-1)^{\deg F} \chi_2(\mathrm{disc}(F)) , \tag{4.4}$$

where χ_2 is the quadratic character of $\mathbb{F}_q$. That allows us to express the LHS of (4.2) as an n-variable character sum and to estimate it by freezing all but one of the variables, and then using the Riemann Hypothesis for curves (Weil's theorem) to bound the one-variable sum. A key point is to bound the number of times when there is no cancellation in the one-variable sum.

4.2. Twin primes. It is an ancient conjecture that there are infinitely many twin primes, and a refined quantitative form, due to Hardy and Littlewood, asserts that given distinct integers $a_1, \ldots, a_r$, the number $\pi(x; a_1, \ldots, a_r)$ of integers $n \leq x$ for which $n + a_1, \ldots, n + a_r$ are simultaneously prime is asymptotically

$$\pi(x; a_1, \ldots, a_r) \sim \mathfrak{S}(a_1, \ldots, a_r)\frac{x}{(\log x)^r}, \quad x \to \infty , \tag{4.5}$$

for a certain constant $\mathfrak{S}(a_1, \ldots, a_r)$, which is positive whenever there are no local congruence obstructions. Despite the striking recent breakthroughs by Zhang [37] and Maynard [31], this conjecture is still open even for $r = 2$ (twin primes).

Recently the function field version of the problem was solved. Bary-Soroker [3] proved that for given n, r then for any sequence of finite fields $\mathbb{F}_q$ of odd cardinality q, and distinct polynomials $a_1, \ldots, a_r \in \mathbb{F}_q[x]$ of degree less than n, the number $\pi_q(n; a_1, \ldots, a_r)$ of monic polynomials $f \in \mathbb{F}_q[x]$ of degree n such that $f + a_1, \ldots, f + a_r$ are simultaneously irreducible satisfies

$$\pi_q(n; a_1, \ldots, a_r) \sim \frac{q^n}{n^r}, \quad q \to \infty . \tag{4.6}$$

This improves on earlier results by Pollack [33] and by Bary-Soroker [2].

4.3. The additive divisor problem. The divisor function $d_r(n)$ is the number of ways of writing a positive integer n as a product of r positive integers. In particular for $r = 2$ we recover the classical divisor function $d_2(n) = \sum_{d|n} 1$. The mean value of d_r is

$$\frac{1}{x} \sum_{n \leq x} d_r(n) \sim \frac{(\log x)^{r-1}}{(r-1)!}, \quad x \to \infty . \tag{4.7}$$

Likewise, the divisor function $d_r(f)$ for a monic polynomial $f \in \mathbb{F}_q[x]$ is defined as the number of r-tuples of monic polynomials $(a_1, \ldots, a_r)$ so that $f = a_1 \cdot \ldots \cdot a_r$. The mean value of d_r, when averaged over all monic polynomials of degree n, is

$$\frac{1}{q^n} \sum_{f \in \mathcal{M}_n} d_r(f) = \binom{n + r - 1}{r - 1} = \frac{n^{r-1}}{(r-1)!} + \ldots , \tag{4.8}$$

which is a polynomial of degree $r - 1$ in n.

The "additive divisor problem" (other names are "shifted divisor" and "shifted convolution") is to understand the autocorrelation of the divisor function, that is the sum (where $h \neq 0$ is fixed for this discussion)

$$D_r(X; h) := \sum_{n \leq X} d_r(n) d_r(n + h) . \tag{4.9}$$

These sums are of importance in studying the moments of the Riemann ζ-function on the critical line, see [19, 7].

For $r = 2$ (the ordinary divisor function), Ingham [18] and Estermann [10] showed that

$$\sum_{n \leq X} d_2(n) d_2(n + h) \sim X P_2(\log X; h), \quad X \to \infty \tag{4.10}$$

where $P_2(u; h)$ is a quadratic polynomial in u.

For $r \geq 3$ it is conjectured that

$$D_r(X; h) \sim X P_{2(r-1)}(\log X; h), \quad X \to \infty \tag{4.11}$$

where $P_{2(r-1)}(u; h)$ is a polynomial in u of degree $2(r - 1)$, whose coefficients depend on h (and r). However to date one is very far from being able to even get good upper bounds on $D_r(X; h)$. Moreover, even a conjectural description of the polynomials $P_{2(r-1)}(u; h)$ is difficult to obtain, see [19, 7].

