Analytic Number Theory in Function Fields (Lecture 4)

Julio Andrade

j.c.andrade.math@gmail.com
http://julioandrade.weebly.com/

University of Oxford

TCC Graduate Course
University of Oxford, Oxford
01 May 2015 - 11 June 2015

Content

Introduction

- In Lecture 2 we touched upon the subject of average value theorems in $A = \mathbb{F}_q[T]$.

Introduction

- In Lecture 2 we touched upon the subject of average value theorems in $A = \mathbb{F}_q[T]$.
- The technique which we used goes back to Carlitz and it is based on Dirichlet series.

Introduction

- In Lecture 2 we touched upon the subject of average value theorems in $A = \mathbb{F}_q[T]$.
- The technique which we used goes back to Carlitz and it is based on Dirichlet series.
- The zeta function of A is so simple that it was possible to arrive at very precise results for the average values in question.

Introduction

- In Lecture 2 we touched upon the subject of average value theorems in $A = \mathbb{F}_q[T]$.
- The technique which we used goes back to Carlitz and it is based on Dirichlet series.
- The zeta function of A is so simple that it was possible to arrive at very precise results for the average values in question.
- We consider average values of the generalizations of some elementary number-theoretic functions in the case of global function fields.

Introduction

- In Lecture 2 we touched upon the subject of average value theorems in $A = \mathbb{F}_q[T]$.
- The technique which we used goes back to Carlitz and it is based on Dirichlet series.
- The zeta function of A is so simple that it was possible to arrive at very precise results for the average values in question.
- We consider average values of the generalizations of some elementary number-theoretic functions in the case of global function fields.
- For global function fields K the zeta function is more complicated and the mean values also becomes a little more complicated.

Let $K/\mathbb{F}$ be an algebraic function field with field of constants $\mathbb{F}$ with $|\mathbb{F}| = q$. We will work with functions on the semigroup of all effective divisors.

Let $K/\mathbb{F}$ be an algebraic function field with field of constants $\mathbb{F}$ with $|\mathbb{F}| = q$. We will work with functions on the semigroup of all effective divisors.

Let $\mathcal{D}_K$ be the group of divisors of K and $\mathcal{D}_K^+$ be the sub-semigroup of effective divisors. We explicitly include the zero divisor as an element of $\mathcal{D}_K^+$. Let $f : \mathcal{D}_K^+ \to \mathbb{C}$ be a function and define

$$\zeta_f(s) = \sum_{D \in \mathcal{D}_K^+} \frac{f(D)}{ND^s}, \tag{1.1}$$

the Dirichlet series associated to f.

Let $K/\mathbb{F}$ be an algebraic function field with field of constants $\mathbb{F}$ with $|\mathbb{F}| = q$. We will work with functions on the semigroup of all effective divisors.

Let $\mathcal{D}_K$ be the group of divisors of K and $\mathcal{D}_K^+$ be the sub-semigroup of effective divisors. We explicitly include the zero divisor as an element of $\mathcal{D}_K^+$. Let $f : \mathcal{D}_K^+ \to \mathbb{C}$ be a function and define

$$\zeta_f(s) = \sum_{D \in \mathcal{D}_K^+} \frac{f(D)}{ND^s}, \tag{1.1}$$

the Dirichlet series associated to f.

When we use D as a summation variable, it will be assumed that the sum is over D in $\mathcal{D}_K^+$ with, perhaps, some other restrictions.

For $N \geq 0$ an integer, define $F(N) = \sum_{\deg D = N} f(D)$. The equation from previous slide can be rewritten

$$\zeta_f(s) = \sum_{N=0}^{\infty} F(N) q^{-Ns}.$$

For $N \geq 0$ an integer, define $F(N) = \sum_{\deg D = N} f(D)$. The equation from previous slide can be rewritten

$$\zeta_f(s) = \sum_{N=0}^{\infty} F(N) q^{-Ns}.$$

Finally, define $Z_f(u)$ as the function for which $Z_f(q^{-s}) = \zeta_f(s)$. Then

$$Z_f(u) = \sum_{N=0}^{\infty} F(N) u^N. \tag{1.2}$$

For $N \geq 0$ an integer, define $F(N) = \sum_{\deg D = N} f(D)$. The equation from previous slide can be rewritten

$$\zeta_f(s) = \sum_{N=0}^{\infty} F(N) q^{-Ns}.$$

Finally, define $Z_f(u)$ as the function for which $Z_f(q^{-s}) = \zeta_f(s)$. Then

$$Z_f(u) = \sum_{N=0}^{\infty} F(N) u^N. \tag{1.2}$$

In the last lecture we investigated the function $b_N(K)$, the number of effective divisors of K with degree N. We showed that if $N > 2g - 2$ (where g is the genus of K)

$$b_N(K) = h_K \frac{q^{N-g+1} - 1}{q - 1}.$$

For $N \geq 0$ an integer, define $F(N) = \sum_{\deg D = N} f(D)$. The equation from previous slide can be rewritten

$$\zeta_f(s) = \sum_{N=0}^{\infty} F(N) q^{-Ns}.$$

Finally, define $Z_f(u)$ as the function for which $Z_f(q^{-s}) = \zeta_f(s)$. Then

$$Z_f(u) = \sum_{N=0}^{\infty} F(N) u^N. \tag{1.2}$$

In the last lecture we investigated the function $b_N(K)$, the number of effective divisors of K with degree N. We showed that if $N > 2g - 2$ (where g is the genus of K)

$$b_N(K) = h_K \frac{q^{N-g+1} - 1}{q - 1}.$$

Definition

Let $f : \mathcal{D}_K^+ \to \mathbb{C}$ be a function. The average value of f is defined to be

$$Ave(f) = \lim_{N \to \infty} \frac{\sum_{degD=N} f(D)}{\sum_{degD=N} 1} = \lim_{N \to \infty} \frac{F(N)}{b_N(K)},$$

provided the limit exists.

Before we present the main tool that we will be using we have to establish a convention that will be used through the lecture. The function q^{-s} is easily seen to be periodic with period $2\pi i/\log(q)$. The same therefore applies to all functions of q^{-s} such as our functions $\zeta_f(s)$. For this reason, nothing is lost by confining our attention to the region

$$B = \left\{ s \in \mathbb{C} : -\frac{\pi i}{\log(q)} \leq \Im(s) < \frac{\pi i}{\log(q)} \right\}.$$

Before we present the main tool that we will be using we have to establish a convention that will be used through the lecture. The function q^{-s} is easily seen to be periodic with period $2\pi i/\log(q)$. The same therefore applies to all functions of q^{-s} such as our functions $\zeta_f(s)$. For this reason, nothing is lost by confining our attention to the region

$$B = \left\{ s \in \mathbb{C} : -\frac{\pi i}{\log(q)} \leq \mathfrak{I}(s) < \frac{\pi i}{\log(q)} \right\}.$$

In what follows, we will always suppose that s is confined to the region B. This makes life a lot easier. For example, $\zeta_K(s)$ has two simple poles, one at $s = 1$ and one at $s = 0$ if s is confined to B, but it has infinitely many poles on the line $\mathfrak{R}(s) = 1$ and $\mathfrak{R}(s) = 0$ if s is not so confined.

Before we present the main tool that we will be using we have to establish a convention that will be used through the lecture. The function q^{-s} is easily seen to be periodic with period $2\pi i/\log(q)$. The same therefore applies to all functions of q^{-s} such as our functions $\zeta_f(s)$. For this reason, nothing is lost by confining our attention to the region

$$B = \left\{ s \in \mathbb{C} : -\frac{\pi i}{\log(q)} \leq \Im(s) < \frac{\pi i}{\log(q)} \right\}.$$

In what follows, we will always suppose that s is confined to the region B. This makes life a lot easier. For example, $\zeta_K(s)$ has two simple poles, one at $s = 1$ and one at $s = 0$ if s is confined to B, but it has infinitely many poles on the line $\Re(s) = 1$ and $\Re(s) = 0$ if s is not so confined.

Theorem

Let $f : \mathcal{D}_K^+ \to \mathbb{C}$ be given and suppose $\zeta_f(s)$ converges absolutely for $\Re(s) > 1$ and is holomorphic on $\{s \in B : \Re(s) = 1\}$ except for a simple pole at $s = 1$ with residue α. Then, there is a $\delta < 1$ such that

$$F(N) = \sum_{degD=N} f(D) = \alpha \log(q) q^N + O(q^{\delta N}).$$

If $\zeta_f(s) - \frac{\alpha}{s-1}$ is holomorphic in $\Re(s) \geq \delta'$, then the error term can be replaced with $O(q^{\delta' N})$.

Proof of the Theorem

The hypothesis implies that $Z_f(u)$ is holomorphic on the disk $\left\{u \in \mathbb{C} : |u| \leq q^{-1}\right\}$ with the exception of a simple pole at $u = q^{-1}$.

Proof of the Theorem

The hypothesis implies that $Z_f(u)$ is holomorphic on the disk $\left\{u \in \mathbb{C} : |u| \leq q^{-1}\right\}$ with the exception of a simple pole at $u = q^{-1}$. What is the residue of $Z_f(u)$ at $u = q^{-1}$?

Proof of the Theorem

The hypothesis implies that $Z_f(u)$ is holomorphic on the disk $\left\{u \in \mathbb{C} : |u| \leq q^{-1}\right\}$ with the exception of a simple pole at $u = q^{-1}$. What is the residue of $Z_f(u)$ at $u = q^{-1}$? The answer is given by

$$\lim_{u \to q^{-1}} (u - q^{-1}) Z_f(u) = \lim_{s \to 1} \frac{q^{-s} - q^{-1}}{s - 1} (s - 1) \zeta_f(s) = -\frac{\log(q)}{q} \alpha.$$

Proof of the Theorem

The hypothesis implies that $Z_f(u)$ is holomorphic on the disk $\{u \in \mathbb{C} : |u| \leq q^{-1}\}$ with the exception of a simple pole at $u = q^{-1}$. What is the residue of $Z_f(u)$ at $u = q^{-1}$? The answer is given by

$$\lim_{u \to q^{-1}} (u - q^{-1}) Z_f(u) = \lim_{s \to 1} \frac{q^{-s} - q^{-1}}{s - 1} (s - 1) \zeta_f(s) = -\frac{\log(q)}{q} \alpha.$$

Next, notice that since the circle $\{u \in \mathbb{C} : |u| = q^{-1}\}$ is compact, there is a $\delta < 1$ such that $Z_f(u)$ is holomorphic on the disk $\{u \in \mathbb{C} : |u| \leq q^{-\delta}\}$ except for the simple pole at $u = q^{-1}$.

