Exponential sums and the distribution of primes (in function fields)

Christian Bagshaw

Function Fields Down Under 2023

September 5, 2023

Distribution of Primes

If we want to think about how the primes are distributed, we should start with:

Distribution of Primes

If we want to think about how the primes are distributed, we should start with:

- How many primes are there up to some bound?

Distribution of Primes

If we want to think about how the primes are distributed, we should start with:

- How many primes are there up to some bound?
  - By Hadamard and Poussin: if $\pi(x)$ counts the number of primes less than x,

$$\pi(x) \sim \frac{x}{\log x} \text{ as } x \to \infty.$$

Distribution of Primes (in residue classes)

We can then ask the same question about arithmetic progressions!

Distribution of Primes (in residue classes)

We can then ask the same question about arithmetic progressions!

Given coprime integers a and m:

- How many primes are there up to some bound, congruent to a mod m?

Distribution of Primes (in residue classes)

We can then ask the same question about arithmetic progressions!

Given coprime integers a and m:

- How many primes are there up to some bound, congruent to a mod m?
  - If $\pi(x; m, a)$ counts the primes less than x, congruent to a mod m,

$$\pi(x; m, a) \sim \frac{\pi(x)}{\phi(m)} \text{ as } x \to \infty.$$

Distribution of Primes (in residue classes)

$$\pi(x; m, a) \sim \frac{\pi(x)}{\phi(m)} \text{ as } x \to \infty.$$

Distribution of Primes (in residue classes)

$$\pi(x; m, a) \sim \frac{\pi(x)}{\phi(m)} \text{ as } x \to \infty.$$

But how much bigger does x have to be than m?

Distribution of Primes (in residue classes)

$$\pi(x; m, a) \sim \frac{\pi(x)}{\phi(m)} \text{ as } x \to \infty.$$

But how much bigger does x have to be than m?

More precisely: does there exist some function $Q(x)$ (tending to infinity as $x \to \infty$), such that the above holds uniformly for all $m \leq Q(x)$ and all a coprime to m?

Distribution of Primes (in residue classes)

$$\pi(x; m, a) \sim \frac{\pi(x)}{\phi(m)} \text{ as } x \to \infty.$$

But how much bigger does x have to be than m?

More precisely: does there exist some function $Q(x)$ (tending to infinity as $x \to \infty$), such that the above holds uniformly for all $m \leq Q(x)$ and all a coprime to m?

Siegel-Walfisz: $Q(x) = (\log x)^A$.

Distribution of Primes (in residue classes)

$$\pi(x; m, a) \sim \frac{\pi(x)}{\phi(m)} \text{ as } x \to \infty.$$

But how much bigger does x have to be than m?

More precisely: does there exist some function $Q(x)$ (tending to infinity as $x \to \infty$), such that the above holds uniformly for all $m \leq Q(x)$ and all a coprime to m?

Siegel-Walfisz: $Q(x) = (\log x)^A$.

Assuming GRH: $Q(x) = x^{1/2}(\log x)^{-2}$.

Distribution of Primes (in residue classes)

$$\pi(x; m, a) \sim \frac{\pi(x)}{\phi(m)} \text{ as } x \to \infty.$$

But how much bigger does x have to be than m?

More precisely: does there exist some function $Q(x)$ (tending to infinity as $x \to \infty$), such that the above holds uniformly for all $m \leq Q(x)$ and all a coprime to m?

Siegel-Walfisz: $Q(x) = (\log x)^A$.

Assuming GRH: $Q(x) = x^{1/2}(\log x)^{-2}$.

Can we move beyond this barrier of $1/2$?

Distribution of Primes (in residue classes)

$$\pi(x; m, a) \sim \frac{\pi(x)}{\phi(m)} \text{ as } x \to \infty.$$

But how much bigger does x have to be than m?

More precisely: does there exist some function $Q(x)$ (tending to infinity as $x \to \infty$), such that the above holds uniformly for all $m \leq Q(x)$ and all a coprime to m?

