

ON THE DISTRIBUTION OF PRIMES IN $\mathbb{F}_q[x]$

NOAH SNYDER

ABSTRACT. In this paper we prove the analogs of the Prime Number Theorem and Dirichlet's Theorem on Primes in Arithmetic Progressions over $\mathbb{F}_q[x]$. We give several proofs of the first result. Most of these use the well-known formula for the number of primes of a given degree (which we provide two proofs of), but one proof uses only analytic techniques. We also provide one proof of Dirichlet's Theorem which follows the usual proof over the integers very closely.

1. PRIME NUMBER THEOREM

1.1. Direct Proofs.

Definition 1.1.1. Let $\nu_q(n) =$ the number of irreducible monic polynomials of degree n in $\mathbb{F}_q[x]$

Theorem 1.1.2.

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

Proof 1:

For p an irreducible polynomial $\mathbb{F}_q[x]/p(x)$ is a field with $q^{\deg(p)}$ elements. Therefore, $x^{(q^{\deg(p)})} \equiv x \pmod{p(x)}$. Therefore, $p(x) | x^{(q^n)} - x$ for every prime polynomial p such that $\deg(p) | n$. We claim that

$$x^{(q^n)} - x = \prod_{p(x) \text{ prime: } \deg(p) | n} p(x).$$

We've already shown that the right hand side divides the left hand side. To show equality we must show that no other prime polynomials divide the left hand side and that the left hand side has no repeated roots. The derivative of $x^{(q^n)} - x$ is $q^n x^{(q^n-1)} - 1$ and these two polynomials are relatively prime. (To see this look over the algebraic closure of \mathbb{F}_q where the first polynomial has only 0 and roots of unity as roots, and the second clearly has none of these as roots). Therefore the left hand side has no repeated roots.

Suppose $p(x)$ is a prime dividing $x^{(q^n)} - x$ with degree d . Then $p(x) | x^{(q^d)} - x$. So,

$$p(x) | \gcd(x^{(q^d)} - x, x^{(q^n)} - x).$$

It is elementary to check that the greatest common divisor in question is nothing other than $x^{(q^{\gcd(n,d)})} - x$. Raising to the q^{th} power is an automorphism of $\mathbb{F}_q[x]$ and x is an algebraic generator, so

$$y^{(q^{\gcd(n,d)})} - y \equiv 0 \pmod{p(x)}$$

for all polynomials y . But since $\mathbb{F}_q[x]/p(x)$ is a field, a polynomial of degree k can have at most k distinct roots. So, $q^d \leq q^{gcd(n,d)}$. Therefore they must be equal, so $d|n$. So we have shown that all the primes on the right hand side divide the left hand side, that none of them are repeated, and that there are no other prime factors, therefore the equality is proved.

Taking degrees of both sides yields $q^n = \sum_{d|n} \nu_q(d)d$. Now Möbius inversion proves the theorem. \square

Proof 2:

Let $|f|$ denote $q^{\deg(f)}$. Let

$$\zeta_q(s) = \sum_{f \text{ a monic polynomial in } \mathbb{F}_q[x]} |f|^{-s}.$$

(Notice that this zeta function differs from the standard zeta function of $\mathbb{F}_q[x]$ because it excludes the term at infinity which is irrelevant for our purposes). Collect terms of the same degree to find

$$\zeta_q(s) = \sum_{n=0}^{\infty} \frac{1}{q^{ns}} q^n = \sum_{n=0}^{\infty} \frac{1}{q^{n(s-1)}} = \frac{1}{1 - q^{1-s}}.$$

Now, since $|\cdot|$ is multiplicative, $\zeta_q(s)$ has an Euler factorisation. Namely (using an index of π any time we are taking a sum or product over all irreducible monic polynomials in $\mathbb{F}_q[x]$),

$$\frac{1}{1 - q^{1-s}} = \zeta_q(s) = \prod_{\pi} \frac{1}{1 - |\pi|^{-s}} = \prod_{n=1}^{\infty} \left(\frac{1}{1 - q^{-ns}} \right)^{\nu_q(n)}.$$

To get the required result we simply manipulate this equation.

$$\log \frac{1}{1 - q^{1-s}} = \sum_{n=1}^{\infty} \nu_q(n) \log \frac{1}{1 - q^{-ns}}.$$

Taking Taylor series,

$$\sum_{\ell=1}^{\infty} \frac{1}{\ell} q^{\ell(1-s)} = \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} \frac{1}{m} \nu_q(n) q^{-mns}.$$

