Universiteit Utrecht

Bachelor thesis

Mathematics

Counting irreducible polynomials over finite fields

Author:
Alex Braat

Supervisor:
Dr. Gunther Cornelissen

June 14, 2018

Utrecht University

Abstract

The prime number theorem states that for the prime counting function $\pi(x)$, we have

$$\pi(x) \sim \frac{x}{\log(x)} \qquad (x \to \infty).$$

We will look at a analogue of the prime number theorem for polynomials over a finite field $\mathbb{F}_q$. Using the formula of Gauss, we will derive the asymptotic equivalence

$$\pi_q(n) \sim \frac{q}{q-1} \cdot \frac{q^n - 1}{n} \qquad (n \to \infty),$$

where $\pi_q(n)$ is the function that counts the monic irreducible polynomials in $\mathbb{F}_q[T]$ with degree less or equal to an positive integer n. Unlike the prime number theorem, this result cannot be extended to the positive real numbers. In order to solve this issue, we will look at the following encoding: For a non-negative integer n, write n is base q, i.e. $n = a_n q^n + \cdots + a_1 q + a_0$, and associate it with the polynomial $a_n T^n + \cdots + a_1 T + a_0 \in \mathbb{F}_q[T]$. We consider the counting function $\hat{\pi}_q(X)$ that counts irreducible polynomials in $\mathbb{F}_q[T]$ that are encoded by an integer smaller than a positive real number X. We then prove an analogue of the prime number theorem that does extend to the positive real numbers,

$$\hat{\pi}_q(X) \sim \frac{X}{\log_q(X)} \qquad (X \to \infty),$$

by using a result by Pollack that grounded in Weil's Riemann Hypothesis for function fields.

1 Introduction

One of the problems studied in number theory is the distribution of primes. One observes that the small primes lie relatively close together, while the larger primes are more spaced apart. One question we could then ask ourselves is how the density of primes is related to their size. By creating large tables of primes, and studying the density, Gauss noted that "around x the density of primes is approximately $1/\log(x)$" [12]. This observation is key to formulating the prime number theorem.

In order to properly formalize this observation, Gauss studied the following prime counting function: Let $x > 0$ be a real number. Then let $\pi(x)$ denote the number of primes smaller or equal to x. Thus we have $\pi(x) = \sum_{p \leq x} 1$. As we expect the density of primes around x to be $1/\log(x)$, it is only natural to expect $\pi(x)$ to be approximately equal to the logarithmic sum or logarithmic integral, which are respectively given by:

$$\operatorname{ls}(x) := \sum_{2 \leq n \leq x} \frac{1}{\log(n)}, \qquad \operatorname{li}(x) := \int_2^x \frac{dt}{\log(t)}.$$

We say two functions f and g are asymptotically equivalent if their quotient $\frac{f(x)}{g(x)}$ tends to 1 as x tends to infinity. We will use the notation $f(x) \sim g(x)$ as $x \to \infty$. For every $x \geq 2$, the difference between $\operatorname{ls}(x)$ and $\operatorname{li}(x)$ is bounded by $1/\log(2)$ [5, Prop. 1.5.1]. Therefore, the logarithmic sum and logarithmic integral are asymptotically equivalent. These functions are also asymptotically equivalent with $x/\log(x)$ [5, Prop. 1.5.3].

The prime number theorem (conjectured by both Gauss (1792) and Legendre (1798)) states that the prime counting function $\pi(x)$ is asymptotically equivalent to these functions. It is most commonly formulated in the form

$$\pi(x) \sim \frac{x}{\log(x)} \qquad (x \to \infty). \tag{1}$$

It was proved one hundred years later in 1896, by both Hadamard and de la Vallée Poussin independently. Their proofs both relied on the Riemann zeta function, the analytic continuation of the sum $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. Riemann showed that the distribution of primes is directly related to the zeros of this function. Hadamard and La Vallée Poussin proved that the Riemann zeta function has no zeros on the line $\mathrm{Re}(s) = 1$, which in turn implied the prime number theorem.

The approximations $\mathrm{ls}(x)$ and $\mathrm{li}(x)$ are more accurate than $x/\log(x)$ and are therefore preferred when looking at error terms. For the error tems we will use the big-$\mathcal{O}$ notation: For any two functions f and g, we have $f(x) = \mathcal{O}(g(x))$ if there exists a constant C such that, for x large enough, the absolute value of $f(x)$ is bounded by $Cg(x)$.

Because $\mathrm{ls}(x)$ and $\mathrm{li}(x)$ only differ by a bounded amount, the following error terms also hold true for $\mathrm{ls}(x)$. Using that ζ has no zeros on the line $\mathrm{Re}(s) = 1$, it can be shown that for a constant c we have [5, Thm. 5.1.8]:

$$\pi(x) = \mathrm{li}(x) + \mathcal{O}(xe^{-c\sqrt{\log(x)}}) \tag{2}$$

The error term can be more generally expressed by the zeros of ζ. Let $\Theta = \sup_{\zeta(s)=0} \mathrm{Re}(s)$ be the supremum of the real parts of the zeros of ζ. Then we have [11, p. 45]:

$$\pi(x) = \mathrm{li}(x) + \mathcal{O}(x^{\Theta} \log(x)) \tag{3}$$

Riemann conjectured that all the non-trivial zeros of ζ lie on the line $\mathrm{Re}(s) = \frac{1}{2}$. This conjecture is known as the Riemann hypothesis. The Riemann hypothesis implies $\Theta = \frac{1}{2}$, giving us the approximation $\pi(x) = \mathrm{li}(x) + \mathcal{O}(\sqrt{x}\log(x))$.

There also exists an *elementary* proof of the prime number theorem given by Erdős and Selberg in 1949, which does not depend on complex analysis. Although elementary, it is by no means simple.

For more details on the prime number theorem we would like to point our readers to [11], [5] and [1, Ch. 4].

In this bachelor thesis we will study an analogue of the prime number theorem in the ring $\mathbb{F}_q[T]$ consisting of polynomials with coefficients in a finite field $\mathbb{F}_q$, i.e. polynomials of the form

$$f(T) = a_n T^n + \cdots + a_1 T + a_0,$$

with $a_0, \ldots, a_n \in \mathbb{F}_q$. We will be researching the asymptotic behavior of functions that count irreducible polynomials, and compare these results with the prime counting function $\pi(x)$. One of the advantages of working with $\mathbb{F}_q[T]$ will be the formula of Gauss, a direct formula for the number of monic irreducible polynomials of degree n, which will be a powerful tool to research the asymptotic behavior of these counting functions.

2 Preliminary results

In this section we will prove some preliminary results about finite fields and the Möbius function. These results will mainly be used to prove the formula of Gauss for the number of monic irreducible polynomials of degree n.

2.1 Finite fields

If p is prime, the ring $\mathbb{Z}/p\mathbb{Z}$ is a field with exactly p elements. This is the only finite field (up to isomorphism) that contains exactly p elements. If L is a field with p elements, let p' be the characteristic of L. Then $\mathbb{Z}/p'\mathbb{Z}$ is isomorphic to a subfield of L, which implies p' divides p. But this is only possible if $p' = p$, and therefore $L \cong \mathbb{Z}/p\mathbb{Z}$. We will use the notation $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

In general, if q is a power of a prime, then there exists a unique finite field with q elements, which we will denote by $\mathbb{F}_q$.

Theorem 2.1. *Let q be the power of a prime, i.e. $q = p^k$ for some prime p. The following holds:*

i. Let q be the power of a prime, i.e. $q = p^k$ for some prime p. Then there exists a unique field (up to isomorphism) with exactly q elements. This field is the splitting field of $T^q - T$ over $\mathbb{F}_p[T]$.

ii. If L is a finite field with q elements, then q is the power of a prime.

Proof. i. We consider the splitting field L of the polynomial $P(T) = T^q - T \in \mathbb{F}_p[T]$. This is the smallest field that contains $\mathbb{F}_p$ and zeros of P such that P can be factored in linear terms. Notice that $P'(T) = qT^{q-1} - 1 = p^k T^{q-1} - 1 = -1$. Thus P is separable, meaning all it's zeros are distinct. So L contains q distinct zeros of P. Furthermore, for any two zeros α, β of P we have $P(\alpha - \beta) = 0$ and if $\beta \neq 0$ then $P(\alpha\beta^{-1}) = 0$, and therefore the zeros of P form a subfield of the splitting field L. But for every $a \in \mathbb{F}_p$ we have $P(a) = a^q - a = a^{p^k} - a = a - a = 0$. So $\mathbb{F}_p$ is contained in the field in the subfield of zeros. Then, by definition, the splitting field L of P is exactly the set of zeros of P, and thus L has q elements.

If L is a finite field with q elements, then $L^* = L \setminus \{0\}$ has order $q - 1$. But then if $a \in L$, we have $a^q = a$ and therefore a is a root of $P(T) = T^q - T$. Thus L is the splitting field of $P(T)$.

ii. Let L be a field with q elements. Let p be the characteristic of L. Then L is a finite field extension of $\mathbb{F}_p$. Let $k = [L : \mathbb{F}_p]$ be the degree of this extension. Then there exist a $\mathbb{F}_p$-linearly independent basis $a_1, \ldots, a_k \in L$, such that

$$L = \{a_1 x_1 + \cdots + a_k x_k : x_i \in \mathbb{F}_p\}.$$

Therefore L has exactly p^k elements, giving us $q = p^k$ with p prime.