Siegel-Walfisz: $Q(x) = (\log x)^A$.

Assuming GRH: $Q(x) = x^{1/2}(\log x)^{-2}$.

Can we move beyond this barrier of $1/2$?

I have no idea...

Distribution of Primes (in residue classes)

$$\pi(x; m, a) \sim \frac{\pi(x)}{\phi(m)} \text{ as } x \to \infty.$$

But how much bigger does x have to be than m?

More precisely: does there exist some function $Q(x)$ (tending to infinity as $x \to \infty$), such that the above holds uniformly for all $m \leq Q(x)$ and all a coprime to m?

Siegel-Walfisz: $Q(x) = (\log x)^A$.

Assuming GRH: $Q(x) = x^{1/2}(\log x)^{-2}$.

Can we move beyond this barrier of $1/2$?

I have no idea... but we can think about it in function fields...

Moving to Function Fields

Let q be an odd prime power, and $\mathbb{F}_q[T]$ the set of univariate polynomials over $\mathbb{F}_q$.

Moving to Function Fields

Let q be an odd prime power, and $\mathbb{F}_q[T]$ the set of univariate polynomials over $\mathbb{F}_q$.

Moving to Function Fields

Let q be an odd prime power, and $\mathbb{F}_q[T]$ the set of univariate polynomials over $\mathbb{F}_q$.

What is important to remember is that there are similarities between the properties of prime numbers and the properties of irreducible polynomials.

Distribution of Irreducibles

We can reframe the questions asked at the start but for $\mathbb{F}_q[T]$!

Distribution of Irreducibles

We can reframe the questions asked at the start but for $\mathbb{F}_q[T]$!

- How many (monic) irreducible polynomials are there of degree n?

Distribution of Irreducibles

We can reframe the questions asked at the start but for $\mathbb{F}_q[T]$!

- How many (monic) irreducible polynomials are there of degree n?
  - If $\pi(n)$ counts the number of (monic) irreducible polynomials of degree n then by a counting argument

$$\pi(n) \sim \frac{q^n}{n} \text{ as } n \to \infty$$

Distribution of Irreducibles (in residue classes)

We could also ask about arithmetic progressions!

Distribution of Irreducibles (in residue classes)

We could also ask about arithmetic progressions!

Given coprime $A, F \in \mathbb{F}_q[T]$,

Distribution of Irreducibles (in residue classes)

We could also ask about arithmetic progressions!

Given coprime $A, F \in \mathbb{F}_q[T]$,

- How many (monic) irreducible polynomials are there of degree n, congruent to A mod F?

Distribution of Irreducibles (in residue classes)

We could also ask about arithmetic progressions!

Given coprime $A, F \in \mathbb{F}_q[T]$,

- How many (monic) irreducible polynomials are there of degree n, congruent to A mod F?

Again, let's focus on this one!

Distribution of Irreducibles (in residue classes)

If $\pi(n; F, A)$ count the number of monic irreducible polynomials of degree n, congruent to A mod F, then

$$\pi(n; F, A) \sim \frac{\pi(n)}{\phi(F)} \text{ as } n \to \infty.$$

Distribution of Irreducibles (in residue classes)

If $\pi(n; F, A)$ count the number of monic irreducible polynomials of degree n, congruent to A mod F, then

$$\pi(n; F, A) \sim \frac{\pi(n)}{\phi(F)} \text{ as } n \to \infty.$$

For how big of a range of F (in terms of n) does this hold uniformly?

Distribution of Irreducibles (in residue classes)

If $\pi(n; F, A)$ count the number of monic irreducible polynomials of degree n, congruent to A mod F, then

$$\pi(n; F, A) \sim \frac{\pi(n)}{\phi(F)} \text{ as } n \to \infty.$$

For how big of a range of F (in terms of n) does this hold uniformly?

It turns out GRH holds here, so $\deg F < \left(\frac{1}{2} - \epsilon\right) n$.