In joint work with Andrade and Bary-Soroker [1], we study a version of the additive divisor problem for $\mathbb{F}_q[x]$. We show:

Theorem 4.2. *Let* $0 \neq h \in \mathbb{F}_q[x]$*, and* $n > \deg h$*. Then for* q *odd,*

$$\frac{1}{q^n} \sum_{f \in \mathcal{M}_n} d_r(f) d_r(f + h) = \binom{n + r - 1}{r - 1}^2 + O_n(q^{-1/2}) , \tag{4.12}$$

the implied constant depending only on n*.*

Note that $\binom{n+r-1}{r-1}^2$ is a polynomial in n of degree $2(r-1)$ with leading coefficient $1/[(r - 1)!]^2$.

4.4. About proofs. The results of this section can all be deduced from one principle (though this was not the original proof of most), namely that for a random monic polynomial $f \in \mathcal{M}_n$ of degree n, the cycle structure of f and its shift $f + \alpha$ are *independent* as $q \to \infty$. Precisely, in [1] we show that for for fixed $n > 1$, and two partitions $\lambda', \lambda'' \vdash n$, given any sequence of finite fields $\mathbb{F}_q$ of odd cardinality q, and nonzero $\alpha \in \mathbb{F}_q[x]$ of degree less than n, then

$$\lim_{q \to \infty} \frac{1}{q^n} \#\{f \in \mathcal{M}_n : \lambda(f) = \lambda', \lambda(f + \alpha) = \lambda''\} = p(\lambda') \times p(\lambda'') \tag{4.13}$$

where $p(\lambda)$, as in (2.4), (2.5), is the probability that a random permutation on n letters has cycle structure λ. This result is an elaboration of earlier work by

Bary-Soroker [3] which dealt with the case of n-cycles, where $\lambda = \tilde{\lambda} = (0, \ldots, 0, n)$. There is also a version allowing several distinct shifts.

To prove (4.13) we need to compute a certain Galois group: Let $\mathbb{F}$ be an algebraic closure of $\mathbb{F}_q$, $\mathbf{A} = (A_0, \ldots, A_{n-1})$ be indeterminates, and

$$\mathcal{F}(\mathbf{A}, x) = x^n + A_{n-1}x^{n-1} + \cdots + A_0 \qquad (4.14)$$

the generic polynomial of degree n, whose Galois group over $\mathbb{F}(\mathbf{A})$ is well-known to be the full symmetric group S_n. For nonzero $\alpha \in \mathbb{F}_q[x]$ of degree less than n, let

$$\mathcal{G}(\mathbf{A}, x) = \mathcal{F}(\mathbf{A}, x)\Big(\mathcal{F}(\mathbf{A}, x) + \alpha(x)\Big) . \qquad (4.15)$$

Bary-Soroker [3] shows that for odd q, the Galois group of $\mathcal{G}$ over $\mathbb{F}(\mathbf{A})$ is the product $S_n \times S_n$, the maximal possible group. The proof requires an ingredient from the proof of Chowla's conjecture [6] discussed above.

Once we know the Galois group of $\mathcal{G}(\mathbf{A}, x)$, we apply an explicit version of Chebotarev's theorem for function fields to prove (4.13), see [1] for the details.

5. The variance of sums of arithmetic functions and matrix integrals

I now describe some results concerning the variance of sums of several arithmetic functions. A common feature is that the variance is expressed as a matrix integral.

5.1. Variance of primes in short intervals. The von Mangoldt function is defined as $\Lambda(n) = \log p$ if $n = p^k$ is a prime power, and 0 otherwise. A form of the Prime Number Theorem (PNT) is the assertion that

$$\psi(x) := \sum_{n \leq x} \Lambda(n) \sim x \qquad \text{as } x \to \infty . \qquad (5.1)$$

To study the distribution of primes in short intervals, we define for $1 \leq H \leq x$,

$$\psi(x; H) := \sum_{n \in [x - \frac{H}{2}, x + \frac{H}{2}]} \Lambda(n) . \qquad (5.2)$$

The Riemann Hypothesis guarantees an asymptotic formula $\psi(X; H) \sim H$ as long as $H > X^{\frac{1}{2}+o(1)}$. Goldston and Montgomery [13] studied the variance of $\psi(x; H)$, relating it to the pair correlation function of the zeros of the Riemann zeta function. The conjecture of Goldston and Montgomery, as refined by Montgomery and Soundararajan[1] [32] is that in the range $X^\epsilon < H < X^{1-\epsilon}$, as $X \to \infty$:

$$\frac{1}{X} \int_1^X |\psi(x; H) - H|^2 \, dx \sim H\Big(\log X - \log H - (\gamma + \log 2\pi) \Big) \qquad (5.3)$$

---

[1]based on Hardy-Littlewood type heuristics

with γ being Euler's constant.

