The Function Field Analogue of Dirichlet's Theorem on Primes in Arithmetic Progressions

Gleb Glebov

Abstract

The main aim of this work is to introduce the reader to the function field analogue of the celebrated theorem of Dirichlet on primes in arithmetic progressions. We begin by proving Dirichlet's Theorem, and then using almost identical arguments we prove the analogue. Hence, the purpose of first presenting the proof of Dirichlet's Theorem is to emphasize that all we need to do is to define the polynomial analogue of the prime "numbers" and extend the notion of size to polynomials, namely, we seek to generalized $|n|$, the absolute value of $n \in \mathbb{Z}$. Once we explain what prime "numbers" are in this context, the definitions of many familiar number theoretic functions, such as $\varphi(n)$, will not change drastically. Consequently, both the analogue and the proof thereof will be indistinguishable from Dirichlet's Theorem and its proof, respectively.

1 Introduction

Recall that elementary number theory deals with arithmetic properties of integers (the ring $\mathbb{Z}$), and its field of fractions $\mathbb{Q}$. One may eventually realize that $\mathbb{Z}$ and the ring of polynomials over a finite field, $\mathbb{F}[x]$, have many similar properties. For instance, both $\mathbb{Z}$ and $\mathbb{F}[x]$ are principal ideal domains, both have infinitely many prime elements, and both have finitely many units. So we may suspect that both $\mathbb{Z}$ and $\mathbb{F}[x]$ have some "identical" results. In particular, it turns out that many results which hold for $\mathbb{Z}$ have analogues in $\mathbb{F}[x]$. We shall explore one such result: the analogue of Dirichlet's Theorem.

Algebraic number theory arises from elementary number theory by considering finite algebraic extensions, E, of $\mathbb{Q}$ (such extensions are called algebraic number fields). Moreover, one is interested in investigating properties of the ring of algebraic integers, defined as the *integral closure* of $\mathbb{Z}$ in E. Also, one studies the quotient field, Q, of $\mathbb{F}[x]$, and the finite algebraic extensions of Q. These fields are known as *algebraic function fields*. More specifically, an algebraic function field with a finite constant field is known as a *global* function field. Further, a global function field is the true analogue of an algebraic number field.

Before we proceed we need to state Dirichlet's Theorem. We shall also prove it for the sake of completeness, besides, it will allow us to see how similar both results and proofs are.

2 Dirichlet's Theorem

Dirichlet's Theorem states that an arithmetic progression of terms $ak + \ell$ for $k = 1, 2, 3, \ldots$ contains an infinite number of primes whenever k and ℓ are coprime. Essentially, Dirichlet's Theorem guaranties the existence of infinitely many primes of the form $ak + \ell$, i.e.,

$$\ell, \ell + k, \ell + 2k, \ldots$$

contains infinitely many primes whenever k and ℓ are coprime. Equivalently, if k and ℓ are coprime, then there are infinitely many primes p such that $p \equiv \ell \bmod k$. This result had been conjectured by Gauss [2], but was first proved by Dirichlet (ca. 1837).

Euler [4] was perhaps the first to consider numbers of the form $ak + \ell$, but he had never proven the infinitude of prime of the form $4n + 1$ and $4n + 3$, for example. However, Euler [3, Theorem 7] proved (ca. 1737) that the sum of the reciprocals of the primes diverges, viz.,

$$\lim_{s \to 1^+} \sum_p \frac{1}{p^s} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \cdots = \infty$$

and Dirichlet's Theorem is equivalent to the generalization of this result:

$$\lim_{s \to 1^+} \sum_{p \equiv a \bmod b} \frac{1}{p^s} = \infty. \tag{1}$$

The divergence of $\sum_p 1/p$ is a well-known result and many proofs exist, but we provide yet another proof.

Since

$$\ln(N+1) = \int_0^N \frac{dx}{x+1} \leq \sum_{n=1}^N \frac{1}{n} \leq 1 + \int_1^N \frac{dx}{x} = 1 + \ln N,$$

we have

$$\frac{\ln(N+1)}{\ln N} \leq \frac{\sum_{n=1}^N 1/n}{\ln N} \leq 1 + \frac{1}{\ln N},$$

and thus $\sum_{n=1}^N 1/n \sim \ln N$ as $N \to \infty$, where $\sim$ denotes asymptotic equality. Now let $p \leq N$ be the prime less than or equal to N. Employing Euler's product (3) (see §3 for derivation), we get

$$\sum_{n=1}^N \frac{1}{n} \sim \prod_{p \leq N} \frac{1}{1 - 1/p}.$$

We assert that whenever $f(x) \sim g(x)$ and $g(x) \to \infty$ as $x \to \infty$, $\ln f(x) \sim \ln g(x)$. To prove this, we take the natural logarithm of $f(x)/g(x) \to 1$ to get $\ln f(x) - \ln g(x) \to 0$. Hence it immediately follows that $\ln f(x)/\ln g(x) \to 1$.

