Maier Matrices Beyond $\mathbb{Z}$

Frank Thorne

University of Wisconsin - Madison

October 11, 2007

The prime number theorem

Let $\pi(n)$ denote the number of primes $\leq n$. The **prime number theorem** says that

$$\pi(n) \sim \frac{n}{\log n}.$$

The prime number theorem

Let $\pi(n)$ denote the number of primes $\leq n$. The **prime number theorem** says that

$$\pi(n) \sim \frac{n}{\log n}.$$

Therefore, the "probability" n is prime is $\frac{1}{\log n}$.

The prime number theorem

Let $\pi(n)$ denote the number of primes $\leq n$. The **prime number theorem** says that

$$\pi(n) \sim \frac{n}{\log n}.$$

Therefore, the "probability" n is prime is $\frac{1}{\log n}$.

Can this heuristic be used to make predictions?

The Cramér model

The **Cramér model**: primes as random variables.

The Cramér model

The **Cramér model**: primes as random variables.

Example

The (naive) Cramér model predicts, for a fixed integer h,

$$\#\{n \leq X : n,\ n+h \text{ are both prime}\} \sim \frac{X}{\log^2 X}.$$

The Cramér model

The **Cramér model**: primes as random variables.

Example

The (naive) Cramér model predicts, for a fixed integer h,

$$\#\{n \leq X : n, \ n+h \text{ are both prime}\} \sim \frac{X}{\log^2 X}.$$

False: take $h = 1$. But this prediction can be fixed.

Some recent advances

Today: "Unusual" behavior, using Maier matrices.

Some recent advances

Today: "Unusual" behavior, using Maier matrices.

But first...

Arithmetic progressions of primes

Theorem (Green-Tao)

The primes contain arbitrarily long arithmetic progressions.

Small gaps between primes

Theorem (Goldston, Pintz, Yıldırım)

Let p_n denote the nth prime. Then

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} = 0.$$

Small gaps between primes

Theorem (Goldston, Pintz, Yıldırım)

Let p_n denote the nth prime. Then

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} = 0.$$

Related results:

Small gaps between primes

Theorem (Goldston, Pintz, Yıldırım)

Let p_n denote the nth prime. Then

$$\liminf_{n \to \infty} \frac{p_{n+1} - p_n}{\log p_n} = 0.$$

Related results:

- E_2 numbers: Goldston, Graham, Pintz, Yıldırım

Small gaps between primes

Theorem (Goldston, Pintz, Yıldırım)

Let p_n denote the nth prime. Then

$$\liminf_{n \to \infty} \frac{p_{n+1} - p_n}{\log p_n} = 0.$$

Related results:

- E_2 numbers: Goldston, Graham, Pintz, Yıldırım
- E_r numbers with certain restictions: T.

Short intervals and Maier's theorem

The probabilistic model predicts, for any $A > 2$,

$$\pi(n + \log^A n) - \pi(n) \sim \log^{A-1} n \tag{1}$$

with probability 1.

Short intervals and Maier's theorem

The probabilistic model predicts, for any $A > 2$,

$$\pi(n + \log^A n) - \pi(n) \sim \log^{A-1} n \tag{1}$$

with probability 1.

Theorem (Maier)

The asymptotic (1) does not hold for any A.

Maier's theorem

In particular:

Maier's theorem

In particular:

Theorem (Maier)

For any A there exists $\delta_A > 0$ such that

$$\limsup_{n \to \infty} \frac{\pi(n + \log^A n) - \pi(n)}{\log^{A-1} n} \geq 1 + \delta_A,$$

$$\liminf_{n \to \infty} \frac{\pi(n + \log^A n) - \pi(n)}{\log^{A-1} n} \leq 1 - \delta_A.$$

Overview

In today's talk:

Overview

In today's talk:

- An overview of Maier's proof.

Overview

In today's talk:

- An overview of Maier's proof.
- Related results due to Shiu, Friedlander-Granville, Granville-Soundararajan (among others).

Overview

In today's talk:

- An overview of Maier's proof.
- Related results due to Shiu, Friedlander-Granville, Granville-Soundararajan (among others).
- My own work in number fields and function fields.

The Maier matrix

Consider the **Maier matrix**

$$\begin{bmatrix} Qx_1 + 1 & Qx_1 + 2 & \dots & Qx_1 + y^A \\ Q(x_1+1) + 1 & Q(x_1+1) + 2 & \dots & Q(x_1+1) + y^A \\ \vdots & \vdots & \vdots & \vdots \\ Qx_2 + 1 & Qx_2 + 2 & \dots & Qx_2 + y^A \end{bmatrix},$$

where $Q = \prod_{p<n} p$, $x_2 = Q^{C_1}$, $y = (\log Qx_2) \sim n^{C_1+1}$.

The Maier matrix

Consider the **Maier matrix**

$$\begin{bmatrix} Qx_1+1 & Qx_1+2 & \dots & Qx_1+y^A \\ Q(x_1+1)+1 & Q(x_1+1)+2 & \dots & Q(x_1+1)+y^A \\ \vdots & \vdots & \vdots & \vdots \\ Qx_2+1 & Qx_2+2 & \dots & Qx_2+y^A \end{bmatrix},$$

where $Q = \prod_{p<n} p$, $x_2 = Q^{C_1}$, $y = (\log Qx_2) \sim n^{C_1+1}$.
Rows are intervals, columns are arithmetic progressions.