With J. Keating, we prove a function field analogue of Conjecture 5.3:

Theorem 5.1 ([26]). *For $h \leq n - 5$, as $q \to \infty$,*

$$\frac{1}{q^n} \sum_{A \in \mathcal{M}_n} \Big| \sum_{|f-A| \leq q^h} \Lambda(f) - H \Big|^2 \sim H \int_{U(n-h-2)} \Big| \operatorname{tr} U^n \Big|^2 dU = H(n-h-2) \,.$$

Recall $H := \#\{f : |f - A| \leq q^h\} = q^{h+1}$. Here the matrix integral is over the unitary group $U(n - h - 2)$, equipped with its Haar probability measure.

5.2. Variance of primes in arithmetic progressions. A form of the Prime Number Theorem for arithmetic progression states that for a modulus Q and A coprime to Q,

$$\psi(X; Q, A) := \sum_{\substack{n \leq X \\ n = A \bmod Q}} \Lambda(n) \sim \frac{X}{\phi(Q)}, \quad \text{as } X \to \infty \,. \tag{5.4}$$

In most arithmetic applications it is crucial to allow the modulus to grow with X. For very large moduli $Q > X$, there can be at most one prime in the arithmetic progression $P = A \bmod Q$ so that the interesting range is $Q < X$. To study the fluctuations of $\psi(X; Q, A)$, define

$$G(X, Q) = \sum_{\substack{A \bmod Q \\ \gcd(A,Q)=1}} \Big| \psi(X; Q, A) - \frac{X}{\phi(Q)} \Big|^2 \,. \tag{5.5}$$

Hooley, in his ICM article [17], conjectured that under some (unspecified) conditions,

$$G(X, Q) \sim X \log Q \,. \tag{5.6}$$

Friedlander and Goldston [12] conjecture that (5.6) holds if $X^{1/2+\epsilon} < Q < X$, and further conjecture that if $X^{1/2+\epsilon} < Q < X^{1-\epsilon}$ then

$$G(X, Q) = X \left(\log Q - \Big(\gamma + \log 2\pi + \sum_{p|Q} \frac{\log p}{p-1} \Big) \right) + o(X) \,. \tag{5.7}$$

They show that both (5.6) (in the range $X^{1/2+\epsilon} < Q < X$) and (5.7) (in the range $X^{1/2+\epsilon} < Q < X^{1-\epsilon}$) hold assuming GRH and a strong version of the Hardy-Littlewood conjecture (4.5) on prime pairs. For $Q < X^{1/2}$ little is known. In any case, Hooley's conjecture (5.6) has not been proved in any range.

With J. Keating [26] we resolve the function-field version of Conjecture (5.6):

Theorem 5.2. *Fix $n \geq 2$. Given a sequence of finite fields $\mathbb{F}_q$ and square-free polynomials $Q(x) \in \mathbb{F}_q[x]$ with $2 \leq \deg Q \leq n - 1$, then as $q \to \infty$,*

$$G(n; Q) \sim q^n \int_{U(\deg Q - 1)} |\operatorname{tr} U|^n dU = q^n(\deg Q - 1) \,. \tag{5.8}$$

We can compare our result (5.8) to the conjectures (5.6) and (5.7): The range $X^{1/2} < Q < X$ corresponds to $\deg Q < n < 2\deg Q$, so that we recover the function field version of conjecture (5.6); note that (5.8) holds for all n, not just in that range. Thus we believe that Hooley's conjecture (5.6) should hold for all $Q > X^\epsilon$. We refer to Fiorilli's recent work [11] for a more refined conjecture in this direction.

