Maier Matrices Beyond $\mathbb{Z}$

Frank Thorne

University of Wisconsin - Madison

Integers - October 24-27, 2007

The distribution of the primes

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

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

The distribution of the primes

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

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

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

The distribution of the primes

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

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

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

The "probability" n is prime is $\frac{1}{\log n}$.

Maier's theorem

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

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

with probability 1.

Maier's theorem

This 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

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

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

Strings of congruent primes

Theorem (Shiu)

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

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

Strings of congruent primes

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*

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

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.

The prime number theorem in $\mathbb{F}_q[t]$

The $\mathbb{F}_q[t]$ prime number theorem says,

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

where $\pi(n)$ is the number of monic irreducibles of degree n.

The prime number theorem in $\mathbb{F}_q[t]$

The $\mathbb{F}_q[t]$ prime number theorem says,

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

where $\pi(n)$ is the number of monic irreducibles of degree n.

The "probability" a polynomial of degree n is prime is (about) $1/n$.

Irregularities in short intervals

Definition (short interval)

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

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

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

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

Proof of theorem

Consider the *Maier matrix*

$$\begin{bmatrix} Qf_1 + g_1 & Qf_1 + g_2 & \dots & Qf_1 + g_J \\ Qf_2 + g_1 & Qf_2 + g_2 & \dots & Qf_2 + g_J \\ \vdots & \vdots & \vdots & \vdots \\ Qf_I + g_1 & Qf_I + g_2 & \dots & Qf_I + g_J \end{bmatrix},$$

where

Proof of theorem

Consider the *Maier matrix*

$$\begin{bmatrix} Qf_1 + g_1 & Qf_1 + g_2 & \dots & Qf_1 + g_J \\ Qf_2 + g_1 & Qf_2 + g_2 & \dots & Qf_2 + g_J \\ \vdots & \vdots & \vdots & \vdots \\ Qf_I + g_1 & Qf_I + g_2 & \dots & Qf_I + g_J \end{bmatrix},$$

where

$Q = \prod_{\deg p \leq n} p$,

Proof of theorem

Consider the *Maier matrix*

$$\begin{bmatrix} Qf_1 + g_1 & Qf_1 + g_2 & \dots & Qf_1 + g_J \\ Qf_2 + g_1 & Qf_2 + g_2 & \dots & Qf_2 + g_J \\ \vdots & \vdots & \vdots & \vdots \\ Qf_I + g_1 & Qf_I + g_2 & \dots & Qf_I + g_J \end{bmatrix},$$

where
$Q = \prod_{\deg p \leq n} p$,
f_i: all monic polynomials of degree $2 \deg Q$,

Proof of theorem

Consider the *Maier matrix*

$$\begin{bmatrix} Qf_1 + g_1 & Qf_1 + g_2 & \dots & Qf_1 + g_J \\ Qf_2 + g_1 & Qf_2 + g_2 & \dots & Qf_2 + g_J \\ \vdots & \vdots & \vdots & \vdots \\ Qf_I + g_1 & Qf_I + g_2 & \dots & Qf_I + g_J \end{bmatrix},$$

where
$Q = \prod_{\deg p \leq n} p$,
f_i: all monic polynomials of degree $2 \deg Q$,
g_j: all polynomials of degree $\leq s$.

The Maier matrix

$$\begin{bmatrix} Qf_1 + g_1 & Qf_1 + g_2 & \dots & Qf_1 + g_J \\ Qf_2 + g_1 & Qf_2 + g_2 & \dots & Qf_2 + g_J \\ \vdots & \vdots & \vdots & \vdots \\ Qf_I + g_1 & Qf_I + g_2 & \dots & Qf_I + g_J \end{bmatrix}$$

The rows are short intervals (Qf_i, s).

The Maier matrix

$$\begin{bmatrix} Qf_1 + g_1 & Qf_1 + g_2 & \dots & Qf_1 + g_J \\ Qf_2 + g_1 & Qf_2 + g_2 & \dots & Qf_2 + g_J \\ \vdots & \vdots & \vdots & \vdots \\ Qf_I + g_1 & Qf_I + g_2 & \dots & Qf_I + g_J \end{bmatrix}$$

The rows are short intervals (Qf_i, s).

The columns are arithmetic progressions mod Q.

The Maier matrix

$$\begin{bmatrix} Qf_1 + g_1 & Qf_1 + g_2 & \dots & Qf_1 + g_J \\ Qf_2 + g_1 & Qf_2 + g_2 & \dots & Qf_2 + g_J \\ \vdots & \vdots & \vdots & \vdots \\ Qf_I + g_1 & Qf_I + g_2 & \dots & Qf_I + g_J \end{bmatrix}$$

The rows are short intervals (Qf_i, s).

The columns are arithmetic progressions mod Q. So, the prime number theorem predicts the number of primes in each column.

The Maier matrix: the conclusion

- The total number of primes is determined by the number of g_j coprime to Q.

The Maier matrix: the conclusion

- The total number of primes is determined by the number of g_j coprime to Q.
- These are precisely the g_j without any small prime factors.

The Maier matrix: the conclusion

- The total number of primes is determined by the number of g_j coprime to Q.
- These are precisely the g_j without any small prime factors.
- For small s, the count is not asymptotic to $q^{s+1}\phi(Q)/|Q|$.

