IRREGULARITIES IN THE DISTRIBUTIONS OF PRIMES IN FUNCTION FIELDS

FRANK THORNE

Abstract. We adapt the Maier matrix method to the polynomial ring $\mathbb{F}_q[t]$, and prove analogues of results of Maier [4] and Shiu [10] concerning the distribution of primes in short intervals.

1. Introduction and Statement of Results

Let $\mathbb{F}_q$ be the finite field with q elements, and let $\mathbb{F}_q[t]$ denote the corresponding polynomial ring in one variable. As is well known (see, e.g., [8]), $\mathbb{F}_q[t]$ shares many characteristics with $\mathbb{Z}$. In particular the distribution of primes of $\mathbb{F}_q[t]$ is well understood. The Riemann Hypothesis is known in this setting, and results such as the Prime Number Theorem for arithmetic progressions are readily proved with the strongest possible error terms.

Although we expect the distribution of primes in $\mathbb{F}_q[t]$ to be highly regular, we can expect that some irregularities should occur. In the classical case, Maier [4] proved the surprising result that for any fixed $\lambda_0 > 1$,

$$\limsup_{x\to\infty} \frac{\pi(x + (\log x)^{\lambda_0}) - \pi(x)}{(\log x)^{\lambda_0 - 1}} > 1,$$

and

$$\liminf_{x\to\infty} \frac{\pi(x + (\log x)^{\lambda_0}) - \pi(x)}{(\log x)^{\lambda_0 - 1}} < 1.$$

The proof is by the “Maier matrix” method, which we describe as follows; see Granville's article [3] for a nice exposition and a survey of related results. Let Q be a certain product of small primes, and let $x_1 < x_2$ and y be integers with $y < Q$. We consider the following matrix of integers:

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

2000 *Mathematics Subject Classification.* 11N05, 11T55.

The columns form arithmetic progressions modulo Q, and for those Q which meet appropriate conditions on the associated Dirichlet L-functions, each column will contain roughly the expected number of primes.

Accordingly, we may choose Q to isolate particular behavior of the primes. Maier proved his result by showing that by varying the relative values of Q and y, the matrix can be made to contain more or fewer primes than expected. In related work, Shiu [10] proved the existence of arbitrarily long strings of consecutive primes that are all $\equiv a \mod m$, for any integers a and m with $(a, m) = 1$. For example, if $a = 1$, one takes Q to be the product of m and those small primes which are $\not\equiv 1 \mod m$. It then follows that the majority of primes in the matrix are $\equiv 1 \mod m$.

In the present paper, we will introduce a function field version of the Maier matrix and use it to prove analogues of the aforementioned results of Maier and Shiu. The proofs will be simple adaptations of the original arguments. Indeed, due to the nice characteristics of $\mathbb{F}_q[t]$, we will be able to avoid some of the technical difficulties occuring for $\mathbb{Z}$.

We will require several sieve-theoretic lemmas which are analogues of classical results. In several cases these results can be readily found in the literature; in other cases we will give simple proofs mirroring the classical case.

Setup and notation: We fix a finite field $\mathbb{F}_q$ throughout. We are interested in the distribution of primes (i.e., irreducible monic polynomials) in the polynomial ring $\mathbb{F}_q[t]$. Except as noted (and always when referring to primes) we will assume all of our polynomials to be monic.

For a residue class a modulo m, let $\pi(n; m, a)$ denote the number of primes of $\mathbb{F}_q[t]$ of degree n congruent to a modulo m. By the Prime Number Theorem for arithmetic progressions [8], we have

$$\pi(n; m, a) = \frac{1}{\phi(m)} \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right), \tag{1.1}$$

whenever $(a, m) = 1$. Here the Euler ϕ-function is defined by $\phi(m) = |(\mathbb{F}_q[t]/m\mathbb{F}_q[t])^*|$.

As an important special case we of course have

$$\pi(n) = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right), \tag{1.2}$$

where $\pi(n)$ denotes the number of primes of degree n. Moreover, a simple exact formula for $\pi(n)$ is given in [8].