Proof of the Theorem

The hypothesis implies that $Z_f(u)$ is holomorphic on the disk $\left\{u \in \mathbb{C} : |u| \leq q^{-1}\right\}$ with the exception of a simple pole at $u = q^{-1}$. What is the residue of $Z_f(u)$ at $u = q^{-1}$? The answer is given by

$$\lim_{u \to q^{-1}} (u - q^{-1}) Z_f(u) = \lim_{s \to 1} \frac{q^{-s} - q^{-1}}{s - 1} (s-1) \zeta_f(s) = -\frac{\log(q)}{q} \alpha.$$

Next, notice that since the circle $\left\{u \in \mathbb{C} : |u| = q^{-1}\right\}$ is compact, there is a $\delta < 1$ such that $Z_f(u)$ is holomorphic on the disk $\left\{u \in \mathbb{C} : |u| \leq q^{-\delta}\right\}$ except for the simple pole at $u = q^{-1}$. Let C be the boundary of this disk oriented counterclockwise and let C_ϵ be a small disc about the origin of radius $\epsilon < q^{-1}$. Orient C_ϵ clockwise, and consider the integral

$$\frac{1}{2\pi i} \oint_{C_\epsilon + C} \frac{Z_f(u)}{u^{N+1}} du.$$

Proof of the Theorem

The hypothesis implies that $Z_f(u)$ is holomorphic on the disk $\left\{u \in \mathbb{C} : |u| \leq q^{-1}\right\}$ with the exception of a simple pole at $u = q^{-1}$. What is the residue of $Z_f(u)$ at $u = q^{-1}$? The answer is given by

$$\lim_{u \to q^{-1}} (u - q^{-1}) Z_f(u) = \lim_{s \to 1} \frac{q^{-s} - q^{-1}}{s - 1} (s-1)\zeta_f(s) = -\frac{\log(q)}{q}\alpha.$$

Next, notice that since the circle $\left\{u \in \mathbb{C} : |u| = q^{-1}\right\}$ is compact, there is a $\delta < 1$ such that $Z_f(u)$ is holomorphic on the disk $\left\{u \in \mathbb{C} : |u| \leq q^{-\delta}\right\}$ except for the simple pole at $u = q^{-1}$. Let C be the boundary of this disk oriented counterclockwise and let C_ϵ be a small disc about the origin of radius $\epsilon < q^{-1}$. Orient C_ϵ clockwise, and consider the integral

$$\frac{1}{2\pi i} \oint_{C_\epsilon + C} \frac{Z_f(u)}{u^{N+1}} du.$$

By the Cauchy integral formula, this equals to sum of the residues of $Z_f(u)u^{-N-1}$ between the two circles. There is only one pole at $u = q^{-1}$ and the residue there is

$$-\frac{\log(q)}{q}\alpha q^{N+1} = -\alpha \log(q) q^N.$$

Continuation of the Proof

On the other hand, using the power series expansion of $Z_f(u)$ about $u = 0$, we see

$$\frac{1}{2\pi i}\oint_{C_\epsilon} \frac{Z_f(u)}{u^{N+1}}\,du = -F(N).$$

Continuation of the Proof

On the other hand, using the power series expansion of $Z_f(u)$ about $u = 0$, we see

$$\frac{1}{2\pi i} \oint_{C_\epsilon} \frac{Z_f(u)}{u^{N+1}} du = -F(N).$$

It follows that

$$F(N) = \alpha \log(q) q^N + \frac{1}{2\pi i} \oint_C \frac{Z_f(u)}{u^{N+1}} du.$$

Continuation of the Proof

On the other hand, using the power series expansion of $Z_f(u)$ about $u = 0$, we see

$$\frac{1}{2\pi i} \oint_{C_\epsilon} \frac{Z_f(u)}{u^{N+1}} du = -F(N).$$

It follows that

$$F(N) = \alpha \log(q) q^N + \frac{1}{2\pi i} \oint_C \frac{Z_f(u)}{u^{N+1}} du.$$

Let M be the maximum value of $|Z_f(u)|$ on the circle C. The integral in the last formula is bounded by $Mq^{\delta N}$, which completes the proof of the first assertion of the theorem.

Continuation of the Proof

On the other hand, using the power series expansion of $Z_f(u)$ about $u = 0$, we see

$$\frac{1}{2\pi i} \oint_{C_\epsilon} \frac{Z_f(u)}{u^{N+1}} du = -F(N).$$

It follows that

$$F(N) = \alpha \log(q) q^N + \frac{1}{2\pi i} \oint_C \frac{Z_f(u)}{u^{N+1}} du.$$

Let M be the maximum value of $|Z_f(u)|$ on the circle C. The integral in the last formula is bounded by $Mq^{\delta N}$, which completes the proof of the first assertion of the theorem.

To prove the last part, we may assume $\delta' < 1$ since otherwise the error term would be the same size or bigger than the main term. If $\zeta_f(s) - \alpha/(s-1)$ is holomorphic for $\Re(s) \geq \delta'$, then $Z_f(u)$ is holomorphic on the disc $\left\{u \in \mathbb{C} : |u| \leq q^{-\delta'}\right\}$ except for a simple pole at $u = q^{-1}$.

Continuation of the Proof

On the other hand, using the power series expansion of $Z_f(u)$ about $u = 0$, we see

$$\frac{1}{2\pi i} \oint_{C_\epsilon} \frac{Z_f(u)}{u^{N+1}} du = -F(N).$$

It follows that

$$F(N) = \alpha \log(q) q^N + \frac{1}{2\pi i} \oint_C \frac{Z_f(u)}{u^{N+1}} du.$$

Let M be the maximum value of $|Z_f(u)|$ on the circle C. The integral in the last formula is bounded by $Mq^{\delta N}$, which completes the proof of the first assertion of the theorem.

To prove the last part, we may assume $\delta' < 1$ since otherwise the error term would be the same size or bigger than the main term. If $\zeta_f(s) - \alpha/(s-1)$ is holomorphic for $\Re(s) \geq \delta'$, then $Z_f(u)$ is holomorphic on the disc $\left\{ u \in \mathbb{C} : |u| \leq q^{-\delta'} \right\}$ except for a simple pole at $u = q^{-1}$. In that case we can repeat the above proof with the role of the circle C being replaced by the circle $C' = \left\{ u \in \mathbb{C} : |u| = q^{-\delta'} \right\}$. The result follows.

We illustrate the use of this theorem by investigating the generalization of the questions: what is the probability that a polynomial is square-free? In Lecture 1 we showed, after making the question more precise, that the answer is $1/\zeta_A(2)$.

We illustrate the use of this theorem by investigating the generalization of the questions: what is the probability that a polynomial is square-free? In Lecture 1 we showed, after making the question more precise, that the answer is $1/\zeta_A(2)$.

What would it mean for a divisor to be square-free? A moment's reflection shows that the following to be right definition.

Definition

*An effective divisor D is **square-free** if and only if $\mathrm{ord}_P D$ is either 0 or 1 for all prime divisors P, i.e., if and only if D is a sum of distinct prime divisors.*

We illustrate the use of this theorem by investigating the generalization of the questions: what is the probability that a polynomial is square-free? In Lecture 1 we showed, after making the question more precise, that the answer is $1/\zeta_A(2)$.

What would it mean for a divisor to be square-free? A moment's reflection shows that the following to be right definition.

Definition

*An effective divisor D is **square-free** if and only if $ord_P D$ is either 0 or 1 for all prime divisors P, i.e., if and only if D is a sum of distinct prime divisors.*

Proposition

Let $f : \mathcal{D}_K^+ \to \mathbb{C}$ be the characteristic function of the square-free effective divisors. Then $F(N) = \sum_{degD=N} f(D)$ is the number of square-free effective divisors of degree N. Given $\epsilon > 0$, we have

$$F(N) = \frac{1}{\zeta_K(2)} \frac{h_K}{q^{g-1}(q-1)} q^N + O_\epsilon(q^{(\frac{1}{4}+\epsilon)N}).$$

Moreover, $Ave(f) = \frac{1}{\zeta_K(2)}$.

Proof of the Proposition

Recall that for divisors C and D we have $N(C+D) = NCND$. From this we calculate

$$\zeta_f(s) = \sum_D \frac{f(D)}{ND^s} = \sum_{D \text{ square-free}} \frac{1}{ND^s} = \prod_P \left(1 + \frac{1}{NP^s}\right) = \frac{\zeta_K(s)}{\zeta_K(2s)}.$$

Proof of the Proposition

Recall that for divisors C and D we have $N(C+D) = NCND$. From this we calculate

$$\zeta_f(s) = \sum_D \frac{f(D)}{ND^s} = \sum_{D \text{ square-free}} \frac{1}{ND^s} = \prod_P \left(1 + \frac{1}{NP^s}\right) = \frac{\zeta_K(s)}{\zeta_K(2s)}.$$

By the function-field Riemann Hypothesis we know that all the zeros of $\zeta_K(s)$ are on the line $\Re(s) = \frac{1}{2}$. Thus $1/\zeta_K(2s)$ has no poles in the region $\Re(s) > \frac{1}{4}$. On the other hand, we know that in this region $\zeta_K(s)$ is holomorphic except for a simple pole at $s = 1$.

Proof of the Proposition

Recall that for divisors C and D we have $N(C+D) = NCND$. From this we calculate

$$\zeta_f(s) = \sum_D \frac{f(D)}{ND^s} = \sum_{D \text{ square-free}} \frac{1}{ND^s} = \prod_P \left(1 + \frac{1}{NP^s}\right) = \frac{\zeta_K(s)}{\zeta_K(2s)}.$$

By the function-field Riemann Hypothesis we know that all the zeros of $\zeta_K(s)$ are on the line $\Re(s) = \frac{1}{2}$. Thus $1/\zeta_K(2s)$ has no poles in the region $\Re(s) > \frac{1}{4}$. On the other hand, we know that in this region $\zeta_K(s)$ is holomorphic except for a simple pole at $s = 1$.
Choose $\epsilon > 0$ and set $\delta' = \frac{1}{4} + \epsilon$. Then all the hypotheses of the Tauberian theorem apply to $\zeta_f(s)$ and we find

$$F(N) = \alpha \log(q) q^N + O_\epsilon(q^{(\frac{1}{4}+\epsilon)N}), \tag{1.3}$$

where α is the residue of $\zeta_K(s)/\zeta_K(2s)$ at $s = 1$.

Proof of the Proposition

Recall that for divisors C and D we have $N(C+D) = NCND$. From this we calculate

$$\zeta_f(s) = \sum_D \frac{f(D)}{ND^s} = \sum_{D \text{ square-free}} \frac{1}{ND^s} = \prod_P \left(1 + \frac{1}{NP^s}\right) = \frac{\zeta_K(s)}{\zeta_K(2s)}.$$

By the function-field Riemann Hypothesis we know that all the zeros of $\zeta_K(s)$ are on the line $\Re(s) = \frac{1}{2}$. Thus $1/\zeta_K(2s)$ has no poles in the region $\Re(s) > \frac{1}{4}$. On the other hand, we know that in this region $\zeta_K(s)$ is holomorphic except for a simple pole at $s = 1$.