The Maier matrix

Consider the **Maier matrix**

$$\begin{bmatrix} Qx_1+1 & Qx_1+2 & \dots & Qx_1+y^A \\ Q(x_1+1)+1 & Q(x_1+1)+2 & \dots & Q(x_1+1)+y^A \\ \vdots & \vdots & \vdots & \vdots \\ Qx_2+1 & Qx_2+2 & \dots & Qx_2+y^A \end{bmatrix},$$

where $Q = \prod_{p<n} p$, $x_2 = Q^{C_1}$, $y = (\log Qx_2) \sim n^{C_1+1}$.
Rows are intervals, columns are arithmetic progressions.
Gallagher: For appropriate Q and large C_1, the primes are well-distributed in progressions mod Q.

The Maier matrix (cont.)

$$\begin{bmatrix} Qx_1 + 1 & Qx_1 + 2 & \dots & Qx_1 + y^A \\ Q(x_1+1) + 1 & Q(x_1+1) + 2 & \dots & Q(x_1+1) + y^A \\ \vdots & \vdots & \vdots & \vdots \\ Qx_2 + 1 & Qx_2 + 2 & \dots & Qx_2 + y^A \end{bmatrix}$$

- Total number of primes determined by number of $i \in [1, y^A]$ coprime to Q.

The Maier matrix (cont.)

$$\begin{bmatrix} Qx_1+1 & Qx_1+2 & \dots & Qx_1+y^A \\ Q(x_1+1)+1 & Q(x_1+1)+2 & \dots & Q(x_1+1)+y^A \\ \vdots & \vdots & \vdots & \vdots \\ Qx_2+1 & Qx_2+2 & \dots & Qx_2+y^A \end{bmatrix}$$

- Total number of primes determined by number of $i \in [1, y^A]$ coprime to Q.
- This is not necessarily asymptotic to $y^A \phi(Q)/Q$.

The Maier matrix (conclusion)

Conclusion: For appropriate choices of Q, etc.,

The Maier matrix (conclusion)

Conclusion: For appropriate choices of Q, etc.,

- The matrix contains more or fewer primes than expected, so,

The Maier matrix (conclusion)

Conclusion: For appropriate choices of Q, etc.,

- The matrix contains more or fewer primes than expected, so,
- Some row contains more or fewer primes than expected.

Shiu's theorem

Theorem (Shiu)

If $(a, q) = 1$, then there exist arbitrarily long strings of consecutive primes

$$p_{n+1} \equiv p_{n+2} \equiv \cdots \equiv p_{n+k} \equiv a \mod q.$$

Shiu's theorem

Theorem (Shiu)

If $(a, q) = 1$, then there exist arbitrarily long strings of consecutive primes

$$p_{n+1} \equiv p_{n+2} \equiv \cdots \equiv p_{n+k} \equiv a \mod q.$$

Moreover, for k large, p_{n+1} will satisfy

$$\frac{1}{\phi(q)} \left(\frac{\log\log p_{n+1} \log\log\log\log p_{n+1}}{(\log\log\log p_{n+1})^2} \right)^{1/\phi(q)} \ll k.$$

Proof of Shiu's theorem (sketch)

Special case: $a = 1$.

Let

$$Q = q \prod_{\substack{p \le y \\ p \not\equiv 1 \mod q \\ p \ne p_0}} p.$$

The prime p_0 is removed to a avoid a Siegel zero.

Proof of Shiu's theorem (sketch)

Special case: $a = 1$.
Let

$$Q = q \prod_{\substack{p \leq y \\ p \not\equiv 1 \mod q \\ p \neq p_0}} p.$$

The prime p_0 is removed to a avoid a Siegel zero.

Consider a similar Maier matrix, where:

Proof of Shiu's theorem (sketch)

Special case: $a = 1$.
Let

$$Q = q \prod_{\substack{p \leq y \\ p \not\equiv 1 \mod q \\ p \neq p_0}} p.$$

The prime p_0 is removed to a avoid a Siegel zero.

Consider a similar Maier matrix, where:

- The rows are intervals of length yz,

Proof of Shiu's theorem (sketch)

Special case: $a = 1$.
Let

$$Q = q \prod_{\substack{p \leq y \\ p \not\equiv 1 \mod q \\ p \neq p_0}} p.$$

The prime p_0 is removed to a avoid a Siegel zero.

Consider a similar Maier matrix, where:

- The rows are intervals of length yz,
- The columns are progressions mod Q.

Proof of Shiu's theorem, cont.

For appropriate parameters

Proof of Shiu's theorem, cont.

For appropriate parameters

- Most integers $i \in [1, yz]$ coprime to Q are $\equiv 1 \mod q$.

Proof of Shiu's theorem, cont.

For appropriate parameters

- Most integers $i \in [1, yz]$ coprime to Q are $\equiv 1 \mod q$.
- Most primes in the matrix are $\equiv 1 \mod q$.

Proof of Shiu's theorem, cont.

For appropriate parameters

- Most integers $i \in [1, yz]$ coprime to Q are $\equiv 1 \mod q$.
- Most primes in the matrix are $\equiv 1 \mod q$.
- So, some row contains a string of primes $\equiv 1 \mod q$.