We will be interested in counting the number of primes in short "intervals". We distinguish between two types of intervals. The first definition is rather simplistic: we order all of the monic polynomials of a given degree in lexicographic order, and define intervals and consecutive primes relative to this order. Theorem 1.2 will be proved for intervals of this sort.

Our second definition is more natural in this setting, and a special case of the above. For a fixed polynomial f and an integer $n < \deg f$, we define the interval (f, n) to be the set of polynomials $f + g$, where g ranges over all (not necessary monic or nonzero) polynomials with $\deg g \leq n$. We will write $\pi(f, n)$ to denote the number of primes in this interval.

By (1.1), a randomly selected monic polynomial of degree n is prime with probability about $1/n$. Accordingly, we expect that $\pi(f, n) \sim q^{n+1}/\deg f$ for reasonably large n. The content of our first theorem is that this does not necessarily hold if n is sufficiently small in relation to $\deg f$.

Theorem 1.1. *For any fixed $\lambda_0 > 0$, we have*

$$\limsup_{k\to\infty} \sup_{\deg f = k} \frac{\pi(f, s(k))}{q^{s(k)+1}/k} > 1 \quad \textit{and} \quad \liminf_{k\to\infty} \inf_{\deg f = k} \frac{\pi(f, s(k))}{q^{s(k)+1}/k} < 1,$$

where

$$s(k) := \lceil \lambda_0 \log k \rceil .$$

Here $\lceil x \rceil$ denotes the smallest integer $\geq x$, and the inner supremum and infimum are over all monic polynomials of degree k.

The theorem also holds if $s(k)$ is replaced by any function bounded above by $s(k)$. The proof is an adaptation of the proof of Maier [4], and appears in Section 4.

We also prove the following analogue of Shiu's theorem [10] on strings of consecutive primes:

Theorem 1.2. *For arbitrary polynomials m and a with m monic and $(a, m) = 1$, there exists a constant D' (depending on q and m) such that for any $D > D'$ 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 at most D, where k satisfies

$$k \gg \frac{1}{\phi(m)} \left(\frac{\log D}{(\log\log D)^2} \right)^{1/\phi(m)} . \tag{1.3}$$

The implied constant depends only on q.

Here "consecutive" is to be understood with respect to lexicographic order; all of the p_i will be of the form $p_i = f + g_i$, where f is fixed and the g_i are of comparatively small degree.

One might ask whether one can prove a similar theorem without reference to a particular ordering. In particular, one might hope to prove for each k that there exists an interval (f, n) for some f and n containing at least k primes, such that all of the primes in (f, n) are $\equiv a \mod m$. The counting argument given in Section 5 does not seem to establish this.

We remark further that we expect that the following modest improvement to (1.3) should hold:

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

This would follow from a strengthening of Lemma 3.3 along the lines of work of de Bruijn [1]. For the sake of simplicity we have not attempted this improvement here.

We conclude this section by reviewing our choice of notation. Throughout q will denote the cardinality of the base field, m will denote a monic polynomial in $\mathbb{F}_q[t]$, and a will denote a residue class modulo m, represented by a (not necessarily monic) polynomial of smaller degree. Throughout p will denote a (monic) prime element of $\mathbb{F}_q[t]$, and f and g will denote generic elements of $\mathbb{F}_q[t]$. The prime counting functions $\pi(n; m, a)$ and $\pi(f, n)$ were defined previously in this section. Q will denote a certain product of small primes, and will be different in Sections 4 and 5. In Section 5, c, d, u will denote positive integers, analogous to the quantities y, z, t appearing in [10].

We will write $f(x) \gg g(x)$ to mean that $f(x) > Cg(x)$ for some positive constant C and sufficiently large x. The constant C will depend only on q, but the range of allowable x may depend on other variables as noted.

2. Acknowledgements

I would like to thank Ken Ono for suggesting this project and supervising my work. I would also like to thank Andrew Granville, Eugenijus Manstavičius, Paul Pollack, Noam Tanner, Elena Udovina, and the referee for their numerous helpful comments and suggestions, and for pointing out some of the relevant literature.