□

We will also need the following theorem:

Theorem 2.2. *Let q be the power of a prime and a, b be positive integers. If a divides b, then $\mathbb{F}_{q^a}$ is a subfield of $\mathbb{F}_{q^b}$. Furthermore, the field extension $\mathbb{F}_{q^b}/\mathbb{F}_{q^a}$ is Galois. Then every irreducible polynomial over $\mathbb{F}_{q^a}$,that has a zero in $\mathbb{F}_{q^b}$, is separable and has all of its zeros in $\mathbb{F}_{q^b}$.*

Proof. Let a, b be positive integers such that a divides b. By a similar argument as in the proof of the previous theorem, the splitting field of $P(T) = T^{q^b} - T$ over $\mathbb{F}_{q^a}$ has exactly q^b elements and is isomorphic to $\mathbb{F}_{q^b}$. It also contains $\mathbb{F}_{q^a}$, and thus $\mathbb{F}_{q^a}$ is a subfield of $\mathbb{F}_{q^b}$. Furthermore, because $P(T)$ is separable and $\mathbb{F}_{q^b}$ is the splitting field of P over $\mathbb{F}_{q^a}$, it follows from the field extension $\mathbb{F}_{q^b}/\mathbb{F}_{q^a}$ is indeed Galois. But then it follows that every irreducible polynomial over $\mathbb{F}_{q^a}$, that has a zero in $\mathbb{F}_{q^b}$, is separable and has all of its zeros in $\mathbb{F}_{q^b}$ [4, Thm 14.13]. □

2.2 The Möbius function

An arithmetical function is a complex-valued function $f : \mathbb{Z}_{>0} \to \mathbb{C}$ defined on the positive integers. An important arithmetical function is the Möbius function μ. It is defined as follows:

$$\mu(n) = \begin{cases} 1 & \text{if } n \text{ is squarefree and has an even number of prime factors,} \\ -1 & \text{if } n \text{ is squarefree and has an odd number of prime factors,} \\ 0 & \text{if } n \text{ is not squarefree.} \end{cases}$$

Other examples include

$$1(n) = 1 \qquad \text{and} \qquad I(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

We first prove the following theorem [1, Thm. 2.1]:

Theorem 2.3. *For all $n \geq 1$ we have*

$$\sum_{d|n} \mu(d) = I(n). \tag{4}$$

Proof. If $n = 1$ then the sum is equal to $\mu(1) = 1 = I(1)$. Now take $n > 1$ and let $n = p_1^{k_1} \cdots p_r^{k_r}$ be the prime factorization of n. Then we have

$$\begin{aligned} \sum_{d|n} \mu(d) &= 1 + \sum_{1 \leq i \leq r} \mu(p_i) + \sum_{1 \leq i_1 < i_2 \leq r} \mu(p_{i_1} p_{i_2}) + \cdots + \mu(p_1 \cdots p_r) \\ &= 1 + \binom{r}{1}(-1) + \binom{r}{2}(-1)^2 + \cdots + (-1)^r \\ &= (1 + (-1))^r = 0 = I(n) \end{aligned}$$

and therefore we get the desired result. □

A way to interpret this theorem is by Dirichlet convolution. On any two arithmetical function f, g we define the Dirichlet convolution $f * g$ by

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right). \tag{5}$$

It is clear that the Dirichlet convolution is again an arithmetical function. Moreover, Dirichlet convolution is a commutative group operation on the set of arithmetical functions f with $f(1) \neq 0$. The identity element corresponds with I as we have $I * f = f * I = f$ for every arithmetical function f (for proofs and more details see [1, Ch. 2.6-2.7] and [11, Ch. 4.3]).

Then Theorem 2.2 states that $\mu * 1 = I$, in other words μ and 1 are inverses with regard to Dirichlet convolution. Then we have $f = g * 1$ if and only if $g = f * \mu$. This is called Möbius inversion. As we haven't explicitly proved any of the above mentioned properties of Dirichlet convolution, we will provide a proof for Möbius inversion.

Theorem 2.4 (Möbius inversion)**.** *For all arithmetic function $f, g : \mathbb{N} \to \mathbb{C}$ the following are equivalent:*

i. $f(n) = \sum_{d|n} g(d)$ *for all* $n \geq 1$.

ii. $g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$ *for all* $n \geq 1$.

Proof. We will apply Theorem 2.2 in both directions. For $(i) \Rightarrow (ii)$, assume $f(n) = \sum_{d|n} g(n)$ for all $n \geq 1$. Then we have:

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{e|\frac{n}{d}} g(e) = \sum_{e|n} g(e) \sum_{d|\frac{n}{e}} \mu(d) = \sum_{e|n} g(e) I\left(\frac{n}{e}\right) = g(n).$$

For $(ii) \Rightarrow (i)$, we now assume $g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$ for all $n \geq 1$. Then

$$\begin{aligned}\sum_{d|n} g(d) = \sum_{d|n} g\left(\frac{n}{d}\right) &= \sum_{d|n} \sum_{e|\frac{n}{d}} \mu(e) f\left(\frac{n}{de}\right) \\ &= \sum_{k|n} f\left(\frac{n}{k}\right) \sum_{e|k} \mu(k) = \sum_{k|n} f\left(\frac{n}{k}\right) I(k) = f(n).\end{aligned}$$

□

We will also need following theorem concerning the sum of terms $\mu(n)/n$ later on. We will follow [1, Thm. 3.13]:

Theorem 2.5. *For all $x \geq 1$, we have*

$$\left| \sum_{n \leq x} \frac{\mu(n)}{n} \right| \leq 1. \tag{6}$$

Proof. Let $x \geq 1$. For any real number y we define $[y]$ to be the largest integer less or equal to y, and $\{y\} := y - [y]$. We have

$$\sum_{n \leq x} \mu(n) \left[\frac{x}{n}\right] = \sum_{n \leq x} \mu(n) \sum_{m \leq \frac{x}{n}} 1 = \sum_{nm \leq x} \mu(n) = \sum_{k \leq x} \sum_{d|k} \mu(d) = \sum_{k \leq x} I(k) = 1$$

by applying Theorem 2.2. On the other hand we get

$$\sum_{n \leq x} \mu(n) \left[\frac{x}{n}\right] = \sum_{n \leq x} \mu(n) \left(\frac{x}{n} - \left\{\frac{x}{n}\right\}\right) = x \sum_{n \leq x} \frac{\mu(n)}{n} - \sum_{n \leq x} \mu(n) \left\{\frac{x}{n}\right\}$$

Combining these two gives us

$$x\left|\sum_{n\le x}\frac{\mu(n)}{n}\right| = \left|1+\sum_{n\le x}\mu(n)\left\{\frac{x}{n}\right\}\right| \le 1+\sum_{n\le x}|\mu(n)|\left\{\frac{x}{n}\right\} \le 1+\sum_{n\le x}\left\{\frac{x}{n}\right\}$$
$$= 1+\{x\}+\sum_{2\le n\le x}\left\{\frac{x}{n}\right\} \le 1+\{x\}+[x]-1 = x$$

Then we divide both sides by x to complete the proof. □

3 Analogue between $\mathbb{F}_q[T]$ and $\mathbb{Z}$

On first sight, the rings $\mathbb{Z}$ and $\mathbb{F}_q[T]$ don't look very similar. But actually, as we will see in this section, these rings do have a lot in common. Furthermore, many important theorems in number theory have natural analogues in $\mathbb{F}_q[T]$, and, as we will see with the prime number theorem, most of these analogous theorems are also easier to prove than their original counterparts.

3.1 Common properties between $\mathbb{F}_q[T]$ and $\mathbb{Z}$

Just as with the integers, we can add, subtract and multiply any two polynomials in $\mathbb{F}_q[T]$, but division on the other hand isn't always defined. For instance, we cannot divide 1 by T. We can however, speak of divisibility. For polynomials $f, g \in \mathbb{F}_q[T]$, we say that f divides g (notation $f|g$) if there exists a polynomial $h \in \mathbb{F}_q[T]$ such that $g = fh$.

In $\mathbb{Z}$, even if we cannot divide two integers, we can still look at Euclidean division (also known as division with remainder). Recall for any $a, b \in \mathbb{Z}$ with $b \neq 0$, there exist unique $q, r \in \mathbb{Z}$ such that $a = qb + r$, where $0 \le r < |b|$. Similarly we have Euclidean division for $\mathbb{F}_q[T]$. For $f \in \mathbb{F}_q[T]$ we define the norm of f by $|f| = q^{\deg(f)}$ (if $f = 0$ then $|f| = 0$). Then we get:

Theorem 3.1 (Euclidean division)**.** *For every two polynomials $f, g \in \mathbb{F}_q[T]$ with $g \neq 0$, there exist unique $q, r \in \mathbb{F}_q[T]$ such that*

$$f = qg + r \qquad \textit{and} \qquad |r| < |g|.$$

The idea of the proof relies on the fact that $\mathbb{F}_q$ is a field. Let $d = \deg(g)$. Then any term f_nT^n with $n \ge d$ can be eliminated by subtracting $\frac{f_n}{g_d}T^{n-d}g(T)$ from $f(T)$, leaving only terms with degree smaller than d. For a complete proof see [6, Thm. 15.4]

Because both $\mathbb{Z}$ and $\mathbb{F}_q[T]$ are Euclidean domains (i.e. have Euclidean division), they are also principal ideal domains [4, Prop. 8.1] and therefore unique factorization domains [4, Thm. 8.14].

We could then ask ourselves if we also have primes in $\mathbb{F}_q[T]$. The answer is yes: the irreducible polynomials. In an arbitrary ring, we call an element π, not a unit and nonzero, irreducible if for every factorization $\pi = ab$, either a or b is a unit (i.e. has an multiplicative inverse). For any two elements a, b, if there exists an unit u such that $a = ub$, then we call a and b associates. It is clear that if π is irreducible, then it's associates are also irreducible.

The unit group of $\mathbb{Z}$ is given by $\mathbb{Z}^* = \{-1, 1\}$. Thus an element $p \in \mathbb{Z}$ is irreducible if a or b equals ± 1. But if we take $a = \pm 1$, then $b = \pm p$. Thus the only divisors of p are $\pm 1, \pm p$. If we take p to be positive, then this is exactly the definition of a prime number. Thus the primes in $\mathbb{Z}$ are the positive irreducible integers. Moreover, a negative integer is irreducible if and only if it's positive associative is irreducible. So we only have to study the primes to study the irreducibility of all integers.

