Prime Polynomial Values of Linear Functions in Short Intervals

Efrat Bank

School of Mathematical Sciences
Tel-Aviv University

joint with L. Bary-Soroker

Outline

Outline

The Prime Number Theorem

- *Let* $\mathbb{1}$ *be the prime characteristic function, i.e.,*

$$\mathbb{1}(h) = \begin{cases} 1, & h \text{ is prime} \\ 0, & \text{otherwise.} \end{cases}$$

The Prime Number Theorem

- *Let $\mathbb{1}$ be the prime characteristic function, i.e.,*

$$\mathbb{1}(h) = \begin{cases} 1, & h \text{ is prime} \\ 0, & \text{otherwise.} \end{cases}$$

- *The Prime Number Theorem (PNT):*

$$\sum_{0<h\leq x} \mathbb{1}(h) \sim \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x}$$

as $x \longrightarrow \infty$.

The Prime Polynomial Theorem

- *Let* $\mathcal{M}(k,q) \subseteq \mathcal{P}_{\leq k} \subset \mathbb{F}_q[t]$

The Prime Polynomial Theorem

- *Let* $\mathcal{M}(k,q) \subseteq \mathcal{P}_{\leq k} \subset \mathbb{F}_q[t]$
- *For* $h \in \mathbb{F}_q[t]$ *let* $||h|| = q^{\deg h}$ *and* $||0|| = 0$.

The Prime Polynomial Theorem

- *Let* $\mathcal{M}(k,q) \subseteq \mathcal{P}_{\leq k} \subset \mathbb{F}_q[t]$
- *For* $h \in \mathbb{F}_q[t]$ *let* $||h|| = q^{\deg h}$ *and* $||0|| = 0$.
- *Let* $\mathbb{1}$ *be the prime polynomial characteristic function, i.e.,*

$$\mathbb{1}(h) = \begin{cases} 1, & h \text{ is prime} \\ 0, & \text{otherwise.} \end{cases}$$

(prime polynomial = monic + irreducible polynomial)

The Prime Polynomial Theorem

- *The Prime Polynomial Theorem (PPT):*

$$\sum_{h \in \mathcal{M}(k,q)} \mathbb{1}(h) \sim \frac{q^k}{k}$$

The Prime Polynomial Theorem

- *The Prime Polynomial Theorem (PPT):*

$$\sum_{h \in \mathcal{M}(k,q)} \mathbb{1}(h) \sim \frac{q^k}{k}$$

$$\sum_{h \in \mathcal{M}(k,q)} \mathbb{1}(h) = \frac{q^k}{k} + O\left(\frac{q^{k/2}}{k}\right)$$

The Prime Polynomial Theorem

- *The Prime Polynomial Theorem (PPT):*

$$\sum_{h\in\mathcal{M}(k,q)} \mathbb{1}(h) \sim \frac{q^k}{k}$$

$$\sum_{h\in\mathcal{M}(k,q)} \mathbb{1}(h) = \frac{q^k}{k} + O\left(\frac{q^{k/2}}{k}\right)$$

In comparison with PNT, we replace:

- $0 < h \leq x \leftrightarrow h \in \mathcal{M}(k,q)$
- $|[0,x]| = x \leftrightarrow |\{h \in \mathcal{M}(k,q)\}| = q^k$
- $\log x \leftrightarrow k$

Limit issues

- *In the PNT, we consider the limit $x \longrightarrow \infty$. In the PPT, we consider the limit $q^k \longrightarrow \infty$*

Limit issues

- *In the PNT, we consider the limit* $x \longrightarrow \infty$. *In the PPT, we consider the limit* $q^k \longrightarrow \infty$
- $q^k \longrightarrow \infty$

Limit issues

- *In the PNT, we consider the limit* $x \longrightarrow \infty$*. In the PPT, we consider the limit* $q^k \longrightarrow \infty$
- $q^k \longrightarrow \infty$
  - $k \longrightarrow \infty$