3. Preliminary Lemmas

To prove our main results we will require function field versions of several classical sieve-theoretic results.

Lemma 3.1. *(Mertens' estimate) We have the estimate*

$$\prod_{\deg p \leq n} \left(1 - \frac{1}{q^{\deg p}}\right)^{-1} = ne^{\gamma}(1 + o_n(1)). \tag{3.1}$$

Moreover, for an arithmetic progression $a \mod m$ with $(a, m) = 1$ we have

$$\prod_{\substack{p \equiv a \mod m \\ \deg p \leq n}} \left(1 - \frac{1}{q^{\deg p}}\right)^{-1} = n^{1/\phi(m)} C(a, m)(1 + o_n(1)) \tag{3.2}$$

for some constant $C(a, m)$, which is bounded above and below by absolute constants.

Proof. The first equation is a special case of Theorem 3 of [9]. To prove the second equation, we observe that

$$\log \prod_{\substack{p\equiv a \mod m \\ \deg p\leq n}} \left(1-\frac{1}{q^{\deg p}}\right)^{-1} = -\sum_{1\leq i\leq n} \pi(i;m,a)\log(1-q^{-i}).$$

Plugging in (1.1), this is

$$\frac{1}{\phi(m)}\sum_{1\leq i\leq n}\left(\frac{q^i}{i}+O\Big(\phi(m)\frac{q^{i/2}}{i}\Big)\right)\left(\frac{1}{q^i}+O\Big(\frac{1}{q^{2i}}\Big)\right)=\frac{1}{\phi(m)}\sum_{1\leq i\leq n}\left(\frac{1}{i}+O\Big(\phi(m)\frac{1}{iq^{i/2}}\Big)\right). \tag{3.3}$$

This is equal to $\frac{\log n}{\phi(m)}+C+o_n(1)$ for some constant C, and the O-term is bounded uniformly in m and a; the result follows by exponentiation. □

Lemma 3.2. *(Buchstab's identity) Let $\Phi(r,s)$ denote the number of (not necessarily monic) polynomials of degree $\leq r$, none of whose prime factors are of degree $\leq s$. Then for $r>s$, we have*

$$\Phi(r,s)=\frac{q^{r+1}}{s}\Big(\omega(r/s)+o_s(1)\Big), \tag{3.4}$$

where the function $\omega(u)$ is defined by $\omega(u)=1/u$ for $1<u\leq 2$, and

$$u\omega(u)=1+\int_1^{u-1}\omega(v)dv$$

for $u>2$.

Proof. This is a result of Panario and Richmond ([7], Theorem 3.4), and the function $\omega(u)$ is the same as in the classical case (see, e.g., [2], p. 78).

The result in [7] is established for polynomials of degree exactly r, and we deduce (3.4) by summing over r. In particular, $\omega(u)$ is bounded above and below and has bounded derivative, so that the sum over r is well approximated by a geometric series. □

We define a related function $\Psi(r,s)$ to be the number of monic polynomials of degree at most r, all of whose prime factors are of degree $\leq s$.

Lemma 3.3. *Let $\Psi(r,s)$ be defined as above. We have*

$$\Psi(r,s)\ll q^r s\exp(-r/s). \tag{3.5}$$

In fact, Manstavičius proves in [5] that $\Psi(r,s)\sim\frac{q^{r+1}}{q-1}\rho(r/s)$ when $s/\sqrt{r\log r}\to\infty$, where $\rho(u)$ is the Dickman function (see [2], p. 29). This range of r and s is more than sufficient for our purposes, but for simplicity we will avoid estimating $\rho(u)$ and instead give a direct proof following Theorem 5.3.1 of [2].