Distribution of Irreducibles (in residue classes)

If $\pi(n; F, A)$ count the number of monic irreducible polynomials of degree n, congruent to A mod F, then

$$\pi(n; F, A) \sim \frac{\pi(n)}{\phi(F)} \text{ as } n \to \infty.$$

For how big of a range of F (in terms of n) does this hold uniformly?

It turns out GRH holds here, so $\deg F < \left(\frac{1}{2} - \epsilon\right) n$. This is the same as the $1/2$ barrier over $\mathbb{Z}$!

Distribution of Irreducibles (in residue classes)

If $\pi(n; F, A)$ count the number of monic irreducible polynomials of degree n, congruent to A mod F, then

$$\pi(n; F, A) \sim \frac{\pi(n)}{\phi(F)} \text{ as } n \to \infty.$$

For how big of a range of F (in terms of n) does this hold uniformly?

It turns out GRH holds here, so $\deg F < \left(\frac{1}{2} - \epsilon\right) n$. This is the same as the $1/2$ barrier over $\mathbb{Z}$!

Can we have this hold for $\deg F < \left(\frac{1}{2} + \delta\right) n$ for some $\delta > 0$?

Moving past $1/2$

In a very nice paper, Sawin and Shusterman (among many other things) were able to move past this barrier.

Moving past 1/2

In a very nice paper, Sawin and Shusterman (among many other things) were able to move past this barrier.

Theorem (Sawin and Shusterman (2022))

For q sufficiently large in terms of char$(\mathbb{F}_q)$ *and* ϵ,

$$\pi(n; F, A) \sim \frac{\pi(n)}{\phi(F)} \text{ uniformly for } \deg F < \left(\frac{1}{2} + \frac{1}{126} - \epsilon\right) n \text{ and } F \text{ square-free.}$$

Moving past 1/2

In a very nice paper, Sawin and Shusterman (among many other things) were able to move past this barrier.

Theorem (Sawin and Shusterman (2022))

For q sufficiently large in terms of char$(\mathbb{F}_q)$ *and* ϵ*,*

$$\pi(n; F, A) \sim \frac{\pi(n)}{\phi(F)} \text{ uniformly for } \deg F < \left(\frac{1}{2} + \frac{1}{126} - \epsilon\right) n \text{ and } F \text{ square-free.}$$

Sawin subsequently improved on this.

Moving past 1/2

In a very nice paper, Sawin and Shusterman (among many other things) were able to move past this barrier.

Theorem (Sawin and Shusterman (2022))

For q sufficiently large in terms of char$(\mathbb{F}_q)$ *and* ϵ,

$$\pi(n; F, A) \sim \frac{\pi(n)}{\phi(F)} \text{ uniformly for } \deg F < \left(\frac{1}{2} + \frac{1}{126} - \epsilon\right) n \text{ and } F \text{ square-free.}$$

Sawin subsequently improved on this.

Theorem (Sawin (2023))

For q sufficiently large in terms of ϵ,

$$\pi(n; F, A) \sim \frac{\pi(n)}{\phi(F)} \text{ uniformly for } \deg F < \left(\frac{1}{2} + \frac{1}{2} - \epsilon\right) n \text{ and } F \text{ square-free.}$$

Moving past 1/2

In a very nice paper, Sawin and Shusterman (among many other things) were able to move past this barrier.

Theorem (Sawin and Shusterman (2022))

For q sufficiently large in terms of char($\mathbb{F}_q$) and ϵ,

$$\pi(n; F, A) \sim \frac{\pi(n)}{\phi(F)} \text{ uniformly for } \deg F < \left(\frac{1}{2} + \frac{1}{126} - \epsilon\right) n \text{ and } F \text{ square-free.}$$

Sawin subsequently improved on this.

Theorem (Sawin (2023))

For q sufficiently large in terms of ϵ,

$$\pi(n; F, A) \sim \frac{\pi(n)}{\phi(F)} \text{ uniformly for } \deg F < \left(\frac{1}{2} + \frac{1}{2} - \epsilon\right) n \text{ and } F \text{ square-free.}$$

What about arbitrary modulus F?