Choose $\epsilon > 0$ and set $\delta' = \frac{1}{4} + \epsilon$. Then all the hypotheses of the Tauberian theorem apply to $\zeta_f(s)$ and we find

$$F(N) = \alpha \log(q) q^N + O_\epsilon(q^{(\frac{1}{4}+\epsilon)N}), \tag{1.3}$$

where α is the residue of $\zeta_K(s)/\zeta_K(2s)$ at $s = 1$. We saw in the last lecture that the residue of $\zeta_K(s)$ at $s = 1$ is

$$\rho_K = \frac{h_K}{q^{g-1}(q-1)\log(q)}. \tag{1.4}$$

Proof of the Proposition

Recall that for divisors C and D we have $N(C+D) = NCND$. From this we calculate

$$\zeta_f(s) = \sum_D \frac{f(D)}{ND^s} = \sum_{D \text{ square-free}} \frac{1}{ND^s} = \prod_P \left(1 + \frac{1}{NP^s}\right) = \frac{\zeta_K(s)}{\zeta_K(2s)}.$$

By the function-field Riemann Hypothesis we know that all the zeros of $\zeta_K(s)$ are on the line $\Re(s) = \frac{1}{2}$. Thus $1/\zeta_K(2s)$ has no poles in the region $\Re(s) > \frac{1}{4}$. On the other hand, we know that in this region $\zeta_K(s)$ is holomorphic except for a simple pole at $s = 1$.

Choose $\epsilon > 0$ and set $\delta' = \frac{1}{4} + \epsilon$. Then all the hypotheses of the Tauberian theorem apply to $\zeta_f(s)$ and we find

$$F(N) = \alpha \log(q) q^N + O_\epsilon(q^{(\frac{1}{4}+\epsilon)N}), \tag{1.3}$$

where α is the residue of $\zeta_K(s)/\zeta_K(2s)$ at $s = 1$. We saw in the last lecture that the residue of $\zeta_K(s)$ at $s = 1$ is

$$\rho_K = \frac{h_K}{q^{g-1}(q-1)\log(q)}. \tag{1.4}$$

It follows that $\alpha = \rho_K/\zeta_K(2)$. Substituting this information into equation above completes the proof of the first assertion of the proposition.

Continuation of the Proof

To prove the second assertion recall that $\mathrm{Ave}(f) = \lim_{N\to\infty} F(N)/b_N(K)$ and that for all $N > 2g-2$, $b_N(K) = h_K(q^{N-g+1} - 1)/(q-1)$.

Continuation of the Proof

To prove the second assertion recall that $\mathrm{Ave}(f) = \lim_{N\to\infty} F(N)/b_N(K)$ and that for all $N > 2g-2$, $b_N(K) = h_K(q^{N-g+1}-1)/(q-1)$.

By the first part of the proposition we find, for N in this range,

$$\frac{F(N)}{b_N(K)} = \frac{1}{\zeta_K(2)} \frac{q^{N-g+1}}{q^{N-g+1}-1} + O_\epsilon(q^{(-\frac{3}{4}+\epsilon)N}).$$

Continuation of the Proof

To prove the second assertion recall that $\mathrm{Ave}(f) = \lim_{N\to\infty} F(N)/b_N(K)$ and that for all $N > 2g-2$, $b_N(K) = h_K(q^{N-g+1}-1)/(q-1)$.

By the first part of the proposition we find, for N in this range,

$$\frac{F(N)}{b_N(K)} = \frac{1}{\zeta_K(2)} \frac{q^{N-g+1}}{q^{N-g+1}-1} + O_\epsilon(q^{(-\frac{3}{4}+\epsilon)N}).$$

Now, simply pass to the limit as N tends to ∞.

As a final application of these methods we want to investigate the function $d(D)$, the number of effective divisors of D. More precisely, $d(D) = \#\left\{C \in \mathcal{D}_K^+ : 0 \leq C \leq D\right\}$.

As a final application of these methods we want to investigate the function $d(D)$, the number of effective divisors of D. More precisely, $d(D) = \#\left\{C \in \mathcal{D}_K^+ : 0 \leq C \leq D\right\}$.
It is relatively easy to check that $\zeta_d(s) = \zeta_K(s)^2$. This function has a double pole at $s = 1$ so the Tauberian theorem doens't immediately apply. Moreover, it is hard to imagine any simple trick reducing us to the condition of that theorem. What is needed is a generalization.

As a final application of these methods we want to investigate the function $d(D)$, the number of effective divisors of D. More precisely, $d(D) = \#\left\{C \in \mathcal{D}_K^+ : 0 \leq C \leq D\right\}$.
It is relatively easy to check that $\zeta_d(s) = \zeta_K(s)^2$. This function has a double pole at $s = 1$ so the Tauberian theorem doens't immediately apply. Moreover, it is hard to imagine any simple trick reducing us to the condition of that theorem. What is needed is a generalization.

Theorem

Let $f : \mathcal{D}_K^+ \to \mathbb{C}$ and let $\zeta_f(s)$ be the corresponding Dirichlet series. Suppose this series converges absolutely in the region $\Re(s) > 1$ and is holomorphic in the region $\{s \in B : \Re(s) = 1\}$ except for a pole of order r at $s = 1$. Let $\alpha = \lim_{s\to 1}(s-1)^r \zeta_f(s)$. Then, there is a $\delta < 1$ and constants c_{-i} with $1 \leq i \leq r$ such that

$$F(N) = \sum_{degD=N} f(D) = q^N \left(\sum_{i=1}^{r} c_{-i} \binom{N+i-1}{i-1} (-q)^i\right) + O(q^{\delta N}).$$

The sum in parenthesis is a polynomial in N of degree $r-1$ with leading term

$$\frac{\log(q)^r}{(r-1)!} \alpha N^{r-1}.$$

Proof of the Theorem

As in the proof of the Tauberian theorem, we can find a $\delta < 1$ such that $Z_f(u)$ is holomorphic on the disc $\left\{u \in \mathbb{C} : |u| \leq q^{-\delta}\right\}$. We again let C be the boundary of this disc oriented conterclockwise and C_ϵ a small circle about $s = 0$ oriented clockwise.

Proof of the Theorem

As in the proof of the Tauberian theorem, we can find a $\delta < 1$ such that $Z_f(u)$ is holomorphic on the disc $\left\{u \in \mathbb{C} : |u| \leq q^{-\delta}\right\}$. We again let C be the boundary of this disc oriented conterclockwise and C_ϵ a small circle about $s = 0$ oriented clockwise. By the Cauchy integral theorem, the integral

$$\frac{1}{2\pi i} \oint_{C+C_\epsilon} \frac{Z_f(u)}{u^{N+1}} du$$

is equal to the sum of the residues of the function $Z_f(u)u{-}N - 1$ in the region between the two circles.

Proof of the Theorem

As in the proof of the Tauberian theorem, we can find a $\delta < 1$ such that $Z_f(u)$ is holomorphic on the disc $\left\{ u \in \mathbb{C} : |u| \leq q^{-\delta} \right\}$. We again let C be the boundary of this disc oriented conterclockwise and C_ϵ a small circle about $s = 0$ oriented clockwise. By the Cauchy integral theorem, the integral

$$\frac{1}{2\pi i} \oint_{C+C_\epsilon} \frac{Z_f(u)}{u^{N+1}} du$$

is equal to the sum of the residues of the function $Z_f(u)u{-}N - 1$ in the region between the two circles. There is only one pole in this region. It is located at $u = q^{-1}$. To find the residue there, we expand both $Z_f(u)$ and u^{-N-1} in Laurent series about $u = q^{-1}$, multiply the results together, and pick out the coefficient of $(u - q^{-1})^{-1}$.

Proof of the Theorem

As in the proof of the Tauberian theorem, we can find a $\delta < 1$ such that $Z_f(u)$ is holomorphic on the disc $\left\{u \in \mathbb{C} : |u| \leq q^{-\delta}\right\}$. We again let C be the boundary of this disc oriented conterclockwise and C_ϵ a small circle about $s = 0$ oriented clockwise. By the Cauchy integral theorem, the integral

$$\frac{1}{2\pi i} \oint_{C+C_\epsilon} \frac{Z_f(u)}{u^{N+1}} du$$

is equal to the sum of the residues of the function $Z_f(u)u{-}N-1$ in the region between the two circles. There is only one pole in this region. It is located at $u = q^{-1}$. To find the residue there, we expand both $Z_f(u)$ and u^{-N-1} in Laurent series about $u = q^{-1}$, multiply the results together, and pick out the coefficient of $(u - q^{-1})^{-1}$. By using the Taylor series formula or the general binomial expansion theorem we find

$$u^{-N-1} = q^{N+1} \sum_{j=0}^{\infty} \binom{-N-1}{j} q^j (u - q^{-1})^j.$$

Proof of the Theorem

As in the proof of the Tauberian theorem, we can find a $\delta < 1$ such that $Z_f(u)$ is holomorphic on the disc $\left\{u \in \mathbb{C} : |u| \leq q^{-\delta}\right\}$. We again let C be the boundary of this disc oriented conterclockwise and C_ϵ a small circle about $s = 0$ oriented clockwise. By the Cauchy integral theorem, the integral

$$\frac{1}{2\pi i} \oint_{C+C_\epsilon} \frac{Z_f(u)}{u^{N+1}} du$$

is equal to the sum of the residues of the function $Z_f(u)u{-}N - 1$ in the region between the two circles. There is only one pole in this region. It is located at $u = q^{-1}$. To find the residue there, we expand both $Z_f(u)$ and u^{-N-1} in Laurent series about $u = q^{-1}$, multiply the results together, and pick out the coefficient of $(u - q^{-1})^{-1}$. By using the Taylor series formula or the general binomial expansion theorem we find

$$u^{-N-1} = q^{N+1} \sum_{j=0}^{\infty} \binom{-N-1}{j} q^j (u - q^{-1})^j.$$

The Laurent series for $Z_f(u)$ has the form

$$Z_f(u) = \sum_{i=-r}^{\infty} c_i (u - q^{-1})^i, \qquad \text{with } c_{-r} \neq 0.$$

Continuation of the Proof

Multiplying these two series together and isolating the coefficient of $(u-q^{-1})^{-1}$ in the result yields

$$\mathrm{Res}_{u=q^{-1}} Z_f(u)u^{-N-1} = q^{N+1}\sum_{i=-r}^{-1} c_i \binom{-N-1}{-i-1} q^{-i-1}$$

Continuation of the Proof

Multiplying these two series together and isolating the coefficient of $(u - q^{-1})^{-1}$ in the result yields

$$\begin{aligned}\mathrm{Res}_{u=q^{-1}} Z_f(u) u^{-N-1} &= q^{N+1} \sum_{i=-r}^{-1} c_i \binom{-N-1}{-i-1} q^{-i-1} \\ &= q^N \sum_{i=1}^{r} c_{-i} \binom{-N-1}{i-1} q^i .\end{aligned}$$

Continuation of the Proof

Multiplying these two series together and isolating the coefficient of $(u - q^{-1})^{-1}$ in the result yields

$$\begin{aligned}\mathrm{Res}_{u=q^{-1}} Z_f(u) u^{-N-1} &= q^{N+1} \sum_{i=-r}^{-1} c_i \binom{-N-1}{-i-1} q^{-i-1} \\ &= q^N \sum_{i=1}^{r} c_{-i} \binom{-N-1}{i-1} q^i.\end{aligned}$$

To get the last equality we simply transformed i to $-i$ and redistributed one factor of q.