Besides, $f(x) + c \sim f(x)$ for any constant c. We will also use the Taylor series expansion of $\ln(1-x)$:

$$\ln(1-x) = -\left(x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots\right) \text{ for } |x| < 1.$$

Combining the results above, we see that

$$\begin{aligned}
\ln\ln N &\sim \ln\left(\sum_{n=1}^{N} \frac{1}{n}\right) \\
&\sim \ln\left(\prod_{p\le N} \frac{1}{1-1/p}\right) \\
&= \sum_{p\le N} -\ln(1-1/p) \\
&= \sum_{p\le N} \left(\frac{1}{p} + \frac{1}{2p^2} + \frac{1}{3p^3} + \cdots\right) \\
&= \sum_{p\le N} \frac{1}{p} + \sum_{p\le N} \frac{1}{p^2}\left(\frac{1}{2} + \frac{1}{3p} + \frac{1}{4p^2} + \cdots\right).
\end{aligned}$$

But

$$\begin{aligned}
\sum_{p\le N} \frac{1}{p^2}\left(\frac{1}{2} + \frac{1}{3p} + \frac{1}{4p^2} + \cdots\right) &< \sum_{p\le N} \frac{1}{p^2}\left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) \\
&= \sum_{p\le N} \frac{1}{p^2}\left(\frac{1}{1-1/p}\right) \\
&= \sum_{p\le N} \frac{1}{p(p-1)} \\
&< \sum_{n=1}^{\infty} \frac{1}{n(n-1)} \\
&= 1,
\end{aligned}$$

which means the series on the left-hand side converges as $N \to \infty$, i.e.,

$$\sum_{p\le N} \frac{1}{p} \sim \ln\left(\sum_{n=1}^{N} \frac{1}{n}\right) \sim \ln\ln N \text{ as } N \to \infty,$$

and the result follows.

3 The Proof of Dirichlet's Theorem

We need the following definition:

Definition The *Dirichlet density* of a subset S of the prime numbers is the limit

$$\delta(S) = \lim_{s \to 1^+} \frac{\sum_{p \in S} p^{-s}}{\sum_p p^{-s}}$$

provided it exists.

It is worth remarking that since $0 \leq \delta(S) \leq 1$, $\delta(S)$ is like a probability measure because if $S = S_1 \cup S_2$, then $\delta(S) = \delta(S_1) + \delta(S_2)$ whenever $\delta(S_1)$ and $\delta(S_2)$ exist, and $S_1 \cap S_2 = \emptyset$. Yet, $\delta(S)$ is not countably additive, so it is *not* a probability measure in the conventional sense. Moreover, it is evident that $\delta(S) = 0$ if S is finite.

Our goal is to prove that the set $S_a = \{p : p \equiv a \bmod b, (a, b) = 1\}$ has a finite Dirichlet density, and in particular, $\delta(S_a) = 1/\varphi(b)$, where $\varphi(b)$ is Euler's totient function. In other words,

$$\lim_{s \to 1^+} \left(\sum_{p \equiv a \bmod b} \frac{1}{p^s} - \frac{1}{\varphi(b)} \sum_p \frac{1}{p^s} \right) \tag{2}$$

is finite. Because the sum of the reciprocals of the primes diverges, (2) is finite if and only if (1) holds. Let us prove that (2) is finite.