Limit issues

- *In the PNT, we consider the limit $x \longrightarrow \infty$. In the PPT, we consider the limit $q^k \longrightarrow \infty$*
- $q^k \longrightarrow \infty$
  - $k \longrightarrow \infty$
  - $q \longrightarrow \infty$

Outline

Outline

1. Introduction
2. **Conjectures vs. Theorems**
   - Primes in Short Intervals
   - Primes in Arithmetic Progressions
   - Correlations Between Primes
   - Combined Conjecture
3. Method of proof
4. Recent related works

Prime numbers in short intervals

- *Let* $I = (x, x + \Phi(x)]$. *One may naively expect that,*

$$\sum_{h \in I} \mathbb{1}(h) \sim \frac{\Phi(x)}{\log x}.$$

Prime numbers in short intervals

- *Let $I = (x, x + \Phi(x)]$. One may naively expect that,*

$$\sum_{h \in I} \mathbb{1}(h) \sim \frac{\Phi(x)}{\log x}.$$

- *Clearly, Φ must satisfy $\frac{\Phi(x)}{\log x} \longrightarrow \infty$ as $x \longrightarrow \infty$.*

Prime numbers in short intervals

- *Let* $I = (x, x + \Phi(x)]$. *One may naively expect that,*

$$\sum_{h \in I} \mathbb{1}(h) \sim \frac{\Phi(x)}{\log x}.$$

- *Clearly,* Φ *must satisfy* $\frac{\Phi(x)}{\log x} \longrightarrow \infty$ *as* $x \longrightarrow \infty$.
- *From PNT, the above holds for* $\Phi(x) \sim cx$ *for any fixed* $0 < c < 1$.

Prime numbers in short intervals

- *Let* $I = (x, x + \Phi(x)]$. *One may naively expect that,*

$$\sum_{h \in I} \mathbb{1}(h) \sim \frac{\Phi(x)}{\log x}.$$

- *Clearly,* Φ *must satisfy* $\frac{\Phi(x)}{\log x} \longrightarrow \infty$ *as* $x \longrightarrow \infty$.
- *From PNT, the above holds for* $\Phi(x) \sim cx$ *for any fixed* $0 < c < 1$.
- *Assuming the Riemann Hypothesis, it holds for* $\Phi(x) \sim x^{\frac{1}{2}+\epsilon}$.

Prime numbers in short intervals

- *Let $I = (x, x + \Phi(x)]$. One may naively expect that,*

$$\sum_{h \in I} \mathbb{1}(h) \sim \frac{\Phi(x)}{\log x}.$$

- *Clearly, Φ must satisfy $\frac{\Phi(x)}{\log x} \longrightarrow \infty$ as $x \longrightarrow \infty$.*
- *From PNT, the above holds for $\Phi(x) \sim cx$ for any fixed $0 < c < 1$.*
- *Assuming the Riemann Hypothesis, it holds for $\Phi(x) \sim x^{\frac{1}{2}+\epsilon}$.*
- *For $\Phi(x) \sim \log^2 x$ Selberg showed (assuming RH) that it is true for almost every x, however, Maier showed that it does not hold for all x.*

Conjecture (Primes in short intervals)

$$\sum_{h \in I} \mathbb{1}(h) \sim \frac{x^{\epsilon}}{\log x}.$$

Where $I = (x, x + x^{\epsilon}]$, *$x$ is large and* $0 < \epsilon < 1$.

Conjecture (Primes in short intervals)

$$\sum_{h \in I} \mathbb{1}(h) \sim \frac{x^{\epsilon}}{\log x}.$$

Where $I = (x, x + x^{\epsilon}]$, *x is large and* $0 < \epsilon < 1$.