Continuation of the Proof

Multiplying these two series together and isolating the coefficient of $(u-q^{-1})^{-1}$ in the result yields

$$\begin{aligned}
\mathrm{Res}_{u=q^{-1}} Z_f(u) u^{-N-1} &= q^{N+1} \sum_{i=-r}^{-1} c_i \binom{-N-1}{-i-1} q^{-i-1} \\
&= q^N \sum_{i=1}^{r} c_{-i} \binom{-N-1}{i-1} q^i.
\end{aligned}$$

To get the last equality we simply transformed i to $-i$ and redistributed one factor of q.
It is easy to see that $\binom{-N-1}{k} = (-1)^k \binom{N+k}{k}$, so the residue can be rewritten as

$$-q^N \sum_{i=1}^{r} c_{-i} \binom{N+i-1}{i-1} (-q)^i.$$

Continuation of the Proof

Multiplying these two series together and isolating the coefficient of $(u - q^{-1})^{-1}$ in the result yields

$$\begin{aligned} \mathrm{Res}_{u=q^{-1}} Z_f(u) u^{-N-1} &= q^{N+1} \sum_{i=-r}^{-1} c_i \binom{-N-1}{-i-1} q^{-i-1} \\ &= q^N \sum_{i=1}^{r} c_{-i} \binom{-N-1}{i-1} q^i. \end{aligned}$$

To get the last equality we simply transformed i to $-i$ and redistributed one factor of q.

It is easy to see that $\binom{-N-1}{k} = (-1)^k \binom{N+k}{k}$, so the residue can be rewritten as

$$-q^N \sum_{i=1}^{r} c_{-i} \binom{N+i-1}{i-1} (-q)^i.$$

As in the proof of the previous Tauberian theorem , it now follows that

$$F(N) = q^N \left(\sum_{i=1}^{r} c_{-i} \binom{N+i-1}{i-1} (-q)^i \right) + O(q^{\delta N}).$$

Continuation of the Proof

Finally, we must prove the assertion about the term in parenthesis. First of all, it is clear that when $k \geq 0$, $\binom{N+k}{k}$ is a polynomial in N of degree k, and that its leading term is $k!^{-1}N^k$. Thus the sum in parenthesis is a polynomial in N of degree $r-1$ and its leading term is

$$\frac{c_{-r}}{(r-1)!}(-q)^r N^{r-1}.$$

Continuation of the Proof

Finally, we must prove the assertion about the term in parenthesis. First of all, it is clear that when $k \geq 0$, $\binom{N+k}{k}$ is a polynomial in N of degree k, and that its leading term is $k!^{-1}N^k$. Thus the sum in parenthesis is a polynomial in N of degree $r-1$ and its leading term is

$$\frac{c_{-r}}{(r-1)!}(-q)^r N^{r-1}.$$

It remains to relate $\alpha = \lim_{s\to 1}(s-1)^r \zeta_f(s)$ to c_{-r}.

Continuation of the Proof

Finally, we must prove the assertion about the term in parenthesis. First of all, it is clear that when $k \geq 0$, $\binom{N+k}{k}$ is a polynomial in N of degree k, and that its leading term is $k!^{-1}N^k$. Thus the sum in parenthesis is a polynomial in N of degree $r-1$ and its leading term is

$$\frac{c_{-r}}{(r-1)!}(-q)^r N^{r-1}.$$

It remains to relate $\alpha = \lim_{s\to 1}(s-1)^r \zeta_f(s)$ to c_{-r}. This relationship follows from the calculation

$$c_{-r} \quad = \quad \lim_{u \to q^{-1}} (u - q^{-1})^r Z_f(u)$$

Continuation of the Proof

Finally, we must prove the assertion about the term in parenthesis. First of all, it is clear that when $k \geq 0$, $\binom{N+k}{k}$ is a polynomial in N of degree k, and that its leading term is $k!^{-1}N^k$. Thus the sum in parenthesis is a polynomial in N of degree $r-1$ and its leading term is

$$\frac{c_{-r}}{(r-1)!}(-q)^r N^{r-1}.$$

It remains to relate $\alpha = \lim_{s\to 1}(s-1)^r \zeta_f(s)$ to c_{-r}. This relationship follows from the calculation

$$\begin{aligned} c_{-r} &= \lim_{u\to q^{-1}} (u-q^{-1})^r Z_f(u) \\ &= \lim_{s\to 1} \left(\frac{q^{-s}-q^{-1}}{s-1}\right)^r (s-1)^r \zeta_f(s) = \left(-\frac{\log(q)}{q}\right)^r \alpha. \end{aligned} \tag{1.5}$$

Continuation of the Proof

Finally, we must prove the assertion about the term in parenthesis. First of all, it is clear that when $k \geq 0$, $\binom{N+k}{k}$ is a polynomial in N of degree k, and that its leading term is $k!^{-1}N^k$. Thus the sum in parenthesis is a polynomial in N of degree $r-1$ and its leading term is

$$\frac{c_{-r}}{(r-1)!}(-q)^r N^{r-1}.$$

It remains to relate $\alpha = \lim_{s\to 1}(s-1)^r \zeta_f(s)$ to c_{-r}. This relationship follows from the calculation

$$\begin{aligned} c_{-r} &= \lim_{u\to q^{-1}} (u-q^{-1})^r Z_f(u) \\ &= \lim_{s\to 1} \left(\frac{q^{-s}-q^{-1}}{s-1}\right)^r (s-1)^r \zeta_f(s) = \left(-\frac{\log(q)}{q}\right)^r \alpha. \qquad (1.5) \end{aligned}$$

Substitute this expression for c_{-r} into the previous expression for the leading term of the sum in parentheses and we arrive at

$$\frac{\log(q)^r}{(r-1)!}\alpha N^{r-1}$$

for the leading term. This completes the proof.

Corollary

With the assumptions and notation of the theorem, we have, as $N \to \infty$,

$$F(N) \sim \frac{\log(q)^r}{(r-1)!} \alpha q^N N^{r-1}.$$

Corollary

With the assumptions and notation of the theorem, we have, as $N \to \infty$,

$$F(N) \sim \frac{\log(q)^r}{(r-1)!}\alpha q^N N^{r-1}.$$

Proof.

This is immediate from the theorem. $\square$

We now want to apply the previous theorem to the divisor function $d(D)$ on $\mathcal{D}_K^+$.

We now want to apply the previous theorem to the divisor function $d(D)$ on $\mathcal{D}_K^+$.

Proposition

Let $K/\mathbb{F}$ be a global function field and $d(D)$ the divisor function on the effective divisors. Then, there exist constants μ_K and λ_K such that for fixed $\epsilon > 0$ we have

$$\sum_{degD=N} d(D) = q^N(\lambda_K N + \mu_K) + O_\epsilon(q^{\epsilon N}).$$

More explicitly, $\lambda_K = h_K^2 q^{2-2g}(q-1)^{-2}$.

Proof of the Proposition

We have already seen that $\zeta_d(s) = \zeta_K(s)^2$, a function which has a double pole at $s = 1$ and is otherwise holomorphic for $\Re(s) > 0$.

Proof of the Proposition

We have already seen that $\zeta_d(s) = \zeta_K(s)^2$, a function which has a double pole at $s = 1$ and is otherwise holomorphic for $\Re(s) > 0$. Choose $\epsilon > 0$. Notice that $\lim_{s\to 1}(s-1)^2\zeta_K(s)^2 = \rho_K^2$.

Proof of the Proposition

We have already seen that $\zeta_d(s) = \zeta_K(s)^2$, a function which has a double pole at $s = 1$ and is otherwise holomorphic for $\Re(s) > 0$. Choose $\epsilon > 0$. Notice that $\lim_{s\to 1}(s-1)^2\zeta_K(s)^2 = \rho_K^2$. Applying the previous theorem we find there are constants λ_K and μ_K such that

$$\sum_{\deg D = N} d(D) = q^N(\lambda_K N + \mu_K) + O_\epsilon(q^{\epsilon N}).$$

Proof of the Proposition

We have already seen that $\zeta_d(s) = \zeta_K(s)^2$, a function which has a double pole at $s = 1$ and is otherwise holomorphic for $\Re(s) > 0$. Choose $\epsilon > 0$. Notice that $\lim_{s\to 1}(s-1)^2\zeta_K(s)^2 = \rho_K^2$. Applying the previous theorem we find there are constants λ_K and μ_K such that

$$\sum_{\deg D = N} d(D) = q^N(\lambda_K N + \mu_K) + O_\epsilon(q^{\epsilon N}).$$

Applying the formula for the leading term of the polynomial in the parenthesis given in the statement of the previous theorem, we find

$$\lambda_K = \frac{\log(q)^r}{(r-1)!}\alpha = \frac{\log(q)^2}{1!}\rho_K^2 = \frac{h_K^2}{q^{2g-2}(q-1)^2}.$$

Proof of the Proposition

We have already seen that $\zeta_d(s) = \zeta_K(s)^2$, a function which has a double pole at $s = 1$ and is otherwise holomorphic for $\Re(s) > 0$. Choose $\epsilon > 0$. Notice that $\lim_{s\to 1}(s-1)^2\zeta_K(s)^2 = \rho_K^2$. Applying the previous theorem we find there are constants λ_K and μ_K such that

$$\sum_{\deg D = N} d(D) = q^N(\lambda_K N + \mu_K) + O_\epsilon(q^{\epsilon N}).$$

Applying the formula for the leading term of the polynomial in the parenthesis given in the statement of the previous theorem, we find

$$\lambda_K = \frac{\log(q)^r}{(r-1)!}\alpha = \frac{\log(q)^2}{1!}\rho_K^2 = \frac{h_K^2}{q^{2g-2}(q-1)^2}.$$

This finishes the proof.

Introduction

- In this part I will present function-field version of sieve methods.

Introduction

- In this part I will present function-field version of sieve methods.
- Due to lack of time we will only present one sieve method for function fields.

Introduction

- In this part I will present function-field version of sieve methods.
- Due to lack of time we will only present one sieve method for function fields.
- We will present a function-field version of the classical Selberg's sieve.

- In this part I will present function-field version of sieve methods.
- Due to lack of time we will only present one sieve method for function fields.
- We will present a function-field version of the classical Selberg's sieve.
- Would be interesting to work out all the other sieve methods (as those presented in the book of A. Cojocaru and R. Murty and/or the book of Friedlander and Iwaniec) in the $\mathbb{F}_q[x]$ setting or even for more general global function fields $K/\mathbb{F}$. But we don't do this here.

Introduction

- In this part I will present function-field version of sieve methods.
- Due to lack of time we will only present one sieve method for function fields.
- We will present a function-field version of the classical Selberg's sieve.
- Would be interesting to work out all the other sieve methods (as those presented in the book of A. Cojocaru and R. Murty and/or the book of Friedlander and Iwaniec) in the $\mathbb{F}_q[x]$ setting or even for more general global function fields $K/\mathbb{F}$. But we don't do this here.
- Let us start by remembering the classical Selberg sieve.

The Classical Selberg's Sieve

Let $\mathcal{A}$ be any finite set of elements and $\mathcal{P}$ be a set of primes.

The Classical Selberg's Sieve

Let $\mathcal{A}$ be any finite set of elements and $\mathcal{P}$ be a set of primes. For each prime $p \in \mathcal{P}$, let $\mathcal{A}_p$ be a subset of $\mathcal{A}$.

The Classical Selberg's Sieve

Let $\mathcal{A}$ be any finite set of elements and $\mathcal{P}$ be a set of primes. For each prime $p \in \mathcal{P}$, let $\mathcal{A}_p$ be a subset of $\mathcal{A}$. We denote by d squarefree numbers composed of primes of $\mathcal{P}$.

