MAIER MATRICES BEYOND $\mathbb{Z}$

Frank Thorne[1]
Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706
thorne@math.wisc.edu

Received: , Accepted: , Published:

Abstract

This paper is an expanded version of a talk given at the 2007 Integers Conference, giving an overview of the Maier matrix method and surveying the author's work in extending it beyond the integers.

1. Maier Matrices

Loosely speaking, a *Maier matrix* is a combinatorial device used to prove the existence of irregular or interesting patterns in the distribution of primes or related sequences. We will illustrate the technique with two particularly interesting examples. The first is Maier's 1985 proof [6] that "unexpected" irregularities exist in the distribution of primes in short intervals. In particular, Maier proved that for any $A > 0$ there exists a constant $\delta_A > 0$ such that

$$\limsup_{n\to\infty} \frac{\pi(n + \log^A n) - \pi(n)}{\log^{A-1} n} \geq 1 + \delta_A, \quad \liminf_{n\to\infty} \frac{\pi(n + \log^A n) - \pi(n)}{\log^{A-1} n} \leq 1 - \delta_A. \tag{0.1}$$

These irregularities are unexpected in the sense that they contradict probabilistic heuristics for $A > 2$.

The proof is as follows. For a variable y, let $Q = \prod_{p<y} p$, let $x_1 = Q^D$ for some fixed large D, and let C be a parameter to be determined later. Consider the following matrix of integers:

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

The columns form arithmetic progressions modulo Q, and so the prime number theorem

[1]The author is grateful for financial support from an NSF VIGRE fellowship.

for arithmetic progressions predicts[2] that for each $i \in [1, y^C]$ which is coprime to Q, the corresponding column should contain $\sim \frac{Q}{\phi(Q)} \frac{x_1}{\log(Qx_1)}$ primes. Therefore, the number of primes in the matrix, and thus in an average row, can be asymptotically determined by counting the number of such i. In fact, the latter quantity is

$$\Phi(y^C, y) \sim y^C \frac{\phi(Q)}{Q} e^\gamma \omega(C), \tag{0.2}$$

for a function $\omega(C)$ which converges to $e^{-\gamma}$, but oscillates above and below $e^{-\gamma}$ as $C \to \infty$.[3] The short intervals occuring in the Maier matrix are of the sort considered in (0.1), and Maier's theorem soon follows.

In 1997, Shiu [8] similarly proved the remarkable result that if a, q, and k are arbitrary integers with $(a, q) = 1$, there exists a string of k consecutive primes

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

(Here p_n denotes the nth prime.) Furthermore, for k sufficiently large in terms of q, these primes can be chosen to satisfy the bound

$$\frac{1}{\phi(q)} \left(\frac{\log\log p_{n+1} \log\log\log\log p_{n+1}}{(\log\log\log p_{n+1})^2} \right)^{1/\phi(q)} \ll k. \tag{0.3}$$

To prove (0.3) Shiu constructed a similar Maier matrix; the primary difference is in the choice of Q. For example, if $a = 1$, primes $\not\equiv 1 \pmod{m}$ are excluded from the product. This forces most primes in the matrix to be $\equiv 1 \pmod{m}$, and Shiu's result easily follows.

The method has been similarly adapted to prove a host of interesting results about the distribution of the primes and related integer sequences. For more on this, we recommend the outstanding survey articles of Granville [4] and of Soundararajan [9]. In this article we will consider the problem of adapting the Maier matrix method to different settings. In particular we will describe extensions of the method to the polynomial ring $\mathbb{F}_q[t]$ and to imaginary quadratic fields, where we obtained analogous results.

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

The polynomial ring $\mathbb{F}_q[t]$ (here $\mathbb{F}_q$ is a finite field) has long been studied as an analogue to the integers. Like the integers, $\mathbb{F}_q[t]$ enjoys unique factorization, and has the additional property that the residue class rings are all finite, so that one may naturally talk about the 'size' of elements.

[2]This is not known to be true for all Q, except under GRH. However, a theorem of Gallagher [3] implies the correct asymptotic for an infinite set of such Q, where the error term in the asymptotic depends on D.

[3]In general, $\Phi(x, y)$ denotes the number of $n \le x$, all of whose prime factors are at least y.