Irregularities in arithmetic progressions

Theorem (Friedlander-Granville)

For q "without too many small prime factors", and any $A > 0$, there exist a constant δ_A, arithmetic progressions $a_\pm \mod q$, and $x_\pm \in [q \log^A q, 2q \log^A q]$ with

$$\pi(x_+; q, a_+) \geq (1 + \delta_A) \frac{\pi(x_+)}{\phi(q)},$$

$$\pi(x_-; q, a_-) \leq (1 - \delta_A) \frac{\pi(x_-)}{\phi(q)}.$$

Irregularities in arithmetic progressions

Theorem (Friedlander-Granville)

For q "without too many small prime factors", and any $A > 0$, there exist a constant δ_A, arithmetic progressions $a_\pm \mod q$, and $x_\pm \in [q \log^A q, 2q \log^A q]$ with

$$\pi(x_+; q, a_+) \geq (1 + \delta_A) \frac{\pi(x_+)}{\phi(q)},$$

$$\pi(x_-; q, a_-) \leq (1 - \delta_A) \frac{\pi(x_-)}{\phi(q)}.$$

The proof is similar.

The uncertainty principle

Due to Granville and Soundararajan.

Suppose $\mathcal{A}$ is an *arithmetic sequence*:

The uncertainty principle

Due to Granville and Soundararajan.

Suppose $\mathcal{A}$ is an *arithmetic sequence*:

The proportion of elements of $\mathcal{A}$ divisible by d is $\frac{h(d)}{d}$, where

The uncertainty principle

Due to Granville and Soundararajan.

Suppose $\mathcal{A}$ is an *arithmetic sequence*:

The proportion of elements of $\mathcal{A}$ divisible by d is $\frac{h(d)}{d}$, where

- $h(d)$ is a *multiplicative* function,

The uncertainty principle

Due to Granville and Soundararajan.

Suppose $\mathcal{A}$ is an *arithmetic sequence*:

The proportion of elements of $\mathcal{A}$ divisible by d is $\frac{h(d)}{d}$, where

- $h(d)$ is a *multiplicative* function,
- $h(d)$ takes values in $[0, 1]$,

The uncertainty principle

Due to Granville and Soundararajan.

Suppose $\mathcal{A}$ is an *arithmetic sequence*:

The proportion of elements of $\mathcal{A}$ divisible by d is $\frac{h(d)}{d}$, where

- $h(d)$ is a *multiplicative* function,
- $h(d)$ takes values in $[0, 1]$,
- $h(d)$ is not always close to 1.

The uncertainty principle

Granville and Soundararajan prove

The uncertainty principle

Granville and Soundararajan prove

- (1) $\mathcal{A}$ cannot be uniformly distributed in arithmetic progressions to large moduli, *and*

The uncertainty principle

Granville and Soundararajan prove

- (1) $\mathcal{A}$ cannot be uniformly distributed in arithmetic progressions to large moduli, *and*
- (2) *either*, $\mathcal{A}$ is not uniformly distributed in arithmetic progressions to much smaller moduli, *or*

The uncertainty principle

Granville and Soundararajan prove

- (1) $\mathcal{A}$ cannot be uniformly distributed in arithmetic progressions to large moduli, *and*
- (2) *either*, $\mathcal{A}$ is not uniformly distributed in arithmetic progressions to much smaller moduli, *or*
- $\mathcal{A}$ is not uniformly well-distributed in short intervals.

The uncertainty principle

Granville and Soundararajan prove

- (1) $\mathcal{A}$ cannot be uniformly distributed in arithmetic progressions to large moduli, *and*
- (2) *either*, $\mathcal{A}$ is not uniformly distributed in arithmetic progressions to much smaller moduli, *or*
- $\mathcal{A}$ is not uniformly well-distributed in short intervals.

More details later, in the context of $\mathbb{F}_q[t]$.

Maier matrices beyond $\mathbb{Z}$

Can similar results be proved in other settings?

Maier matrices beyond $\mathbb{Z}$

Can similar results be proved in other settings?

Yes.

Maier matrices in $\mathbb{F}_q[t]$

The function field setting:

Maier matrices in $\mathbb{F}_q[t]$

The function field setting:

- Many classical analogies between $\mathbb{F}_q[t]$ and $\mathbb{Z}$.

Maier matrices in $\mathbb{F}_q[t]$

The function field setting:

- Many classical analogies between $\mathbb{F}_q[t]$ and $\mathbb{Z}$.
- The Riemann Hypothesis is known.

Maier matrices in $\mathbb{F}_q[t]$

The function field setting:

- Many classical analogies between $\mathbb{F}_q[t]$ and $\mathbb{Z}$.
- The Riemann Hypothesis is known.
- Primes are clumped into degrees.

Maier matrices in $\mathbb{F}_q[t]$

The function field setting:

- Many classical analogies between $\mathbb{F}_q[t]$ and $\mathbb{Z}$.
- The Riemann Hypothesis is known.
- Primes are clumped into degrees.
- What do "consecutive" and "short intervals" mean?

Maier matrices in $\mathbb{F}_q[t]$

The function field setting:

- Many classical analogies between $\mathbb{F}_q[t]$ and $\mathbb{Z}$.
- The Riemann Hypothesis is known.
- Primes are clumped into degrees.
- What do "consecutive" and "short intervals" mean?
- How do our results depend on q?

Maier matrices in integer rings $\mathcal{O}_K$

In number fields?

Maier matrices in integer rings $\mathcal{O}_K$

In number fields?

- Correspondence between ideals and elements is murky.

Maier matrices in integer rings $\mathcal{O}_K$

In number fields?

- Correspondence between ideals and elements is murky.
- Again, what do "consecutive" and "short intervals" mean?

Maier matrices in integer rings $\mathcal{O}_K$

In number fields?

- Correspondence between ideals and elements is murky.
- Again, what do "consecutive" and "short intervals" mean?