5.3. Almost-primes.

A variation on this theme was proposed by B. Rodgers [34]. Instead of primes, he considered "almost primes", that is products of two prime powers. A useful weight function for these is the generalized von Mangoldt function

$$\Lambda_2 = \Lambda * \Lambda + \deg \cdot \Lambda = \mu * \deg^2 \tag{5.9}$$

which is supported on products of two prime powers ($*$ means Dirichlet convolution). The mean value of Λ_2 over the set $\mathcal{M}_n$ of monic polynomials of degree n is

$$\frac{1}{q^n} \sum_{f \in \mathcal{M}_n} \Lambda_2(f) = n^2 - (n-1)^2 = 2n - 1 . \tag{5.10}$$

To count almost primes in the short intervals, set for $A \in \mathcal{M}_n$, and $1 \le h < n$

$$\Psi_2(A; h) = \sum_{f \in I(A;h)} \Lambda_2(f) . \tag{5.11}$$

Rodgers showed [34] that the variance of $\Psi_2(A; h)$ is given as $q \to \infty$, for fixed n and $h \le n - 5$, by the matrix integral

$$\operatorname{Var} \Psi_2(\bullet; h) \sim H \int_{U(n-h-2)} \Big| \sum_{j=1}^{n-1} \operatorname{tr} U^j \operatorname{tr} U^{n-j} - n \operatorname{tr} U^n \Big|^2 dU, \quad q \to \infty . \tag{5.12}$$

He shows the matrix integral to be equal to $(4(n-h-2)^3 - (n-h-2))/3$, in fact that

$$\int_{U(N)} \Big| \sum_{j=1}^{n-1} \operatorname{tr} U^j \operatorname{tr} U^{n-j} - n \operatorname{tr} U^n \Big|^2 dU = \sum_{d=1}^{\min(n,N)} (d^2 - (d-1)^2))^2 . \tag{5.13}$$

5.4. Sums of the Möbius function and the Good-Churchhouse conjecture.

It is a standard heuristic to assume that the Möbius function behaves like a random variable taking values ± 1 with equal probability, and supported on the square-free integers (which have density $1/\zeta(2) = 6/\pi^2$). In particular if we consider the sums of $\mu(n)$ in blocks of length H,

$$M(x; H) := \sum_{|n-x| < H/2} \mu(n) \tag{5.14}$$

then when averaged over x, $M(x, H)/\sqrt{H}$ has mean zero, and it was conjectured by Good and Churchhouse [14] in 1968 that $M(x; H)/\sqrt{H}$ has variance $1/\zeta(2)$:

$$\frac{1}{X} \int_X^{2X} |M(x; H)|^2 \sim \frac{H}{\zeta(2)} \tag{5.15}$$

for $X^\epsilon < H = H(X) < X^{1-\epsilon}$. Moreover they conjectured that the normalized sums $M(x; H)/\sqrt{H/\zeta(2)}$ have asymptotically a normal distribution.

We can apply our method to evaluate the variance of sums of the Möbius function in short intervals for $\mathbb{F}_q[x]$. Set

$$\mathcal{N}_\mu(A; h) := \sum_{f \in I(A;h)} \mu(f) . \tag{5.16}$$

The mean value of $\mathcal{N}_\mu(A; h)$ is 0, and the variance is

Theorem 5.3 (Keating-Rudnick [27]). *If $h \leq n - 5$ then as $q \to \infty$,*

$$\operatorname{Var} \mathcal{N}_\mu(\bullet; h) \sim H \int_{U(n-h-2)} |\operatorname{tr} \operatorname{Sym}^n U|^2 dU = H$$

where Sym^n is the representation of the unitary group $U(N)$ on polynomials of degree n in N variables.

Theorem 5.3 is consistent with Conjecture (5.15) if we replace H by $H/\zeta_q(2)$ where $\zeta_q(2) = \sum_f 1/|f|^2$ (the sum over all monic f), which tends to 1 as $q \to \infty$.

5.5. The divisor function in short intervals.
Dirichlet's divisor problem addresses the size of the remainder term $\Delta_2(x)$ in partial sums of the divisor function:

$$\Delta_2(x) := \sum_{n \leq x} d_2(n) - x\left(\log x + (2\gamma - 1)\right) \tag{5.17}$$

where γ is the Euler-Mascheroni constant. For the higher divisor functions one defines a remainder term $\Delta_k(x)$ similarly as the difference between the partial sums $\sum_{n \leq x} d_k(n)$ and a smooth term $x P_{k-1}(\log x)$ where $P_{k-1}(u)$ is a certain polynomial of degree $k - 1$.

Let

$$\Delta_k(x; H) = \Delta_k(x + H) - \Delta_k(x) \tag{5.18}$$

be the remainder term for sums of d_k over short intervals $[x, x + H]$. Jutila [22], Coppola and Salerno [8], and Ivić [20, 21] show that, for $X^\epsilon < H < X^{1/2-\epsilon}$, the mean square of $\Delta_2(x, H)$ is asymptotically equal to

$$\frac{1}{X} \int_X^{2X} \left(\Delta_2(x, H)\right)^2 dx \sim H P_3(\log X - 2\log H) \tag{5.19}$$

for a certain cubic polynomial P_3.