The Classical Selberg's Sieve

Let $\mathcal{A}$ be any finite set of elements and $\mathcal{P}$ be a set of primes. For each prime $p \in \mathcal{P}$, let $\mathcal{A}_p$ be a subset of $\mathcal{A}$. We denote by d squarefree numbers composed of primes of $\mathcal{P}$. Let $\mathcal{A}_1 := \mathcal{A}$ and for squarefree integers d composed of primes of $\mathcal{P}$, let $\mathcal{A}_d := \cap_{p|d}\mathcal{A}_p$.

The Classical Selberg's Sieve

Let $\mathcal{A}$ be any finite set of elements and $\mathcal{P}$ be a set of primes. For each prime $p \in \mathcal{P}$, let $\mathcal{A}_p$ be a subset of $\mathcal{A}$. We denote by d squarefree numbers composed of primes of $\mathcal{P}$. Let $\mathcal{A}_1 := \mathcal{A}$ and for squarefree integers d composed of primes of $\mathcal{P}$, let $\mathcal{A}_d := \cap_{p|d} \mathcal{A}_p$. Let z be a positive real number and set

$$P(z) := \prod_{\substack{p \in \mathcal{P} \\ p < z}} p.$$

The Classical Selberg's Sieve

Let $\mathcal{A}$ be any finite set of elements and $\mathcal{P}$ be a set of primes. For each prime $p \in \mathcal{P}$, let $\mathcal{A}_p$ be a subset of $\mathcal{A}$. We denote by d squarefree numbers composed of primes of $\mathcal{P}$. Let $\mathcal{A}_1 := \mathcal{A}$ and for squarefree integers d composed of primes of $\mathcal{P}$, let $\mathcal{A}_d := \cap_{p|d} \mathcal{A}_p$. Let z be a positive real number and set

$$P(z) := \prod_{\substack{p \in \mathcal{P} \\ p < z}} p.$$

Denote by $S(\mathcal{A}, \mathcal{P}, z)$ the number of elements of

$$A \setminus \cup_{p|P(z)} \mathcal{A}_p.$$

The Classical Selberg's Sieve

Let $\mathcal{A}$ be any finite set of elements and $\mathcal{P}$ be a set of primes. For each prime $p \in \mathcal{P}$, let $\mathcal{A}_p$ be a subset of $\mathcal{A}$. We denote by d squarefree numbers composed of primes of $\mathcal{P}$. Let $\mathcal{A}_1 := \mathcal{A}$ and for squarefree integers d composed of primes of $\mathcal{P}$, let $\mathcal{A}_d := \cap_{p|d}\mathcal{A}_p$. Let z be a positive real number and set

$$P(z) := \prod_{\substack{p \in \mathcal{P} \\ p < z}} p.$$

Denote by $S(\mathcal{A}, \mathcal{P}, z)$ the number of elements of

$$A \setminus \cup_{p|P(z)}\mathcal{A}_p.$$

Theorem (Selberg's sieve, 1947)

We keep the above setting and assume that there exist $X > 0$ and a multiplicative function $f(\cdot)$ satisfying $f(p) > 1$ for any prime $p \in \mathcal{P}$, such that for any squarefree integer d composed of primes of $\mathcal{P}$ we have

$$\#\mathcal{A}_d = \frac{X}{f(d)} + R_d \tag{2.1}$$

for some real number R_d.

Continuation Selberg's sieve

We write

$$f(n) = \sum_{d|n} f_1(d) \tag{2.2}$$

for some multiplicative function $f_1(\cdot)$ that is uniquely determined by f by using the Möbius inversion formula; that is,

$$f_1(n) = \sum_{d|n} \mu(d) f(n/d).$$

Continuation Selberg's sieve

We write

$$f(n) = \sum_{d|n} f_1(d) \tag{2.2}$$

for some multiplicative function $f_1(\cdot)$ that is uniquely determined by f by using the Möbius inversion formula; that is,

$$f_1(n) = \sum_{d|n} \mu(d) f(n/d).$$

Also, we set

$$V(z) := \sum_{\substack{d \leq z \\ d|P(z)}} \frac{\mu^2(d)}{f_1(d)}.$$

Continuation Selberg's sieve

We write

$$f(n) = \sum_{d|n} f_1(d) \tag{2.2}$$

for some multiplicative function $f_1(\cdot)$ that is uniquely determined by f by using the Möbius inversion formula; that is,

$$f_1(n) = \sum_{d|n} \mu(d) f(n/d).$$

Also, we set

$$V(z) := \sum_{\substack{d \le z \\ d|P(z)}} \frac{\mu^2(d)}{f_1(d)}.$$

Then

$$S(\mathcal{A}, \mathcal{P}, z) \le \frac{X}{V(z)} + O\left(\sum_{\substack{d_1, d_2 \le z \\ d_1, d_2 | P(z)}} |R_{[d_1, d_2]}| \right).$$

Some Notation

Let $\mathbb{F}_q[x]$ be the polynomial ring over $\mathbb{F}_q$.

Some Notation

Let $\mathbb{F}_q[x]$ be the polynomial ring over $\mathbb{F}_q$.

Let $A, B, \ldots$ denote monic polynomials in $\mathbb{F}_q[x]$. And P a monic irreducible polynomal.

Some Notation

Let $\mathbb{F}_q[x]$ be the polynomial ring over $\mathbb{F}_q$.

Let $A, B, \ldots$ denote monic polynomials in $\mathbb{F}_q[x]$. And P a monic irreducible polynomal.

We will prove a fairly general k-residue form of Selberg's sieve for $\mathbb{F}_q[x]$ similar to that found in Halberstam and Roth.

Some Notation

Let $\mathbb{F}_q[x]$ be the polynomial ring over $\mathbb{F}_q$.

Let $A, B, \ldots$ denote monic polynomials in $\mathbb{F}_q[x]$. And P a monic irreducible polynomal.

We will prove a fairly general k-residue form of Selberg's sieve for $\mathbb{F}_q[x]$ similar to that found in Halberstam and Roth.

Let

$$\mathcal{A} = \{A_1, A_2, \ldots, A_n\},$$

Some Notation

Let $\mathbb{F}_q[x]$ be the polynomial ring over $\mathbb{F}_q$.

Let $A, B, \ldots$ denote monic polynomials in $\mathbb{F}_q[x]$. And P a monic irreducible polynomal.

We will prove a fairly general k-residue form of Selberg's sieve for $\mathbb{F}_q[x]$ similar to that found in Halberstam and Roth.

Let

$$\mathcal{A} = \{A_1, A_2, \ldots, A_n\},$$

$$\mathcal{P} = \{P_1, P_2, \ldots, P_r\}; \qquad P_i \neq P_j,$$

Some Notation

Let $\mathbb{F}_q[x]$ be the polynomial ring over $\mathbb{F}_q$.

Let $A, B, \ldots$ denote monic polynomials in $\mathbb{F}_q[x]$. And P a monic irreducible polynomal.

We will prove a fairly general k-residue form of Selberg's sieve for $\mathbb{F}_q[x]$ similar to that found in Halberstam and Roth.

Let

$$\mathcal{A} = \{A_1, A_2, \ldots, A_n\},$$

$$\mathcal{P} = \{P_1, P_2, \ldots, P_r\}; \qquad P_i \neq P_j,$$

$$\prod(\mathcal{P}) = \prod_{i=1}^{r} P_i.$$

Let also $\mathcal{D}$ denotes a subset of the divisors of $\prod(\mathcal{P})$.

Let also $\mathcal{D}$ denotes a subset of the divisors of $\prod(\mathcal{P})$. $\mathcal{D}$ is **divisor closed** if $D \in \mathcal{D}$ implies every divisor of D is also in $\mathcal{D}$.

Let also $\mathcal{D}$ denotes a subset of the divisors of $\prod(\mathcal{P})$. $\mathcal{D}$ is **divisor closed** if $D \in \mathcal{D}$ implies every divisor of D is also in $\mathcal{D}$.

With each P_i we associate k_i residue class $\mathcal{R}_{i1}, \ldots, \mathcal{R}_{ik_i}$ modulo P_i. Let $\mathcal{S} = \{A_j \in \mathcal{A} : A_j$ is in none of the classes $\mathcal{R}_{ik}\}$ and $|\mathcal{S}|$ be the number of elements in $\mathcal{S}$.

Let also $\mathcal{D}$ denotes a subset of the divisors of $\prod(\mathcal{P})$. $\mathcal{D}$ is **divisor closed** if $D \in \mathcal{D}$ implies every divisor of D is also in $\mathcal{D}$.

With each P_i we associate k_i residue class $\mathcal{R}_{i1}, \ldots, \mathcal{R}_{ik_i}$ modulo P_i. Let $\mathcal{S} = \{A_j \in \mathcal{A} : A_j \text{ is in none of the classes } \mathcal{R}_{ik}\}$ and $|\mathcal{S}|$ be the number of elements in $\mathcal{S}$.

Let $\sigma(A) = \prod P_i$ where the product is over those P_i for which A is in one of the residue classes $\mathcal{R}_{ik}$, the empty product being 1.

Let also $\mathcal{D}$ denotes a subset of the divisors of $\prod(\mathcal{P})$. $\mathcal{D}$ is **divisor closed** if $D \in \mathcal{D}$ implies every divisor of D is also in $\mathcal{D}$.

With each P_i we associate k_i residue class $\mathcal{R}_{i1}, \ldots, \mathcal{R}_{ik_i}$ modulo P_i. Let $\mathcal{S} = \{A_j \in \mathcal{A} : A_j \text{ is in none of the classes } \mathcal{R}_{ik}\}$ and $|\mathcal{S}|$ be the number of elements in $\mathcal{S}$.

Let $\sigma(A) = \prod P_i$ where the product is over those P_i for which A is in one of the residue classes $\mathcal{R}_{ik}$, the empty product being 1.

Now let f be a multiplicative function defined on the divisors of $\prod(\mathcal{P})$ satisfying

$$1 < f(P) \leq |P| = q^{\deg(P)}, \tag{2.3}$$

Let also $\mathcal{D}$ denotes a subset of the divisors of $\prod(\mathcal{P})$. $\mathcal{D}$ is **divisor closed** if $D \in \mathcal{D}$ implies every divisor of D is also in $\mathcal{D}$.

With each P_i we associate k_i residue class $\mathcal{R}_{i1}, \ldots, \mathcal{R}_{ik_i}$ modulo P_i. Let $\mathcal{S} = \{A_j \in \mathcal{A} : A_j \text{ is in none of the classes } \mathcal{R}_{ik}\}$ and $|\mathcal{S}|$ be the number of elements in $\mathcal{S}$.

Let $\sigma(A) = \prod P_i$ where the product is over those P_i for which A is in one of the residue classes $\mathcal{R}_{ik}$, the empty product being 1.

Now let f be a multiplicative function defined on the divisors of $\prod(\mathcal{P})$ satisfying

$$1 < f(P) \leq |P| = q^{\deg(P)}, \tag{2.3}$$

$$\sum_{\substack{j \\ D|\sigma(A_j)}} 1 = \frac{n}{f(D)} + R_D. \tag{2.4}$$

Let $\mathcal{C}$ denote the class of all functions s representable in the form

$$s(A) = \sum_{D|\sigma(A)} \lambda(D), \tag{2.5}$$

where λ is a real valued function.