Restrict to $\mathbb{Q}(\sqrt{-D})$, where $h(\sqrt{-D}) = 1$, so that:

Maier matrices in integer rings $\mathcal{O}_K$

In number fields?

- Correspondence between ideals and elements is murky.
- Again, what do "consecutive" and "short intervals" mean?

Restrict to $\mathbb{Q}(\sqrt{-D})$, where $h(\sqrt{-D}) = 1$, so that:

- Ideals *almost* correspond to elements.

Maier matrices in integer rings $\mathcal{O}_K$

In number fields?

- Correspondence between ideals and elements is murky.
- Again, what do "consecutive" and "short intervals" mean?

Restrict to $\mathbb{Q}(\sqrt{-D})$, where $h(\sqrt{-D}) = 1$, so that:

- Ideals *almost* correspond to elements.
- Primes can be nicely visualized in $\mathbb{C}$.

Irregularities in short intervals

Definition (short interval)

If $n < \deg f$, (f, n) is the set of g such that $\deg(f - g) \leq n$.

Theorem

For any $A > 0$, there exists $\delta_{A,q}$ such that we have

$$\limsup_{k \to \infty} \sup_{\deg f = k} \frac{\pi(f, \lceil A \log k \rceil)}{q^{\lceil A \log k \rceil + 1} / k} \geq 1 + \delta_{A,q},$$

$$\liminf_{k \to \infty} \inf_{\deg f = k} \frac{\pi(f, \lceil A \log k \rceil)}{q^{\lceil A \log k \rceil + 1} / k} \leq 1 - \delta_{A,q}.$$

Strings of consecutive primes

Theorem

If $(a, m) = 1$, then there exist arbitrarily long strings of consecutive primes

$$p_{r+1} \equiv p_{r+2} \equiv \cdots \equiv p_{r+k} \equiv a \mod m.$$

For k large, these primes may be chosen so that their degree D satisfies

$$\frac{1}{\phi(m)} \left(\frac{\log D}{(\log \log D)^2} \right)^{1/\phi(m)} \ll k.$$

Strings of consecutive primes

Theorem

If $(a, m) = 1$, then there exist arbitrarily long strings of consecutive primes

$$p_{r+1} \equiv p_{r+2} \equiv \cdots \equiv p_{r+k} \equiv a \mod m.$$

For k large, these primes may be chosen so that their degree D satisfies

$$\frac{1}{\phi(m)} \left(\frac{\log D}{(\log \log D)^2} \right)^{1/\phi(m)} \ll k.$$

"Consecutive" is with respect to lexicographic order.

Strings of consecutive primes (II)

Theorem (Tanner)

If $(a, m) = 1$, there exists D_0 such that for each $D \geq D_0$, there exists a string of consecutive primes

$$p_{r+1} \equiv p_{r+2} \equiv \cdots \equiv p_{r+k} \equiv a \mod m$$

of degree D. For large k, D_0 satisfies

$$\frac{1}{\phi(m)} \left(\frac{\log D_0}{(\log \log D_0)^2} \right)^{1/\phi(m)} \ll k.$$

Strings of consecutive primes (II)

Theorem (Tanner)

If $(a, m) = 1$, there exists D_0 such that for each $D \geq D_0$, there exists a string of consecutive primes

$$p_{r+1} \equiv p_{r+2} \equiv \cdots \equiv p_{r+k} \equiv a \mod m$$

of degree D. For large k, D_0 satisfies

$$\frac{1}{\phi(m)} \left(\frac{\log D_0}{(\log \log D_0)^2} \right)^{1/\phi(m)} \ll k.$$

In other words, such strings occur in **every** large degree.

Setup and notation

- K is an imaginary quadratic field of class number 1.

Setup and notation

- K is an imaginary quadratic field of class number 1.
- $a \mod q$ is an arithmetic progression with $(a, q) = 1$.

Setup and notation

- K is an imaginary quadratic field of class number 1.
- $a \mod q$ is an arithmetic progression with $(a, q) = 1$.
- $k > 0$ is a large integer.

Setup and notation

- K is an imaginary quadratic field of class number 1.
- $a \mod q$ is an arithmetic progression with $(a, q) = 1$.
- $k > 0$ is a large integer.
- For technical reasons, assume $q \neq 2$.

Setup and notation

- K is an imaginary quadratic field of class number 1.
- $a \mod q$ is an arithmetic progression with $(a, q) = 1$.
- $k > 0$ is a large integer.
- For technical reasons, assume $q \neq 2$.
- $\omega_K := \#\mathcal{O}_K^\times$, and $\phi_K(q) := \#((\mathcal{O}_K/(q))^\times$.

Bubbles of congruent primes

Theorem

Assuming the above, there exists a "bubble"

$$B(r, x_0) = \{x \in \mathbb{C} : |x - x_0| < r\}$$

with $\geq k$ primes, all congruent to ua modulo q for units $u \in \mathcal{O}_K$.

Bubbles of congruent primes

Theorem

Assuming the above, there exists a "bubble"

$$B(r, x_0) = \{x \in \mathbb{C} : |x - x_0| < r\}$$

with $\geq k$ *primes, all congruent to* ua *modulo* q *for units* $u \in \mathcal{O}_K$*. Furthermore,* x_0 *will satisfy*

$$\frac{\omega_K}{\phi_K(q)} \left(\frac{\log \log |x_0| \log \log \log \log |x_0|}{(\log \log \log |x_0|)^2} \right)^{\omega_K / \phi_K(q)} \ll k.$$

Bubbles: the proof

If $a \equiv 1 \mod q$, write

$$\mathfrak{Q} = (Q) := q \prod_{\substack{\mathbb{N}\mathfrak{p} \le y \\ \mathfrak{p} \ne \mathfrak{p}_0 \\ \mathfrak{p} \not\equiv 1 \mod q}} \mathfrak{p}.$$

$\mathfrak{p} \equiv a \mod q$ means $p \equiv a$ for some generator p of $\mathfrak{p}$.