Lester and Yesha [28] showed that $\Delta_2(x, H)$, normalized to have unit mean-square using (5.19), has a Gaussian value distribution at least for a narrow range of H below $X^{1/2}$: $H = \sqrt{X}/L$, where $L = L(X) \to \infty$ with X, but $L \ll X^{o(1)}$, (see [28] for the precise statement), the conjecture being that this should hold for $X^\epsilon < H < X^{1/2-\epsilon}$ for any $\epsilon > 0$.

In joint work with J. Keating and E. Roditty-Gershon [25], we study the corresponding problem of the sum of $d_k(f)$ over short intervals for $\mathbb{F}_q[x]$. Set

$$\mathcal{N}_{d_k}(A; h) := \sum_{f \in I(A; h)} d_k(f) \,. \tag{5.20}$$

The mean value is

$$\frac{1}{q^n} \sum_{A \in \mathcal{M}_n} \mathcal{N}_{d_k}(A; h) = q^{h+1} \binom{n+k-1}{k-1} \,. \tag{5.21}$$

In analogy with (5.17), (5.18) we set

$$\Delta_k(A; h) := \mathcal{N}_{d_k}(A; h) - q^{h+1} \binom{n+k-1}{k-1} \,. \tag{5.22}$$

It can be shown that $\Delta_k(A; h) \equiv 0$ vanishes identically for $h > (1 - \frac{1}{k})n - 1$. Using Theorem 3.2 [4], we can show that for all $3 \le h < n$

$$\Delta_k(A; h) \ll_{n,k} q^{h+\frac{1}{2}} \tag{5.23}$$

is smaller than the main term.

We express the mean square of $\Delta_k(A, h)$ (which is the variance of $\mathcal{N}_{d_k}(A; h)$) in terms of a matrix integral. Let $\Lambda^j : U(N) \to GL(\Lambda^j \mathbb{C}^N)$ be the exterior j-th power representation ($0 \le j \le N$). Define the matrix integrals over the group $U(N)$ of $N \times N$ unitary matrices

$$I_k(m; N) := \int_{U(N)} \Big| \sum_{\substack{j_1 + \cdots + j_k = m \\ 0 \le j_1, \ldots, j_k \le N}} \operatorname{tr} \Lambda^{j_1}(U) \ldots \operatorname{tr} \Lambda^{j_k}(U) \Big|^2 dU \,, \tag{5.24}$$

the integral with respect to the Haar probability measure.

By definition, $I_k(m; N) = 0$ for $m > kN$. We have a functional equation $I_k(m; N) = I_k(kN - m; N)$ and

$$I_k(m; N) = \binom{m + k^2 - 1}{k^2 - 1}, \quad m \le N \,. \tag{5.25}$$

The identity (5.25) can be proved by various means, for instance using the work of Diaconis and Gamburd [9] relating matrix integrals to counting magic squares.

Theorem 5.4 ([25]). *Let $n \ge 5$, and $h \le \min(n - 5, (1 - \frac{1}{k})n - 2)$. Then as $q \to \infty$,*

$$\frac{1}{q^n} \sum_{A \in \mathcal{M}_n} |\Delta_k(A; h)|^2 \sim H \cdot I_k(n; n - h - 2) \,.$$

In particular for the standard divisor function ($k = 2$), if $h \le n/2 - 2$ and $n \ge 8$ then

$$\frac{1}{q^n} \sum_{A \in \mathcal{M}_n} |\Delta_2(A; h)|^2 \sim H \frac{(n - 2h + 5)(n - 2h + 6)(n - 2h + 7)}{6} \,. \tag{5.26}$$

This is consistent with (5.19), which leads us to expect a cubic polynomial in $(n - 2h)$.

6. How to compute the variance

Our results on variance described in § 5 depend on expressing the variance in terms of zeros of Dirichlet L-functions for $\mathbb{F}_q[x]$, and using recent equidistribution results of Katz [23], [24], tailor-made for this purpose. To describe how this is done, we give some background on L-functions.