- *Heath-Brown (1988) proved this for* $\epsilon = \frac{7}{12}$

Conjecture (Primes in short intervals)

$$\sum_{h \in I} \mathbb{1}(h) \sim \frac{x^{\epsilon}}{\log x}.$$

Where $I = (x, x + x^{\epsilon}]$, x *is large and* $0 < \epsilon < 1$.

- *Heath-Brown (1988) proved this for* $\epsilon = \frac{7}{12}$
- *The barrier is* $\epsilon = \frac{1}{2}$.

Prime Polynomials in short intervals

- *An interval* $\mathcal{I}$ *around* $f_0 \in \mathcal{M}(k, q)$ *is defined as*

$$\mathcal{I} = \mathcal{I}(f_0, m) = \{h \in \mathbb{F}_q[t] \,:\, ||f_0 - h|| \leq q^m\} = f_0 + \mathcal{P}_{\leq m}$$

Prime Polynomials in short intervals

- *An interval* $\mathcal{I}$ *around* $f_0 \in \mathcal{M}(k, q)$ *is defined as*

$$\mathcal{I} = \mathcal{I}(f_0, m) = \{h \in \mathbb{F}_q[t] \,:\, ||f_0 - h|| \leq q^m\} = f_0 + \mathcal{P}_{\leq m}$$

- *We want to estimate the number of primes in short intervals, i.e., when* $m < k$.

Theorem (B., Bary-Soroker, Rosenzweig)

Let $f_0 \in \mathcal{M}(k,q)$, $3 \leq m < k$, and $\mathcal{I} = \mathcal{I}(f_0, m)$. Then,

$$\sum_{f \in \mathcal{I}} \mathbb{1}(f) = \frac{\#\mathcal{I}}{k}\left(1 + O_k(q^{-1/2})\right),$$

as $q \longrightarrow \infty$ and where the constant depends only on k.

Theorem (B., Bary-Soroker, Rosenzweig)

Let $f_0 \in \mathcal{M}(k,q)$, $3 \leq m < k$, and $\mathcal{I} = \mathcal{I}(f_0, m)$. Then,

$$\sum_{f \in \mathcal{I}} \mathbb{1}(f) = \frac{\#\mathcal{I}}{k}(1 + O_k(q^{-1/2})),$$

as $q \longrightarrow \infty$ and where the constant depends only on k.

- *In particular, if we let $\epsilon = \frac{m}{k}$ we get the full analogue of the Number Theory case.*

Theorem (B., Bary-Soroker, Rosenzweig)

Let $f_0 \in \mathcal{M}(k,q)$, $3 \leq m < k$, *and* $\mathcal{I} = \mathcal{I}(f_0, m)$. *Then,*

$$\sum_{f \in \mathcal{I}} \mathbb{1}(f) = \frac{\#\mathcal{I}}{k}(1 + O_k(q^{-1/2})),$$

as $q \longrightarrow \infty$ *and where the constant depends only on* k.

- *In particular, if we let* $\epsilon = \frac{m}{k}$ *we get the full analogue of the Number Theory case.*
- *We also deal with the cases* $m < 3$.

Theorem (B., Bary-Soroker, Rosenzweig)

Let $f_0 \in \mathcal{M}(k, q)$, $3 \leq m < k$, and $\mathcal{I} = \mathcal{I}(f_0, m)$. Then,

$$\sum_{f \in \mathcal{I}} \mathbb{1}(f) = \frac{\#\mathcal{I}}{k}(1 + O_k(q^{-1/2})),$$

as $q \longrightarrow \infty$ and where the constant depends only on k.

- *In particular, if we let $\epsilon = \frac{m}{k}$ we get the full analogue of the Number Theory case.*
- *We also deal with the cases $m < 3$.*
    - *For $m = 2$ we show that it holds under additional conditions.*

Theorem (B., Bary-Soroker, Rosenzweig)

Let $f_0 \in \mathcal{M}(k, q)$, $3 \leq m < k$, and $\mathcal{I} = \mathcal{I}(f_0, m)$. Then,

$$\sum_{f \in \mathcal{I}} \mathbb{1}(f) = \frac{\#\mathcal{I}}{k}(1 + O_k(q^{-1/2})),$$

as $q \longrightarrow \infty$ and where the constant depends only on k.