Bubbles: the proof (cont.)

The rows are bubbles $x_0 + b$, for

Bubbles: the proof (cont.)

The rows are bubbles $x_0 + b$, for

$$b \in B := \{x \in \mathcal{O}_K : \ \mathbb{N}x \leq yz\}.$$

Bubbles: the proof (cont.)

The rows are bubbles $x_0 + b$, for

$$b \in B := \{x \in \mathcal{O}_K : \ \mathbb{N}x \leq yz\}.$$

$$S := \{i \in B; (i, Q) = 1; i \equiv ua \mod q \text{ for some } u \in \mathcal{O}_K^\times\}$$
$$T := \{i \in 3B; (i, Q) = 1; i \not\equiv ua \mod q \text{ for any } u \in \mathcal{O}_K^\times\}.$$

Bubbles: the proof (cont.)

The rows are bubbles $x_0 + b$, for

$$b \in B := \{x \in \mathcal{O}_K : \ \mathbb{N}x \leq yz\}.$$

$$S := \{i \in B; (i, Q) = 1; i \equiv ua \mod q \text{ for some } u \in \mathcal{O}_K^\times\}$$
$$T := \{i \in 3B; (i, Q) = 1; i \not\equiv ua \mod q \text{ for any } u \in \mathcal{O}_K^\times\}.$$

Can show: S is much larger than T.

Primes in arithmetic progression

Proposition 1

Suppose the Hecke L-functions modulo q have a zero-free region

$$\sigma > 1 - C_1 / \log[(\mathbb{N}q)(|t| + 1)].$$

Then uniformly for $(a, q) = 1$ and $x \geq \mathbb{N}q^D$ we have

$$\pi(2x; q, a) - \pi(x; q, a) = (1 + o_{x,D}(1)) \frac{x}{\phi_K(q) \log x}.$$

Primes in arithmetic progression

Proposition 1

Suppose the Hecke L-functions modulo q have a zero-free region

$$\sigma > 1 - C_1 / \log[(\mathbb{N}q)(|t| + 1)].$$

Then uniformly for $(a, q) = 1$ and $x \geq \mathbb{N}q^D$ we have

$$\pi(2x; q, a) - \pi(x; q, a) = (1 + o_{x,D}(1)) \frac{x}{\phi_K(q) \log x}.$$

Exclude u, $2u$, or $\frac{-3 \pm \sqrt{-3}}{2} u$ for units u of $\mathcal{O}_K$.

Primes in arithmetic progression: the conclusion

$T = o(S)$, so almost all primes in the matrix are $\equiv ua \mod q$.

Proof of Proposition 1

We need to count **ideals** in arithmetic progressions.

Proof of Proposition 1

We need to count **ideals** in arithmetic progressions.

The *ray class group modulo q* is

$$H^q := J^q / P^q,$$

$J^q :=$ fractional ideals coprime to q,
$P^q :=$ fractional ideals $(a) = (b)(c)^{-1}$:
$b, c \in \mathcal{O}_K, \; b \equiv c \equiv 1 \mod \mathfrak{q}$.

Proof of Proposition 1

We need to count **ideals** in arithmetic progressions.

The *ray class group modulo q* is

$$H^q := J^q / P^q,$$

$J^q :=$ fractional ideals coprime to q,
$P^q :=$ fractional ideals $(a) = (b)(c)^{-1}$:
$b, c \in \mathcal{O}_K, \; b \equiv c \equiv 1 \mod \mathfrak{q}$.
Elements of H^q correspond to sets $\{ua \mod q\}$.

Proof of Proposition 1

We need to count **ideals** in arithmetic progressions.

The *ray class group modulo q* is

$$H^q := J^q / P^q,$$

$J^q :=$ fractional ideals coprime to q,
$P^q :=$ fractional ideals $(a) = (b)(c)^{-1}$:
$b, c \in \mathcal{O}_K, \; b \equiv c \equiv 1 \mod \mathfrak{q}$.
Elements of H^q correspond to sets $\{ua \mod q\}$.
We obtain *Hecke characters* of finite order.

Character sums in number fields

If χ is a Hecke character of K, the associated *Hecke L-function* is

$$L(s,\chi) := \sum_{\mathfrak{a}} \chi(\mathfrak{a})(\mathbb{N}\mathfrak{a})^{-s}.$$

Character sums in number fields

If χ is a Hecke character of K, the associated *Hecke L-function* is

$$L(s, \chi) := \sum_{\mathfrak{a}} \chi(\mathfrak{a})(\mathbb{N}\mathfrak{a})^{-s}.$$

Proposition 2

Assume the zero-free region mentioned before. Then for $\exp(\log^{1/2} x) \leq \mathbb{N}q \leq x^{C_2}$,

$$\sum_{\chi} \Bigg| \sum_{\mathbb{N}\mathfrak{p} \in [x, 2x]} \chi(\mathfrak{p}) \log(\mathbb{N}\mathfrak{p}) \Bigg| \ll x \exp\left(- C_3 \frac{\log x}{\log \mathbb{N}\mathfrak{q}} \right).$$

The first sum is over nonprincipal characters of finite order mod q.