6.1. Dirichlet L-functions. Let $Q(x) \in \mathbb{F}_q[x]$ be a polynomial of positive degree. A Dirichlet character modulo Q is a homomorphism $\chi : (\mathbb{F}_q[x]/(Q))^\times \to \mathbb{C}^\times$. A Dirichlet character χ is "even" if $\chi(cF) = \chi(F)$ for all $0 \neq c \in \mathbb{F}_q$, and χ is *primitive* if there is no proper divisor $Q' \mid Q$ so that $\chi(F) = 1$ whenever F is coprime to Q and $F = 1 \mod Q'$. The number of Dirichlet characters modulo Q is $\Phi(Q)$, and the number of even characters modulo Q is $\Phi^{ev}(Q) = \Phi(Q)/(q-1)$.

The L-function $\mathcal{L}(u, \chi)$ attached to χ is defined as

$$\mathcal{L}(u, \chi) = \sum_{\substack{f \text{ monic} \\ (f,Q)=1}} \chi(f) u^{\deg f} = \prod_{P \nmid Q} (1 - \chi(P) u^{\deg P})^{-1} \tag{6.1}$$

where the product, over all monic irreducible polynomials in $\mathbb{F}_q[x]$, is absolutely convergent for $|u| < 1/q$.

If $Q \in \mathbb{F}_q[x]$ is a polynomial of degree $\deg Q \geq 2$, and $\chi \neq \chi_0$ is a nontrivial character mod Q, then the L-function $\mathcal{L}(u, \chi)$ is a polynomial in u of degree at most $\deg Q - 1$. Moreover, if χ is an even character there is a "trivial" zero at $u = 1$.

For a primitive even character modulo Q, we can write

$$\mathcal{L}(u, \chi) = (1 - u) \det(I - u q^{1/2} \Theta_\chi) \tag{6.2}$$

where the matrix $\Theta_\chi \in U(\deg Q - 2)$ is unitary (as follows from the Riemann Hypothesis for curves), uniquely defined up to conjugacy. It is called the unitarized Frobenius matrix of χ. Likewise, if χ is odd and primitive then $\mathcal{L}(u, \chi) = \det(I - u q^{1/2} \Theta_\chi)$ where $\Theta_\chi \in U(\deg Q - 1)$ is unitary.

Katz [24] showed that as χ varies over all primitive even characters modulo x^{N+2}, the unitarized Frobenii Θ_χ become uniformly distributed in the projectivized unitary group $PU(N)$ for $N \geq 3$ as $q \to \infty$ (and also for $N = 2$ if q is coprime to 2 and 5). Thus for any nice class function F on $U(N)$, which is invariant under the center ($F(zU) = F(u)$, z on the unit circle), we have

$$\lim_{q \to \infty} \frac{1}{\Phi_{ev}(x^{N+2})} \sum_{\substack{\chi \mod x^{N+2} \\ \text{even primitive}}} F(\Theta_\chi) = \int_{PU(N)} F(U) dU . \tag{6.3}$$

6.2. Short intervals as arithmetic progressions. Our method to handle sums over short intervals $I(A; h) = \{f : |f - A| \leq q^h\}$ is to relate them to arithmetic progressions modulo x^{n-h}.

Denote by $\mathcal{P}_{\leq n}$ the set of all polynomials of degree at most n. We define a map $\theta_n : \mathcal{P}_{\leq n} \to \mathcal{P}_{\leq n}$ by

$$\theta_n(f) = x^n f(\frac{1}{x}) \tag{6.4}$$

which takes $f(x) = f_0 + f_1 x + \cdots + f_n x^n$, $n = \deg f$ to the "reversed" polynomial

$$\theta_n(f)(x) = f_0 x^n + f_1 x^{n-1} + \cdots + f_n . \tag{6.5}$$

Then for $B \in \mathcal{M}_{n-h-1}$, the map θ_n takes the "interval" $I(T^{h+1}B; h)$ bijectively onto the arithmetic progression $\{g \in \mathcal{P}_{\leq n} : g \equiv \theta_{n-h-1}(B) \mod x^{n-h}\}$.

6.3. A formula for the variance.

The identification of short intervals with arithmetic progressions allows us to express sums of several arithmetic functions in terms of even Dirichlet characters. For the case of the von Mangoldt function, this is done in [26]. I illustrate this identification in the case of the Möbius function (Theorem 5.3): We denoted by $\mathcal{N}_\mu(A; h) = \sum_{f \in I(A;h)} \mu(f)$. Then for $B \in \mathcal{M}_{m-h-1}$,

$$\mathcal{N}_\mu(T^{h+1}B; h) = \frac{1}{\Phi_{ev}(x^{n-h})} \sum_{\substack{\chi \bmod x^{n-h} \\ \chi \neq \chi_0 \text{ even}}} \bar{\chi}(\theta_{n-h-1}(B))(\mathcal{M}(n; \mu\chi) - \mathcal{M}(n-1; \mu\chi))$$

$$\tag{6.6}$$

where

$$\mathcal{M}(n; \mu\chi) = \sum_{f \in \mathcal{M}_n} \mu(f)\chi(f) . \tag{6.7}$$