The Maier matrix: the conclusion

- The total number of primes is determined by the number of g_j coprime to Q.
- These are precisely the g_j without any small prime factors.
- For small s, the count is not asymptotic to $q^{s+1}\phi(Q)/|Q|$.
- Thus, the matrix (and thus some row) contains more or fewer primes than expected.

The Maier matrix: the conclusion

- The total number of primes is determined by the number of g_j coprime to Q.
- These are precisely the g_j without any small prime factors.
- For small s, the count is not asymptotic to $q^{s+1}\phi(Q)/|Q|$.
- Thus, the matrix (and thus some row) contains more or fewer primes than expected.
- This allows us to find irregular intervals.

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.

Sketch of proof

In the special case $a = 1$, let

$$Q = m \prod_{\substack{\deg p \leq y \\ p \not\equiv 1 \mod m}} p.$$

Sketch of proof

In the special case $a = 1$, let

$$Q = m \prod_{\substack{\deg p \leq y \\ p \not\equiv 1 \mod m}} p.$$

Construct a similar Maier matrix, so that again:

Sketch of proof

In the special case $a = 1$, let

$$Q = m \prod_{\substack{\deg p \leq y \\ p \not\equiv 1 \mod m}} p.$$

Construct a similar Maier matrix, so that again:

- The rows are short intervals,

Sketch of proof

In the special case $a = 1$, let

$$Q = m \prod_{\substack{\deg p \leq y \\ p \not\equiv 1 \mod m}} p.$$

Construct a similar Maier matrix, so that again:

- The rows are short intervals,
- The columns are progressions mod Q.

Sketch of proof, cont.

For appropriate parameters

Sketch of proof, cont.

For appropriate parameters

- Most small polynomials coprime to Q are $\equiv a \mod q$.

Sketch of proof, cont.

For appropriate parameters

- Most small polynomials coprime to Q are $\equiv a \mod q$.
- Most primes in the matrix are $\equiv a \mod q$.

Sketch of proof, cont.

For appropriate parameters

- Most small polynomials coprime to Q are $\equiv a \mod q$.
- Most primes in the matrix are $\equiv a \mod q$.
- So, some row contains a string of primes $\equiv a \mod q$.

Granville-Soundararajan's uncertainty principle

Let $\mathcal{A} \subseteq \mathbb{Z}$ be an "arithmetic sequence".

Granville-Soundararajan's uncertainty principle

Let $\mathcal{A} \subseteq \mathbb{Z}$ be an "arithmetic sequence".

Granville and Soundararajan proved that

Granville-Soundararajan's uncertainty principle

Let $\mathcal{A} \subseteq \mathbb{Z}$ be an "arithmetic sequence".

Granville and Soundararajan proved that

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

Granville-Soundararajan's uncertainty principle

Let $\mathcal{A} \subseteq \mathbb{Z}$ be an "arithmetic sequence".

Granville and Soundararajan proved that

- (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*

Granville-Soundararajan's uncertainty principle

Let $\mathcal{A} \subseteq \mathbb{Z}$ be an "arithmetic sequence".

Granville and Soundararajan proved that

- (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.

Uncertainty in $\mathbb{F}_q[t]$

Theorem

The Granville-Soundararajan results translate nicely to $\mathbb{F}_q[t]$.

Uncertainty in $\mathbb{F}_q[t]$

Theorem

The Granville-Soundararajan results translate nicely to $\mathbb{F}_q[t]$.

This theorem implies (among other results)

Uncertainty in $\mathbb{F}_q[t]$

Theorem

The Granville-Soundararajan results translate nicely to $\mathbb{F}_q[t]$.

This theorem implies (among other results)

- An improved "short intervals" result as described before,

Uncertainty in $\mathbb{F}_q[t]$

Theorem

The Granville-Soundararajan results translate nicely to $\mathbb{F}_q[t]$.

This theorem implies (among other results)

- An improved "short intervals" result as described before,
- Irregular distribution in arithmetic progressions to large moduli.

Maier matrices in number fields

Do Maier matrices “work” in the rings of integers of number fields?

Maier matrices in number fields

Do Maier matrices "work" in the rings of integers of number fields?

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

Maier matrices in number fields

Do Maier matrices "work" in the rings of integers of number fields?

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

- Ideals *almost* correspond to elements.

Maier matrices in number fields

Do Maier matrices "work" in the rings of integers of number fields?

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

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

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

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

Brief sketch of proof

The proof involves

Brief sketch of proof

The proof involves

- A Maier matrix calculation with “good” and “bad” matrices,

Brief sketch of proof

The proof involves

- A Maier matrix calculation with “good” and “bad” matrices,
- A result on primes in certain arithmetic progressions, proved using Hecke L-functions,

Brief sketch of proof

The proof involves

- A Maier matrix calculation with “good” and “bad” matrices,
- A result on primes in certain arithmetic progressions, proved using Hecke L-functions,
- Some combinatorial geometry, finding bubbles of “good” primes within “mostly good” bubbles.

In summary...

The conclusion: Maier matrices "work" beyond $\mathbb{Z}$.

In summary...

The conclusion: Maier matrices "work" beyond $\mathbb{Z}$.

Question: Can further results be proved along these lines?

We have every reason to believe so.