Proof. If $1/2 < \delta < 1$, we have

$$\begin{aligned}(3.6)\quad \Psi(r,s) = {\sum_{\deg f \leq r}}' 1 &\leq {\sum_{\deg f \leq r}}' \Big(\frac{q^r}{q^{\deg f}}\Big)^{\delta} \\ &\leq (q^r)^{\delta} \prod_{\deg p \leq s} \Big(1 - \frac{1}{(q^{\deg p})^{\delta}}\Big)^{-1} \ll (q^r)^{\delta} \prod_{\deg p \leq s} \Big(1 + \frac{1}{(q^{\deg p})^{\delta}}\Big).\end{aligned}$$

Here the dashes on the sums restrict to those f counted by $\Psi(r,s)$. We choose $\delta = 1 - 1/\log(q^s)$ to obtain

$$\Psi(r,s) \ll q^r \exp(-r/s) \prod_{\deg p \leq s} \Big(1 + \frac{1}{q^{\deg p}} \exp\Big(\frac{\deg p}{s}\Big)\Big).$$

We apply the inequality $1 + x \leq e^x$ to obtain

$$\Psi(r,s) \ll q^r \exp(-r/s) \exp\Big(\sum_{\deg p \leq s} \frac{1}{q^{\deg p}} \exp\Big(\frac{\deg p}{s}\Big)\Big). \tag{3.7}$$

The sum over p is

$$\sum_{\deg p \leq s} \frac{1}{q^{\deg p}} + O\Big(\sum_{\deg p \leq s} \frac{1}{q^{\deg p}} \frac{\deg p}{s}\Big). \tag{3.8}$$

The main term of (3.8) is $\log s + O(1)$ as in (3.3), and the error term is

$$\ll \frac{1}{s} \sum_{\deg p \leq s} \frac{\deg p}{q^{\deg p}} = \frac{1}{s} \sum_{i=1}^{s} \Big(\frac{i}{q^i} \Big(\frac{q^i}{i} + O(q^{i/2})\Big)\Big) = O(1).$$

Substituting these estimates into (3.7), we obtain (3.5). □

Lemma 3.4. *We have*

$$\lim_{u \to \infty} \omega(u) = e^{-\gamma}.$$

Moreover, the function $\omega(u) - e^{-\gamma}$ changes sign in any interval $[a-1, a]$ with $a \geq 2$.

Proof. This is originally due to de Bruijn and Iwaniec, and a proof appears in Lemma 4 of [4]. □

Lemma 3.5. *For any m, let $S(u)$ denote the set of polynomials of degree u whose prime factors are all congruent to 1 modulo m. Then we have*

$$|S(u)| = (C_m + o(1)) q^u u^{-1 + 1/\phi(m)}, \tag{3.9}$$

where

$$C_m := \lim_{s \to 1^+} \frac{1}{\Gamma(1/\phi(m))} (1 - q^{1-s})^{1/\phi(m)} \prod_{p \equiv 1 \mod m} \Big(1 - (q^{\deg p})^{-s}\Big)^{-1}. \tag{3.10}$$

This is a special case of a result of Manstavičius and Skrabutėnas ([6], Theorem 1). We remark that the result is the exact analogue of Lemma 3 of [10].

The implied constant in (3.9) depends on $\phi(m)$. We remark that making this dependence explicit would allow us to determine the constant D' occuring in Theorem 1.2.

4. Proof of Theorem 1.1

For a fixed degree n, denote

$$Q = Q(n) := \prod_{\deg p \leq n} p. \tag{4.1}$$

Since there are $\sim q^k/k$ primes of degree k, we have

$$\deg Q = \sum_{\deg p \leq n} \deg p \sim q^n + q^{n-1} + \cdots \sim \frac{q^{n+1}}{q-1}. \tag{4.2}$$

We introduce a variable s to be chosen later. Our Maier matrix M will have entries $a_{ij} := g_i Q + h_j$, where g_i ranges over all monic polynomials of degree $2\deg Q$, and h_j ranges over all (not necessarily monic or nonzero) polynomials of degree $\leq s$. The rows of M are intervals of the form $(g_i Q, s)$, and the columns are arithmetic progressions modulo Q. Only those columns for which $(Q, h_j) = 1$ will contain primes.