Changing variables,

$$\sum_{\ell=1}^{\infty} \frac{1}{\ell} q^{\ell} q^{-\ell s} = \sum_{\ell=1}^{\infty} \sum_{d|\ell} \frac{1}{\ell} \nu_q(d) dq^{-\ell s}.$$

Comparing terms we find that $q^{\ell} = \sum_{d|\ell} \nu_q(d)d$. Just as before, Möbius inversion yields the expected result. \square

Now that we have some handle on the number of primes of a given size we make the following definition:

Definition 1.1.3.

$$\pi_q(x) = \sum_{|\pi| < x} 1$$

We want to get estimates on $\pi_q(q^k)$ for large integers k . Of course, $\pi_q(q^k) = \sum_{n \leq k} \nu_q(n)$. So, using the formula for $\nu_q(n)$ we could directly find estimates on the size of π_q , but just as in \mathbb{Z} it is easier to introduce the following functions.

Definition 1.1.4.

$$\vartheta_q(x) = \sum_{|\pi| < x} \log |\pi|$$

Definition 1.1.5.

$$\psi_q(x) = \sum_{|\pi|^k < x} \log |\pi|$$

Theorem 1.1.6.

$$\vartheta_q(q^k) = \log q \frac{q^{k+1} - q}{q - 1} + O(q^{k/2}k)$$

Notice that,

$$\vartheta_q(q^k) = \sum_{i=1}^k \nu_q(i) (\log q) i = \sum_{i=1}^k (\log q) i \frac{1}{i} \sum_{d|i} \mu(i/d) q^d.$$

Now only the largest term in the inner sum contributes asymptotically. Specifically,

$$\vartheta_q(q^k) = \log q \frac{q^{k+1} - q}{q - 1} + O(q^{k/2}k).$$

□

Of course ϑ_q and ψ_q are related by $\psi_q(x) = \vartheta_q(x) + \vartheta_q(x^{1/2}) + \vartheta_q(x^{1/3}) + \dots$. So ψ_q has the same asymptotics as ϑ_q . Amazingly if we turn our attention to ψ_q the dominant term is actually exactly correct with no error term.

Theorem 1.1.7.

$$\psi_q(q^k) = \log q \frac{q^{k+1} - q}{q - 1}$$

We know,

$$\psi_q(q^k) = \sum_{i=1}^k \sum_{d|i} \nu_q(d) (\log q) d = \sum_{i=1}^k \sum_{d|i} (\log q) d \frac{1}{d} \sum_{e|d} \mu(d/e) q^e.$$

So by Möbius inversion,

$$\psi_q(q^k) = \sum_{i=1}^k q^i \log q = \log q \frac{q^{k+1} - q}{q - 1}.$$

□

Now it remains to relate this formulas back to $\pi_q(q^k)$. Since $\pi_q(x) = \int_1^x \vartheta_q(t) dt$, by integration by parts we have the following theorem.

Theorem 1.1.8.

$$\begin{aligned}
\pi_q(q^k) &= \frac{\vartheta_q(q^k)}{\log q^k} + \int_1^{q^k} \frac{\vartheta_q(t)}{t(\log t)^2} dt \\
&= \frac{q^{k+1} - q}{q-1} \frac{1}{k} + \sum_{i=0}^{k-1} \int_{q^i}^{q^{i+1}} \frac{\frac{q^{i+1}-q}{q-1} \log q}{t(\log t)^2} dt + O(q^{k/2}k) \\
&= \frac{q^{k+1} - q}{q-1} \frac{1}{k} + O\left(\frac{q^{k+1} - q}{q-1} \frac{1}{k^2}\right)
\end{aligned}$$

Notice that just as in the case of the integers we have a difficult formula with a small error term (here the error is very small as we would expect since Riemann Hypothesis is trivially true here) and a simple formula with a large error. Unfortunately in this case we can't combine the integral term with the main term into an Li term as we could in the case of the integers. This is because π_q has really large jumps and so even though $\pi_q(q^k)$ has a nice asymptotic formula $\pi_q(x)$ does not. Therefore, we can't combine the main term and the integral term through integration by parts as we would like to.

1.2. A Purely Analytic Proof.

In this section we prove the asymptotic formula for $\psi_q(q^k)$ using only properties of the zeta function without resorting to the formula for $\nu_q(n)$. This proof more directly resembles standard proofs of Prime Number Theorem over the integers. The difference lies in the fact that here we have to worry about not zeroes of the zeta function, but poles of the zeta function. Fortunately we have a closed formula for the zeta function so we know precisely where this poles are. This explains how we can find an exact formula for $\psi_q(q^k)$.