Arbitrary Modulus

The methods used to prove Sawin's most recent result are very high-powered and specialized to square-free modulus.

The methods used to prove Sawin's most recent result are very high-powered and specialized to square-free modulus. But one of the ingredients in their first result can be worked on, to give the following.

Arbitrary Modulus

The methods used to prove Sawin's most recent result are very high-powered and specialized to square-free modulus. But one of the ingredients in their first result can be worked on, to give the following.

Theorem (B.)

For q sufficiently large in terms of char$(\mathbb{F}_q)$ and ϵ,

$$\pi(n; F, A) \sim \frac{\pi(n)}{\phi(F)} \text{ uniformly for } \deg F < \left(\frac{1}{2} + \frac{1}{62} - \epsilon\right) n.$$

Which ingredient?

Using the von Mangoldt function, Vaughan's identity reduces the problem to bounding sums of the form

$$\sum_{\substack{\deg X < a \\ (X,F)=1}} \mu(X) \sum_{\substack{\deg Y < b \\ XY \equiv A \pmod{F}}} 1.$$

Which ingredient?

Using the von Mangoldt function, Vaughan's identity reduces the problem to bounding sums of the form

$$\sum_{\substack{\deg X < a \\ (X,F)=1}} \mu(X) \sum_{\substack{\deg Y < b \\ XY \equiv A \pmod{F}}} 1.$$

In certain ranges of a and b, it is very difficult to get the type of cancellation needed (what Sawin and Shusterman did using some algebraic geometry).

Which ingredient?

Using the von Mangoldt function, Vaughan's identity reduces the problem to bounding sums of the form

$$\sum_{\substack{\deg X < a \\ (X,F)=1}} \mu(X) \sum_{\substack{\deg Y < b \\ XY \equiv A \pmod{F}}} 1.$$

In certain ranges of *a* and *b*, it is very difficult to get the type of cancellation needed (what Sawin and Shusterman did using some algebraic geometry).

But in other ranges, it turns out to be a job for exponential sums...

Detour on Exponential Sums

Let G be some (additive) group. A character of G is a homomorphism

$$\psi : G \;\to\; \{z \in \mathbb{C} \;:\; |z| = 1\}.$$

Detour on Exponential Sums

Let G be some (additive) group. A character of G is a homomorphism

$$\psi : G \ \rightarrow \ \{z \in \mathbb{C} \ : \ |z| = 1\}.$$

We are interested in them here because we can often represent counting problems as a "character sum";

Detour on Exponential Sums

Let G be some (additive) group. A character of G is a homomorphism

$$\psi : G \to \{z \in \mathbb{C} : |z| = 1\}.$$

We are interested in them here because we can often represent counting problems as a "character sum"; due to the orthogonality relation (for finite G)

$$\sum_{x \in G} \psi(x) = \begin{cases} |G|, & \psi \text{ is trivial} \\ 0, & \text{otherwise} \end{cases}$$

Back in $\mathbb{R}$ for a moment

Recall that in $\mathbb{R}$, there is a "canonical" additive character often used:

$$e^{2i\pi x}.$$

Back in $\mathbb{R}$ for a moment

Recall that in $\mathbb{R}$, there is a "canonical" additive character often used:

$$e^{2i\pi x}.$$

This is defined on all of $\mathbb{R}$, but also mixes very well over $\mathbb{Z}$.

Back in $\mathbb{R}$ for a moment

Recall that in $\mathbb{R}$, there is a "canonical" additive character often used:

$$e^{2i\pi x}.$$

This is defined on all of $\mathbb{R}$, but also mixes very well over $\mathbb{Z}$.

For any integer m, the function

$$x \to e^{2i\pi x/m}$$

is a non-trivial additive character of $\mathbb{Z}/m\mathbb{Z}$.