By (1.1) each admissible column will contain $(1 + o_n(1))\frac{q^{3\deg Q}}{3\phi(Q)\deg Q}$ primes. The admissible columns correspond precisely to those h_j whose prime factors are all of degree $> n$. Lemma 3.2 then implies that there are

$$\Phi(s,n) = \frac{q^{s+1}}{n}\omega(s/n)(1 + o_n(1))$$

of them. The total number of primes in the matrix is therefore

$$(1 + o_n(1))\frac{q^{2\deg Q + s + 1}}{3\deg Q}\frac{q^{\deg Q}}{n\phi(Q)}\omega(s/n),$$

and Lemma 3.1 implies that the quotient $\frac{q^{\deg Q}}{n\phi(Q)}$ converges to e^{γ}. Since there are $q^{2\deg Q}$ rows, it follows that at least one row will contain at least

$$(1 + o_n(1))\frac{q^{s+1}}{3\deg Q}e^{\gamma}\omega(s/n) \tag{4.3}$$

primes. As each row of M consists of q^{s+1} polynomials of degree $3\deg Q$, the expected number of primes in this row is $\frac{q^{s+1}}{3\deg Q}$.

To show the first part of Theorem 1.1 for $s(k) = \lceil \lambda_0 \log k \rceil$, we first show that the theorem is true with a sequence of values of s bounded below by $s(k)$. In particular, we use Lemma 3.4 to choose an arbitrarily large $\alpha > \lambda_0 \log q$ for which $\omega(\alpha) > e^{-\gamma}$, and for each n we define $s := \lceil (n+3)\alpha \rceil$, so that $\lim_{n\to\infty} s/n = \alpha$. Choosing a polynomial f_n occuring in the row constructed in (4.3), we see that

$$\limsup_{n\to\infty} \frac{\pi(f_n, s)}{q^{s+1}/\deg f_n} \geq \omega(\alpha)e^{\gamma} > 1. \tag{4.4}$$

Although we have defined s in terms of n, we regard it as a function of $\deg f_n$, i.e., of k in the notation of Theorem 1.1. To show that $s > s(\deg f_n)$ for each large n, we observe that the estimate (4.2) implies that $\deg f_n = 3 \deg Q < q^{n+3}$, so that $\lambda_0 \log(\deg f_n) < \lambda_0 (n+3) \log q < \alpha(n+3) \leq s$.

To see that we can replace s with $s(\deg f_n)$ in (4.4), we observe that the rows chosen in (4.3) may be subdivided into intervals of the form $(f_n + h_j, s(\deg f_n))$, for various polynomials h_j of degree $\leq s$. One of these will contain at least $(1 + o_n(1))\frac{q^{s(\deg f_n)+1}}{\deg f_n} e^{\gamma}\omega(s/n)$ primes, and the first part of Theorem 1.1 follows.

To prove the second part of Theorem 1.1, we choose a row containing at most the number of primes given in (4.3), choose an α for which $\omega(\alpha) < e^{-\gamma}$, and repeat the same argument.

5. Proof of Theorem 1.2

The proof of Theorem 1.2 is a straightforward adaptation of Shiu's proof [10]. We may assume that $\phi(m) > 1$, and we introduce a variable c, as well as variables d and u which will be chosen as unbounded, nondecreasing functions of c satisfying $d < u = o(c)$. For $a \neq 1$ we define a set of primes $\mathcal{P}$ by

$$\mathcal{P} := \begin{cases} \{p : \deg p \leq c, p \not\equiv 1, a \mod m\} \\ \cup \{p : u \leq \deg p \leq c, p \equiv 1 \mod m\} \\ \cup \{p : \deg p \leq c + d - u, p \equiv a \mod m\}. \end{cases} \tag{5.1}$$

For the case $a = 1$ we define instead

$$\mathcal{P} := \begin{cases} \{p : \deg p \leq c, p \not\equiv 1 \mod m\} \\ \cup \{p : u \leq \deg p \leq c + d - u, p \equiv 1 \mod m\}. \end{cases} \tag{5.2}$$

Although the latter definition does not yield optimal bounds for $a = 1$, it simplifies our treatment by allowing us to treat both cases simultaneously.