First, recall that the Dirichlet L-series are defined by

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \quad \Re[s] > 1$$

where χ is a number theoretic function known as the *Dirichlet character*. Formally, a character χ of a finite Abelian group G is a homomorphism $\chi : G \to \mathbf{T}$ mapping G to the unit circle, however, one often sets $G = (\mathbb{Z}/b\mathbb{Z})^*$. The circle group $\mathbf{T}$, which is a subgroup of $\mathbb{C}^*$, is the multiplicative group of all complex numbers with modulus 1, i.e., the unit circle in the complex plane, so each χ maps G to the nth roots of unity for some $n \geq 1$. Since χ is a homomorphism, $\ker \chi = H$ is a subgroup of G, and χ maps each H-coset of G to a distinct root of unity. Thus χ maps an equal number of elements of G to each root of unity. We define character multiplication by $\chi\chi' : g \mapsto \chi(g)\chi'(g)$, where $g \in G$, so with this definition it is readily seen that the Dirichlet characters form a group $\hat{G}$, with the *trivial* character χ_0, defined by

$$\chi_0(g) = \begin{cases} 1 & \text{if } (g, b) = 1 \\ 0 & \text{otherwise} \end{cases},$$

as the identity element. Observe also that since χ maps to the unit circle, $\chi^{-1}(g) = 1/\chi(g) = \overline{\chi(g)}$, the complex conjugate of $\chi(g)$.

We will require Euler's product:

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}, \quad \Re[s] > 1 \tag{3}$$

where the product runs over all primes and $\zeta(s)$ is the zeta function defined by $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ for $\Re[s] > 1$. However, we are primarily interested in the generalized Euler's product:

$$L(s, \chi) = \prod_p \frac{1}{1 - \chi(p)p^{-s}}.$$

Yet, we will derive Euler's product instead as it is less cumbersome, besides, the proof of the generalized Euler's product is completely analogous.

We proceed à la Euler [3]. Take

$$\frac{1}{2^s}\zeta(s) = \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \cdots$$

and subtract it from $\zeta(s)$ to get

$$\zeta(s)\left(1 - \frac{1}{2^s}\right) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \cdots$$

This removes all the elements that have a factor of $1/2^s$. Now subtract

$$\frac{1}{3^s}\zeta(s)\left(1 - \frac{1}{2^s}\right) = \frac{1}{3^s} + \frac{1}{9^s} + \frac{1}{15^s} + \frac{1}{21^s} + \cdots$$

from

$$1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \cdots$$

to get

$$\zeta(s)\left(1 - \frac{1}{2^s}\right)\left(1 - \frac{1}{3^s}\right) = 1 + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{11^s} + \frac{1}{13^s} + \cdots$$

This sieves all the multiples of $1/3^s$ out. Essentially, Euler applied the sieve of Eratosthenes to $\zeta(s)$. Continuing this process *ad infinitum* sieves all the multiples of the prime numbers out. Hence,

$$\zeta(s)\left(1 - \frac{1}{2^s}\right)\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{1}{5^s}\right)\left(1 - \frac{1}{7^s}\right)\left(1 - \frac{1}{11^s}\right)\cdots = 1$$

because 1 is not a multiple of any prime number. Thus we obtain the Euler product:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}}.$$

A slightly more rigorous proof requires the Fundamental Theorem of Arithmetic:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \sum_{\alpha_1,\alpha_2,\alpha_3,\ldots \geq 0} \frac{1}{(2^{\alpha_1}3^{\alpha_2}5^{\alpha_3}\cdots)^s} = \prod_p \left(\sum_{\alpha \geq 0} \frac{1}{p^{\alpha s}}\right) = \prod_p \frac{1}{1 - p^{-s}}.$$

Anyhow, it is now straightforward to show that

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1-\chi(p)p^{-s}} \tag{4}$$

as the proof is identical.

By far the hardest part of the proof of Dirichlet's Theorem is the proof of the following lemma:

Lemma 3.1 We have $\lim_{s\to 1} L(s,\chi_0) = \infty$, while $\lim_{s\to 1} L(s,\chi) < \infty$ and $\lim_{s\to 1} L(s,\chi) \neq 0$ for $\chi \neq \chi_0$.

Proof The proof of the first statement is trivial. If we use the definition of χ_0, (3), and (4), we deduce that

$$\begin{aligned} L(s,\chi_0) &= \prod_p \frac{1}{1-\chi_0(p)p^{-s}} \\ &= \prod_{p\nmid b} \frac{1}{1-p^{-s}} \\ &= \prod_p \frac{1}{1-p^{-s}} \left(\prod_{p|b} \frac{1}{1-p^{-s}} \right)^{-1} \\ &= \zeta(s) \prod_{p|b} (1-p^{-s}). \end{aligned}$$

Notice that this shows that $L(s,\chi_0)$ is almost the same as $\zeta(s)$. Nonetheless, since $\lim_{s\to 1} \prod_{p|b}(1-p^{-s}) > 0$ for all p, $L(s,\chi_0) \to \infty$ as $s \to 1$ (because $\zeta(1)$ is the harmonic series). In other words, $L(s,\chi_0)$ has a simple pole at $s = 1$. The proof of the nonvanishing of $L(1,\chi)$ for $\chi \neq \chi_0$ and $\lim_{s\to 1} L(s,\chi) < \infty$ is given elsewhere [1, §6.10].