Proofs of propositions

By usual analytic methods, we have

$$\sum_{\mathbb{N}\mathfrak{a} \in [x, 2x]} \chi(\mathfrak{a})\Lambda(\mathfrak{a}) = \delta_\chi x - \sum_\rho \frac{(2x)^\rho - x^\rho}{\rho} + O\Big(\frac{x \log^3 x}{T}\Big).$$

$\delta_\chi = 1$ or 0 depending on whether χ is principal.

Proofs of propositions

By usual analytic methods, we have

$$\sum_{\mathbb{N}\mathfrak{a}\in[x,2x]} \chi(\mathfrak{a})\Lambda(\mathfrak{a}) = \delta_\chi x - \sum_\rho \frac{(2x)^\rho - x^\rho}{\rho} + O\Big(\frac{x\log^3 x}{T}\Big).$$

$\delta_\chi = 1$ or 0 depending on whether χ is principal.

Following methods of Gallagher, Proposition 2 follows from

Proofs of propositions

By usual analytic methods, we have

$$\sum_{\mathbb{N}\mathfrak{a}\in[x,2x]} \chi(\mathfrak{a})\Lambda(\mathfrak{a}) = \delta_\chi x - \sum_\rho \frac{(2x)^\rho - x^\rho}{\rho} + O\Big(\frac{x \log^3 x}{T}\Big).$$

$\delta_\chi = 1$ or 0 depending on whether χ is principal.

Following methods of Gallagher, Proposition 2 follows from

- The zero-free region given before,

Proofs of propositions

By usual analytic methods, we have

$$\sum_{\mathbb{N}\mathfrak{a}\in[x,2x]} \chi(\mathfrak{a})\Lambda(\mathfrak{a}) = \delta_\chi x - \sum_\rho \frac{(2x)^\rho - x^\rho}{\rho} + O\left(\frac{x\log^3 x}{T}\right).$$

$\delta_\chi = 1$ or 0 depending on whether χ is principal.

Following methods of Gallagher, Proposition 2 follows from

- The zero-free region given before,
- A log-free zero density estimate, due to Fogels.

Proofs of propositions

By usual analytic methods, we have

$$\sum_{\mathbb{N}\mathfrak{a}\in[x,2x]} \chi(\mathfrak{a})\Lambda(\mathfrak{a}) = \delta_\chi x - \sum_\rho \frac{(2x)^\rho - x^\rho}{\rho} + O\Big(\frac{x\log^3 x}{T}\Big).$$

$\delta_\chi = 1$ or 0 depending on whether χ is principal.

Following methods of Gallagher, Proposition 2 follows from

- The zero-free region given before,
- A log-free zero density estimate, due to Fogels.

Proposition 1 follows from Proposition 2.

Construction of good moduli

Is the assumption in Proposition 1 workable?

Construction of good moduli

Is the assumption in Proposition 1 workable?

Write

$$\mathcal{P}(y, q, \mathfrak{p}_0) := q \prod_{\mathbb{N}\mathfrak{p} \leq y; \mathfrak{p} \neq \mathfrak{p}_0} \mathfrak{p}.$$

Proposition 3

For large x, there exist moduli $N\mathcal{P}(y, q, \mathfrak{p}_0)$ with $x < \mathbb{N}\mathcal{P}(y, q, \mathfrak{p}_0) \ll x \log^3 x$ and $\mathbb{N}\mathfrak{p}_0 \gg \log y$, such that the L-functions modulo $\mathcal{P}(y, q, \mathfrak{p}_0)$ have the zero-free region in Proposition 1.

All finished?

In conclusion, we find a row (bubble) of our matrix either

All finished?

In conclusion, we find a row (bubble) of our matrix either

- containing only “good” primes, or

All finished?

In conclusion, we find a row (bubble) of our matrix either

- containing only "good" primes, or
- containing a lot of good primes, and few bad ones.

All finished?

In conclusion, we find a row (bubble) of our matrix either

- containing only “good” primes, or
- containing a lot of good primes, and few bad ones.

We’re not quite done...

All finished?

In conclusion, we find a row (bubble) of our matrix either

- containing only “good” primes, or
- containing a lot of good primes, and few bad ones.

We’re not quite done...

Bubbles are not easy to subdivide.

A result in combinatorial geometry

Given bubbles B and $3B$ in the plane such that

A result in combinatorial geometry

Given bubbles B and $3B$ in the plane such that

- B contains g good points,

A result in combinatorial geometry

Given bubbles B and $3B$ in the plane such that

- B contains g good points,
- $3B$ contains b bad points, where $b = o(g)$.

A result in combinatorial geometry

Given bubbles B and $3B$ in the plane such that

- B contains g good points,
- $3B$ contains b bad points, where $b = o(g)$.
- There might be bad points outside $3B$ too.

A result in combinatorial geometry

Given bubbles B and $3B$ in the plane such that

- B contains g good points,
- $3B$ contains b bad points, where $b = o(g)$.
- There might be bad points outside $3B$ too.

Proposition 4

There exists a ball in the plane containing $\gg g/b$ good points and no bad points.

The Delaunay triangulation

Definition

Given a set of points $\mathcal{P}$.

In a *Delaunay triangulation*, no point of $\mathcal{P}$ is inside the circumcircle of any triangle.

The Delaunay triangulation

Definition

Given a set of points $\mathcal{P}$.
In a *Delaunay triangulation*, no point of $\mathcal{P}$ is inside the circumcircle of any triangle.