The unit group of $\mathbb{F}_q[T]$ is equal to $\mathbb{F}_q^*$, as $fg = 1$ implies $\deg(f) = \deg(g) = 0$. For a given polynomial $f \in \mathbb{F}_q[T]$ the set of associates of f is given by $\{af : a \in \mathbb{F}_q^*\}$. Let a_n be the leading coefficient of f. Then $a_n^{-1}f$ is an associate of f which is monic, i.e. it has leading coefficient equal to 1. Thus every polynomial has exactly one associate that is monic. Therefore, just as with positive integers, we only have to study monic polynomials to study the irreducibility of all polynomials.

All of the properties we just mentioned hold for $K[T]$ for any (not necessarily finite) field K. Let us now look at a property that only hold for finite fields. For every number $n > 0$ there are finitely many integers $a \in \mathbb{Z}$ such that $|a| \leq n$. Also for every $a \in \mathbb{Z}$ we have $|\mathbb{Z}/(a)| = |a|$. Similarly for every number $n > 0$ there are only finitely many polynomials $f \in \mathbb{F}_q[T]$ such that $|f| \leq n$, namely the polynomials with degree smaller or equal to $\log_q(n)$. Also, every residue classes in $\mathbb{F}_q[T]/(f)$ correspond with exactly one unique representative g with $\deg(g) < \deg(f)$. Therefore

$$|\mathbb{F}_q[T]/(f)| = |\{g \in \mathbb{F}_q[T] : \deg(g) < \deg(f)\}| = q^{\deg(f)} = |f|$$

exactly as we have with the integers.

3.2 Analogous theorems

Using the common properties from the last section, we can create a dictionary between $\mathbb{Z}$ and $\mathbb{F}_q[T]$, see table 1. Using this dictionary, "much of the elementary [number] theory carries over almost word-for-word" (Pollack, [8]). For instance, let's take a look at the following proof of Fermat's little theorem.

integer $a \in \mathbb{Z}$	polynomial $f \in \mathbb{F}_q[T]$
units $-1, 1$	units $\mathbb{F}_q^*$
prime	irreducible
positive	monic
$|a|$, absolute value	$|f| = q^{\deg(f)}$

Table 1: Dictionary between $\mathbb{Z}$ and $\mathbb{F}_q[T]$.

Theorem 3.2. *Let $p \in \mathbb{Z}$ be a prime. Then for every integer $a \in \mathbb{Z}$, we have*

$$a^p \equiv a \mod p. \tag{7}$$

Proof. If $p|a$ then the theorem holds. Note that $p = |\mathbb{Z}/p\mathbb{Z}|$. As p is prime, $\mathbb{Z}/p\mathbb{Z}$ is a field. Then $|(\mathbb{Z}/p\mathbb{Z})^*| = p - 1$. Then for every $a \in \mathbb{Z}_q[T]$ with $p \not| a$, we have $a^{p-1} \equiv 1 \mod p$, and therefore $a^p \equiv a \mod p$. □

With some minor adjustments, this proof can be transformed into a proof for its analogous counterpart in $\mathbb{F}_q[T]$:

Theorem 3.3. *Let q be the power of a prime, and let $P \in \mathbb{F}_q$ be an irreducible polynomial. Then for every polynomial $f \in \mathbb{F}_q[T]$, we have*

$$f^{|P|} \equiv f \mod P. \tag{8}$$

Proof. If $P|f$ then the theorem holds. Note that $|P| = |\mathbb{F}_q[T]/(P)|$. As P is irreducible and $\mathbb{F}_q[T]$ is a principal ideal domain, the ideal (P) is maximal [4, Prop. 8.7]. Therefore, $\mathbb{F}_q[T]/(P)$ is a field [4, Prop. 7.12]. Then $|(\mathbb{F}_q[T]/(P))^*| = |P| - 1$. Then for every $f \in \mathbb{F}_q[T]$, such that $P \not| f$, we have $f^{|P|-1} \equiv 1 \mod P$, and therefore $f^{|P|} \equiv f \mod P$. □

A more interesting example is Fermat's last theorem, which has the following analogue in $\mathbb{F}_q[T]$ [8]:

Theorem 3.4. *Let q be the power of prime p. If $n \geq 3$ and $p \not| n$, then there exists no coprime solution to*

$$X^n + Y^n = Z^n, \tag{9}$$

with $X, Y, Z \in \mathbb{F}_q[T]$ such that $XYZ \neq 0$ and X', Y', Z' not all equal to zero.

This version allows a much simpler proof than the original version of Fermat's last theorem, involving Mason's Theorem.

Theorem 3.5. *Let K be a field and A, B, C be coprime nonzero elements of $K[T]$ with $A + B + C = 0$. If $\max(\deg(A), \deg(B), \deg(C)) \geq \deg(\mathrm{rad}(ABC))$, where $\mathrm{rad}(ABC)$ is the square-free part of ABC, then $A' = B' = C' = 0$.*

For a proof of Mason's Theorem, see [10]. We will now prove the analogue of Fermat's last theorem for polynomials over finite fields, following [8].

Proof. Assume there exist coprime X, Y, Z such that $X^n + Y^n = Z^n$ for some $n \geq 1$, such that $p \not| n$. Then $X^n + Y^n - Z^n = 0$ and $(X^n)', (Y^n)', (Z^n)'$ not all zero. Then Mason's Theorem implies

$$\begin{aligned} n \max(\deg(X), \deg(Y), \deg(Z)) &< \deg(\mathrm{rad}((XYZ)^n)) \\ &= \deg(\mathrm{rad}(XYZ)) \\ &\leq \deg(XYZ) \\ &\leq 3 \max(\deg(X), \deg(Y), \deg(Z)) \end{aligned}$$

which implies that $n < 3$. □

4 Counting irreducible polynomials

4.1 Number of monic irreducible polynomials of degree n

In this section we will look at the number of monic irreducible polynomials of degree n. Let $\pi(q; n)$ denote the number of monic irreducible polynomials of degree n over $\mathbb{F}_q[T]$, i.e.

$$\pi(q; n) = \#\{f \in \mathbb{F}_q[T] : f \text{ monic, irreducible and } \deg(f) = n\}.$$

There exists a direct formula for calculating $\pi(q;n)$, discovered by Gauss, which goes as follows:

Theorem 4.1 (Formula of Gauss)**.** *Let $q = p^k$ be a power of a prime p. Then the number of monic irreducible polynomials of degree n over $\mathbb{F}_q$ is given by*

$$\pi(q;n) = \frac{1}{n}\sum_{d|n} q^d \mu\left(\frac{n}{d}\right), \tag{10}$$

where μ is the Möbius function.

We will give two proofs:

Proof 1. Let $q = p^k$ be the power of a prime p and let $n \geq 1$. We claim: For every $a \in \mathbb{F}_{q^n}$ there is exactly one irreducible monic polynomial $f \in \mathbb{F}_q[T]$ such that a is a zero of f and $\deg(f)$ divides n. Conversely, every monic irreducible polynomial $f \in \mathbb{F}_q[T]$ with degree dividing n has all of its zeros in $\mathbb{F}_{q^n}$ and is separable.

We prove the claim. Let $a \in \mathbb{F}_{q^n}$. Because $\mathbb{F}_{q^n}$ is an finite extension of $\mathbb{F}_q$, a is algebraic over $\mathbb{F}_q$. Let $f \in \mathbb{F}_q[T]$ be the minimal polynomial of a. Then f is monic and irreducible, and is the only monic irreducible polynomial with a as a zero. Furthermore $\mathbb{F}_q(a)$ is an intermediate field between $\mathbb{F}_{q^n}$ and $\mathbb{F}_q$ and thus $\deg(f) = [\mathbb{F}_q(a) : \mathbb{F}_q]$ divides $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$.

Conversely let $f \in \mathbb{F}_q[T]$ be a monic irreducible polynomial with degree dividing n. Then we have $|\mathbb{F}_q[T]/(f)| = \deg(f)$, and because finite fields are unique up to isomorphism, this implies $\mathbb{F}_q[T]/(f) \cong \mathbb{F}_{q^{\deg(f)}}$. Note that T is a zero of f in $\mathbb{F}_q[T]/(f)$. Then f has a zero in $\mathbb{F}_{q^{\deg(f)}}$. By Theorem 2.2, the extension $\mathbb{F}_{q^{\deg(f)}}/\mathbb{F}_q$ is Galois, and is therefore a normal and separable extension, so f is separable and has all of its zeros in $\mathbb{F}_{q^{\deg(f)}}$. But $\deg(f)$ divides n and thus (by Theorem 2.2) $\mathbb{F}_{q^{\deg(f)}}$ is a subfield of $\mathbb{F}_{q^n}$. This proves the claim.

Let $M(q,n) = \{f \in \mathbb{F}_q[T] : f \text{ monic and irreducible and } \deg(f)|n\}$. It follows from the claim that

$$\prod_{f \in M(q,n)} f = \prod_{a \in \mathbb{F}_{q^n}} (T - a).$$

Taking the degree on both sides gives us

$$\sum_{f \in M(q,n)} \deg(f) = q^n.$$

The left side is equal to $\sum_{d|n} d\pi(q;d)$, thus we obtain

$$\sum_{d|n} d\pi(q;d) = q^n.$$

We then Möbius inversion to find:

$$n\pi(q;n) = \sum_{d|n} q^d \mu\left(\frac{n}{d}\right).$$

Dividing both sides by n gives us the desired formula. □

The second proof of this formula uses the inclusion-exclusion principle. We will follow [3].