Q.E.D.

Let us now finish the proof of Dirichlet's Theorem. In view of the fact that $\sum_p \chi(p)/p^s$ is absolutely convergent for $\Re[s] > 1$, we have

$$\sum_{\chi\in\hat{G}} \chi\left(\frac{1}{a}\right) \sum_p \frac{\chi(p)}{p^s} = \sum_p \frac{\sum_{\chi\in\hat{G}} \chi(p/a)}{p^s} = \sum_{p\equiv a \bmod b} \frac{\varphi(b)}{p^s}. \tag{5}$$

Further, the left-hand side of (5) can be written as

$$\chi_0(1/a) \sum_p \frac{\chi_0(p)}{p^s} + \sum_{\chi\neq\chi_0} \chi(1/a) \sum_p \frac{\chi(p)}{p^s} = \sum_p \frac{1}{p^s} + \sum_{\chi\neq\chi_0} \chi(1/a) \sum_p \frac{\chi(p)}{p^s}. \tag{6}$$

Combining (5) together with (6) leads to

$$\sum_{p\equiv a \bmod b} \frac{1}{p^s} - \frac{1}{\varphi(b)} \sum_p \frac{1}{p^s} = \frac{1}{\varphi(b)} \sum_{\chi\neq\chi_0} \chi(1/a) \sum_p \frac{\chi(p)}{p^s}, \tag{7}$$

so to show that (2) is finite we only need to prove that the right-hand side of (7) remains finite as $s \to 1^+$. In particular, we seek to establish that $\sum_p \chi(p)/p^s$ converges for all $\chi \neq \chi_0$ as $s \to 1^+$.

Proposition 3.1 The infinite series $\sum_p \chi(p)/p^s$ converges for all $\chi \neq \chi_0$ as $s \to 1^+$.

Proof The proof is very similar to the proof of $\sum_p 1/p = \infty$. Let us examine the difference $\ln L(s,\chi) - \sum_p \chi(p)/p^s$. Using (4), and the Taylor series for $\ln(1-x)$ with $|x| < 1$, we conclude that

$$\begin{aligned}
\ln L(s,\chi) - \sum_p \frac{\chi(p)}{p^s} &= \ln\left(\prod_p \frac{1}{1-\chi(p)p^{-s}}\right) - \sum_p \frac{\chi(p)}{p^s} \\
&= \sum_p \left[-\ln\left(1 - \frac{\chi(p)}{p^s}\right) - \frac{\chi(p)}{p^s}\right] \\
&= \sum_p \left[\sum_{n=1}^{\infty} \frac{(\chi(p)/p^s)^n}{n} - \frac{\chi(p)}{p^s}\right] \\
&= \sum_p \sum_{n=2}^{\infty} \frac{(\chi(p)/p^s)^n}{n}.
\end{aligned}$$

Since $\chi \neq \chi_0$, we use Lemma 3.1 and set $s = 1$ to infer that

$$\begin{aligned}
\left|\sum_p \sum_{n=2}^{\infty} \frac{(\chi(p)/p)^n}{n}\right| &\leq \sum_p \sum_{n=2}^{\infty} \left|\frac{(\chi(p)/p)^n}{n}\right| \\
&= \sum_p \sum_{n=2}^{\infty} \frac{1}{np^n} \\
&< \sum_p \left(\frac{1}{p^2} + \frac{1}{p^3} + \frac{1}{p^4} + \cdots\right) \\
&= \sum_p \frac{1}{p^2}\left(\frac{1}{1-1/p}\right) \\
&= \sum_p \frac{1}{p(p-1)} \\
&< \sum_{n=1}^{\infty} \frac{1}{n(n-1)} \\
&= 1.
\end{aligned}$$

Q.E.D.