Classical methods of analytic number theory have been extremely successful in analyzing the distribution of primes (e.g., monic irreducible polynomials) in $\mathbb{F}_q[t]$. For example, one defines the zeta function as

$$\zeta_{\mathbb{F}_q[t]}(s) := \sum_{x \in \mathbb{F}_q[t]} \frac{1}{|x|^s}, \tag{0.4}$$

where the sum is over all monic polynomials x, and $|x| := \#|\mathbb{F}_q[t]/(x)| = q^{\deg x}$. As there are exactly q^n monics of degree n, one easily obtains the formula

$$\zeta_{\mathbb{F}_q[t]}(s) = \frac{1}{1 - q^{1-s}}.$$

The Riemann hypothesis is then a triviality, and in fact one has an exact prime number theorem

$$\pi(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}.$$

Thinking of n as $\log_q(q^n)$, this closely mirrors the classical case.

It is therefore natural to ask whether the Maier matrix method can be adapted to $\mathbb{F}_q[t]$, and we have answered this question in the affirmative. To start with, we have the following

Theorem 2.1 ([11], Theorem 1.1). For any fixed $A > 0$, there exists a constant $\delta_A > 0$ (depending also on q) such that

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

Here $\pi(f, i)$ denotes the number of irreducible monic polynomials p with $\deg(f - p) \leq i$.

The proof follows similar lines. We write $Q = \prod_{\deg p \leq n} p$, and consider the following matrix:

$$\begin{bmatrix} Qg_1 + h_1 & Qg_1 + h_2 & \dots & Qg_1 + h_j \\ Qg_2 + h_1 & Qg_2 + h_2 & \dots & Qg_2 + h_j \\ \vdots & \vdots & \vdots & \vdots \\ Qg_i + h_1 & Qg_i + h_2 & \dots & Qg_i + h_j \end{bmatrix}$$

Here g_1 through g_i range through all monic polynomials of degree $2 \deg Q$ (or of degree $\alpha \deg Q$ for any fixed $\alpha > 1$), and h_1 through h_j run through all polynomials of degree s (of arbitrary leading coefficient), for a parameter s to be determined later. The number of primes in the whole matrix is $\sim \frac{ij}{3 \deg Q} e^\gamma \omega(s/n)$, and by appropriately choosing s in terms of n, the matrix and thus some row can be made to contain more or fewer primes than expected.

We also proved the following function field analogue of Shiu's theorem:

Theorem 2.2 ([11], Theorem 1.2). Suppose that k is a positive integer, and a and m

are polynomials with m monic and $(a, m) = 1$. Then there exists a string of consecutive primes

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

Furthermore, for sufficiently large k, these primes may be chosen so that their common degree D satisfies

$$\frac{1}{\phi(m)} \left(\frac{\log D}{(\log \log D)^2} \right)^{1/\phi(m)} \ll k. \tag{0.5}$$

The implied constant depends only on q.

The observant reader will notice that it is not obvious what "consecutive" means; the elements of $\mathbb{F}_q[t]$ are not naturally ordered in the same way as the integers. We may in fact order our primes with respect to any ordering compatible with our Maier matrix construction, and in particular our theorem applies with respect to lexicographic order.

This theorem was extended in an interesting way by Tanner [10], who proved the following:

Theorem (Tanner). Under the same hypotheses there exists an integer D_0 (depending on q, k, and m) such that for each $D \geq D_0$ there exists a string of consecutive primes

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

of degree D. Furthermore, for sufficiently large k, D_0 satisfies (0.5).

Tanner's proof is an extension of the author's proof; the point is that since there are many polynomials of the same degree in $\mathbb{F}_q[t]$, it is possible to construct appropriate Maier matrices where all the polynomials in the matrix are of a given degree.

3. 'Prime bubbles' in imaginary quadratic fields

We will now consider the problem of adapting Maier's matrix method to number fields. Let K be an imaginary quadratic field. In this setting a positive proportion of ideals correspond to elements (although the unit group interferes), and the prime elements of $\mathcal{O}_K$ can be naturally visualized as lattice points in $\mathbb{Z}$. Adapting the proof of Shiu's theorem, we proved that there are clumps of primes, all of which lie in an arbitrary fixed arithmetic progression, up to multiplication by units:

Theorem 3.1 ([12], Theorem 1.1). Suppose K is an imaginary quadratic field, k is a positive integer, and a and q are elements of $\mathcal{O}_K$ with $q \neq 2$ and $(a, q) = 1$. Then there exists a "bubble"

$$B(r, x_0) := \{x \in \mathbb{C} : |x - x_0| < r\} \tag{0.6}$$

with at least k primes, all of which are congruent to ua modulo q for units $u \in \mathcal{O}_K$. Furthermore, for k sufficiently large in terms of q (and K), x_0 can be chosen to satisfy

$$\frac{1}{\phi_K(q)}\left(\frac{\log\log|x_0|\log\log\log\log|x_0|}{(\log\log\log|x_0|)^2}\right)^{\omega_K/h_K\phi_K(q)} \ll k. \tag{0.7}$$

The implied constant is absolute.