Proof 2. Let $\mathcal{R}_n$ denote the set of zeros of monic irreducible polynomials of degree n. Because every monic irreducible is separable and has simple zeros, $|\mathcal{R}_n| = n\pi(q;n)$. Now notice that $\mathcal{R}_n$ is exactly the subset of elements $\mathbb{F}_{q^n}$ that don't belong to a proper subfield of $\mathbb{F}_{q^n}$, and therefore don't belong to a proper maximal subfield of $\mathbb{F}_{q^n}$. The proper maximal subfields of $\mathbb{F}_{q^n}$ are exactly the subfields $\mathbb{F}_{q^{\frac{n}{u}}}$, with u a prime divisor of n. Let $n = u_1^{k_1} \cdots u_r^{k_r}$ be the prime factorization of n. Note that $\mathbb{F}_{q^{\frac{n}{u_i}}} \cap \mathbb{F}_{q^{\frac{n}{u_j}}} = \mathbb{F}_{q^{\frac{n}{u_i u_j}}}$. Then by the inclusion-exclusion principle

$$\begin{aligned}
n\pi(q;n) = |\mathcal{R}_n| &= \left|\mathbb{F}_{q^n} \setminus (\mathbb{F}_{q^{\frac{n}{u_1}}} \cup \cdots \cup \mathbb{F}_{q^{\frac{n}{u_1}}})\right| \\
&= |\mathbb{F}_{q^n}| - \left|\bigcup_{i=1}^{r} \mathbb{F}_{q^{\frac{n}{u_i}}}\right| \\
&= |\mathbb{F}_{q^n}| - \sum_{1\le i\le r} \left|\mathbb{F}_{q^{\frac{n}{u_i}}}\right| + \sum_{1\le i<j\le r} \left|\mathbb{F}_{q^{\frac{n}{u_i u_j}}}\right| \\
&\quad - \cdots + (-1)^r \left|\mathbb{F}_{q^{\frac{n}{u_1 \cdots u_r}}}\right| \\
&= \sum_{d|n} \mu(d) |\mathbb{F}_{q^{\frac{n}{d}}}| = \sum_{d|n} \mu(d) q^{\frac{n}{d}}.
\end{aligned}$$

And now we divide by n. □

Next we formulate some bounds on $\pi(q;n)$.

Theorem 4.2. *Let $q = p^k$ be a power of a prime p. Then the number of monic irreducible polynomials of degree n over $\mathbb{F}_q$ is bounded by*

$$\frac{q^n}{n} - 2\frac{q^{n/2}}{n} < \pi(q;n) \le \frac{q^n}{n}, \tag{11}$$

and moreover the last inequality is strict for $n > 1$.

Proof. For $n = 1$, we have the equality $\pi(q;n) = q$ and thus the theorem holds. If $n > 1$, we get:

$$\frac{q^n}{n} - \pi(q;n) = \frac{q^n}{n} - \frac{1}{n}\sum_{d|n} q^d \mu\left(\frac{n}{d}\right) = -\frac{1}{n}\sum_{d|n, d\neq n} q^d \mu\left(\frac{n}{d}\right). \tag{12}$$

Let p' be the smallest prime divisor of n. Then the right side of (12) is equal to

$$\frac{1}{n}\left(q^{\frac{n}{p'}} - \sum_{d|n, d<\frac{n}{p'}} q^d \mu\left(\frac{n}{d}\right)\right). \tag{13}$$

Now on the one hand we have

$$q^{\frac{n}{p'}} - \sum_{d|n, d<\frac{n}{p'}} q^d \mu\left(\frac{n}{d}\right) \ge q^{\frac{n}{p'}} - \sum_{1\le d<\frac{n}{p'}} q^d \ge q^{\frac{n}{p'}} - \frac{q^{\frac{n}{p'}} - q}{q-1} \tag{14}$$

and because $q \geq 2$ the last part is greater or equal to $q^{\frac{n}{p'}} - q^{\frac{n}{p'}} + q = q > 0$ and thus $\pi(q;n) < \frac{q^n}{n}$.

On the other hand we have

$$q^{\frac{n}{p'}} - \sum_{d|n, d<\frac{n}{p'}} q^d \mu\left(\frac{n}{d}\right) \leq q^{\frac{n}{p'}} + \sum_{1 \leq d < \frac{n}{p'}} q^d \leq q^{\frac{n}{p'}} + \frac{q^{\frac{n}{p'}} - q}{q-1} \tag{15}$$

and because $q \geq 2$ this is smaller than $2q^{\frac{n}{2}}$, therefore $\pi(q;n) > \frac{q^n}{n} - 2\frac{q^{\frac{n}{2}}}{n}$. □

As a final result we will show that $\pi(q;n)$ and $\frac{q^n}{n}$ are asymptotically equivalent.

Theorem 4.3. *For any $q = p^k$ with p prime and $n \geq 1$ we have*

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

and therefore, as $n \to \infty$,

$$\pi_q(n) \sim \frac{q^n}{n}.$$

Proof. From Theorem 4.2 it follows directly that $\pi_q(n) = \frac{q^n}{n} + \mathcal{O}\left(\frac{q^{n/2}}{n}\right)$. Furthermore, note that $\frac{q^{n/2}}{q^n} = q^{-n/2} \to 0$ for $n \to \infty$. Thus we get

$$\lim_{n\to\infty} \frac{\pi_q(n)}{\frac{q^n}{n}} = 1$$

and therefore by definition $\pi_q(n) \sim \frac{q^n}{n}$ as $n \to \infty$. □

The last two theorem state that the density of irreducible polynomials of degree n is approximately $\frac{1}{n}$. This is very similar to the statement that the density of primes around x is approximately $\frac{1}{\log(x)}$. Furthermore, one could say that this is sort of an analogue of the prime number theorem. If we write $X = q^n$ then we have $\pi(q;n) \sim \frac{X}{\log_q(X)}$. However, the counting functions are very different, which we would like to remedy in the next section by counting up to a certain degree.

4.2 Counting multiple degrees

Let $\pi_q(n)$ denote the number of monic irreducible polynomials over $\mathbb{F}_q$ with degree $\leq n$, thus

$$\pi_q(n) = \sum_{k \leq n} \pi(q;k).$$

As the density of irreducible polynomials around f is approximately $1/\deg(f)$, we would expect that $\pi_q(n)$ is approximately equal to

$$\mathrm{ls}_q(n) := \sum_{\substack{f \text{ monic} \\ 1 \leq \deg(f) \leq n}} \frac{1}{\deg(f)},$$

which is an analogue of the logarithmic sum used in the prime number theorem. Using that the number of monic polynomials of degree k is equal to q^k, we can split this sum up by degrees to get:

$$\mathrm{ls}_q(n) = \sum_{k \leq n} \frac{q^k}{k}.$$

In the last section we saw that the number of monic irreducible polynomials of degree k equals $\pi(q;k) = \frac{q^k}{k} + \mathcal{O}(\frac{q^{\frac{k}{2}}}{k})$. Simply summing over these terms and collecting all the $\mathcal{O}$-terms into the term $\mathcal{O}(q^{\frac{n}{2}})$ gives us

$$\pi_q(n) = \mathrm{ls}_q(n) + \mathcal{O}(q^{\frac{n}{2}}). \tag{16}$$

We can however prove this with a better error term. To do this, we first take a closer look at the partial sums $\sum_{k \leq n} \frac{q^k}{k}$.

At first glance there isn't a simple direct formula for the partial sum $\sum_{k \leq n} \frac{q^k}{k}$. Expanding it gives us

$$\sum_{k \leq n} \frac{q^k}{k} = q + \frac{q^2}{2} + \frac{q^3}{3} + \cdots + \frac{q^{n-2}}{n-2} + \frac{q^{n-1}}{n-1} + \frac{q^n}{n} \tag{17}$$

As $q \geq 2$, for large n the sum is dominated by the largest terms. If we look at the $(j+1)$-th largest term with $j \ll n$, then its denominator $n - j$ is approximately n. In other words, if k very close to n, then the k-th term $\frac{q^k}{k}$ is approximately equal to $\frac{q^k}{n}$. Therefore, we would expect that the partial sum $\sum_{k \leq n} \frac{q^k}{k}$ would behave similarly to $\sum_{k \leq n} \frac{q^k}{n}$. This will be useful as the latter is the partial sum of a geometric series which has a direct formula:

$$\sum_{k \leq n} \frac{q^k}{n} = \frac{q}{q-1} \cdot \frac{q^n - 1}{n}. \tag{18}$$

Let us denote $F_q(n) := \sum_{k \leq n} \frac{q^k}{k}$ and $G_q(n) := \sum_{k \leq n} \frac{q^k}{n} = \frac{q}{q-1} \frac{q^n-1}{n}$. In figure 1 one can find a plot of the fraction $H_q(n) = \frac{F_q(n)}{G_q(n)}$ for a couple of values of q. The first thing we notice is that $H_q(n)$ seems to be bounded below by 1 for every q. The bound above however, is dependent on q. It turns out that $H_q(n)$ is bounded above by $\frac{q+1}{q}$. The fraction also seems to converge to 1 for every q, which would imply $F_q(n) \sim G_q(n)$ for $n \to \infty$.

Now let us prove these observations (for the second part we use [2, Lemma 9.3], case $a_l = 1$ for all l):

Theorem 4.4. *Let $q \geq 2$, $F_q(n) := \sum_{k \leq n} \frac{q^k}{k}$ and $G_q(n) := \sum_{k \leq n} \frac{q^k}{n}$. Then the following holds:*

i. For all $n \geq 1$ we have

$$G_q(n) \leq F_q(n) < \frac{q+1}{q} G_q(n) \tag{19}$$

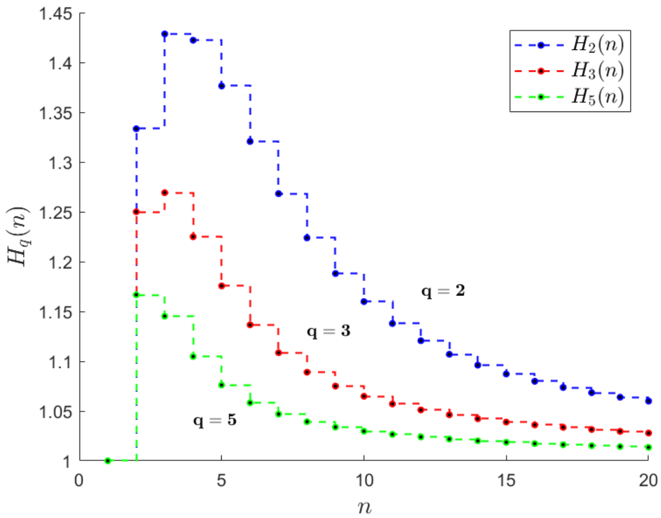

Figure 1: The fraction $H_q(n) = \frac{F_q(n)}{G_q(n)}$, where $F_q(n) = \sum_{k \leq n} \frac{q^k}{k}$ and $G_q(n) = \frac{q}{q-1} \frac{q^n - 1}{n}$, for $q = 2, 3, 5$.

ii. For $n \to \infty$ we have $F_q(n) \sim G_q(n)$.