Therefore the right-hand side of (7) is finite and so is (2), hence $\delta(S_a) = 1/\varphi(b)$. We can now prove the analogue of Dirichlet's Theorem.

4 The Function Field Analogue of Dirichlet's Theorem

We start with a definition.

Definition Let $F = \mathbb{F}[x]$ be a finite field with q elements, and suppose $f(x) \in F$. We define the *size* of f by

$$|f| = \begin{cases} q^{\deg f} & \text{if } f \neq 0 \\ 0 & \text{if } f = 0 \end{cases}.$$

Note that if $f = n \in \mathbb{Z}$, then $|n|$ is the usual absolute value, i.e., the number of elements in $\mathbb{Z}/n\mathbb{Z}$. Similarly, $|f|$ is the number of elements in F/fF. In fact, we have the following proposition:

Proposition 4.1 If $f \in F$ is non-zero, then F/fF is a finite ring with $q^{\deg f}$ elements.

To prove Proposition 4.1 we need to first prove the analogue of the division algorithm (which shows that F is a Euclidean domain and thus a principle ideal domain as well as a unique factorization domain):

Theorem (Division Algorithm) If $f, g \in F$ and $g \neq 0$, then there exist unique $q, r \in F$ such that $f = qg + r$, where $r = 0$ or $\deg r < \deg g$.
Proof The proof is by induction on $n = \deg f$. The details are left as an exercise for the reader.

Q.E.D.

To prove Proposition 4.1 we use the division algorithm to conclude that $\{r \in F : \deg r < \deg g\}$ is a complete set of representatives for F/fF. If $d = \deg g$, then each polynomial $r \in F$ can be written as

$$r = \alpha_{d-1}x^{d-1} + \alpha_{d-2}x^{d-2} + \cdots + \alpha_0, \quad \alpha_0, \alpha_1, \ldots, \alpha_{d-1} \in \mathbb{F}.$$

Since $\alpha_0, \alpha_1, \ldots, \alpha_{d-1}$ vary independently through $\mathbb{F}$, there are $q^d = q^{\deg g}$ such polynomials. We are done because we can now interchange the roles of f and g.

Recall that by definition a non-constant polynomial $f \in F$ is *irreducible* if it cannot be written as a product of two polynomials, each of positive degree. Since every ideal in F is principal, every polynomial is irreducible if and only if it is prime. Moreover, every non-zero polynomial can be written uniquely as a non-zero constant multiple of a monic polynomial. Hence, every ideal in F has a unique monic generator. This result is analogous to the statement that every non-zero ideal in $\mathbb{Z}$ has a unique positive generator. In general, if F^* is the group of units of F, then every non-zero $f \in F$ can be written

as $f = \alpha P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_N^{\alpha_N}$, where $\alpha \in F^*$, each P_i is a monic irreducible with $P_i \neq P_j$ for all $i \neq j$, and $\alpha_1, \alpha_2, \ldots, \alpha_N \in \mathbb{Z}_{\geq 0}$.

We define $\varphi(f)$ to be the number of elements in $(F/fF)^*$. However, if we take into account the division algorithm, we see that each r represents a unit in F/fF if and only if r is relatively prime to f, i.e., $\varphi(f)$ is the number of non-zero polynomials of degree $< \deg f$ and relatively prime to f. Many results involving $\varphi(n)$ have function field analogues. For instance, Euler's product formula,

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

has a function filed analogue (see [6, p. 5]),

$$\varphi(f) = |f| \prod_{P|n} \left(1 - \frac{1}{|P|}\right).$$

What is more, it is straightforward to prove both the analogue of Fermat's Little Theorem and the generalization thereof (Euler's Theorem).

Theorem (Euler's Theorem) If $N \in F$ is non-zero, and $A \in F$ is relatively prime to N, then $A^{\varphi(N)} \equiv 1 \bmod N$.

Corollary (Fermat's Little Theorem) If $P \in F$ is irreducible, and $A \in F$ is a polynomial not divisible by P, then $A^{|P|-1} \equiv 1 \bmod P$.

The function field analogue of Dirichlet's Theorem was first proven by Heinrich Kornblum in his PhD thesis written, just before the onset of World War I, under the direction of Edmund Landau. After completing the work on his thesis, but before writing it up, Kornblum enlisted in the army. He died in the fighting on the Eastern Front. After the war, Landau completed the sad duty of writing up and publishing his student's results (see [5]).