We next express the sums $\mathcal{M}(n; \mu\chi)$ in terms of zeros of the L-function $\mathcal{L}(u, \chi)$; for χ primitive this means in terms of the unitarized Frobenius matrix Θ_χ. The connection is made by writing the generating function identity

$$\sum_{n=0}^{\infty} \mathcal{M}(n; \mu\chi)u^n = \frac{1}{\mathcal{L}(u, \chi)} . \tag{6.8}$$

Therefore we find that for χ primitive and even,

$$\mathcal{M}(n; \mu\chi) = \sum_{k=0}^{n} q^{k/2} \operatorname{tr} \operatorname{Sym}^k \Theta_\chi \tag{6.9}$$

where for $N > 1$, $\operatorname{Sym}^n : GL(N, \mathbb{C}) \to \operatorname{Sym}^n \mathbb{C}^N$ is the symmetric n-th power representation. Consequently we obtain

$$\operatorname{Var} \mathcal{N}_\mu(\bullet; h) = \frac{q^{h+1}}{\Phi_{ev}(x^{n-h})} \sum_{\substack{\chi \bmod x^{n-h} \\ \chi \text{ even and primitive}}} |\operatorname{tr} \operatorname{Sym}^n \Theta_\chi|^2 + O(q^h) . \tag{6.10}$$

Using Katz's equidistribution theorem (6.3) we get

$$\lim_{q \to \infty} \frac{\operatorname{Var}(\mathcal{N}_\mu(\bullet; h))}{q^{h+1}} = \int_{PU(n-h-2)} |\operatorname{tr} \operatorname{Sym}^n U|^2 \, dU . \tag{6.11}$$

The matrix integrals equals 1, hence we conclude that $\text{Var}(\mathcal{N}_\mu(;h)) \sim q^{h+1} = H$, which is Theorem 5.3.

7. Acknowledgements

I am grateful to J. Andrade, L. Bary-Soroker, J. Keating, E. Kowalski, S. Lester, E. Roditty-Gershon and K. Soundararajan for their comments on earlier versions of this survey.

References

[1] J. Andrade, L. Bary-Soroker and Z. Rudnick *The additive divisor problem over the rational function field*, preprint 2014.

[2] L. Bary-Soroker. *Irreducible values of polynomials.* Advances in Mathematics 2012;229(2):854-74.

[3] L. Bary-Soroker, *Hardy-Littlewood tuple conjecture over large finite fields*, Int. Math. Res. Not., 2012, 1–8 (2012).

[4] E. Bank, L. Bary-Soroker and L. Rosenzweig, *Prime polynomials in short intervals and in arithmetic progressions*, arXiv:1302.0625 [math.NT]. To appear in Duke Math. J.

[5] J. Bourgain, P. Sarnak and T. Ziegler, *Disjointness of Möbius from horocycle flows*, From Fourier analysis and number theory to radon transforms and geometry, 67–83, Dev. Math., 28, Springer, New York, 2013.

[6] D. Carmon and Z. Rudnick, *The autocorrelation of the Mobius function and Chowla's conjecture for the rational function field*, Q J Math (2014) 65 (1): 53-61.

[7] J. B. Conrey and S. M. Gonek, *High Moments of the Riemann Zeta-Function*, Duke Math. J. 107, 577–604 (2001).

[8] G. Coppola and S. Salerno. *On the symmetry of the divisor function in almost all short intervals.* Acta Arith. 113 (2004), no. 2, 189–201.

[9] P. Diaconis and A. Gamburd. *Random matrices, magic squares and matching polynomials.* Electron. J. Combin. 11 (2004/06), no. 2, Research Paper 2, 26 pp.

[10] T. Estermann, *Über die Darstellungen einer Zahl als Differenz von zwei Produkten.* Journal für die reine und angewandte Mathematik 164 (1931): 173–182.

[11] D. Fiorilli, *The distribution of the variance of primes in arithmetic progressions*, arXiv:1301.5663 [math.NT]. To appear in Int. Math. Res. Not.