- *In particular, if we let $\epsilon = \frac{m}{k}$ we get the full analogue of the Number Theory case.*
- *We also deal with the cases $m < 3$.*
    - *For $m = 2$ we show that it holds under additional conditions.*
    - *For $m = 1, 0$ we show that it fails.*

Outline

Primes in Arithmetic Progressions

- *Let a and b be fixed, relatively prime integers.*

Primes in Arithmetic Progressions

- *Let a and b be fixed, relatively prime integers.*
- *The Prime Number Theorem for Arithmetic Progressions:*

$$\sum_{\substack{0<h<x \\ h\equiv a \pmod b}} \mathbb{1}(h) \sim \frac{1}{\varphi(b)} \cdot \frac{x}{\log(x)}$$

Conjecture (Primes in AP with large modulus)

For every $\delta > 0$,

$$\sum_{\substack{0<h<x \\ h \equiv a \pmod{b}}} \mathbb{1}(h) \sim \frac{1}{\varphi(b)} \cdot \frac{x}{\log(x)}$$

holds in the range $0 < a < b < x^{1-\delta}$

Conjecture (Primes in AP with large modulus)

For every $\delta > 0$,

$$\sum_{\substack{0<h<x \\ h\equiv a \pmod b}} \mathbb{1}(h) \sim \frac{1}{\varphi(b)} \cdot \frac{x}{\log(x)}$$

holds in the range $0 < a < b < x^{1-\delta}$

- *Assuming GRH, the above remains true when $b < x^{\frac{1}{2}-o(1)}$.*

Conjecture (Primes in AP with large modulus)

For every $\delta > 0$,

$$\sum_{\substack{0<h<x \\ h\equiv a \pmod b}} \mathbb{1}(h) \sim \frac{1}{\varphi(b)} \cdot \frac{x}{\log(x)}$$

holds in the range $0 < a < b < x^{1-\delta}$

- *Assuming GRH, the above remains true when $b < x^{\frac{1}{2}-o(1)}$.*
- *Bombieri-Vinogradov: true for almost all $b < x^{\frac{1}{2}-o(1)}$.*

Theorem (B., Bary-Soroker, Rosenzweig)

Let k be a fixed integer and $\delta > 0$. Then,

$$\sum_{\substack{h \in \mathcal{M}(k,q) \\ h \equiv a \pmod{b}}} \mathbb{1}(h) \sim \frac{1}{\varphi(b)} \cdot \frac{q^k}{k}$$

holds uniformly for all relatively prime $a(t), b(t) \in \mathbb{F}_q[t]$ with $\deg b < k(1-\delta)$

Conjecture (Primes in AP in short intervals)

Let $L(X) = bX + a, \qquad a, b \in \mathbb{Z}$

$$\sum_{h \in [x, x+x^{\epsilon}]} \mathbb{1}(L(h)) \sim \frac{b}{\varphi(b)} \cdot \frac{x^{\epsilon}}{\log(L(x))}, \quad x \to \infty,$$

where $0 < a < b$, $b^{\delta} < x$ *or* $b < 0$, $|b|^{1+\delta} < a$ *and* $|b|x^{\alpha} < a < |b|x^{\beta}$ *for* $1 < \alpha < \beta$.

Outline

Correlations between primes

Conjecture (The Hardy-Littlewood n-tuple conjecture)

$$\sum_{0<h\leq x} \mathbb{1}(h+a_1)\cdots\mathbb{1}(h+a_n) \sim \mathfrak{S}(a_1,\ldots,a_n)\frac{x}{(\log x)^n}, \quad x\to\infty,$$

where the a_i's are distinct and $\mathfrak{S}(a_1,\ldots,a_n)$ is a constant depending on the a_i's.