Again, the most difficult part of Kornblum's argument is the proof of the analogue of Lemma 3.1. We will not prove this here, but the diligent reader is encouraged to see [6, pp. 37–39] and/or [5].

To tackle the analogue of Dirichlet's Theorem we will need to define the analogue of $\zeta(s)$.

Definition The *zeta function* associated with F is defined by

$$\zeta_F(s) = \sum_{\substack{f \in F \\ f \text{ monic}}} \frac{1}{|f|^s}, \quad \Re[s] > 1.$$

First, notice that this definition is rather formal. More specifically, this definition does not tell us how one ought to order monic polynomials in F. However,

it is readily seen that $\zeta_F(s)$ is absolutely convergent just like $\zeta(s)$, so any rearrangement of the original series converges to the same value. Notwithstanding, because there are q^d monic polynomials of degree d in F,

$$\sum_{\deg f \leq d} \frac{1}{|f|^s} = 1 + \frac{q}{q^s} + \left(\frac{q}{q^s}\right)^2 + \cdots + \left(\frac{q}{q^s}\right)^d = \frac{1 - q^{(1-s)(d+1)}}{1 - q^{1-s}}.$$

Evidently, $\sum_{\deg f \leq d} |f|^{-s}$ is the dual of $\sum_{n=1}^{N} n^{-s}$, the partial sum of $\zeta(s)$, so we let $d \to \infty$ (just like we would let $N \to \infty$) to conclude that

$$\zeta_F(s) = \frac{1}{1 - q^{1-s}}, \quad \Re[s] > 1 \tag{8}$$

since $|q^{1-s}| < 1$ for $\Re[s] > 1$.

It is noteworthy to mention that proofs involving $\zeta_F(s)$ are much simpler than their counterparts. We have already seen how to use the Fundamental Theorem of Arithmetic to rigorously prove that

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}, \quad \Re[s] > 1.$$

Exact same reasoning leads to

$$\zeta_F(s) = \prod_{\substack{P \text{ irreducible} \\ P \text{ monic}}} \frac{1}{1 - |P|^{-s}}, \quad \Re[s] > 1. \tag{9}$$

Euler used the product representation of $\zeta(s)$ to prove the infinitude of primes: If there were only finitely many primes, then $\lim_{s \to 1^+} \prod_p 1/(1 - p^{-s})$ would be finite, but $\zeta(1)$ is the harmonic series, which is absurd. Similarly, (9) allows us to prove the infinitude of irreducible polynomials in F. We proceed by *reductio ad absurdum*. If there were only finitely many such polynomials, then the right-hand side of (9) would be finite for $s = 1$, but (8) shows that $\zeta_F(s)$ has a pole at $s = 1$, a contradiction.

Proposition 4.2 Let s be real. Then

$$\ln \zeta_F(s) < \sum_P \frac{1}{|P|^s} + 2\zeta_F(2).$$

Moreover, $\lim_{s \to 1+} \sum_P |P|^{-s} = \infty$.

Proof The strategy of the proof is almost indistinguishable from the method we used to prove $\sum_p 1/p = \infty$ in §2. Using (9) and the Taylor series for $\ln(1 - x)$

with $|x| < 1$, yields

$$\begin{aligned}\ln \zeta_F(s) &= \ln\left(\prod_P \frac{1}{1-|P|^{-s}}\right)\\ &= -\sum_P \ln(1-1/|P|^s)\\ &= \sum_P \left(\frac{1}{|P|^s} + \frac{1}{2|P|^{2s}} + \frac{1}{3|P|^{3s}} + \cdots\right)\\ &= \sum_P \frac{1}{|P|^s} + \sum_P \frac{1}{|P|^{2s}}\left(\frac{1}{2} + \frac{1}{3|P|^s} + \frac{1}{4|P|^{2s}} + \cdots\right).\end{aligned}$$

We claim that the latter series is just some constant because

$$\begin{aligned}\sum_P \frac{1}{|P|^{2s}}\left(\frac{1}{2} + \frac{1}{3|P|^s} + \frac{1}{4|P|^{2s}} + \cdots\right) &< \sum_P \frac{1}{|P|^{2s}}\left(1 + \frac{1}{|P|^s} + \frac{1}{|P|^{2s}} + \cdots\right)\\ &= \sum_P \frac{1}{|P|^{2s}}\left(\frac{1}{1-1/|P|^s}\right)\\ &< \sum_P \frac{2}{|P|^{2s}},\end{aligned}$$

where the last inequality follows from the fact that $q \geq 2$ (every field must contain at least two elements), i.e., $|P|^s = q^{s \deg P} \geq 2^{s \deg P} > 2$ owing to the fact that $s > 1$ and $\deg P \geq 1$. Consequently, $\sum_P 2/|P|^2 < 2\zeta_F(2)$. It therefore follows that $\sum_P |P|^{-s}$ diverges as $s \to 1^+$ since $\zeta_F(s)$ has a pole at $s = 1$.