Back in $\mathbb{R}$ for a moment

Recall that in $\mathbb{R}$, there is a "canonical" additive character often used:

$$e^{2i\pi x}.$$

This is defined on all of $\mathbb{R}$, but also mixes very well over $\mathbb{Z}$.

For any integer m, the function

$$x \to e^{2i\pi x/m}$$

is a non-trivial additive character of $\mathbb{Z}/m\mathbb{Z}$. This provides the orthogonality relation

$$\frac{1}{m}\sum_{x=0}^{m-1} e^{2i\pi ax/m} = \begin{cases} 0, & a \not\equiv 0 \pmod{m} \\ 1, & a \equiv 0 \pmod{m}. \end{cases}$$

Defining an additive character in $\mathbb{F}_q[T]$

Recall that we are working in $\mathbb{F}_q[T]$.

Defining an additive character in $\mathbb{F}_q[T]$

Recall that we are working in $\mathbb{F}_q[T]$. It might be nice to have an additive character defined as explicitly as $e^{2i\pi x}$.

Defining an additive character in $\mathbb{F}_q[T]$

Recall that we are working in $\mathbb{F}_q[T]$. It might be nice to have an additive character defined as explicitly as $e^{2i\pi x}$.

To do this, we first are going to view $\mathbb{F}_q[T]$ as living inside some larger space.

Defining an additive character in $\mathbb{F}_q[T]$

Recall that we are working in $\mathbb{F}_q[T]$. It might be nice to have an additive character defined as explicitly as $e^{2i\pi x}$.

To do this, we first are going to view $\mathbb{F}_q[T]$ as living inside some larger space. We are going to let $\mathbb{F}_q(T)_\infty$ denote the set of Laurent series in $1/T$, so elements look like

$$\sum_{-\infty}^{n} a_i T^i = a_n T^n + ... + a_1 T + a_0 + a_{-1} T^{-1} + a_{-2} T^{-2} + ...$$

Defining an additive character in $\mathbb{F}_q[T]$

Recall that we are working in $\mathbb{F}_q[T]$. It might be nice to have an additive character defined as explicitly as $e^{2i\pi x}$.

To do this, we first are going to view $\mathbb{F}_q[T]$ as living inside some larger space. We are going to let $\mathbb{F}_q(T)_\infty$ denote the set of Laurent series in $1/T$, so elements look like

$$\sum_{-\infty}^{n} a_i T^i = a_n T^n + ... + a_1 T + a_0 + a_{-1} T^{-1} + a_{-2} T^{-2} + ...$$

$\mathbb{F}_q[T]$ very naturally sits inside $\mathbb{F}_q(T)_\infty$ (polynomials are the Laurent series with no negative powers of T).

Building additive characters

We will define the function

$$e_q\left(\sum_{i=-\infty}^{n} a_i T^i\right) = e^{2\pi i \ \mathrm{Tr}(a_{-1})/p}$$

where $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the absolute trace (p being the characteristic of $\mathbb{F}_q$).

Building additive characters

We will define the function

$$e_q\left(\sum_{i=-\infty}^{n} a_i T^i\right) = e^{2\pi i \ \mathrm{Tr}(a_{-1})/p}$$

where $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the absolute trace (p being the characteristic of $\mathbb{F}_q$). As an example, if q is prime then our function becomes

$$e_q\left(\sum_{i=-\infty}^{n} a_i T^i\right) = e^{2\pi i(a_{-1})/p}$$

Building additive characters

We will define the function

$$e_q\left(\sum_{i=-\infty}^{n} a_i T^i\right) = e^{2\pi i \ \mathrm{Tr}(a_{-1})/p}$$

where $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the absolute trace (p being the characteristic of $\mathbb{F}_q$). As an example, if q is prime then our function becomes

$$e_q\left(\sum_{i=-\infty}^{n} a_i T^i\right) = e^{2\pi i (a_{-1})/p}$$

First, one can easily verify that this function satisfies

$$e_q(X + Y) = e_q(X)e_q(Y).$$

Orthogonality

Why the coefficient on $1/T$?