Hardy-Littlewood for function fields

Theorem (Hardy-Littlewood for function fields)

$$\sum_{h \in \mathcal{M}(k,q)} \mathbb{1}(h+a_1)\cdots\mathbb{1}(h+a_n) = \frac{q^k}{k^n}(1+O_{k,n}(q^{-1/2})),$$

holds uniformly on all $a_1, \ldots, a_n \in \mathbb{F}_q[t]$ *of degrees* $\deg(a_i) < k$ *and for a fixed* k*.*

Hardy-Littlewood for function fields

Theorem (Hardy-Littlewood for function fields)

$$\sum_{h \in \mathcal{M}(k,q)} \mathbb{1}(h+a_1)\cdots\mathbb{1}(h+a_n) = \frac{q^k}{k^n}(1+O_{k,n}(q^{-1/2})),$$

holds uniformly on all $a_1, \ldots, a_n \in \mathbb{F}_q[t]$ *of degrees* $\deg(a_i) < k$ *and for a fixed* k*.*

- *Bender and Pollack (2009) proved this for the case* $n = 2$ *and* q *odd.*

Hardy-Littlewood for function fields

Theorem (Hardy-Littlewood for function fields)

$$\sum_{h\in\mathcal{M}(k,q)} \mathbb{1}(h+a_1)\cdots\mathbb{1}(h+a_n) = \frac{q^k}{k^n}(1+O_{k,n}(q^{-1/2})),$$

holds uniformly on all $a_1,\ldots,a_n \in \mathbb{F}_q[t]$ of degrees $\deg(a_i) < k$ and for a fixed k.

- *Bender and Pollack (2009) proved this for the case $n = 2$ and q odd.*
- *Bary-Soroker (2014) proved this for any n and q odd.*

Hardy-Littlewood for function fields

Theorem (Hardy-Littlewood for function fields)

$$\sum_{h\in\mathcal{M}(k,q)} \mathbb{1}(h+a_1)\cdots\mathbb{1}(h+a_n) = \frac{q^k}{k^n}(1+O_{k,n}(q^{-1/2})),$$

holds uniformly on all $a_1,\dots,a_n \in \mathbb{F}_q[t]$ of degrees $\deg(a_i) < k$ and for a fixed k.

- *Bender and Pollack (2009) proved this for the case $n = 2$ and q odd.*
- *Bary-Soroker (2014) proved this for any n and q odd.*
- *Dan Carmon (2015) resolved the above for fields of characteristic 2.*

Outline

Let $L_i = b_i X + a_i$, $i = 1, \ldots, n$ be distinct primitive linear functions, i.e, $\gcd(a_i, b_i) = 1$. One may expect that,

Conjecture (Combined conjecture)

$$\sum_{h \in [x, x+x^{\epsilon}]} \mathbb{1}(L_1(h)) \cdots \mathbb{1}(L_n(h)) \sim \mathfrak{S}(L_1, \ldots, L_n) \frac{x^{\epsilon}}{\prod_{i=1}^{n} \log(L_i(x))},$$

holds uniformly, when $x \to \infty$ and $\mathfrak{S}(L_1, \ldots, L_n)$ is a constant depending on the L_i's.