Let $\mathcal{C}$ denote the class of all functions s representable in the form

$$s(A) = \sum_{D|\sigma(A)} \lambda(D), \tag{2.5}$$

where λ is a real valued function. The characteristic function of $\mathcal{S}$, $s^{(0)}$, is in $\mathcal{C}$ taking λ to be the Möbius function. Hence,

$$|\mathcal{S}| = \sum_{j=1}^{n} s^{(0)}(A_j) = \sum_{j=1}^{n} \sum_{D|\sigma(A_j)} \mu(D).$$

Let $\mathcal{C}$ denote the class of all functions s representable in the form

$$s(A) = \sum_{D|\sigma(A)} \lambda(D), \tag{2.5}$$

where λ is a real valued function. The characteristic function of $\mathcal{S}$, $s^{(0)}$, is in $\mathcal{C}$ taking λ to be the Möbius function. Hence,

$$|\mathcal{S}| = \sum_{j=1}^{n} s^{(0)}(A_j) = \sum_{j=1}^{n} \sum_{D|\sigma(A_j)} \mu(D).$$

Let $\mathcal{C}^{(+)}$ and $\mathcal{C}^{(-)}$ denote the subclasses of $\mathcal{C}$ whose elements satisfy respectively,

$$s^{(+)}(A) \geq s^{(0)}(A) \qquad \text{with equality if } \sigma(A) = 1, \tag{2.6}$$

Let $\mathcal{C}$ denote the class of all functions s representable in the form

$$s(A) = \sum_{D|\sigma(A)} \lambda(D), \tag{2.5}$$

where λ is a real valued function. The characteristic function of $\mathcal{S}$, $s^{(0)}$, is in $\mathcal{C}$ taking λ to be the Möbius function. Hence,

$$|\mathcal{S}| = \sum_{j=1}^{n} s^{(0)}(A_j) = \sum_{j=1}^{n} \sum_{D|\sigma(A_j)} \mu(D).$$

Let $\mathcal{C}^{(+)}$ and $\mathcal{C}^{(-)}$ denote the subclasses of $\mathcal{C}$ whose elements satisfy respectively,

$$s^{(+)}(A) \geq s^{(0)}(A) \qquad \text{with equality if } \sigma(A) = 1, \tag{2.6}$$

$$s^{(-)}(A) \leq s^{(0)}(A) \qquad \text{with equality if } \sigma(A) = 1. \tag{2.7}$$

Let $\mathcal{C}$ denote the class of all functions s representable in the form

$$s(A) = \sum_{D|\sigma(A)} \lambda(D), \tag{2.5}$$

where λ is a real valued function. The characteristic function of $\mathcal{S}$, $s^{(0)}$, is in $\mathcal{C}$ taking λ to be the Möbius function. Hence,

$$|\mathcal{S}| = \sum_{j=1}^{n} s^{(0)}(A_j) = \sum_{j=1}^{n} \sum_{D|\sigma(A_j)} \mu(D).$$

Let $\mathcal{C}^{(+)}$ and $\mathcal{C}^{(-)}$ denote the subclasses of $\mathcal{C}$ whose elements satisfy respectively,

$$s^{(+)}(A) \geq s^{(0)}(A) \qquad \text{with equality if } \sigma(A) = 1, \tag{2.6}$$

$$s^{(-)}(A) \leq s^{(0)}(A) \qquad \text{with equality if } \sigma(A) = 1. \tag{2.7}$$

$\mathcal{C}$ and $\mathcal{C}^{(+)}$ are closed with respect to multiplication, and $\mathcal{C}^{(-)}$ is not.

Let $\mathcal{C}$ denote the class of all functions s representable in the form

$$s(A) = \sum_{D|\sigma(A)} \lambda(D), \tag{2.5}$$

where λ is a real valued function. The characteristic function of $\mathcal{S}$, $s^{(0)}$, is in $\mathcal{C}$ taking λ to be the Möbius function. Hence,

$$|\mathcal{S}| = \sum_{j=1}^{n} s^{(0)}(A_j) = \sum_{j=1}^{n} \sum_{D|\sigma(A_j)} \mu(D).$$

Let $\mathcal{C}^{(+)}$ and $\mathcal{C}^{(-)}$ denote the subclasses of $\mathcal{C}$ whose elements satisfy respectively,

$$s^{(+)}(A) \geq s^{(0)}(A) \qquad \text{with equality if } \sigma(A) = 1, \tag{2.6}$$

$$s^{(-)}(A) \leq s^{(0)}(A) \qquad \text{with equality if } \sigma(A) = 1. \tag{2.7}$$

$\mathcal{C}$ and $\mathcal{C}^{(+)}$ are closed with respect to multiplication, and $\mathcal{C}^{(-)}$ is not.
If $s_1 \in \mathcal{C}^{(+)}$ and $s_2\mathcal{C}^{(-)}$ then we clearly have

$$\sum_{j=1}^{n} s_2(A_j) \leq \mathcal{C} \leq \sum_{j=1}^{n} s_1(A_j). \tag{2.8}$$

Let $\mathcal{D}$ be a divisor closed subset of $\prod(\mathcal{P})$, and with each $D \in \mathcal{D}$ associate the real variable X_D.

Let $\mathcal{D}$ be a divisor closed subset of $\prod(\mathcal{P})$, and with each $D \in \mathcal{D}$ associate the real variable X_D. Consider all sets of values of

$$X = \{X_D : D \in \mathcal{D}, X_1 = 1\}.$$

Let $\mathcal{D}$ be a divisor closed subset of $\prod(\mathcal{P})$, and with each $D \in \mathcal{D}$ associate the real variable X_D. Consider all sets of values of

$$X = \{X_D : D \in \mathcal{D}, X_1 = 1\}\,.$$

To each set of values X there corresponds a function

$$s_1(A) = \left(\sum_{\substack{D \in \mathcal{D} \\ D \mid \sigma(A)}} X_D \right)^2 . \tag{2.9}$$

Let $\mathcal{D}$ be a divisor closed subset of $\prod(\mathcal{P})$, and with each $D \in \mathcal{D}$ associate the real variable X_D. Consider all sets of values of

$$X = \{X_D : D \in \mathcal{D}, X_1 = 1\}.$$

To each set of values X there corresponds a function

$$s_1(A) = \left(\sum_{\substack{D \in \mathcal{D} \\ D | \sigma(A)}} X_D \right)^2. \tag{2.9}$$

Then $s_1 \in \mathcal{C}^+$ with

$$\lambda_1(D) = \sum_{\substack{D_1, D_2 \in \mathcal{D} \\ \mathrm{lcm}(D_1, D_2) = D}} X_{D_1} X_{D_2},$$

and $\lambda(D) = 0$ outside the set

$$\mathcal{D}^* = \{D : D = \mathrm{lcm}(D_1, D_2); D_1, D_2 \in \mathcal{D}\}. \tag{2.10}$$

Let $\mathcal{D}$ be a divisor closed subset of $\prod(\mathcal{P})$, and with each $D \in \mathcal{D}$ associate the real variable X_D. Consider all sets of values of

$$X = \{X_D : D \in \mathcal{D}, X_1 = 1\}.$$

To each set of values X there corresponds a function

$$s_1(A) = \left(\sum_{\substack{D \in \mathcal{D} \\ D | \sigma(A)}} X_D \right)^2. \tag{2.9}$$

Then $s_1 \in \mathcal{C}^+$ with

$$\lambda_1(D) = \sum_{\substack{D_1, D_2 \in \mathcal{D} \\ \mathrm{lcm}(D_1, D_2) = D}} X_{D_1} X_{D_2},$$

and $\lambda(D) = 0$ outside the set

$$\mathcal{D}^* = \{D : D = \mathrm{lcm}(D_1, D_2); D_1, D_2 \in \mathcal{D}\}. \tag{2.10}$$

Now

$$\begin{aligned} |\mathcal{S}| \quad &\leq \quad \sum_{j=1}^{n} s_1(A_j) = \sum_{D | \prod(\mathcal{P})} \lambda_1(D) \sum_{\substack{j \\ D | \sigma(A_j)}} 1 && (2.11) \\ &\leq \quad n \sum_{D \in \mathcal{D}^*} \frac{\lambda_1(D)}{f(D)} + E, \end{aligned}$$

where

$$E = \sum_{D \in \mathcal{D}^*} |\lambda_1(D) R_D|. \tag{2.12}$$

where

$$E = \sum_{D \in \mathcal{D}^*} |\lambda_1(D) R_D|. \tag{2.12}$$

Define the function g by

$$g(D) = f(D) \prod_{P|D} \left(1 - \frac{1}{f(P)}\right). \tag{2.13}$$

where

$$E = \sum_{D \in \mathcal{D}^*} |\lambda_1(D) R_D|. \tag{2.12}$$

Define the function g by

$$g(D) = f(D) \prod_{P|D} \left(1 - \frac{1}{f(P)}\right). \tag{2.13}$$

We are now ready to estimate $\sum_{D \in \mathcal{D}^*} \lambda_1(D)/f(D)$.

where

$$E = \sum_{D \in \mathcal{D}^*} |\lambda_1(D) R_D|. \tag{2.12}$$

Define the function g by

$$g(D) = f(D) \prod_{P|D} \left(1 - \frac{1}{f(P)}\right). \tag{2.13}$$

We are now ready to estimate $\sum_{D \in \mathcal{D}^*} \lambda_1(D)/f(D)$.

Lema (1)

$$\inf_X \sum_{D \in \mathcal{D}^*} \frac{\lambda_1(D)}{f(D)} = \left(\sum_{D \in \mathcal{D}} \frac{1}{g(D)}\right)^{-1} = Q^{-1} \tag{2.14}$$

where

$$E = \sum_{D \in \mathcal{D}^*} |\lambda_1(D) R_D|. \tag{2.12}$$

Define the function g by

$$g(D) = f(D) \prod_{P|D} \left(1 - \frac{1}{f(P)}\right). \tag{2.13}$$

We are now ready to estimate $\sum_{D \in \mathcal{D}^*} \lambda_1(D)/f(D)$.