Proposition

If not all points are collinear, a Delaunay triangulation of $\mathcal{P}$ exists.

Proof of Proposition 4

Let $\mathcal{P}$ consist of:

Proof of Proposition 4

Let $\mathcal{P}$ consist of:

- All bad points in $3B$,

Proof of Proposition 4

Let $\mathcal{P}$ consist of:

- All bad points in $3B$,
- A 30-gon, centered at the origin, of radius $2B$.

Proof of Proposition 4

Let $\mathcal{P}$ consist of:

- All bad points in $3B$,
- A 30-gon, centered at the origin, of radius $2B$.

Construct a Delaunay triangulation of $\mathcal{P}$.

Proof of Proposition 4 (cont.)

Given our triangulation,

Proof of Proposition 4 (cont.)

Given our triangulation,

- The circumcircles contain all the good points, and none of the bad (inside $3B$).

Proof of Proposition 4 (cont.)

Given our triangulation,

- The circumcircles contain all the good points, and none of the bad (inside $3B$).
- (The hard part) Any circle covering B is contained in $3B$.

Proof of Proposition 4 (cont.)

Given our triangulation,

- The circumcircles contain all the good points, and none of the bad (inside $3B$).
- (The hard part) Any circle covering B is contained in $3B$.
- There are $\ll b$ circles, which contain g points.

Proof of Proposition 4 (cont.)

Given our triangulation,

- The circumcircles contain all the good points, and none of the bad (inside $3B$).
- (The hard part) Any circle covering B is contained in $3B$.
- There are $\ll b$ circles, which contain g points.
- One circle is our bubble of congruent primes.

The uncertainty principle: notation

Given an arithmetic function

$$a(x) : \mathbb{F}_q[t] \longrightarrow \mathbb{R}^{\geq 0}.$$

The uncertainty principle: notation

Given an arithmetic function

$$a(x) : \mathbb{F}_q[t] \longrightarrow \mathbb{R}^{\geq 0}.$$

Think: $a(x)$ is the characteristic function of some set $\mathcal{A}$.

The uncertainty principle: notation

Given an arithmetic function

$$a(x) : \mathbb{F}_q[t] \to \mathbb{R}^{\geq 0}.$$

Think: $a(x)$ is the characteristic function of some set $\mathcal{A}$.

$$\mathcal{A}(n) := \sum_{\deg r = n} a(r),$$

$$\mathcal{A}(n; m, a) := \sum_{\substack{\deg r = n \\ n \equiv a \mod m}} a(r).$$

Some notation (cont.)

For fixed monic r and $i < \deg r$,

$$\mathcal{A}(r,i) := \sum_{\deg s \leq i} a(r+s),$$

with no restriction on leading coefficient of s.

Some notation (cont.)

For fixed monic r and $i < \deg r$,

$$\mathcal{A}(r, i) := \sum_{\deg s \leq i} a(r + s),$$

with no restriction on leading coefficient of s.

Could also write

$$\mathcal{A}(r, i) := \sum_{x \in (r,i)} a(x).$$

Some notation (cont.)

For fixed monic r and $i < \deg r$,

$$\mathcal{A}(r, i) := \sum_{\deg s \leq i} a(r + s),$$

with no restriction on leading coefficient of s.

Could also write

$$\mathcal{A}(r, i) := \sum_{x \in (r, i)} a(x).$$

This talk: assume $q \neq 2$.

Arithmetic sequences in $\mathbb{F}_q[t]$

Assume, for m coprime to a finite “bad” set $\mathcal{S}$, that

$$\mathcal{A}(n; m, 0) \sim \frac{h(m)}{|m|} \mathcal{A}(n)$$

where $h(m)$

Arithmetic sequences in $\mathbb{F}_q[t]$

Assume, for m coprime to a finite “bad” set $\mathcal{S}$, that

$$\mathcal{A}(n; m, 0) \sim \frac{h(m)}{|m|} \mathcal{A}(n)$$

where $h(m)$

- is *multiplicative*,

Arithmetic sequences in $\mathbb{F}_q[t]$

Assume, for m coprime to a finite "bad" set $\mathcal{S}$, that

$$\mathcal{A}(n; m, 0) \sim \frac{h(m)}{|m|} \mathcal{A}(n)$$

where $h(m)$

- is *multiplicative*,
- takes values in $[0, 1]$,

Arithmetic sequences in $\mathbb{F}_q[t]$

Assume, for m coprime to a finite "bad" set $\mathcal{S}$, that

$$\mathcal{A}(n; m, 0) \sim \frac{h(m)}{|m|}\mathcal{A}(n)$$

where $h(m)$

- is *multiplicative*,
- takes values in $[0, 1]$,
- is not always close to 1.

Arithmetic sequences in $\mathbb{F}_q[t]$

Assume, for m coprime to a finite "bad" set $\mathcal{S}$, that

$$\mathcal{A}(n; m, 0) \sim \frac{h(m)}{|m|} \mathcal{A}(n)$$

where $h(m)$

- is *multiplicative*,
- takes values in $[0, 1]$,
- is not always close to 1.