We define a polynomial Q by

$$Q := mt^{c+d+1} \prod_{p \in \mathcal{P}} p, \tag{5.3}$$

and we define a Maier matrix M consisting of the following set of integers:

$$M := \bigcup_{\deg f = 2\deg Q} \; \bigcup_{\deg g = c+d} Qf + g. \tag{5.4}$$

Here f and g range over monic polynomials of the indicated degrees. We arrange the g in lexicographic order, and as $t^{c+d+1}|Q$, this ensures that each row is in lexicographic order.

Each row of M will be an interval of the form $(Qf+t^{c+d}, c+d-1)$, and each column of M will be the arithmetic progression of all monic polynomials of degree $3\deg Q$ which are congruent to a fixed g modulo Q. By (1.1), each column containing primes will contain asymptotically the same number of primes. Moreover, whether or not a particular element $Qf+g$ is congruent to a modulo m depends only on g, and our choice of Q will ensure that most g with $(g,Q)=1$ fall into the desired congruence class.

We define sets

$$\begin{aligned} S &:= \{h : \deg h = c+d, (h,Q)=1, h \equiv a \mod m\}, \\ T &:= \{h : \deg h = c+d, (h,Q)=1, h \not\equiv a \mod m\}. \end{aligned} \tag{5.5}$$

We will show that $|S|$ is much larger than $|T|$ for appropriate choices of u, c, and d. We assume throughout that c is sufficiently large in relation to q and m; the same will then also be true of u and d. With this restriction, constants implied by $\ll$ and $\gg$ will depend only on q.

To estimate $|S|$, we observe that S contains all products of the form pn, where $p \equiv a \mod m$ and $\deg p > c+d-u$, and n is a product of primes $\equiv 1 \mod m$. We thus have

$$|S| \geq \sum_{i=0}^{u-1} \pi(c+d-i; m, a) S(i),$$

where $S(i)$ is the quantity defined in Lemma 3.5. We use the prime number theorem for arithmetic progressions and Lemma 3.5 to conclude that

$$|S| \gg \frac{C_m}{\phi(m)} q^{c+d} \sum_{i=i_0}^{u-1} \frac{1}{c+d-i} \frac{1}{i^{1-1/\phi(m)}}. \tag{5.6}$$

Here C_m is the constant defined in (3.10), and i_0 is a lower bound (depending on m) for those i for which (3.9) gives an asymptotic estimate.

We have $c+d-i \sim c+d$ because $u = o(c)$, and we approximate the remaining sum over i by the corresponding integral to obtain

$$|S| \gg \frac{C_m}{\phi(m)} \frac{q^{c+d}}{c+d} \int_{i_0}^{u-1} \frac{1}{t^{1-1/\phi(m)}} dt = C_m \frac{q^{c+d}}{c+d} \Big((u-1)^{1/\phi(m)} - {i_0}^{1/\phi(m)} \Big), \tag{5.7}$$

and under our assumption that u is sufficiently large we obtain

$$|S| \gg C_m \frac{q^{c+d}}{c+d} u^{1/\phi(m)}. \tag{5.8}$$

To estimate $|T|$, we split T into two sets T' and T''. T' will consist of elements having some prime factor of degree $> c$ and all other prime factors $\equiv 1 \mod m$.

(Note: these other factors will then automatically have degree $< u$.) T'' will be empty if $a = 1$, and will otherwise consist of elements whose prime factors are all $\equiv 1 \mod m$ and of degree $< u$.