Orthogonality

Why the coefficient on $1/T$?
It turns out that for any $F \in \mathbb{F}_q[T]$,

$$X \to e_q\left(\frac{X}{F}\right)$$

defines a non-trivial additive character modulo F,

Orthogonality

Why the coefficient on $1/T$?
It turns out that for any $F \in \mathbb{F}_q[T]$,

$$X \to e_q\left(\frac{X}{F}\right)$$

defines a non-trivial additive character modulo F, yielding the orthogonality relation

$$\frac{1}{q^{\deg F}} \sum_{\deg X < \deg F} e_q\left(\frac{AX}{F}\right) = \begin{cases} 0, & A \not\equiv 0 \pmod{F} \\ 1, & A \equiv 0 \pmod{F}. \end{cases}$$

Orthogonality

Why the coefficient on $1/T$?
It turns out that for any $F \in \mathbb{F}_q[T]$,

$$X \to e_q\left(\frac{X}{F}\right)$$

defines a non-trivial additive character modulo F, yielding the orthogonality relation

$$\frac{1}{q^{\deg F}} \sum_{\deg X < \deg F} e_q\left(\frac{AX}{F}\right) = \begin{cases} 0, & A \not\equiv 0 \pmod{F} \\ 1, & A \equiv 0 \pmod{F}. \end{cases}$$

Additionally, a very nice property in this setting is that

$$\frac{1}{q^n} \sum_{\deg X < n} e_q\left(\frac{AX}{F}\right) = \begin{cases} 1, & \deg(A \bmod F) < \deg F - n \\ 0, & \text{otherwise.} \end{cases} .$$

Orthogonality

Why the coefficient on $1/T$?
It turns out that for any $F \in \mathbb{F}_q[T]$,

$$X \to e_q\left(\frac{X}{F}\right)$$

defines a non-trivial additive character modulo F, yielding the orthogonality relation

$$\frac{1}{q^{\deg F}} \sum_{\deg X < \deg F} e_q\left(\frac{AX}{F}\right) = \begin{cases} 0, & A \not\equiv 0 \pmod{F} \\ 1, & A \equiv 0 \pmod{F}. \end{cases}$$

Additionally, a very nice property in this setting is that

$$\frac{1}{q^n} \sum_{\deg X < n} e_q\left(\frac{AX}{F}\right) = \begin{cases} 1, & \deg(A \bmod F) < \deg F - n \\ 0, & \text{otherwise.} \end{cases}.$$

Together with other properties, $e_q(X)$ is familiar enough to adapt tools for dealing with exponential sums over the real numbers.

Back to prime distribution

Now recall we were talking about the distribution of irreducible polynomials in residue classes,

Back to prime distribution

Now recall we were talking about the distribution of irreducible polynomials in residue classes, which reduced to a sum of the form

$$\sum_{\deg X < a} \mu(X) \sum_{\substack{\deg Y < b \\ XY \equiv A \pmod{F}}} 1.$$

Back to prime distribution

Now recall we were talking about the distribution of irreducible polynomials in residue classes, which reduced to a sum of the form

$$\sum_{\deg X < a} \mu(X) \sum_{\substack{\deg Y < b \\ XY \equiv A \pmod{F}}} 1.$$

Orthogonality now means

$$\sum_{\deg X < a} \mu(X) \sum_{\substack{\deg Y < b \\ XY \equiv A \pmod{F}}} 1 = \frac{1}{q^b} \sum_{\deg Y < \deg F - b} \sum_{\deg X < a} \mu(X) e_q\left(\frac{AX^{-1}Y}{F}\right)$$

Back to Distribution of Irreducibles

Now recall we were talking about the distribution of irreducible polynomials in residue classes, which reduced to a sum of the form

$$\sum_{\deg X<a} \mu(X) \sum_{\substack{\deg Y<b \\ XY\equiv A \pmod{F}}} 1.$$

Orthogonality now means

$$\sum_{\deg X<a} \mu(X) \sum_{\substack{\deg Y<b \\ XY\equiv A \pmod{F}}} 1 = \frac{1}{q^b} \sum_{\deg Y<\deg F-b} \sum_{\deg X<a} \mu(X) e_q\left(\frac{AX^{-1}Y}{F}\right)$$

The specifics don't matter so much, but what is important is that these types of exponential sums have been dealt with before over the integers.