Prime polynomial values of several linear functions in short intervals

Theorem (B., Bary-Soroker)

Let $B > 0$ *and* $f_0 \in \mathcal{M}(k,q)$, $2 \leq m < k$, $\mathcal{I}(f_0,m)$. *Then,*

$$\sum_{f \in \mathcal{I}(f_0,m)} \mathbb{1}(L_1(f)) \cdots \mathbb{1}(L_n(f)) = \frac{\#\mathcal{I}(f_0,m)}{\prod_{i=1}^{n} \deg(L_i(f_0))}(1 + O_B(q^{-1/2}))$$

holds uniformly as $q \longrightarrow \infty$ *odd, for:*

Prime polynomial values of several linear functions in short intervals

Theorem (B., Bary-Soroker)

Let $B > 0$ *and* $f_0 \in \mathcal{M}(k,q)$, $2 \leq m < k$, $\mathcal{I}(f_0,m)$. *Then,*

$$\sum_{f \in \mathcal{I}(f_0,m)} \mathbb{1}(L_1(f)) \cdots \mathbb{1}(L_n(f)) = \frac{\#\mathcal{I}(f_0,m)}{\prod_{i=1}^{n} \deg(L_i(f_0))}(1 + O_B(q^{-1/2}))$$

holds uniformly as $q \longrightarrow \infty$ *odd, for:*

- $L_1(X), \ldots, L_n(X)$ *distinct primitive linear functions*

Prime polynomial values of several linear functions in short intervals

Theorem (B., Bary-Soroker)

Let $B > 0$ *and* $f_0 \in \mathcal{M}(k,q)$, $2 \leq m < k$, $\mathcal{I}(f_0,m)$. *Then,*

$$\sum_{f\in\mathcal{I}(f_0,m)} \mathbb{1}(L_1(f))\cdots\mathbb{1}(L_n(f)) = \frac{\#\mathcal{I}(f_0,m)}{\prod_{i=1}^{n}\deg(L_i(f_0))}(1+O_B(q^{-1/2}))$$

holds uniformly as $q \longrightarrow \infty$ *odd, for:*

- $L_1(X),\ldots,L_n(X)$ *distinct primitive linear functions*
- *The* L_i*'s are of bounded height, i.e.,* $\max\{\deg a_i(t), \deg b_i(t)\} \leq B$

Prime polynomial values of several linear functions in short intervals

Theorem (B., Bary-Soroker)

Let $B > 0$ *and* $f_0 \in \mathcal{M}(k, q)$, $2 \leq m < k$, $\mathcal{I}(f_0, m)$. *Then,*

$$\sum_{f \in \mathcal{I}(f_0,m)} \mathbb{1}(L_1(f)) \cdots \mathbb{1}(L_n(f)) = \frac{\#\mathcal{I}(f_0, m)}{\prod_{i=1}^{n} \deg(L_i(f_0))}(1 + O_B(q^{-1/2}))$$

holds uniformly as $q \longrightarrow \infty$ *odd, for:*

- $L_1(X), \ldots, L_n(X)$ *distinct primitive linear functions*
- *The* L_i*'s are of bounded height, i.e.,* $\max\{\deg a_i(t), \deg b_i(t)\} \leq B$
- $1 \leq n \leq B$

Prime polynomial values of several linear functions in short intervals

Theorem (B., Bary-Soroker)

Let $B > 0$ *and* $f_0 \in \mathcal{M}(k,q)$, $2 \leq m < k$, $\mathcal{I}(f_0, m)$. *Then,*

$$\sum_{f \in \mathcal{I}(f_0,m)} \mathbb{1}(L_1(f)) \cdots \mathbb{1}(L_n(f)) = \frac{\#\mathcal{I}(f_0,m)}{\prod_{i=1}^{n} \deg(L_i(f_0))}(1 + O_B(q^{-1/2}))$$

holds uniformly as $q \longrightarrow \infty$ *odd, for:*

- $L_1(X), \ldots, L_n(X)$ *distinct primitive linear functions*
- *The* L_i*'s are of bounded height, i.e.,* $\max\{\deg a_i(t), \deg b_i(t)\} \leq B$
- $1 \leq n \leq B$
- $3 \leq k \leq B$

Outline

Main idea

- *The main idea is to consider a generic polynomial $\mathcal{F} \in \mathcal{I}(f_0, m)$. This means that we think of such a polynomial as a polynomial of the form*

$$\mathcal{F}(\mathbf{A}, t) = f_0(t) + \sum_{i=0}^{m} A_i t^i \in \mathbb{F}_q[A_0, \dots, A_m][t]$$