To estimate $|T'|$ we observe that

$$|T'| \leq \sum_{i=0}^{d-1} \pi(c + d - i)S(i),$$

and therefore

$$|T'| \ll C_m q^{c+d} \sum_{i=i_0}^{d-1} \frac{1}{c+d-i} \frac{1}{i^{1-1/\phi(m)}} + i_0 \frac{q^{c+d}}{c+d}.$$

Here we have estimated $S(i)$ trivially for $i < i_0$. We estimate this sum in the same way as (5.7) and see that for sufficiently large c we have

$$|T'| \ll \phi(m) C_m \frac{q^{c+d}}{c+d} d^{1/\phi(m)}.$$

To estimate $|T''|$ we fix $u = \lfloor c/2 \log c \rfloor$ (here $\lfloor x \rfloor$ denotes the greatest integer $\leq x$) and observe that Lemma 3.3 then implies that

$$|T''| \ll q^{c+d} \frac{c}{2 \log c} \exp\Big(-2 \log c \frac{c+d}{c}\Big)$$

which is substantially smaller than $|T'|$. We conclude that

$$|T| \ll \phi(m) C_m \frac{q^{c+d}}{c+d} d^{1/\phi(m)}.$$

As in [10], we split into two cases. Either the majority of primes $\equiv a \mod m$ (henceforth "good" primes) occur in rows containing "bad" primes $\not\equiv a \mod m$, or they occur in rows not containing any bad primes. In the former case at least one row containing a bad prime contains at least $\gg |S|/|T|$ times as many good primes as bad, and hence contains a string of length $\gg \frac{1}{\phi(m)}(u/d)^{1/\phi(m)}$. In the latter case there is a row containing no bad primes, and $\gg \pi'/q^{2 \deg Q}$ good primes, where π' denotes the total number of good primes in the matrix. From our estimation of $|S|$ we conclude that

$$\pi' \gg C_m \frac{q^{c+d}}{c+d} u^{1/\phi(m)} \frac{q^{3 \deg Q}}{(3 \deg Q)\phi(Q)}.$$

We incorporate the estimate

$$\deg Q \ll (\deg m + c + d + 1) + q^c + q^{c-1} + \cdots \ll q^c \tag{5.9}$$

and Lemma 3.1 implies that we have (for either $a \neq 1$ or $a = 1$)

$$\frac{q^{\deg Q}}{\phi(Q)} \gg \frac{m}{\phi(m)} c^{1-2/\phi(m)} \left(\frac{c}{u}\right)^{1/\phi(m)} (c + d - u)^{1/\phi(m)} \gg c u^{-1/\phi(m)}.$$

We put these estimates together to conclude that our row contains $\gg C_m q^d$ good primes and no bad primes.

As one of our two cases must occur, M will contain a progression of primes of length

$$\gg \min\left(\frac{1}{\phi(m)}\left(\frac{u}{d}\right)^{1/\phi(m)}, C_m q^d\right).$$

With the choices $u = \lfloor c/2\log c\rfloor$ and $d = \lfloor \log c\rfloor$ we obtain a progression of length

$$\gg \frac{1}{\phi(m)}\left(\frac{c}{\log^2 c}\right)^{\frac{1}{\phi(m)}}.$$

Theorem 1.2 follows, with the quantitative estimate (1.3) following from (5.9).

References

[1] N. G. de Bruijn, *On the number of positive integers $\leq x$ and free of prime factors $\geq y$*, Indag. Math. **13** (1951), 50-60.

[2] A. C. Cojocaru and M. R. Murty, *An introduction to sieve methods and their applications*, Cambridge University Press, Cambridge, 2005.

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

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

[5] E. Manstavičius, *Remarks on elements of semigroups that are free of large prime factors*, Lithuanian Math. J. **32** (1992), 400-409.

[6] E. Manstavičius and R. Skrabutėnas, *Summation of values of multiplicative functions on semigroups*, Lithuanian Math. J. **33** (1993), 255-264.

[7] D. Panario and B. Richmond, *Analysis of Ben-Or's polynomial irreducibility test*, Proceedings of the Eighth International Conference "Random Structures and Algorithms" (Poznan, 1997), Random Structures Algorithms **13** (1998), 439-456.

[8] M. Rosen, *Number theory in function fields*, GTM 210, Springer-Verlag, New York, 2002.

[9] M. Rosen, *A generalization of Mertens' theorem*, J. Ramanujan Math. Soc. **14** (1999), 1-19.

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

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706
E-mail address: thorne@math.wisc.edu