Bounds on exponential sums

The most important case is

$$\sum_{\deg X < \deg F} \mu(X) e_q\left(\frac{AX^{-1}}{F}\right)$$

Bounds on exponential sums

The most important case is

$$\sum_{\deg X < \deg F} \mu(X) e_q\left(\frac{AX^{-1}}{F}\right)$$

Sawin and Shusterman adapted some methods of Fouvry and Michel (1998) to prove the following.

Bounds on exponential sums

The most important case is

$$\sum_{\deg X < \deg F} \mu(X) e_q\left(\frac{AX^{-1}}{F}\right)$$

Sawin and Shusterman adapted some methods of Fouvry and Michel (1998) to prove the following.

Theorem (Sawin and Shusterman)

For F square-free and arbitrary A, an upper-bound of $\ll q^{\deg F(31/32+\epsilon)}$.

Bounds on exponential sums

The most important case is

$$\sum_{\deg X < \deg F} \mu(X) e_q\left(\frac{AX^{-1}}{F}\right)$$

Sawin and Shusterman adapted some methods of Fouvry and Michel (1998) to prove the following.

Theorem (Sawin and Shusterman)

For F square-free and arbitrary A, an upper-bound of $\ll q^{\deg F(31/32+\epsilon)}$.

By adapting some methods of Garaev (2010) and Fouvry and Shparlinski (2011), this can be improved.

Bounds on exponential sums

The most important case is

$$\sum_{\deg X < \deg F} \mu(X) e_q \left(\frac{AX^{-1}}{F} \right)$$

Sawin and Shusterman adapted some methods of Fouvry and Michel (1998) to prove the following.

Theorem (Sawin and Shusterman)

For F square-free and arbitrary A, an upper-bound of $\ll q^{\deg F(31/32+\epsilon)}$.

By adapting some methods of Garaev (2010) and Fouvry and Shparlinski (2011), this can be improved.

Theorem (B.)

For F and A arbitrary, an upper-bound of $\ll q^{\deg F(15/16+\epsilon)}$.

Best hope for arbitrary modulus (at the moment)?

Best hope for arbitrary modulus (at the moment)?

If one could obtain square-root cancellation

Best hope for arbitrary modulus (at the moment)?

If one could obtain square-root cancellation

$$\sum_{\deg X < \deg F} \mu(X) e_q\left(\frac{AX^{-1}}{F}\right) \ll q^{\deg F(1/2+\epsilon)}.$$

Best hope for arbitrary modulus (at the moment)?

If one could obtain square-root cancellation

$$\sum_{\deg X < \deg F} \mu(X) e_q\left(\frac{AX^{-1}}{F}\right) \ll q^{\deg F(1/2+\epsilon)}.$$

then

$$\pi(n; F, A) \sim \frac{\pi(n)}{\phi(F)} \text{ uniformly for } \deg F < \left(\frac{1}{2} + \frac{1}{6} - \epsilon\right) n.$$

Time permitting

We wanted to bound

$$\frac{1}{q^b}\sum_{\deg Y<\deg F-b}\sum_{\deg X<a}\mu(X)e_q\left(\frac{AX^{-1}Y}{F}\right).$$

Expanding using Vaughan's identity yields something like an average over bilinear Kloosterman sums of the form

$$\sum_{\deg Y<n}\sum_{\deg X_1<m_1}\sum_{\deg X_2<m_2}\alpha_{X_1}\beta_{X_2}e_F(AYX_1^{-1}X_2^{-1}).$$

Sufficiently strong bounds on these might help.

Thank you!