For example, assume

$$\sum_{\deg p \leq y} \frac{1 - h(p)}{|p|} \deg p =: \alpha y \geq 39 \log y.$$

Expectations for arithmetic sequences

We expect

$$\mathcal{A}(n; m, a) \sim \frac{f_m(a)}{|m|\gamma_m}\mathcal{A}(n),$$

for certain quantities $f_m(a)$, γ_m, and

$$\mathcal{A}(n, i) \sim \frac{\mathcal{A}(n)}{q^{n-(i+1)}}.$$

Expectations for arithmetic sequences

We expect

$$\mathcal{A}(n; m, a) \sim \frac{f_m(a)}{|m|\gamma_m}\mathcal{A}(n),$$

for certain quantities $f_m(a)$, γ_m, and

$$\mathcal{A}(n, i) \sim \frac{\mathcal{A}(n)}{q^{n-(i+1)}}.$$

Main result: One or both asymptotics fail.

Irregularities in arithmetic progressions

Theorem

Assume the above. Write $\eta = \min(\alpha/3, 1/100)$*. Then for every* $u \in [5y/\eta^2, e^{\eta y/2}]$ *and every* $n \geq 5q^y$ *there exists an arithmetic progression* $a \mod m$ *with* $\deg m \leq n - u$ *and* $(m, \mathcal{S}) = 1$ *which satisfies*

$$\frac{\left|\mathcal{A}(n; m, a) - \frac{f_m(a)}{|m|\gamma_m}\mathcal{A}(n)\right|}{\frac{\mathcal{A}(n)}{\phi(m)}} \geq \frac{1}{3}\exp\left(-\frac{u}{\eta y}(1+25\eta)\log\left(\frac{2u}{y\eta^3}\right)\right).$$

Irregularities in arithmetic progressions

Theorem

Assume the above. Write $\eta = \min(\alpha/3, 1/100)$. *Then for every* $u \in [5y/\eta^2, e^{\eta y/2}]$ *and every* $n \geq 5q^y$ *there exists an arithmetic progression* $a \mod m$ *with* $\deg m \leq n - u$ *and* $(m, \mathcal{S}) = 1$ *which satisfies*

$$\frac{\left|\mathcal{A}(n; m, a) - \frac{f_m(a)}{|m|\gamma_m}\mathcal{A}(n)\right|}{\frac{\mathcal{A}(n)}{\phi(m)}} \geq \frac{1}{3}\exp\left(-\frac{u}{\eta y}(1 + 25\eta)\log\left(\frac{2u}{y\eta^3}\right)\right).$$

RHS $\gg 1$ for fixed u/y.

The uncertainty principle

Theorem

Under the same conditions, at least one of the following is true:

(i) *There exists an arithmetic progression* $a \mod m$ *with* $\deg m \leq 2q^{(1-\eta)y}$ *and* $(m, \mathcal{S}) = 1$ *which satisfies*

$$\left|\mathcal{A}(n; m, a) - \frac{f_m(a)}{|m|\gamma_m}\mathcal{A}(n)\right| \Big/ \frac{\mathcal{A}(n)}{\phi(m)} \geq \frac{1}{2}\exp(\cdots).$$

(ii) *There exists an interval* $(f, u-1)$ *with* $\deg f = n$*, such that*

$$\left|\mathcal{A}(f, u-1) - \frac{\mathcal{A}(n)}{q^{n-u}}\right| \Big/ \frac{\mathcal{A}(n)}{q^{n-u}} \geq \frac{1}{2}\exp(\cdots).$$

Maier's theorem revisited

How was Maier's theorem proved?

Maier's theorem revisited

How was Maier's theorem proved?

- Write $Q = \prod_{p<n} p$.

Maier's theorem revisited

How was Maier's theorem proved?

- Write $Q = \prod_{p<n} p$.
- Count number of $i \in [1, n^A]$ coprime to Q.

Maier's theorem revisited

How was Maier's theorem proved?

- Write $Q = \prod_{p<n} p$.
- Count number of $i \in [1, n^A]$ coprime to Q.
- This is asymptotic to

$$\frac{\phi(Q)}{Q} y^A \cdot f(A)$$

where $f(A)$ is an oscillatory function that approaches 1.

Maier's theorem revisited

How was Maier's theorem proved?

- Write $Q = \prod_{p<n} p$.
- Count number of $i \in [1, n^A]$ coprime to Q.
- This is asymptotic to

$$\frac{\phi(Q)}{Q} y^A \cdot f(A)$$

  where $f(A)$ is an oscillatory function that approaches 1.
- $f(A)$ is not identically 1.

Generalizing Maier's method

Let Q be a product of small primes.

Generalizing Maier's method

Let Q be a product of small primes.

Define $f_Q(a)$ in terms of $h(a)$ as before, and

Generalizing Maier's method

Let Q be a product of small primes.

Define $f_Q(a)$ in terms of $h(a)$ as before, and

$$E(u) := \frac{1}{q^u} \sum_{\deg x = u} (f_Q(x) - \gamma_Q).$$

On average $E(u) = 0$ but not always.

Generalizing Maier's method

Let Q be a product of small primes.

Define $f_Q(a)$ in terms of $h(a)$ as before, and

$$E(u) := \frac{1}{q^u} \sum_{\deg x = u} (f_Q(x) - \gamma_Q).$$

On average $E(u) = 0$ but not always.

The hard part: Analyze oscillation of $E(u)$ in detail.

Distribution of primes in arithmetic progressions

Corollary

Let $n \geq 5q^y$. The primes of degree n are not uniformly distributed in arithmetic progressions to moduli $\leq n - Cy$ for any C.

Distribution of primes in short intervals

Corollary

Let $n \geq 5q^y$. The primes of degree n are not uniformly distributed in short intervals (f, i) for any $i < Cy$.

The function field version of Maier again.