Q.E.D.

In a principal ideal domain, any irreducible element is a prime element, and because F is a principle ideal domain we shall refer to monic irreducible polynomials as primes. So if S is a set of prime in F, then the analogue of $\delta(S)$ is defined by

$$\delta(S) = \lim_{s \to 1} \frac{\sum_{P \in S} |P|^{-s}}{\sum_P |P|^{-s}}$$

for real s in some open interval $(1, b)$ if and only if the limit exists. Next, we wish to prove the analogue of the result in §3, namely, if $S_A = \{P \in F : P \equiv A \bmod B, (A, B) = 1\}$, then $\delta(S_A) = 1/\varphi(B)$. First, however, we need to introduce the analogue of the Dirichlet characters and the L-series.

Suppose $A \in F$ is a polynomial of positive degree, then a Dirichlet character modulo B, χ, is a function from F to $\mathbb{C}$ with the following properties:

1. $\chi(A + A'B) = \chi(A)$ for all $A, A' \in F$.
2. $\chi(AA') = \chi(A)\chi(A')$ for all $A, A' \in F$.
3. $\chi(A) \neq 0$ if and only if $(A, B) = 1$.

Clearly, $\chi : (A/BA)^* \to \mathbb{C}^*$ is a homomorphism, and also, given a homomorphism there is a unique corresponding χ. We define the *trivial* character χ_0 by

$$\chi_0(A) = \begin{cases} 1 & \text{if } (A,B) = 1 \\ 0 & \text{otherwise} \end{cases}.$$

One can verify that there are exactly $\varphi(B)$ characters modulo B and that $|(A/BA)^*| = \varphi(B)$. We define character multiplication by $\chi\chi'(A) = \chi(A)\chi'(A)$, and so the analogue of $\hat{G}$ also forms a group with χ_0 as the identity element. We define the inverse of $\chi(A)$ by

$$\chi^{-1}(A) = \begin{cases} 1/\chi(A) & \text{if } (A,B) = 1 \\ 0 & \text{otherwise} \end{cases},$$

but since χ maps to the unit circle, the value of χ is either zero or a root of unity, so $\chi^{-1}(A) = \overline{\chi(A)}$. We will need to employ a useful orthogonality relation:

$$\sum_{\chi} \chi(A)\overline{\chi(A')} = \begin{cases} \varphi(B) & \text{if } A \equiv A' \bmod B \\ 0 & \text{otherwise} \end{cases}, \tag{10}$$

where $(A, A') = 1$. The proof of this identity is similar to the proof of the corresponding relation over $\mathbb{Z}$: We see that A' has a multiplicative inverse $\overline{A'}$ modulo B. Obviously, if $A'' = A\overline{A'}$, then $\chi(A')\chi(A'') = \chi(A'A'') = \chi(A'A\overline{A'}) = \chi(A)$, and thus $\chi(A'') = \chi(A)/\chi(A') = \chi(A)\overline{\chi(A')}$. But $A'' = A\overline{A'} \equiv 1 \bmod B$ if and only if $A \equiv A' \bmod B$, so

$$\sum_{\chi} \chi(A'') = \begin{cases} \varphi(B) & \text{if } A'' \equiv 1 \bmod B \\ 0 & \text{otherwise} \end{cases}$$

because there are exactly $\varphi(B)$ characters modulo B. The result follows.