Here ω_K denotes the number of units in $\mathcal{O}_K$, h_K is the class number of K, and $\phi_K(q) := |(\mathcal{O}_K/(q))^\times|$. As an example of such a 'prime bubble' in $\mathbb{Z}[i]$ (which we found by computer search), the ball of radius $\sqrt{23.5}$ centered at $59+779i$ contains six primes, all congruent to ± 1 or $\pm i$ modulo $5+i$.

To prove our result we construct the following Maier matrix:

$$\begin{bmatrix} Qi_1+b_1 & Qi_1+b_2 & \dots & Qi_1+b_J \\ Qi_2+b_1 & Qi_2+b_2 & \dots & Qi_2+b_J \\ \vdots & \vdots & \vdots & \vdots \\ Qi_I+b_1 & Qi_I+b_2 & \dots & Qi_I+b_J \end{bmatrix} \tag{0.8}$$

Q is defined to be any generator of the ideal $\mathfrak{Q}$, given by

$$\mathfrak{Q} := \mathfrak{q} \prod_{\mathfrak{p}\in\mathcal{P},\mathfrak{p}\neq\mathfrak{p}_0} \mathfrak{p}, \tag{0.9}$$

where $\mathcal{P}$ ranges over primes of norm $\le y$ with restrictions on the residue classes modulo q (which depend on a). The need to exclude one prime $\mathfrak{p}_0$ will be explained shortly.

The i range over all elements of $\mathcal{O}_K$ with norm in $(\mathbb{N}Q^D, 2\mathbb{N}Q^D)$, and the b range over all elements of norm less than either yz or $9yz$ (where z will be chosen later in terms of y). In effect we are constructing two Maier matrices, a "good" matrix (the smaller one, where $\mathbb{N}b < yz$) and a "bad" one. We then prove that nearly all of the primes in the matrix are $\equiv a \pmod q$, where "good" primes $\equiv a \pmod q$ are counted only in the good matrix, and "bad" primes $\not\equiv a \pmod q$ are counted in the larger bad matrix.

There are two more important ingredients in the proof. The first is an appropriate version of the prime number theorem for arithmetic progressions, valid when the relative size of Q and i is as in (0.8). We cannot expect to prove such a result for all Q, but we can for a large class of moduli $\mathfrak{Q}$, as defined in (0.9). The starting point is a zero-density estimate for Hecke L-functions proved by Fogels [2], and we then follow techniques of Gallagher [3] and Shiu to obtain our result. (We remove the prime $\mathfrak{p}_0$ to ensure that the associated L-functions do not have any Siegel zeroes.)

The last ingredient in the proof is a bit of combinatorial geometry. Using the above techniques, we can prove that that some row of our Maier matrix is a pair of concentric balls in the complex plane, such that the inner ball contains many more good primes than the

outer ball has bad. We must now prove that this bubble contains a sub-bubble containing many good primes and *no* bad ones.

To do this we rely on the existence of a *Delaunay triangulation.* The Delaunay triangulation of a set of points has the property that no point in the triangulation is inside the circumcircle of any triangle. We take our set of points to be the set all bad primes within the outer ball, as well as a regular 7-gon (of a certain radius) outside the inner ball but inside the outer one. The circumcircles associated to the Delaunay triangulation contain all of the good points and none of the bad, and the number of such circumcircles is easily bounded from above. Moreover, any circumcircle intersecting the inner ball can be proved to lie entirely within the outer ball. The circumcircle containing the most good primes is therefore our bubble of congruent primes.