Proof. i. If $k \leq n$ then $\frac{q^k}{n} \leq \frac{q^k}{k}$. This implies $G_q(n) = \sum_{k \leq n} \frac{q^k}{n} \leq \sum_{k \leq n} \frac{q^k}{k} = F_q(n)$. Now notice:

$$2G_q(n) - F_q(n) = 2 \sum_{k \leq n} \frac{q^k}{n} - \sum_{k \leq n} \frac{q^k}{k} = \sum_{k \leq n} \frac{2k - n}{kn} q^k.$$

If n is even then the term for $k = \frac{n}{2}$ equals zero, so we can split the sum up in terms $k < \frac{n}{2}$, $\frac{n}{2} < k < n$ and $k = n$. We get

$$\begin{aligned}
\sum_{k \leq n} \frac{2k - n}{kn} q^k &= \sum_{k < \frac{n}{2}} \frac{2k - n}{kn} q^k + \sum_{\frac{n}{2} < k < n} \frac{2k - n}{kn} q^k + \frac{q^n}{n} \\
&= \sum_{k < \frac{n}{2}} \frac{2k - n}{kn} q^k + \sum_{k < \frac{n}{2}} \frac{2(n-k) - n}{(n-k)n} q^{n-k} + \frac{q^n}{n} \\
&= \frac{q^n}{n} + \sum_{k < \frac{n}{2}} \frac{(n-k)(2k-n)q^k + k(n-2k)q^{n-k}}{kn(n-k)} \\
&= \frac{q^n}{n} + \sum_{k < \frac{n}{2}} \frac{(n-2k)q^k}{kn(n-k)} (kq^{n-2k} - n + k)
\end{aligned}$$

But as $q \geq 2$ we have $q^x \geq 2x$ for all $x \in \mathbb{R}$. Thus $kq^{n-2k} - n + k \geq 2k(n-2k) - n + k = n(2k-1) - 4k^2 + k \geq (2k+1)(2k-1) - 4k^2 + k = 4k^2 - 1 - 4k^2 + k = k - 1 \geq 0$, and now we use that $2k - 1 > 0$ and $n \geq 2k + 1$

and therefore all the terms in the last sum are non-negative. Thus

$$2G_q(n) - F_q(n \geq \frac{q^n}{n} > \frac{q^n - 1}{n} = \frac{q-1}{q} \sum_{k \leq n} \frac{q^k}{n} = \frac{q-1}{q} G_q(n)$$

and therefore

$$F_q(n) < (2 - \frac{q-1}{q}) G_q(n) = \frac{q+1}{q} G_q(n).$$

This proves i.

ii. In order to prove $F_q(n) \sim G_q(n)$ for $n \to \infty$, it suffices to prove that

$$\lim_{n \to \infty} \left| \frac{F_q(n) - G_q(n)}{G_q(n)} \right| = 0. \tag{20}$$

Notice that $G_q(n) = \sum_{k \leq n} \frac{q^k}{n} \geq \frac{q^n}{n}$ and thus

$$\left| \frac{F_q(n) - G_q(n)}{G_q(n)} \right| \leq \left| \frac{F_q(n) - G_q(n)}{\frac{q^n}{n}} \right| = \sum_{k \leq n} \frac{n-k}{k} q^{k-n}.$$

We split this last sum into terms $k < \frac{n}{2}$ and terms $\frac{n}{2} \leq k < n$ (the n-th term is 0). For the first part we get:

$$\sum_{k < \frac{n}{2}} \frac{n-k}{k} q^{k-n} \leq \sum_{k < \frac{n}{2}} n q^{k-n} \leq n \frac{q^{-\frac{n}{2}} - q^{1-n}}{q-1} \leq n q^{-\frac{n}{2}}.$$

For terms $\frac{n}{2} \leq k \leq n$ it holds that

$$\begin{aligned}\sum_{\frac{n}{2} \leq k < n} \frac{n-k}{k} q^{k-n} &\leq \sum_{\frac{n}{2} \leq k < n} \frac{n-k}{\frac{n}{2}} q^{k-n} = \frac{2}{n} \sum_{\frac{n}{2} \leq k < n} (n-k) q^{k-n} \\ &= \frac{2}{n} \sum_{m \leq \frac{n}{2}} m q^{-m} \leq \frac{2}{n} \sum_{m=1}^{\infty} m q^{-m}\end{aligned}$$

Now note that for $|x| < 1$,

$$\sum_{m=1}^{\infty} m x^m = x \frac{d}{dx} \sum_{m=0}^{\infty} x^m = x \frac{d}{dx} \frac{1}{1-x} = \frac{x}{(1-x)^2},$$

and therefore

$$\frac{2}{n} \sum_{m=1}^{\infty} m q^{-m} = \frac{2q^{-1}}{n(1-q^{-1})^2} = \frac{2q}{n(q-1)^2}.$$

We conclude that

$$\left| \frac{F_q(n) - G_q(n)}{G_q(n)} \right| \leq n q^{-\frac{n}{2}} + \frac{2q}{n(q-1)^2} \to 0 \qquad (n \to \infty),$$

thus indeed $F_q(n) \sim G_q(n)$.

□

Using this we can prove the main theorem of this section.

Theorem 4.5. *Let q be the power of a prime and $n \geq 1$. Then the number of monic irreducible polynomials over $\mathbb{F}_q$ with degree $\leq n$ is equal to*

$$\pi_q(n) = \mathrm{ls}_q(n) + \mathcal{O}\left(\frac{q^{\frac{n}{2}}}{n}\right). \tag{21}$$

Furthermore, for $n \to \infty$, we have

$$\pi_q(n) \sim \mathrm{ls}_q(n) \quad \textit{and} \quad \pi_q(n) \sim \frac{q}{q-1} \cdot \frac{q^n - 1}{n}.$$

Proof. We use the formula of Gauss to get

$$\pi_q(n) = \sum_{k \leq n} \pi(q;k) = \sum_{k \leq n} \sum_{d|k} \frac{q^d}{k} \mu\left(\frac{k}{d}\right) = \sum_{dm \leq n} \frac{q^d}{dm} \mu(m) = \sum_{d \leq n} \frac{q^d}{d} \sum_{m \leq \frac{n}{d}} \frac{\mu(m)}{m}$$

Therefore it follows

$$|\pi_q(n) - \mathrm{ls}(n)| = (\left|\pi_q(n) - \sum_{k \leq n} \frac{q^k}{k}\right| \leq \sum_{k \leq n} \frac{q^k}{k} \left|1 - \sum_{m \leq \frac{n}{k}} \frac{\mu(m)}{m}\right|.$$

We split the sum into terms $k \leq \frac{n}{2}$ and terms $\frac{n}{2} < k \leq n$. Note that for $\frac{n}{2} < k \leq n$ we have $\frac{n}{k} < 2$ and therefore

$$\sum_{\frac{n}{2} < k \leq n} \frac{q^k}{k} \left|1 - \sum_{m \leq \frac{n}{k}} \frac{\mu(m)}{m}\right| = \sum_{\frac{n}{2} < k \leq n} \frac{q^k}{k} \left|1 - \frac{\mu(1)}{1}\right| = 0.$$

Therefore the only terms that remain are $k \leq \frac{n}{2}$ and we get:

$$\sum_{k \leq \frac{n}{2}} \frac{q^k}{k} \left|1 - \sum_{m \leq \frac{n}{k}} \frac{\mu(m)}{m}\right| \leq \sum_{k \leq \frac{n}{2}} \frac{q^k}{k} \left(1 + \left|\sum_{m \leq \frac{n}{k}} \frac{\mu(m)}{m}\right|\right)$$

We apply Theorem 2.5 and Theorem 4.4 (part i.) and find

$$\begin{aligned}
\sum_{k \leq \frac{n}{2}} \frac{q^k}{k} \left(1 + \left|\sum_{m \leq \frac{n}{k}} \frac{\mu(m)}{m}\right|\right) &\leq \sum_{k \leq \frac{n}{2}} \frac{q^k}{k} (1+1) = 2 \sum_{k \leq \frac{n}{2}} \frac{q^k}{k} \\
&\leq \frac{2(q+1)}{q} \sum_{k \leq \frac{n}{2}} \frac{q^k}{\frac{n}{2}} \\
&\leq \frac{4(q+1)}{q-1} \frac{q^{\frac{n}{2}} - 1}{n} \\
&= \mathcal{O}\left(\frac{q^{\frac{n}{2}}}{n}\right),
\end{aligned}$$

Therefore, as $\mathrm{ls}_q(n) = \sum_{k \leq n} \frac{q^k}{k}$, we obtain $\pi_q(n) = \mathrm{ls}_q(n) + \mathcal{O}\left(\frac{q^{\frac{n}{2}}}{n}\right)$.