We already know that $\zeta_q(s) = \frac{1}{1-q^{1-s}}$. Therefore ζ_q has no zeroes and has simple poles of order one at $1 + 2\pi in / \log q$ for n an integer. Now, just as in the case of the integers we find a formula for $\frac{\zeta'_q(s)}{\zeta_q(s)}$ in terms of ψ_q use Melin inversion and evaluate the integral over the left half plane.

$$-\zeta'_q(s) = \sum_f \log |f| |f|^{-s} = \left(\sum_f \frac{\Lambda_q(f)}{|f|^s} \right) \zeta_q(s).$$

Where

$$\Lambda_q(f) = \begin{cases} \log |\pi| & \text{if } f = \pi^k, \\ 0 & \text{otherwise.} \end{cases}$$

Now,

$$-\frac{\zeta'_q(s)}{\zeta_q(s)} = \sum_f \frac{\Lambda_q(f)}{|f|^s} = \int_0^\infty x^{-s} d\tilde{\psi}_q(x).$$

Where,

$$\tilde{\psi}_q(x) = \begin{cases} \frac{\psi_q(q^{k+1}) - \psi_q(q^k)}{2} & \text{if } x = q^k \\ \psi_q(x) & \text{else.} \end{cases}$$

By integration by parts,

$$-\frac{\zeta'_q(s)}{\zeta_q(s)} = \int_0^\infty \tilde{\psi}_q(x) x^{-s-1} dx.$$

Now we apply Melin inversion to find that

$$\tilde{\psi}_q(x) = -\frac{1}{2\pi i} \int_{\sigma-i\infty}^{\sigma+i\infty} -\frac{\zeta'_q(s)}{\zeta_q(s)} \frac{1}{s} x^s ds$$

for any $\sigma > 1$.

Now we hope to re-write the integral on the right hand side as a limit of finite contour integrals and so be able to evaluate it by summing the residues in the left half plane. As one might expect we choose the contour to be symmetric with respect to the real axis and to avoid the poles of the integrand. Let γ_k be the positively oriented rectangle with corners at $-k + \ell_k i$, $2 + \ell_k i$, $-k - \ell_k i$, and $2 - \ell_k i$ (where $\ell_k = \frac{2\pi(k+1/2)}{\log q}$). The choice of ℓ_k takes this contour furthest away from the poles and lets us get a good bound on the integral over the top and bottom sides. I claim that as k goes to infinity the integral over all sides except for the right one go to zero. On the left side all the terms of the integrand decay and the x^s decays exponentially so the integral along that side goes to zero. The top and bottom sides are more difficult but exactly the same as each other, so we only look at the top side. Now for s on the top line,

$$\left| \frac{\zeta'_q(s)}{\zeta_q(s)} \right| = \left| \frac{\log q}{q^{1-s} - 1} \right| = \left| \frac{\log q}{1 - q^{1-s}} \right| \leq \log q$$

because q^{1-s} is negative on the top line.

Therefore, for some positive constant c ,

$$\begin{aligned} \left| \int_{\text{the top side}} \log q \frac{1}{s} x^s ds \right| &\leq \left| \int_{-\infty}^2 \log q \frac{1}{t + \frac{2\pi i(k+1/2)}{\log q}} x^{t + \frac{2\pi i(k+1/2)}{\log q}} dt \right| \\ &\leq \int_{-\infty}^2 c \left| \frac{1}{k+1/2} \right| x^t dt \leq c \frac{1}{k+1/2} \frac{x^2}{\log x} \rightarrow 0 \text{ as } k \rightarrow \infty. \end{aligned}$$

Hence, $\tilde{\psi}_q(x)$ is equal to the symmetric sum of the residues of the poles of $-\zeta'_q(s)/\zeta_q(s) \cdot 1/s \cdot x^s$. $-\zeta'_q(s)/\zeta_q(s)$ has poles at $1 + 2\pi i n / \log q$ ($n \in \mathbb{Z}$) with residue 1. $1/s$ has a pole at 0 with residue 1.