Lema (1)

$$\inf_X \sum_{D \in \mathcal{D}^*} \frac{\lambda_1(D)}{f(D)} = \left(\sum_{D \in \mathcal{D}} \frac{1}{g(D)}\right)^{-1} = Q^{-1} \tag{2.14}$$

and this lower bound is attained when

$$X_D = \frac{\mu(D) f(D)}{Q} \sum_{\substack{C \in \mathcal{D} \\ D|C}} \frac{1}{g(C)}. \tag{2.15}$$

Proof of the Lemma

Let

$$Y_C = \sum_{C|D} \frac{X_D}{f(D)},$$

then

$$\sum_{D\in\mathcal{D}^*} \frac{\lambda_1(D)}{f(D)} = \sum_{D\in\mathcal{D}^*} \frac{1}{f(D)} \sum_{\substack{D_1,D_2\in\mathcal{D} \\ \mathrm{lcm}(D_1,D_2)=D}} X_{D_1}X_{D_2}$$

Proof of the Lemma

Let

$$Y_C = \sum_{C|D} \frac{X_D}{f(D)},$$

then

$$\begin{aligned}\sum_{D\in\mathcal{D}^*} \frac{\lambda_1(D)}{f(D)} &= \sum_{D\in\mathcal{D}^*} \frac{1}{f(D)} \sum_{\substack{D_1,D_2\in\mathcal{D}\\ \operatorname{lcm}(D_1,D_2)=D}} X_{D_1}X_{D_2} \\ &= \sum_{D_1,D_2\in\mathcal{D}} \frac{X_{D_1}X_{D_2}}{f(D_1)f(D_2)} \sum_{C|(D_1,D_2)} g(C)\end{aligned}$$

Proof of the Lemma

Let

$$Y_C = \sum_{C|D} \frac{X_D}{f(D)},$$

then

$$\begin{aligned}
\sum_{D\in\mathcal{D}^*} \frac{\lambda_1(D)}{f(D)} &= \sum_{D\in\mathcal{D}^*} \frac{1}{f(D)} \sum_{\substack{D_1,D_2\in\mathcal{D}\\ \mathrm{lcm}(D_1,D_2)=D}} X_{D_1}X_{D_2} \\
&= \sum_{D_1,D_2\in\mathcal{D}} \frac{X_{D_1}X_{D_2}}{f(D_1)f(D_2)} \sum_{C|(D_1,D_2)} g(C) \\
&= \sum_{C\in\mathcal{D}} g(C) \left(\sum_{\substack{C|D\\ D\in\mathcal{D}}} X_D/f(D) \right)^2 = \sum_{C\in\mathcal{D}} g(C) Y_C^2
\end{aligned}$$

Proof of the Lemma

Let

$$Y_C = \sum_{C|D} \frac{X_D}{f(D)},$$

then

$$\begin{aligned}
\sum_{D\in\mathcal{D}*} \frac{\lambda_1(D)}{f(D)} &= \sum_{D\in\mathcal{D}*} \frac{1}{f(D)} \sum_{\substack{D_1,D_2\in\mathcal{D} \\ \mathrm{lcm}(D_1,D_2)=D}} X_{D_1}X_{D_2} \\
&= \sum_{D_1,D_2\in\mathcal{D}} \frac{X_{D_1}X_{D_2}}{f(D_1)f(D_2)} \sum_{C|(D_1,D_2)} g(C) \\
&= \sum_{C\in\mathcal{D}} g(C)\left(\sum_{\substack{C|D \\ D\in\mathcal{D}}} X_D/f(D)\right)^2 = \sum_{C\in\mathcal{D}} g(C)Y_C^2 \\
&= \sum_{C\in\mathcal{D}} \frac{1}{g(C)} \left\{g(C)Y_C - \mu(C)Q^{-1}\right\}^2 + Q^{-1}.
\end{aligned}$$

Proof of the Lemma

Let

$$Y_C = \sum_{C|D} \frac{X_D}{f(D)},$$

then

$$\begin{aligned}
\sum_{D\in\mathcal{D}^*} \frac{\lambda_1(D)}{f(D)} &= \sum_{D\in\mathcal{D}^*} \frac{1}{f(D)} \sum_{\substack{D_1,D_2\in\mathcal{D}\\ \mathrm{lcm}(D_1,D_2)=D}} X_{D_1}X_{D_2} \\
&= \sum_{D_1,D_2\in\mathcal{D}} \frac{X_{D_1}X_{D_2}}{f(D_1)f(D_2)} \sum_{C|(D_1,D_2)} g(C) \\
&= \sum_{C\in\mathcal{D}} g(C)\left(\sum_{\substack{C|D\\ D\in\mathcal{D}}} X_D/f(D)\right)^2 = \sum_{C\in\mathcal{D}} g(C)Y_C^2 \\
&= \sum_{C\in\mathcal{D}} \frac{1}{g(C)} \left\{g(C)Y_C - \mu(C)Q^{-1}\right\}^2 + Q^{-1}.
\end{aligned}$$

The result follows by setting the quantity in braces equal to zero.

We now assume that X is defined as in Equation (2.15), i.e., $X = X_D$. We then have the following form of the function-field Selberg's sieve.

We now assume that X is defined as in Equation (2.15), i.e., $X = X_D$. We then have the following form of the function-field Selberg's sieve.

Theorem (Selberg's sieve)

$$|\mathcal{S}| \leq \frac{n}{Q} + \sum_{D_1, D_2 \in \mathcal{D}} |X_{D_1} X_{D_2} R_{[D_1, D_2]}|, \tag{2.16}$$

where [] denotes the lcm.

We now assume that X is defined as in Equation (2.15), i.e., $X = X_D$. We then have the following form of the function-field Selberg's sieve.

Theorem (Selberg's sieve)

$$|\mathcal{S}| \leq \frac{n}{Q} + \sum_{D_1, D_2 \in \mathcal{D}} |X_{D_1} X_{D_2} R_{[D_1, D_2]}|, \tag{2.16}$$

where [] denotes the lcm.

Proof.

By Lemma 1 and the previous estimate on $|\mathcal{S}|$ (2.11) we have

$$|\mathcal{S}| \leq \frac{n}{Q} + E,$$

where

$$E = \sum_{D \in \mathcal{D}*} |\lambda_1(D) R_D| = \sum_{D \in \mathcal{D}*} \left| \sum_{\substack{D_1, D_2 \in \mathcal{D} \\ [D_1, D_2] = D}} X_{D_1} X_{D_2} R_D \right|$$

We now assume that X is defined as in Equation (2.15), i.e., $X = X_D$. We then have the following form of the function-field Selberg's sieve.

Theorem (Selberg's sieve)

$$|\mathcal{S}| \leq \frac{n}{Q} + \sum_{D_1, D_2 \in \mathcal{D}} |X_{D_1} X_{D_2} R_{[D_1, D_2]}|, \tag{2.16}$$

where [] denotes the lcm.

Proof.

By Lemma 1 and the previous estimate on $|\mathcal{S}|$ (2.11) we have

$$|\mathcal{S}| \leq \frac{n}{Q} + E,$$

where

$$\begin{aligned} E &= \sum_{D \in \mathcal{D}^*} |\lambda_1(D) R_D| = \sum_{D \in \mathcal{D}^*} \left| \sum_{\substack{D_1, D_2 \in \mathcal{D} \\ [D_1, D_2] = D}} X_{D_1} X_{D_2} R_D \right| \\ &\leq \sum_{D_1, D_2 \in \mathcal{D}} |X_{D_1} X_{D_2} R_{[D_1, D_2]}| \end{aligned}$$

which proves the theorem. $\square$

Similarly we can prove the following version of Selberg's lower bound sieve.

Similarly we can prove the following version of Selberg's lower bound sieve.

Let $\mathcal{D}_i$ denote a divisor closed subset of $\prod_{j=1}^{i-1} P_i$.

Similarly we can prove the following version of Selberg's lower bound sieve.

Let $\mathcal{D}_i$ denote a divisor closed subset of $\prod_{j=1}^{i-1} P_i$.

Now define Q_i and $X^{(i)}$ by (2.14) and (2.15) using $\mathcal{D}_i$ instead of $\mathcal{D}$. We then have

Similarly we can prove the following version of Selberg's lower bound sieve.

Let $\mathcal{D}_i$ denote a divisor closed subset of $\prod_{j=1}^{i-1} P_i$.

Now define Q_i and $X^{(i)}$ by (2.14) and (2.15) using $\mathcal{D}_i$ instead of $\mathcal{D}$. We then have

Theorem

$$|\mathcal{S}| \geq n\left(1 - \sum_{i=1}^{r} \frac{1}{f(P_i)Q_i}\right) - \sum_{i=1}^{r} \sum_{D_1, D_2 \in \mathcal{D}_i} |X_{D_1}^{(i)} X_{D_2}^{(i)} R_{P_i[D_1, D_2]}|. \tag{2.17}$$

Applications of Selberg's Sieve

Let $\pi(m, K, L)$ denote the number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree m which are congruent to L modulo K. We assume $(L, K) = 1$, $\deg K = k < m$ and $\deg L < k$. L need not be monic.

Applications of Selberg's Sieve

Let $\pi(m, K, L)$ denote the number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree m which are congruent to L modulo K. We assume $(L, K) = 1$, $\deg K = k < m$ and $\deg L < k$. L need not be monic.

We take

$$\mathcal{A} = \{L + AK : \deg A = m - k\}$$

Applications of Selberg's Sieve

Let $\pi(m, K, L)$ denote the number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree m which are congruent to L modulo K. We assume $(L, K) = 1$, $\deg K = k < m$ and $\deg L < k$. L need not be monic.

We take
$$\mathcal{A} = \{L + AK : \deg A = m - k\}$$
and
$$\mathcal{P} = \left\{P : \deg P \leq \left[\frac{m}{2}\right], P \nmid K\right\}$$
so $\mathcal{P}$ contains only irreducible polynomials.

Applications of Selberg's Sieve

Let $\pi(m, K, L)$ denote the number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree m which are congruent to L modulo K. We assume $(L, K) = 1$, $\deg K = k < m$ and $\deg L < k$. L need not be monic.

We take

$$\mathcal{A} = \{L + AK : \deg A = m - k\}$$

and

$$\mathcal{P} = \left\{P : \deg P \leq \left[\frac{m}{2}\right], P \nmid K\right\}$$

so $\mathcal{P}$ contains only irreducible polynomials. Also, take $f(D) = |D|$. It is easily checked that $|R_D| \leq 1$.

Applications of Selberg's Sieve

Let $\pi(m, K, L)$ denote the number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree m which are congruent to L modulo K. We assume $(L, K) = 1$, $\deg K = k < m$ and $\deg L < k$. L need not be monic.

We take

$$\mathcal{A} = \{L + AK : \deg A = m - k\}$$

and

$$\mathcal{P} = \left\{P : \deg P \leq \left[\frac{m}{2}\right], P \nmid K\right\}$$

so $\mathcal{P}$ contains only irreducible polynomials. Also, take $f(D) = |D|$. It is easily checked that $|R_D| \leq 1$.

The set $\mathcal{D}$ is defined by

$$\mathcal{D} = \left\{D : D \mid \prod(\mathcal{P}) \text{ and } |D| \leq q^{(m-k)/4}\right\}.$$

With $\mathcal{D}$ thus defined,

$$Q = \sum_{D \in \mathcal{D}} \frac{1}{g(D)} > \sum_{D \in \mathcal{D}} \frac{1}{|D|} \geq c_1 \prod_{\substack{P \in \mathcal{P} \\ \deg P \leq (m-k)/4}} \left(1 - \frac{1}{|P|}\right)^{-1}$$

With $\mathcal{D}$ thus defined,

$$\begin{aligned} Q &= \sum_{D\in\mathcal{D}} \frac{1}{g(D)} > \sum_{D\in\mathcal{D}} \frac{1}{|D|} \geq c_1 \prod_{\substack{P\in\mathcal{P} \\ \deg P\leq(m-k)/4}} \left(1-\frac{1}{|P|}\right)^{-1} \\ &\geq c_2 \prod_{\deg P\leq(m-k)/4} \left(1-\frac{1}{|P|}\right)^{-1} \frac{\Phi(K)}{|K|} \geq c_3 \frac{\Phi(K)}{|K|}(m-k), \end{aligned}$$

where c_i are constants, and $\Phi(K)$ is Euler's Φ function defined for $\mathbb{F}_q[x]$.