This, combined with $\mathrm{ls}_q(n) = F_q(n) \geq \frac{q^n}{n}$, implies that

$$\lim_{n\to\infty} \frac{\pi_q(n)}{\mathrm{ls}_q(n)} = \lim_{n\to\infty} \frac{\mathrm{ls}_q(n) + \mathcal{O}(\frac{q^{\frac{n}{2}}}{n})}{\mathrm{ls}_q(n)} = 1 + \lim_{n\to\infty} \frac{\mathcal{O}(\frac{q^{\frac{n}{2}}}{n})}{\mathrm{ls}_q(n)} = 1 + \lim_{n\to\infty} \mathcal{O}(q^{-\frac{n}{2}}) = 1,$$

and thus we get $\pi_q(n) \sim \mathrm{ls}_q(n)$. But the relation $\sim$ is transitive, i.e. $f(x) \sim g(x)$ and $g(x) \sim h(x)$ implies $f(x) \sim h(x)$. In Theorem 4.4 we proved $\mathrm{ls}_q(n) = F_q(n) \sim G_q(n)$ and thus we get the asymptotic formula

$$\pi_q(n) \sim \frac{q}{q-1} \frac{q^n - 1}{n}. \tag{22}$$

□

Let's compare this result to the prime number theorem. Recall, the prime number theorem states that the number of primes smaller or equal to a real number x is asymptotic to $\frac{x}{\log(x)}$. If we take x to be a positive integer, we can look at this formula as follows: The number of integers we consider is equal to the numerator x. Then we multiply this by the density of primes around x, which is approximately $\frac{1}{\log(x)}$. In the case of polynomials, we consider all the monic polynomials of degree $\leq n$. The number of monic polynomials of degree k is equal to q^k (as the leading coefficient $a_k = 1$ and we can choose the coefficients $a_{k-1}, \dots, a_0$ freely). Then the number of monic polynomials with degree $\leq n$ is equal to $\sum_{k\leq n} q^k = \frac{q}{q-1}(q^n - 1)$. We then multiply this with the density of irreducible polynomials of degree n, which is approximately $\frac{1}{n}$. Both asymptotic functions can therefore be interpreted as the product of the number of elements considered times the approximate density at the largest element.

We could ask ourselves why we have to multiply with the density at the largest element. If we take the density of monic irreducible polynomials around a monic polynomial f to be $\frac{1}{\deg(f)}$, then the average density $E(n)$, taken over all monic polynomials with degree $\leq n$, is (by Theorem 4.4) asymptotic to

$$E(n) = \frac{\sum_{\substack{f\in\mathcal{M}_q \\ \deg(f)\leq n}} \frac{1}{\deg(f)}}{\sum_{\substack{f\in\mathcal{M}_q \\ \deg(f)\leq n}} 1} = \frac{\sum_{k\leq n} \frac{q^k}{k}}{\sum_{k\leq n} q^k} = \frac{F_q(n)}{nG_q(n)} \sim \frac{1}{n}, \tag{23}$$

as n tends to infinity.

Note that $\frac{q}{q-1}\frac{q^n-1}{n} \sim \frac{q}{q-1}\frac{q^n}{n}$, and therefore we could also consider the asymptotic formula $\pi_q(n) \sim \frac{q}{q-1}\frac{X}{\log_q(X)}$, where $X = q^n$. This looks like an analogue of the prime number theorem, but with a factor $\frac{q}{q-1}$. We could go even further and get rid of this factor if we altered our counting function. Define $\pi_q^1(n)$ to be the number of irreducible polynomials (not necessarily monic) with degree $< n$. Then $\pi_q^1(n) = (q-1)\pi_q(n-1)$, and therefore $\pi_q^1(n) \sim \frac{q^n}{n-1} \sim \frac{q^n}{n} = \frac{X}{\log_q(X)}$, where $X = q^n$.

The error term in (21) can be written as $\mathcal{O}(\frac{q^{\frac{n}{2}}}{n}) = \mathcal{O}(\frac{\sqrt{X}}{\log_q(X)})$, where $X = q^n$. This gives us

$$\pi_q(n) = \mathrm{ls}_q(n) + \mathcal{O}\left(\frac{\sqrt{X}}{\log_q(X)}\right), \tag{24}$$

which seems to be a better approximation than its analogue in the prime number theorem, which states

$$\pi(x) = \mathrm{ls}(x) + \mathcal{O}(\sqrt{x}\log(x)).$$

4.3 Continuity

In case of the prime number theorem, the counting function $\pi(x) = \sum_{p\leq x} 1$ is defined for every real number x, giving us a step-function. We can easily extend the counting function π_q for monic irreducible polynomials to the real numbers by

$$\pi_q(x) = \sum_{\substack{f\in\mathcal{M}_q \\ \deg(f)\leq x}} 1,$$

where $\mathcal{M}_q$ is the set of monic irreducible polynomials in $\mathbb{F}_q[T]$.

In the same manner we can extend

$$\mathrm{ls}(x) = \sum_{\substack{f \text{ monic} \\ 1\leq\deg(f)\leq x}} \frac{1}{\deg(f)} \quad \text{and} \quad F_q(x) = \sum_{k\leq x} \frac{q^k}{k}$$

to the real numbers. Then $\mathrm{ls}_q(x) = F_q(x)$ still holds and Theorem 4.5 can easily generalized to the real case, as

$$|\pi_q(x) - \mathrm{ls}_q(x)| = |\pi_q([x]) - \mathrm{ls}_q([x])| = \mathcal{O}\left(\frac{q^{\frac{[x]}{2}}}{[x]}\right) = \mathcal{O}\left(\frac{q^{\frac{x}{2}}}{x}\right).$$

This then implies $\pi_q(x) \sim \mathrm{ls}_q(x)$ for $x \to \infty$.

More interesting is the question whether or not $\pi_q(x)$ is asymptotic with the continuous extension $G_q(x) = \frac{q}{q-1}\frac{q^x-1}{x}$. If we take a look at figure 2, we can see that this most likely does not hold true. The fraction $\frac{F_2(x)}{G_2(x)}$, when considering a real variable, no longer seems to converge. If this is the case, then $F_q(x)$ is not asymptotic to $G_q(x)$ and by transitivity $\pi_q(x)$ cannot be asymptotic to $G_q(x)$.

Let $0 \leq y < 1$ and consider the sequence $x_n = n + y$ for $n \geq 1$. Then we have:

$$\lim_{n\to\infty} \frac{F_q(x_n)}{G_q(x_n)} = \lim_{n\to\infty} \frac{F_q(n)}{\frac{q}{q-1}\frac{q^{n+y}-1}{n+y}} = \lim_{n\to\infty} \frac{F_q(n)}{\frac{q}{q-1}\frac{q^n-1}{n}} \cdot \lim_{n\to\infty} \frac{(n+y)(q^n-1)}{n(q^{n+y}-1)} = \frac{1}{q^y}.$$

For every value of y the limit converges to a different value, and therefore the limit $\lim_{x\to\infty} \frac{F_q(x)}{G_q(x)}$ does not exist.

Therefore the counting function $\pi_q(x)$ is not asymptotically equivalent with the continuous function $G_q(x) = \frac{q}{q-1}\frac{q^x-1}{x}$. Is there maybe another continuous function f such that π_q is asymptotic with f? As a matter of fact, there is not. To prove this, we need the following theorem.

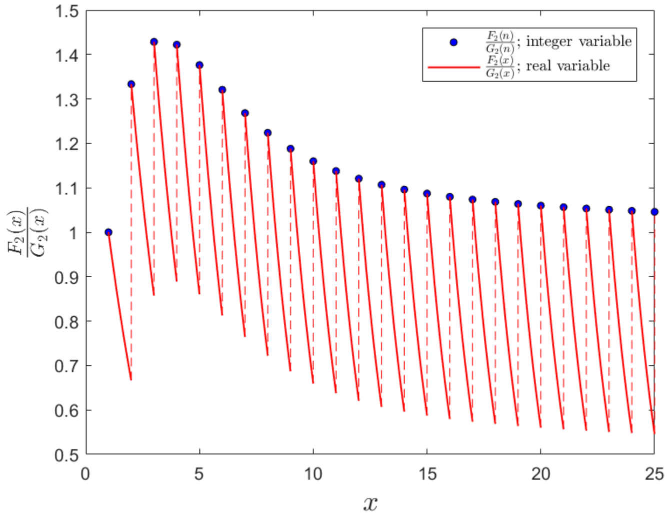

Figure 2: The fraction $\frac{F_2(x)}{G_2(x)}$, where $F_2(x) = \sum_{k \leq x} \frac{2^k}{k}$ and $G_2(x) = 2 \cdot \frac{2^x - 1}{x}$, comparing real variable against discrete integer

Theorem 4.6. *Let $f : \mathbb{R} \to \mathbb{R}$ be a continuous function. Then*

$$\limsup_{x \to \infty} \left| \frac{\pi_q(x) - f(x)}{\frac{q^x}{x}} \right| \geq \frac{1}{2}. \tag{25}$$

Proof. Let $f : \mathbb{R} \to \mathbb{R}$ be a continuous function. Let $e(x) := |\pi_q(x) - f(x)|$. We claim: For every $n \geq 2$ there exist a real number $x_n \in [n-1, n]$ such that $e(x_n) \geq \frac{q^n}{2n} - \frac{q^{\frac{n}{2}}}{n} =: \delta_n$. Let $n \geq 2$. If either $e(n-1)$ or $e(n)$ is greater or equal to δ_n then we're done. So assume both $e(n-1) < \delta_n$ and $e(n) < \delta_n$. Recall, $\pi_q(n) - \pi_q(n-1) = \pi(q; n) > \frac{q^n}{n} - \frac{2q^{\frac{n}{2}}}{n} = 2\delta_n$ (Theorem 4.2). Then we have

$$f(n-1) < \pi_q(n-1) + \delta_n < \pi_q(n) - \delta_n < f(n).$$

By the intermediate value theorem there exists a $x_n \in (n-1, n)$ such that $f(x) = \pi_q(n-1) + \delta_n$. Therefore $e(x_n) = \delta_n$. This proves our claim.