Therefore,

$$\tilde{\psi}_q(x) = \frac{-q \log q}{q-1} + \sum_{n \in \mathbb{Z}} \frac{x^{1 + \frac{2\pi i n}{\log q}}}{1 + \frac{2\pi i n}{\log q}}.$$

Hence,

$$\begin{aligned} \tilde{\psi}_q(q^k) &= \frac{-q \log q}{q-1} + q^k \sum_{n \in \mathbb{Z}} \frac{e^{2\pi i n k}}{1 + \frac{2\pi i n}{\log q}} = \frac{-q \log q}{q-1} + q^k \sum_{n \in \mathbb{Z}} \frac{1}{1 + \frac{2\pi i n}{\log q}} \\ &= \frac{-q \log q}{q-1} + q^k \left(1 + \sum_{n=1}^{\infty} \frac{2}{1 + \left(\frac{2\pi i n}{\log q} \right)^2} \right) \\ &= \frac{-q \log q}{q-1} + q^k \left(1 + 2 \left(\frac{\log q}{2\pi} \right)^2 \sum_{n=1}^{\infty} \frac{1}{\left(\frac{\log q}{2\pi} \right)^2 + n^2} \right). \end{aligned}$$

This final sum can be evaluated using the Poissin summation formula. A well known application of this formula yields

$$\sum_{n=1}^{\infty} \frac{1}{\varepsilon^2 + n^2} = -\frac{1}{2\varepsilon^2} + \frac{\pi}{2\varepsilon} \left(\frac{1 + e^{-2\pi\varepsilon}}{1 - e^{-2\pi\varepsilon}} \right).$$

Therefore, taking $\varepsilon = \frac{\log q}{2\pi}$,

$$\begin{aligned} \tilde{\psi}_q(q^k) &= \frac{-q \log q}{q-1} + q^k \left(1 + 2\varepsilon^2 \sum_{n=1}^{\infty} \frac{1}{\varepsilon^2 + n^2} \right) \\ &= \frac{-q \log q}{q-1} + q^k \left(1 - 1 + \varepsilon\pi \left(\frac{1 + e^{-2\pi\varepsilon}}{1 - e^{-2\pi\varepsilon}} \right) \right) \\ &= \frac{-q \log q}{q-1} + q^k \left(\frac{\log q}{2} \frac{1 + 1/q}{1 - 1/q} \right) \\ &= \frac{\log q}{2} \left(\frac{q^{k+1} - q}{q-1} + \frac{q^k - q}{q-1} \right). \end{aligned}$$

From this we can find the formula for ψ_q . Notice that we can recover ψ_q from $\tilde{\psi}_q$ uniquely. Therefore, the obvious guess $\psi_q(q^k) = \frac{q^{k+1}-1}{q-1} \log q$ must be true. Thus we have proved Theorem 1.1.7. without using the formula for $\nu_q(n)$.

2. DIRICHLET'S THEOREM ON PRIMES IN ARITHMETIC PROGRESSION

Throughout this entire discussion we fix some polynomial $m(x)$ in $\mathbb{F}_q[x]$. We prove that infinitely many prime polynomials lie in each residue class of $(\mathbb{F}_q[x]/m(x))^\times$. Just as in the case of the integers we can do this by showing that the sum of the reciprocals of the primes in each residue class diverges. To prove this we introduce Dirichlet L-series. A character of the group $(\mathbb{F}_q[x]/p(x))^\times$ can be extended to all of $\mathbb{F}_q[x]$ by defining it to be zero on polynomials not coprime to $m(x)$. Such a function is called a Dirichlet character.

Definition 2.0.1. If χ is a Dirichlet character let the Dirichlet L-series be

$$L_q(s, \chi) = \sum_f \frac{\chi(f)}{|f|^s}.$$

Theorem 2.0.2.

$$\log L_q(s, \chi) = \sum_{\pi} \frac{\chi(\pi)}{|\pi|^s} + O(1)$$

To prove this theorem we expand the L-series as an Euler product and then take the log of both sides and expand some Taylor series.

$$\log L_q(s, \chi) = \log \prod_{\pi} \frac{1}{1 - \frac{\chi(\pi)}{|\pi|^s}} = \sum_{\pi} \sum_{n=1}^{\infty} \frac{\left(\frac{\chi(\pi)}{|\pi|^s} \right)^n}{n}.$$

Now we remove the first term from each inner series to get the sum that we want. All that remains to show is that the rest of the sum is bounded. To show

this it is enough to note that $|\pi| \geq q \geq 2$. So,

$$\begin{aligned} \log L_q(s, \chi) &= \sum_{\pi} \frac{\chi(\pi)}{|\pi|^s} + \sum_{n=2}^{\infty} \sum_{\pi} \frac{\left(\frac{\chi(\pi)}{|\pi|^s}\right)^n}{n} \\ &= \sum_{\pi} \frac{\chi(\pi)}{|\pi|^s} + O\left(\sum_{n=2}^{\infty} \frac{1}{2^{sn}}\right) = \sum_{\pi} \frac{\chi(\pi)}{|\pi|^s} + O(1). \end{aligned}$$

□

So,

$$\frac{1}{|G|} \sum_{\chi \in \hat{G}} \bar{\chi}(a) \log L_q(s, \chi) = \sum_{\substack{\pi \equiv a(x) \\ \text{mod } m(x)}} \frac{1}{|\pi|^s} + O(1).$$

Therefore we need only show that $L_q(s, \chi)$ has neither a pole nor a zero at $s = 1$ unless χ is the trivial character. By the orthogonality relation of characters of abelian groups if χ is nontrivial,

$$L_q(s, \chi) = \sum_{\deg \pi < n} \frac{\chi(\pi)}{|\pi|^s}.$$

So, $L_q(s, \chi)$ has no poles.