Main idea

- *The main idea is to consider a generic polynomial $\mathcal{F} \in \mathcal{I}(f_0, m)$. This means that we think of such a polynomial as a polynomial of the form*

$$\mathcal{F}(\mathbf{A}, t) = f_0(t) + \sum_{i=0}^{m} A_i t^i \in \mathbb{F}_q[A_0, ..., A_m][t]$$

- *We are interested in the number of substitutions $A_i \mapsto a_i$ where $a_i \in \mathbb{F}_q$ such that $L_i(\mathcal{F}(a_0, ..., a_m, t))$, $i = 1, ..., n$ are all prime polynomials.*

Main idea

- *The main idea is to consider a generic polynomial $\mathcal{F} \in \mathcal{I}(f_0, m)$. This means that we think of such a polynomial as a polynomial of the form*

$$\mathcal{F}(\mathbf{A}, t) = f_0(t) + \sum_{i=0}^{m} A_i t^i \in \mathbb{F}_q[A_0, ..., A_m][t]$$

- *We are interested in the number of substitutions $A_i \mapsto a_i$ where $a_i \in \mathbb{F}_q$ such that $L_i(\mathcal{F}(a_0, ..., a_m, t))$, $i = 1, ..., n$ are all prime polynomials.*
- *Using this idea, the proof is divided into two main parts:*
    - *Computing Galois groups.*
    - *Counting argument.*

Computing Galois group

Proposition

Let $L_1, \cdots, L_n$ *be distinct primitive linear functions and* $f_0 \in \mathbb{F}[t]$ *a monic polynomial of degree* k. *Let* $\mathcal{F} = f_0 + \sum_{j=0}^{m} A_j t^j$ *where* $2 \leq m < k$. *Then,*

$$\mathrm{Gal}\left(\prod_{i=1}^{n} L_i(\mathcal{F}), \mathbb{F}(\mathbf{A})\right) = \prod_{i=1}^{n} \mathrm{Gal}(L_i(\mathcal{F}), \mathbb{F}(\mathbf{A})) = S_{k_1} \times \cdots \times S_{k_n},$$

where $k_i = \deg(L_i(f_0))$.

Sketch proof of the proposition

Proof:

- The splitting fields of $L_i(\mathcal{F})$ are linearly disjoint.

Sketch proof of the proposition

Proof:

- The splitting fields of $L_i(\mathcal{F})$ are linearly disjoint.
- $\mathrm{Gal}(L_i(\mathcal{F}), \mathbb{F}(\mathbf{A})) = S_{k_i}$ where $k_i = \deg(L_i(f_0))$

Sketch proof of the proposition

Proof:

- The splitting fields of $L_i(\mathcal{F})$ are linearly disjoint.
- $\mathrm{Gal}(L_i(\mathcal{F}), \mathbb{F}(\mathbf{A})) = S_{k_i}$ where $k_i = \deg(L_i(f_0))$
  - $L_i(\mathcal{F})$ is separable in t and irreducible in the ring $\mathbb{F}(\mathbf{A})[t]$.

Sketch proof of the proposition

Proof:

- The splitting fields of $L_i(\mathcal{F})$ are linearly disjoint.
- $\mathrm{Gal}(L_i(\mathcal{F}), \mathbb{F}(\mathbf{A})) = S_{k_i}$ where $k_i = \deg(L_i(f_0))$
    - $L_i(\mathcal{F})$ is separable in t and irreducible in the ring $\mathbb{F}(\mathbf{A})[t]$.
    - The Galois group of $L_i(\mathcal{F})$ over $\mathbb{F}(\mathbf{A})$ is doubly transitive.