Now consider the fraction

$$A(x) = \left| \frac{\pi_q(x) - f(x)}{\frac{q^x}{x}} \right| = \frac{e(x)}{\frac{q^x}{x}}.$$

Notice, for $x > 0$, $\frac{d}{dx} \frac{q^x}{x} = q^{x-1} > 0$, and therefore for $0 < y \leq x$ we have $\frac{q^y}{y} \leq \frac{q^x}{x}$. Thus

$$A(x_n) = \frac{e(x_n)}{\frac{q^x}{x}} \geq \frac{\frac{q^n}{2n} - \frac{q^{\frac{n}{2}}}{n}}{\frac{q^n}{n}} = \frac{1}{2} - q^{-\frac{n}{2}}.$$

As $\lim_{n\to\infty} q^{-\frac{n}{2}} = 0$, then for every $\epsilon > 0$ there exists a N such that for every $n \geq N$, $q^{-\frac{n}{2}} < \epsilon$ and therefore $A(x_n) \geq \frac{1}{2} - \epsilon$. But there are infinitely many x such that $A(x) \geq \frac{1}{2} - \epsilon$, and thus we we have $\limsup_{x\to\infty} A(x) \geq \frac{1}{2} - \epsilon$. As this is true for every $\epsilon > 0$, it follows that $\limsup_{x\to\infty} A(x) \geq \frac{1}{2}$. □

This Theorem basically states that the error term $|\pi_q(x) - f(x)|$ grows at least as fast as $\frac{q^x}{x}$. In number theory, one often uses the notation $f(x) = \Omega(g(x))$ if $\limsup_{x\to\infty} \frac{f(x)}{g(x)} > 0$. Thus we have $|\pi_q(x) - f(x)| = \Omega(\frac{q^x}{x})$. This poses a problem, because $\pi_q(x)$ itself is $\mathcal{O}(\frac{q^x}{x})$.

Theorem 4.7. *Let q be the power of a prime. There exists no continuous function $f : \mathbb{R} \to \mathbb{R}$ such that $\pi_q(x)$ is asymptotic to f.*

Proof. Let $f : \mathbb{R} \to \mathbb{R}$ be a continuous function such that $\pi_q(x) \sim f$ as $x \to \infty$. Then

$$\lim_{x\to\infty} \frac{|\pi_q(x) - f(x)|}{\pi_q(x)} = 0$$

Note that by Theorem 4.2 and Theorem 4.4, we have

$$\pi_q(x) \leq \sum_{k\leq x} \frac{q^k}{k} \leq \frac{q+1}{q} \sum_{k\leq x} \frac{q^k}{[x]} = \frac{q+1}{q-1} \cdot \frac{q^{[x]}-1}{[x]} \leq \frac{q+1}{q-1} \cdot \frac{q^x}{x}.$$

Therefore

$$\frac{|\pi_q(x) - f(x)|}{\pi_q(x)} \geq \frac{q-1}{q+1} \cdot \frac{|\pi_q(x) - f(x)|}{\frac{q^x}{x}}$$

which implies $\lim_{x\to\infty} \frac{|\pi_q(x)-f(x)|}{\frac{q^x}{x}} = 0$. This is in contradiction with Theorem 4.6, which states $\limsup_{x\to\infty} \frac{|\pi_q(x)-f(x)|}{\frac{q^x}{x}} \geq \frac{1}{2}$. We conclude that there does not exist a continuous f such that for $x \to \infty$, $\pi_q(x) \sim f$. □

4.4 Adjusting the counting function

To get a proper analogue of the prime number theorem that does extend to the real numbers, we borrow a counting function and a couple theorems from Pollack [9]. Consider the following bijection from the positive integers to polynomials over $\mathbb{F}_q$: Given a positive integer N, write N in base q. Let n be the largest integer such that $q^n \leq N$. Then there exist unique $0 \leq a_0, \dots a_n \leq q-1$ such that

$$N = a_n q^n + \cdots + a_1 q + a_0.$$

Then we send N to the polynomial

$$f(T) = a_n T^n + \cdots + a_1 T + a_0.$$

This is clearly a bijection. We now denote $||f|| = N$. For any interval $I \subset \mathbb{R}$ define the counting function $\hat{\pi}_q(I) = \#\{f \in \mathbb{F}_q[T] : f \text{ irreducible and } ||f|| \in I\}$, and $\hat{\pi}_q(X) := \hat{\pi}_q([0, X))$. Instead of counting per degree, we have spread out the polynomials over the positive integers. This solves the problem of having the number of polynomials counted at each step increase exponentially. Note that in order to do this, we can no longer restrict ourselves to monic polynomials only.

If $X = q^n$, then $\hat{\pi}_q(q^n) = (q-1)\pi_q(n-1)$, as the polynomials $f \in \mathbb{F}_q[T]$ for which $||f|| < q^n$ are exactly the polynomials with $\deg(f) < n$. However, if X is not a power of q, we can no longer rely only on the formula of Gauss.

Let l be a non-negative integer. Let $A = T^n + a_{n-1}T^{n-1} + \cdots + a_0$ and $B = T^m + b_{m-1}T^{m-1} + \cdots + b_0$ be monic polynomials. We say A and B have the same first l next-to-leading coefficients if $a_{n-i} = b_{m-i}$ for $i = 1, \ldots, l$. We define a relation $\mathcal{R}_l$ on the monic polynomials in $\mathbb{F}_q[T]$ by:

$$A \equiv B \bmod \mathcal{R}_l \iff A \text{ and } B \text{ have the same first } l \text{ next to leading coefficients}$$

We need the following theorem by Pollack [9, Lemma 2]:

Theorem 4.8. *Let l be a non-negative integer. The number of monic irreducibles of degree n belonging to a prescribed residue class $\mathcal{R}_l$ is*

$$\frac{q^{n-l}}{n} + \mathcal{O}\left((l+1)\frac{q^{\frac{n}{2}}}{n}\right) \tag{26}$$

We will use this theorem without providing a proof, as the theory required to do so falls outside the scope of this thesis. It is interesting to note that the theorem is grounded in Weil's Riemann Hypothesis for function fields (see [7]) and, as we shall see, this will give us an error term that is equivalent to the error term we get in the prime number theorem when we assume the Riemann Hypothesis to be true.

If we take a closer look at this Theorem, we see that it states that the density of irreducible polynomials of degree n belonging to a prescribed residue class modulo $\mathcal{R}_l$ is approximately $\frac{1}{n}$, as there are exactly q^{n-l} polynomials of degree n that belong to a prescribed residue class modulo $\mathcal{R}_l$. We would therefore expect that the irreducible polynomials of degree n are somewhat evenly distributed. This leads us to the approximation for $\hat{\pi}_q(X)$:

$$\begin{aligned}\sum_{\substack{||f||<X \\ \deg(f)>0}} \frac{1}{\deg(f)} &= \sum_{\substack{||f||<q^n \\ \deg(f)>0}} \frac{1}{\deg(f)} + \sum_{\substack{q^n \le ||f||<X \\ \deg(f)>0}} \frac{1}{\deg(f)} \\ &= (q-1)\sum_{k\le n-1} \frac{q^k}{k} + \frac{[X]-q^n}{n}.\end{aligned}$$

Right now this is still a step-function, but we can easily change it to a continuous piece-wise linear function by simply replacing the term $[X]$ by X. We will do this and define the function

$$\hat{\operatorname{ls}}_q(X) := (q-1)\sum_{k\le n-1} \frac{q^k}{k} + \frac{X-q^n}{n}$$

We will prove the following Theorem by Pollack [9, Thm. 1]:

Theorem 4.9. *Let q be the power of prime and let $X \ge q$. Let n be the integer such that $q^n \le X < q^{n+1}$. Then*

$$\hat{\pi}_q(X) = \hat{\operatorname{ls}}_q(X) + \mathcal{O}(nq^{\frac{n}{2}}) \tag{27}$$

Proof. We follow Pollack with some small adjustments. Write $[X]$ in base q, i.e. $[X] = a_n q^n + \cdots + a_1 q + a_0$. Notice that

$$\hat{\pi}_q(X) = \hat{\pi}_q([0, q^n)) + \hat{\pi}_q([q^n, a_n q^n)) + \hat{\pi}_q([a_n q^n, X)).$$

The first part $\hat{\pi}_q([0, q^n))$ is just the number of irreducible polynomials of degree $\leq n-1$, and by theorem 4.5, is therefore equal to

$$\hat{\pi}_q([0, q^n)) = (q-1) \sum_{k \leq n-1} \frac{q^k}{k} + \mathcal{O}\left(\frac{q^{\frac{n-1}{2}}}{n-1}\right).$$

The second part $\hat{\pi}_q([q^n, a_n q^n)) = \sum_{k=1}^{a_n - 1} \hat{\pi}_q([kq^n, (k+1)q^n))$. Each of the terms $\hat{\pi}_q([kq^n, (k+1)q^n))$ is equal the number of irreducibles of degree n with leading coefficient k, which in turn is equal to the number of monic irreducibles of degree n. Therefore, by Theorem 4.3

$$\hat{\pi}_q([q^n, a_n q^n)) = (a_n - 1)\frac{q^n}{n} + \mathcal{O}\left(\frac{q^{\frac{n}{2}}}{n}\right).$$

Lastly for the third part we have $\hat{\pi}_q([a_n q^n, X)) = \hat{\pi}_q([a_n q^n, \sum_{i=0}^{n} a_i q^i))$. We split this up by adding a single coefficient each time, i.e.

$$\hat{\pi}_q([a_n q^n, \sum_{i=0}^{n} a_i q^i)) = \sum_{j=1}^{n} \hat{\pi}_q([\sum_{i=j}^{n} a_i q^i, \sum_{i=j-1}^{n} a_i q^i)).$$

Each of the terms $\hat{\pi}_q([\sum_{i=j}^{n} a_i q^i, \sum_{i=j-1}^{n} a_i q^i))$ in turn can be written as a summation over different values of the coefficient of the $j-1$-th term, giving us

$$\sum_{j=1}^{n} \sum_{k=0}^{a_{j-1}-1} \hat{\pi}_q([\sum_{i=j}^{n} a_i q^i + kq^{j-1}, \sum_{i=j}^{n} a_i q^i + (k+1)q^{j-1}))$$