[12] J. B. Friedlander and D. A. Goldston, *Variance of distribution of primes in residue classes.* Quart. J. Math. Oxford Ser. (2) 47 (1996), no. 187, 313–336.

[13] D. A. Goldston, and H. L. Montgomery, *Pair correlation of zeros and primes in short intervals.* Analytic number theory and Diophantine problems (Stillwater, OK, 1984), 183–203, Progr. Math., 70, Birkhäuser Boston, Boston, MA, 1987.

[14] I. J. Good and R. F. Churchhouse. *The Riemann Hypothesis and Pseudorandom Features of the Möbius Sequence*, Mathematics of Computation 22, No. 104, (1968), 857–861.

[15] A. Granville and K. Soundararajan, *An uncertainty principle for arithmetic sequences.* Ann. of Math. (2) 165 (2007), no. 2, 593–635.

[16] B. Green and T. Tao, *The Möbius function is strongly orthogonal to nilsequences.* Ann. of Math. (2) 175 (2012), no. 2, 541–566.

[17] C. Hooley, *The distribution of sequences in arithmetic progression*, Proc. ICM Vancouver (1974), 357–364.

[18] A. E. Ingham, *Mean-value theorems in the theory of the Riemann Zeta-function*, Proc. London Math. Soc. (2) 27 (1928), 273–300.

[19] A. Ivić, *On the ternary additive divisor problem and the sixth moment of the zeta-function*, Sieve methods, exponential sums, and their applications in number theory (Cardiff, 1995), 205–243, London Math. Soc. Lecture Note Ser., 237, Cambridge Univ. Press, Cambridge, 1997.

[20] A. Ivić. *On the mean square of the divisor function in short intervals.* J. Théor. Nombres Bordeaux 21 (2009), no. 2, 251–261.

[21] A. Ivić. *On the divisor function and the Riemann zeta-function in short intervals.* Ramanujan J. 19 (2009), no. 2, 207–224.

[22] M. Jutila. *On the divisor problem for short intervals.* Studies in honour of Arto Kustaa Salomaa on the occasion of his fiftieth birthday. Ann. Univ. Turku. Ser. A I No. 186 (1984), 23–30.

[23] N. M. Katz, *On a Question of Keating and Rudnick about Primitive Dirichlet Characters with Squarefree Conductor*, Int Math Res Notices (2013) Vol. 2013 3221-3249,

[24] N. M. Katz. *Witt vectors and a question of Keating and Rudnick*, Int Math Res Notices (2013) Vol. 2013 3613–3638.

[25] J. P. Keating, E. Roditty-Gershon and Z. Rudnick, in preparation.

[26] J. P. Keating and Z. Rudnick *The variance of the number of prime polynomials in short intervals and in residue classes.* Int Math Res Notices (2014) 2014 (1): 259-288.

[27] J. P. Keating and Z. Rudnick, in preparation.

[28] S. Lester and N. Yesha, *On the distribution of the divisor function and Hecke eigenvalues*, arXiv:1404.1579 [math.NT].

[29] J. Liu and P. Sarnak, *The Möbius function and distal flows.* arXiv:1303.4957 [math.NT]

[30] H. Maier, *Primes in short intervals.* Michigan Math. J. 32 (1985), 221–225.

[31] J. Maynard, *Small gaps between primes*, arXiv:1311.4600 [math.NT]. To appear in Ann. of Math.

[32] Montgomery, H. L.; Soundararajan, K. *Beyond pair correlation.* Paul Erdos and his mathematics, I (Budapest, 1999), 507–514, Bolyai Soc. Math. Stud., 11, Janos Bolyai Math. Soc., Budapest, 2002. arXiv:math/0003234 [math.NT]

[33] P. Pollack *Simultaneous prime specializations of polynomials over finite fields*, in Proceedings of the London Mathematical Society. Third Series. Vol. 97. 2008; p. 545–67.

[34] B. Rodgers, *The covariance of almost-primes in* $\mathbb{F}_q[T]$, arXiv:1311.4905 [math.NT]

[35] P. Sarnak, *Three lectures on Möbius randomness*, (2011) available at http://www.math.ias.edu/files/wam/2011/PSMobius.pdf

[36] F. Thorne, *Irregularities in the distributions of primes in function fields*. J. Number Theory 128 (2008), no. 6, 1784–1794.

[37] Y. Zhang, *Bounded gaps between primes*, Annals of Mathematics, Volume 179 Issue 3 (2014), 1121–1174.

Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel

E-mail: rudnick@post.tau.ac.il