4. Concluding remarks

In the first place, we would like to discuss some additional results which we do not have the space to fully describe here. In particular, Granville and Soundararajan [5] recently generalized Maier's theorem and proved that similar irregularities occur in any arithmetic sequence. Here an "arithmetic sequence" is any sequence $\mathcal{A}$ of integers, such that for all integers d coprime to some 'bad' modulus $\mathcal{S}$, the proportion of elements of $\mathcal{A}$ divisible by d is asymptotic to $h(d)/d$, where $h(d)$ is a multiplicative function $h(d)$ taking values in $[0, 1]$. It is also assumed that a suitable weighted average of $h(p)$ is sufficiently smaller than 1.

Examples of such sequences include the primes and arbitrary subsets thereof, almost primes, sums of two squares, norms of algebraic integers from extensions of $\mathbb{Q}$, and many other interesting sequences. Granville and Soundararajan's main result is then that any such sequence cannot be uniformly distributed in both short intervals and arithmetic progressions to somewhat large moduli. To prove their result they combine a generalized Maier matrix construction with a detailed analysis of oscillation in arithmetic functions (such as the function $\omega(C)$ occuring in (0.2)).

In [13], the present author translated their mechanism to $\mathbb{F}_q[t]$. In brief, the method works. In particular we obtained several results on general arithmetic sequences in $\mathbb{F}_q[t]$, exactly along the lines suggested by Granville and Soundararajan's work. Furthermore, in some cases we were be able to be quite precise about where irregularities occur, proving (for example) that they occur among the polynomials of every sufficiently large degree.

We conclude with a few remarks about some related work and some questions that remain. Recently, Pollack [7] has proved an $\mathbb{F}_q[t]$ version of the quantitative Bateman-Horn conjecture (which implies the Hardy-Littlewood prime tuple conjecture as a special case), valid when q is coprime to $2n$ and large in relation to n. Conversely, Conrad, Conrad, and Gross [1] have found a global obstruction to a somewhat different version of this conjecture.

This obstruction is related to a certain average of the Möbius function, and these authors propose a revised conjecture based on geometric considerations as well as numerical calculations. Finite extensions of $\mathbb{F}_q[t]$ are naturally associated to algebraic curves, and one wonders whether the geometry of these curves may have additional consequences for the distribution of primes.

In the number field case we have only scratched the surface, and one could hope to prove all sorts of additional results. For example, one might ask whether one could prove a result similar to Theorem 2.2 for any number field. The statement of such a result might be somewhat more involved, but certainly we believe that the proof should generalize.

One might also ask whether irregularities of the form (0.1) can be proved to exist in number fields. The *norms* of primes are already known to be irregularly distributed, as these form an arithmetic sequence in the sense of [5]. But nothing has yet been proved about these sequences themselves. We are optimistic that techniques similar to those discussed in this article should yield interesting results.

Acknowledgements

I would like to thank the very many people who read my papers and who listened to my talk at Integers Conference 2007 and elsewhere, and who made many useful suggestions. I would also like to again point out the excellent survey articles of Granville [4] and Soundararajan [9], from which I learned much.

References

[1] B. Conrad, K. Conrad, and R. Gross, *Prime specialization in genus 0*, Trans. Amer. Math. Soc. **360** (2008), 2867-2908.

[2] E. Fogels, *On the zeros of L-functions*, Acta Arith. **11** (1965), 67-96.

[3] P. X. Gallagher, *A large sieve density estimate near* $\sigma = 1$, Invent. Math. **11** (1970), 329-339.

[4] A. Granville, *Unexpected irregularities in the distribution of prime numbers*, Proceedings of the International Congress of Mathematicians (Zürich, 1994), 388-399, Birkhäuser, Basel, 1995.

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

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

[7] P. Pollack, *Simultaneous prime specializations of polynomials over finite fields*, Proc. London Math. Soc., accepted for publication.

[8] D. K. L. Shiu, *Strings of congruent primes*, J. London Math. Soc. **61** (2000), 359-373.

[9] K. Soundararajan, *The distribution of prime numbers*, Equidistribution in number theory, an introduction, 59-83, NATO Sci. Ser. II Math. Phys. Chem. **237**, Springer, Dordrecht, 2007.

[10] N. Tanner, *Strings of consecutive primes in function fields*, Int. J. Number Theory, accepted for publication.

[11] F. Thorne, *Irregularities in the distribution of primes in function fields*, J. Number Theory **128** (2008), 1784-1794.

[12] F. Thorne, *Bubbles of congruent primes*, submitted.

[13] F. Thorne, *An uncertainty principle for function fields*, submitted.