A term $\hat{\pi}_q([\sum_{i=j}^{n} a_i q^i + kq^{j-1}, \sum_{i=j}^{n} a_i q^i + (k+1)q^{j-1}))$ is equal to the number of irreducible polynomials of degree n for which the leading coefficient and the $n-j+1$ next to leading coefficients are fixed. But this is exactly equal to the number of monic irreducibles belonging to a prescribed residue class modulo $\mathcal{R}_{n-j+1}$ and therefore by Theorem 4.8 we get

$$\begin{aligned}
\hat{\pi}_q([a_n q^n, X)) &= \sum_{j=1}^{n} \sum_{k=0}^{a_{j-1}-1} \left(\frac{q^{j-1}}{n} + \mathcal{O}\left((n-j+2)\frac{q^{\frac{n}{2}}}{n}\right)\right) \\
&= \sum_{j=1}^{n} \left(\frac{a_{j-1} q^{j-1}}{n} + \mathcal{O}\left((n-j+2)\frac{q^{\frac{n}{2}}}{n}\right)\right) \\
&= \frac{[X] - a_n q^n}{n} + \sum_{j=1}^{n} \mathcal{O}\left((n-j+2)\frac{q^{\frac{n}{2}}}{n}\right) \\
&= \frac{X - a_n q^n}{n} + \mathcal{O}\left(\frac{1}{n}\right) + \sum_{j=1}^{n} \mathcal{O}\left((n-j+2)\frac{q^{\frac{n}{2}}}{n}\right).
\end{aligned}$$

Combining these results and collecting all the $\mathcal{O}$-terms into $\mathcal{O}(nq^{\frac{n}{2}})$ gives us

$$\begin{aligned}\hat{\pi}_q(X) &= (q-1)\sum_{k\leq n-1}\frac{q^k}{k} + \frac{(a_n-1)q^n}{n} + \frac{X-a_nq^n}{n} + \mathcal{O}(nq^{\frac{n}{2}})\\ &= (q-1)\sum_{k\leq n-1}\frac{q^k}{k} + \frac{X-q^n}{n} + \mathcal{O}(nq^{\frac{n}{2}}),\end{aligned}$$

which completes the proof. □

Unlike with our previous counting function, this analogue does have the same error term as the logarithmic sum in the prime number theorem when we assume the Riemann Hypothesis to be true. As $q^n \leq X$, we have $nq^{\frac{n}{2}} \leq \sqrt{X}\log_q(x)$. We can thus rewrite the $\mathcal{O}$-term to obtain

$$\hat{\pi}_q(X) = \hat{\mathrm{ls}}_q(X) + \mathcal{O}(\sqrt{X}\log_q(X)). \tag{28}$$

This is indeed an analogue to

$$\pi(x) = \mathrm{ls}(x) + \mathcal{O}(\sqrt{x}\log(x)).$$

We now show that $\hat{\pi}_q(X)$ and $\hat{\mathrm{ls}}_q(X)$ are asymptotically equivalent.

Theorem 4.10. *Let q be the power of a prime. Then, for $X \to \infty$, along all real numbers, we have*

$$\hat{\pi}_q(X) \sim \hat{\mathrm{ls}}_q(X). \tag{29}$$

Proof. For each X, let $n = [\log_q(X)]$. Then $q^n \leq X < q^{n+1}$. We first prove:

$$\lim_{X\to\infty}\frac{nq^{\frac{n}{2}}}{\hat{\mathrm{ls}}_q(X)} = 0$$

Note that

$$\hat{\mathrm{ls}}_q(X) \geq (q-1)\sum_{k\leq n-1}\frac{q^k}{k} \geq \frac{q^{n-1}}{n-1}.$$

Thus

$$0 \leq \lim_{X\to\infty}\frac{nq^{\frac{n}{2}}}{\hat{\mathrm{ls}}_q(X)} \leq \lim_{X\to\infty}\frac{n(n-1)\cdot q}{q^{\frac{n}{2}}} = 0,$$

which proves our claim. This then implies

$$\lim_{X\to\infty}\frac{\hat{\pi}_q(X)}{\hat{\mathrm{ls}}_q(X)} = \lim_{X\to\infty}\frac{\hat{\mathrm{ls}}_q(X) + \mathcal{O}(nq^{\frac{n}{2}})}{\hat{\mathrm{ls}}_q(X)} = 1,$$

and therefore $\hat{\pi}_q(X) \sim \hat{\mathrm{ls}}_q(X)$. □

This allows us to finally prove an analogue of the prime number theorem, in its familiar form, which does allow a real variable.

Theorem 4.11. *Let q be the power of a prime. Then*

$$\hat{\pi}_q(X) \sim \frac{X}{\log_q(X)}, \tag{30}$$

as X tends to infinity, along the real numbers.

Proof. As $\hat{\pi}_q(X) \sim \hat{\text{ls}}_q(X)$, it is sufficient to show that $\hat{\text{ls}}_q(X) \sim \frac{X}{\log_q(X)}$. For every X, let $n = [\log_q(X)]$ and $y = \{\log_q(X)\}$. Then $X = q^{n+y}$. Then we obtain:

$$\lim_{X\to\infty} \frac{\hat{\text{ls}}_q(X)}{\frac{X}{\log_q(X)}} = \lim_{X\to\infty} \frac{(q-1)\sum_{k\le n-1}\frac{q^k}{k}}{\frac{q^{n+y}}{n+y}} + \frac{\frac{q^{n+y}-q^n}{n}}{\frac{q^{n+y}}{n+y}}.$$

By Theorem 4.4, for $n \to \infty$, we have $(q-1)\sum_{k\le n-1}\frac{q^k}{k} \sim q\cdot\frac{q^{n-1}-1}{n-1} \sim \frac{q^n}{n}$. Then

$$\lim_{X\to\infty} \frac{(q-1)\sum_{k\le n-1}\frac{q^k}{k}}{\frac{q^{n+y}}{n+y}} = \lim_{X\to\infty} \frac{n+y}{nq^y}\cdot\frac{(q-1)\sum_{k\le n-1}\frac{q^k}{k}}{\frac{q^n}{n}} = \lim_{X\to\infty} q^{-y}.$$

On the other hand we get

$$\lim_{X\to\infty} \frac{\frac{q^{n+y}-q^n}{n}}{\frac{q^{n+y}}{n+y}} = \lim_{X\to\infty} \frac{(n+y)(1-q^{-y})}{n} = \lim_{X\to\infty} 1-q^{-y}.$$

If we combine these results, we obtain

$$\lim_{X\to\infty} \frac{\hat{\text{ls}}_q(X)}{\frac{X}{\log_q(X)}} = \lim_{X\to\infty} q^{-y} + 1 - q^{-y} = 1.$$

□

5 Conclusion

Using finite field theory one can show that density of irreducible polynomials of degree n is approximately $\frac{1}{n}$. This is similar to the statement that the density of primes around x is approximately $\frac{1}{\log(x)}$. However, this does not lead to a full analogue of the Prime Number Theorem. As we do not have any information about how the irreducible polynomials are distributed within a degree, we are limited to counting per degree instead of counting individual polynomials. The amount of polynomials considered per degree increases exponentially and as a result the analogue fails when we try to extend it to a real variable.

In order to improve the analogue, we borrowed a theorem that stated that the density of irreducible polynomials of degree n, belonging to a prescribed residue class $\mathcal{R}_l$, is also approximately $\frac{1}{n}$. This allowed us to consider a counting function $\hat{\pi}_q$ which does count individual polynomials. We showed that

$$\hat{\pi}_q(X) \sim \frac{X}{\log_q(X)},$$

which is an analogue of the prime number theorem that does hold for the real variable X. Another indicator that this approach does indeed give us an good analogue, is that the error term in the equation

$$\hat{\pi}_q(X) = \hat{\mathrm{ls}}_q(X) + \mathcal{O}(\sqrt{X}\log_q(X))$$

is the same error term one has in the prime number theorem if one assumes the Riemann Hypothesis to be true.

References

[1] T. M. Apostol. *Introduction to analytic number theory*. Springer Science & Business Media, 2013.

[2] J. Byszewski et al. "Dynamics on abelian varieties in positive characteristic". In: *ArXiv e-prints* (Feb. 2018). arXiv: 1802.07662 [math.NT].

[3] S. K. Chebolu and J. Mináč. "Counting irreducible polynomials over finite fields using the inclusion-exclusion principle". In: *Mathematics Magazine* 85.5 (2011), pp. 369–371.

[4] D. S. Dummit and R. M. Foote. *Abstract algebra (Vol. 3)*. Hoboken: Wiley, 2004.

[5] G. J. O. Jameson. *The prime number theorem (Vol 53)*. Cambridge University Press, 2003.

[6] T. Judson. *Abstract algebra: theory and applications*. Stephen F. Austin State University, 2014.

[7] J. Milne. "The Riemann Hypothesis over Finite Fields: From Weil to the Present Day". In: *ArXiv e-prints* (Sept. 2015). arXiv: 1509.00797 [math.HO].

[8] P. Pollack. *Analogies between integers and polynomials*. 2013. URL: http://pollack.uga.edu/CIMPA2013/Part1.pdf.

[9] P. Pollack. "Revisiting Gauss's analogue of the prime number theorem for polynomials over a finite field". In: *Finite Fields and Their Applications* 16.4 (2010), pp. 290–299.

[10] N. Snyder. "An alternate proof of Mason's theorem". In: *Elemente der Mathematik* 55.3 (2000), pp. 93–94.

[11] G. Tenenbaum and M. M. France. *The prime numbers and their distribution (Vol. 6)*. American Mathematical Soc., 2000.

[12] Y. Tschinkel. "About the cover: on the distribution of primes—Gauss' tables". In: *Bulletin of the American Mathematical Society* 43.1 (2006), pp. 89–91.