With $\mathcal{D}$ thus defined,

$$\begin{aligned} Q &= \sum_{D\in\mathcal{D}} \frac{1}{g(D)} > \sum_{D\in\mathcal{D}} \frac{1}{|D|} \geq c_1 \prod_{\substack{P\in\mathcal{P} \\ \deg P\leq (m-k)/4}} \left(1-\frac{1}{|P|}\right)^{-1} \\ &\geq c_2 \prod_{\deg P\leq (m-k)/4} \left(1-\frac{1}{|P|}\right)^{-1} \frac{\Phi(K)}{|K|} \geq c_3 \frac{\Phi(K)}{|K|}(m-k), \end{aligned}$$

where c_i are constants, and $\Phi(K)$ is Euler's Φ function defined for $\mathbb{F}_q[x]$.

Also the error term is quite small, $E = O(m^2 q^{(m-k)/2})$.

With $\mathcal{D}$ thus defined,

$$\begin{aligned}
Q &= \sum_{D \in \mathcal{D}} \frac{1}{g(D)} > \sum_{D \in \mathcal{D}} \frac{1}{|D|} \geq c_1 \prod_{\substack{P \in \mathcal{P} \\ \deg P \leq (m-k)/4}} \left(1 - \frac{1}{|P|}\right)^{-1} \\
&\geq c_2 \prod_{\deg P \leq (m-k)/4} \left(1 - \frac{1}{|P|}\right)^{-1} \frac{\Phi(K)}{|K|} \geq c_3 \frac{\Phi(K)}{|K|}(m-k),
\end{aligned}$$

where c_i are constants, and $\Phi(K)$ is Euler's Φ function defined for $\mathbb{F}_q[x]$.

Also the error term is quite small, $E = O(m^2 q^{(m-k)/2})$.

The previous estimates are obtained by using variations of the standard techniques used on similar expressions involving the rational integers.

Thus by Selberg's sieve theorem we have

Theorem

$$\pi(m, K, L) = |\mathcal{S}| \leq c\frac{q^{m-k}|K|}{\Phi(K)(m-k)} = c\frac{q^m}{\Phi(K)(m-k)}.$$

Thus by Selberg's sieve theorem we have

Theorem

$$\pi(m, K, L) = |\mathcal{S}| \leq c\frac{q^{m-k}|K|}{\Phi(K)(m-k)} = c\frac{q^m}{\Phi(K)(m-k)}.$$

This result is not as powerful as the "prime number theorem" for $\mathbb{F}_q[x]$ when degree of K is small. This is particularly true since the Riemann hypothesis is known to be true. But the above theorem is still effective when k is almost as large as m, and of course is essentially elementary.

Brun's theorem

Let K be a fixed polynomial, not necessarily monic and let $\mathcal{N}(n, K)$ be the number of monic irreducibles polynomials P of degree $\leq n$, such that $P + K$ is also irreducibe.

Brun's theorem

Let K be a fixed polynomial, not necessarily monic and let $\mathcal{N}(n, K)$ be the number of monic irreducibles polynomials P of degree $\leq n$, such that $P + K$ is also irreducibe.
We take $n > \deg K$. Letting

$$\mathcal{A} = \{A(A+K) : \deg A \leq n\},$$

$$\mathcal{P} = \left\{P : \deg P \leq \frac{n}{2}, P \nmid K\right\}$$

and $f(D) = |D|/\alpha(D)$ where $\alpha(D)$ is the number of solutions of $A(A+K) \equiv 0 (\bmod\ D)$.

Brun's theorem

Let K be a fixed polynomial, not necessarily monic and let $\mathcal{N}(n, K)$ be the number of monic irreducibles polynomials P of degree $\leq n$, such that $P + K$ is also irreducibe.
We take $n > \deg K$. Letting

$$\mathcal{A} = \{A(A+K) : \deg A \leq n\},$$

$$\mathcal{P} = \left\{P : \deg P \leq \frac{n}{2}, P \nmid K\right\}$$

and $f(D) = |D|/\alpha(D)$ where $\alpha(D)$ is the number of solutions of $A(A+K) \equiv 0 (\bmod\ D)$. Clearly $\alpha(D) = 2^{\omega(D)}$, where $\omega(D)$ denotes the number of distinct irreducibles dividing D, for $D \mid \prod(\mathcal{P})$.

Brun's theorem

Let K be a fixed polynomial, not necessarily monic and let $\mathcal{N}(n, K)$ be the number of monic irreducibles polynomials P of degree $\leq n$, such that $P + K$ is also irreducibe.

We take $n > \deg K$. Letting

$$\mathcal{A} = \{A(A+K) : \deg A \leq n\},$$

$$\mathcal{P} = \left\{P : \deg P \leq \frac{n}{2}, P \nmid K\right\}$$

and $f(D) = |D|/\alpha(D)$ where $\alpha(D)$ is the number of solutions of $A(A+K) \equiv 0 \pmod{D}$. Clearly $\alpha(D) = 2^{\omega(D)}$, where $\omega(D)$ denotes the number of distinct irreducibles dividing D, for $D \mid \prod(\mathcal{P})$. We find by routine calculation that

$$|R_D| \leq \frac{|D|}{f(D)}.$$

Brun's theorem

Let K be a fixed polynomial, not necessarily monic and let $\mathcal{N}(n, K)$ be the number of monic irreducibles polynomials P of degree $\leq n$, such that $P + K$ is also irreducibe.
We take $n > \deg K$. Letting

$$\mathcal{A} = \{A(A+K) : \deg A \leq n\},$$

$$\mathcal{P} = \left\{P : \deg P \leq \frac{n}{2}, P \nmid K\right\}$$

and $f(D) = |D|/\alpha(D)$ where $\alpha(D)$ is the number of solutions of $A(A+K) \equiv 0 (\bmod\ D)$. Clearly $\alpha(D) = 2^{\omega(D)}$, where $\omega(D)$ denotes the number of distinct irreducibles dividing D, for $D \mid \prod(\mathcal{P})$. We find by routine calculation that

$$|R_D| \leq \frac{|D|}{f(D)}.$$

Letting $\mathcal{D} = \left\{D : D \mid \prod(\mathcal{P}) \text{ and } |D| \leq N^{1/4}\right\}$ where $N = |\mathcal{A}| = (q^{n+1} - q)/(q-1)$, and applying the Selberg's sieve theorem we have

$$|\mathcal{S}| \leq \frac{N}{Q} + N^{1/2} \prod_{P \in \mathcal{P}} \left(1 - \frac{1}{f(P)}\right)^{-2}. \tag{2.18}$$

Now

$$Q = \sum_{D \in \mathcal{D}} \frac{1}{g(D)} \geq \sum_{D \in \mathcal{D}} \frac{\alpha(D)}{|D|} = \sum_{\substack{|D| \leq N^{1/4} \\ (D,K)=1}} \frac{2^{\omega(D)}}{|D|}$$

Now

$$
\begin{aligned}
Q &= \sum_{D \in \mathcal{D}} \frac{1}{g(D)} \geq \sum_{D \in \mathcal{D}} \frac{\alpha(D)}{|D|} = \sum_{\substack{|D| \leq N^{1/4} \\ (D,K)=1}} \frac{2^{\omega(D)}}{|D|} \\
&\geq c_1 \sum_{\substack{|P| \leq N^{1/4} \\ P \nmid K}} \left(1 - \frac{2}{|P|}\right)^{-1} \geq c_2 \log^2 N
\end{aligned}
$$

where c_2 depends on K.

Now

$$
\begin{aligned}
Q &= \sum_{D\in\mathcal{D}} \frac{1}{g(D)} \geq \sum_{D\in\mathcal{D}} \frac{\alpha(D)}{|D|} = \sum_{\substack{|D|\leq N^{1/4}\\(D,K)=1}} \frac{2^{\omega(D)}}{|D|} \\
&\geq c_1 \sum_{\substack{|P|\leq N^{1/4}\\P\nmid K}} \left(1-\frac{2}{|P|}\right)^{-1} \geq c_2 \log^2 N
\end{aligned}
$$

where c_2 depends on K. Since $\prod_{P\in\mathcal{P}}(1-1/f(P))^{-2} \leq \log^4 N$, from (2.18) we obtain

$$
|\mathcal{S}| \leq c_3 \frac{N}{\log^2 N}. \tag{2.19}
$$

Now $\mathcal{S}$ contains irreducibles P such that $P + K$ is also irreducible and $n/2 < \deg P \leq n$.

Now $\mathcal{S}$ contains irreducibles P such that $P+K$ is also irreducible and $n/2 < \deg P \leq n$. Thus

$$\mathcal{N}(n,K) = |\mathcal{S}| + \#\{P \text{ irreducible} : P+K \text{ irreducible}, \deg P \leq n/2\}$$

.

Now $\mathcal{S}$ contains irreducibles P such that $P+K$ is also irreducible and $n/2 < \deg P \leq n$. Thus

$$\mathcal{N}(n,K) = |\mathcal{S}| + \#\left\{P \text{ irreducible} : P+K \text{ irreducible}, \deg P \leq n/2\right\}$$

.

Hence by (2.19) we have

$$\mathcal{N}(n,K) \leq c_3 \frac{N}{\log^2 N} + c_4 q^{n/2} \leq c_5 \frac{N}{\log^2 N}.$$

Now $\mathcal{S}$ contains irreducibles P such that $P+K$ is also irreducible and $n/2 < \deg P \leq n$. Thus

$$\mathcal{N}(n,K) = |\mathcal{S}| + \#\left\{P \text{ irreducible} : P+K \text{ irreducible}, \deg P \leq n/2\right\}$$

.

Hence by (2.19) we have

$$\mathcal{N}(n,K) \leq c_3 \frac{N}{\log^2 N} + c_4 q^{n/2} \leq c_5 \frac{N}{\log^2 N}.$$

Thus we have proved

Theorem

If $\mathcal{N}(n,K)$ is the number of monic irreducibles polynomials P of degree $\leq n$ such that $P+K$ is also irreducible, then

$$\mathcal{N}(n,K) \leq c \frac{q^n}{n^2}. \tag{2.20}$$

Now $\mathcal{S}$ contains irreducibles P such that $P+K$ is also irreducible and $n/2 < \deg P \leq n$. Thus

$$\mathcal{N}(n,K) = |\mathcal{S}| + \#\{P \text{ irreducible} : P+K \text{ irreducible}, \deg P \leq n/2\}$$

.
Hence by (2.19) we have

$$\mathcal{N}(n,K) \leq c_3 \frac{N}{\log^2 N} + c_4 q^{n/2} \leq c_5 \frac{N}{\log^2 N}.$$

Thus we have proved

Theorem

If $\mathcal{N}(n,K)$ is the number of monic irreducibles polynomials P of degree $\leq n$ such that $P+K$ is also irreducible, then

$$\mathcal{N}(n,K) \leq c \frac{q^n}{n^2}. \tag{2.20}$$

Corollary

$\sum 1/|P|$ converges, where the summation is over all monic irreducibles P such that $P+K$ is also irreducible.