Now, suppose $L_q(1, \chi) = 0$. We notice that $\prod_{\chi \in \hat{G}} L_q(1, \chi) \geq 1$ because the log of this product has summation formula that has no negative terms. Therefore, since the trivial character is the only one with a pole at one the others can have at most one zero between them. Therefore, χ would have to be real. Now we can eliminate this case with any of the same tricks we use in the case of the integers.

Theorem 2.0.3. *If χ is a non-trivial character then its L-series does not vanish at $s = 1$.*

As mentioned before χ would have to be a real character. In this case define

$$F(s) = \frac{L_q(s, \chi)L_q(s, 1)}{L_q(2s, 1)}.$$

By our assumption F is holomorphic for $\sigma > 1/2$ and $F(s) \rightarrow 0$ as $s \rightarrow 1/2$.

Expand the Euler products of the L-series to find that

$$\begin{aligned} F(s) &= \prod_{\pi: \chi(\pi)=1} \frac{(1 - |\pi|^{-s})^{-1}(1 - |\pi|^{-s})^{-1}}{(1 - |\pi|^{-s})^{-2}} \prod_{\pi: \chi(\pi)=-1} \frac{(1 + |\pi|^{-s})^{-1}(1 - |\pi|^{-s})^{-1}}{(1 - |\pi|^{-s})^{-2}} \\ &= \prod_{\pi: \chi(\pi)=1} \frac{1 + |\pi|^{-s}}{1 - |\pi|^{-s}}. \end{aligned}$$

Now this has a Dirichlet series with only nonnegative coefficients. We want to use this fact to contradict the assumption that $F(s) \rightarrow 0$ as $s \rightarrow 1/2$. To this end we expand F as a Dirichlet series and then as a Taylor series. So, we have

$$F(s) = \prod_{\pi: \chi(\pi)=1} \frac{1 + |\pi|^{-s}}{1 - |\pi|^{-s}} = \sum_{n=1}^{\infty} a_n n^{-s}$$

(where each a_n is a non-negative integer and $a_1 = 1$). Therefore,

$$\begin{aligned} F(s) &= \sum_{k=1}^{\infty} \frac{F^{(k)}(2)}{k!} (s-2)^k = \sum_{k=1}^{\infty} \frac{(-1)^k \sum_{\ell=1}^{\infty} a_{\ell} (\log \ell)^k \ell^{-2}}{k!} (s-2)^k \\ &= \sum_{k=1}^{\infty} \frac{(-1)^k b_m}{k!} (s-2)^k \end{aligned}$$

(where b_m is nonnegative and $b_0 \geq a_1 \cdot 1^2 = 1$). So, if s is a real number between $1/2$ and 2 then all the terms of the last sum are nonnegative. Therefore,

$$F(s) \geq F(2) \geq b_0 \geq 1.$$

This, as we hoped, contradicts the fact that $F(s) \rightarrow 0$ as $s \rightarrow 1/2$. \square

Theorem 2.0.4. *If $m(x)$ is a polynomial then there exist infinitely many prime polynomials in each residue class of $(\mathbb{F}_q[x]/m(x))^{\times}$.*

In fact, by Theorems 2.02 and 2.03

$$\sum_{\substack{\pi \equiv a(x) \\ \text{mod } m(x)}} \frac{1}{|\pi|^s} = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \bar{\chi}(a) \log L_q(s, \chi) + O(1) \rightarrow \infty \text{ as } s \rightarrow 1/2.$$

So there must be infinitely many $\pi \equiv a(x) \pmod{m(x)}$ for this sum to diverge. \square

There are two obvious related questions that are not answered in this paper. The first is whether the expected asymptotic formula for the number of prime polynomials in a given congruence class is true. The second question is whether there are any proofs of Theorem 2.0.4 that are not the same as the proof over the integers. Since the L -series here are actually finite it seems as though there might be a more direct proof that they do not vanish at 1.