Sketch proof of the proposition

Proof:

- The splitting fields of $L_i(\mathcal{F})$ are linearly disjoint.
- $\mathrm{Gal}(L_i(\mathcal{F}), \mathbb{F}(\mathbf{A})) = S_{k_i}$ where $k_i = \deg(L_i(f_0))$
  - $L_i(\mathcal{F})$ is separable in t and irreducible in the ring $\mathbb{F}(\mathbf{A})[t]$.
  - The Galois group of $L_i(\mathcal{F})$ over $\mathbb{F}(\mathbf{A})$ is doubly transitive.
  - The Galois group of $L_i(\mathcal{F})$ contains a transposition.

Counting argument

Proposition (An explicit Chebotarev density theorem)

Let

$$\mathcal{H}(\mathbf{A}, t) = \mathcal{F}_1 \cdots \mathcal{F}_n \in \mathbb{F}_q[A_0, ..., A_m][t]$$

Assume that $\mathrm{Gal}(\mathcal{H}, \mathbb{F}_q(\mathbf{A})) = S_{k_1} \times \cdots \times S_{k_n}$ *where* $k_i = \deg_t(\mathcal{F}_i)$. *Then,*

$$\sum_{\mathbf{a} \in \mathbb{F}_q^{m+1}} \mathbb{1}(\mathcal{F}_1(\mathbf{a}, t)) \cdots \mathbb{1}(\mathcal{F}_n(\mathbf{a}, t)) = \frac{q^{m+1}}{\prod_{i=1}^{n} k_i}(1 + O_{m,B}(q^{-1/2}))$$

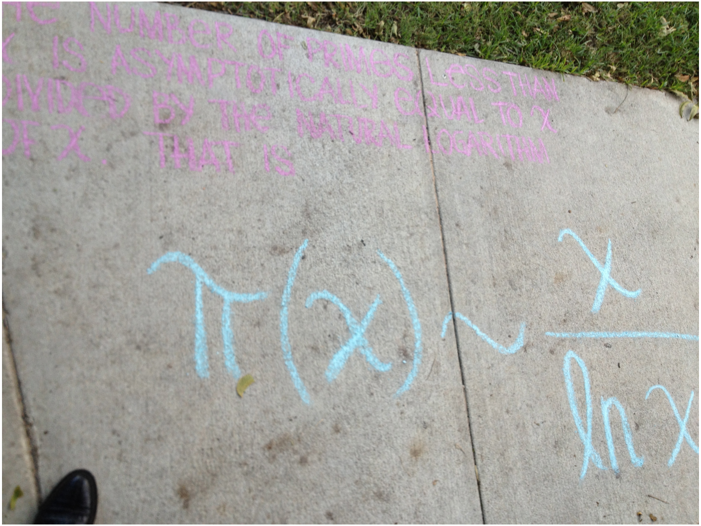
Outline

- *Keating-Rudnick (2014)- The variance of primes in short intervals.*

- *Keating-Rudnick (2014)- The variance of primes in short intervals.*
- *Carmon-Rudnick, Carmon (2014,2015)- Autocorrelations of the Mobius function and Chowla's conjecture.*

- *Keating-Rudnick (2014)- The variance of primes in short intervals.*
- *Carmon-Rudnick, Carmon (2014,2015)- Autocorrelations of the Mobius function and Chowla's conjecture.*
- *Entin (2015)- Bateman-Horn conjecture.*

- *Keating-Rudnick (2014)- The variance of primes in short intervals.*
- *Carmon-Rudnick, Carmon (2014,2015)- Autocorrelations of the Mobius function and Chowla's conjecture.*
- *Entin (2015)- Bateman-Horn conjecture.*
- *Rodgers (2015)- The covariance of almost-primes.*


NUMBER OF PRIMES LESS THAN
IS ASYMPTOTICALLY EQUAL TO X
BY THE NATURAL LOGARITHM
X. THAT IS
$\pi(x) \sim \frac{x}{\ln x}$