At this point it should not be difficult to guess what the definition of $L_F(s,\chi)$ ought to be: We define $L_F(s,\chi)$ by

$$L_F(s,\chi) = \sum_{\substack{f \in F \\ f \text{ monic}}} \frac{\chi(f)}{|f|^s}, \quad \Re[s] > 1.$$

Besides, we have the following analogue of (4):

$$L_F(s,\chi) = \prod_{P} \frac{1}{1 - \chi(P)|P|^{-s}}, \tag{11}$$

the derivation of which is routine and is quite similar to that of (4). Further, one can easily prove the analogue of the identity $L(s,\chi_0) = \zeta(s)\prod_{p|b}(1-p^{-s})$, namely,

$$L_F(s,\chi_0) = \zeta_F(s) \prod_{P|B} (1 - |P|^{-s}). \tag{12}$$

Once again, the most challenging part of proving that $\delta(S_A) = 1/\varphi(B)$, is showing that $L_F(1,\chi) \neq 0$ for $\chi \neq \chi_0$ (modulo B). This fact is much easier to prove than its counterpart. Nevertheless, we will not prove this (for derivation see Rosen [6, pp. 37–39]). In particular, Rosen [6, p. 39] concludes that if s is real and > 1, then $\lim_{s\to 1} \ln L_F(s,\chi_0) = \infty$ and $\lim_{s\to 1} \ln L_F(s,\chi) < \infty$ for $\chi \neq \chi_0$. Here, $\ln z$ is the principal value of the natural logarithm. Now we can finally prove the analogue of Dirichlet's Theorem.

Theorem (Kornblum) Let $A, B \in F$ be two relatively prime polynomials with $\deg B > 0$. If $S_A = \{P \in F : P \equiv A \bmod B, (A,B) = 1\}$, then $\delta(S_A) = 1/\varphi(B)$. Moreover, S_A is an infinite set.

Proof Using (11) and the technique similar to the one used in the proof of Proposition 4.2, we obtain

$$\ln L_F(s,\chi) = \sum_P \frac{\chi(P)}{|P|^s} + R(s,\chi),$$

where $\lim_{s\to 1^+} R(s,\chi)$ is bounded. Multiply both sides by $\overline{\chi(A)}$, sum over all χ (modulo B), and apply (10) to get

$$\sum_\chi \overline{\chi(A)} \ln L(s,\chi) = \sum_{P\equiv A \bmod B} \frac{\varphi(B)}{|P|^s} + R(s), \tag{13}$$

where $R(s)$ remains bounded as $s \to 1^+$ (cf. (5)). Now, to compute $\delta(S_A)$, we divide (13) by $\sum_P |P|^{-s}$, which yields

$$\frac{\sum_\chi \overline{\chi(A)} \ln L(s,\chi)}{\sum_P |P|^{-s}} = \varphi(B)\delta(S_A) + \frac{R(s)}{\sum_P |P|^{-s}}. \tag{14}$$

But

$$\lim_{s\to 1^+} \frac{\sum_\chi \overline{\chi(A)} \ln L(s,\chi)}{\sum_P |P|^{-s}} = \lim_{s\to 1^+} \frac{\overline{\chi_0(A)} \ln L(s,\chi_0)}{\sum_P |P|^{-s}}$$

since both $\overline{\chi(A)}$ and $\ln L(1,\chi)$ are finite for $\chi \neq \chi_0$ and $\lim_{s\to 1^+} \sum_P |P|^{-s} = \infty$. Using Proposition 4.2, the definition of χ_0, and (12), we conclude that

$$\lim_{s\to 1^+} \frac{\overline{\chi_0(A)} \ln L(s,\chi_0)}{\sum_P |P|^{-s}} = 1.$$

Needless to say, $R(s)/\sum_P |P|^{-s} \to 0$ as $s \to 1^+$, and thus (14) reduces to $\delta(S_A) = 1/\varphi(B)$.

Q.E.D.

References

[1] T. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, NY, 1976.

[2] J. Derbyshire, *Prime Obsession: Bernhard Riemann and the Greatest Unsolved Problem in Mathematics* 9th ed., Joseph Henry Press, Washington, DC, 2006.

[3] L. Euler, Variae observationes circa series infinitas, *Comm. Acad. Sci. Petropolit.* **9** (1744) 160–188, available at `EulerArchive.org`.

[4] ——, Theoremata circa divisores numerorum in hac forma $paa \pm qbb$ contentorum, *Comm. Acad. Sci. Petropolit.* **14** (1751) 151–181, available at `EulerArchive.org`.

[5] H. Kornblum, and E. Landau, Uber die Primfunktionen in einer Arithmetischen Progression, *Math. Z.* **5** (1919) 100–111.

[6] M. Rosen, *Number Theory in Function Fields*, Springer-Verlag, NY, 2002.