Analytic Number Theory in Function Fields (Lecture 1)

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

1. Introduction

2. Polynomials over Finite Fields
   - Euler's ϕ-function and the little theorems of Euler and Fermat
   - Dictionary between A and $\mathbb{Z}$

3. Primes, Arithmetic Functions and the Zeta Function
   - Arithmetic Functions

What is this course about?

Introduction

What is this course about?

We will study some classical analytic number theory problems and techniques in the context of polynomials over finite fields.

Introduction

What is this course about?

We will study some classical analytic number theory problems and techniques in the context of polynomials over finite fields.

- Elementary number theory is concerned with arithmetic properties of $\mathbb{Z}$ and its field of fractions $\mathbb{Q}$.

Introduction

What is this course about?

We will study some classical analytic number theory problems and techniques in the context of polynomials over finite fields.

- Elementary number theory is concerned with arithmetic properties of $\mathbb{Z}$ and its field of fractions $\mathbb{Q}$.
- Early on the development of the subject it was noticed that $\mathbb{Z}$ has many properties in common with $A = \mathbb{F}_q[T]$, the ring of polynomials over a finite field.

Introduction

What is this course about?

We will study some classical analytic number theory problems and techniques in the context of polynomials over finite fields.

- Elementary number theory is concerned with arithmetic properties of $\mathbb{Z}$ and its field of fractions $\mathbb{Q}$.
- Early on the development of the subject it was noticed that $\mathbb{Z}$ has many properties in common with $A = \mathbb{F}_q[T]$, the ring of polynomials over a finite field.
    - both rings are principal ideal domains.

Introduction

What is this course about?

We will study some classical analytic number theory problems and techniques in the context of polynomials over finite fields.

- Elementary number theory is concerned with arithmetic properties of $\mathbb{Z}$ and its field of fractions $\mathbb{Q}$.
- Early on the development of the subject it was noticed that $\mathbb{Z}$ has many properties in common with $A = \mathbb{F}_q[T]$, the ring of polynomials over a finite field.
  - both rings are principal ideal domains.
  - both have the property that the residue class ring of any non-zero ideal is finite.

Introduction

What is this course about?

We will study some classical analytic number theory problems and techniques in the context of polynomials over finite fields.

- Elementary number theory is concerned with arithmetic properties of $\mathbb{Z}$ and its field of fractions $\mathbb{Q}$.
- Early on the development of the subject it was noticed that $\mathbb{Z}$ has many properties in common with $A = \mathbb{F}_q[T]$, the ring of polynomials over a finite field.
  - both rings are principal ideal domains.
  - both have the property that the residue class ring of any non-zero ideal is finite.
  - both rings have infinitely many prime elements.

Introduction

What is this course about?

We will study some classical analytic number theory problems and techniques in the context of polynomials over finite fields.

- Elementary number theory is concerned with arithmetic properties of $\mathbb{Z}$ and its field of fractions $\mathbb{Q}$.
- Early on the development of the subject it was noticed that $\mathbb{Z}$ has many properties in common with $A = \mathbb{F}_q[T]$, the ring of polynomials over a finite field.
  - both rings are principal ideal domains.
  - both have the property that the residue class ring of any non-zero ideal is finite.
  - both rings have infinitely many prime elements.
  - both rings have finitely many units.

Introduction

What is this course about?

We will study some classical analytic number theory problems and techniques in the context of polynomials over finite fields.

- Elementary number theory is concerned with arithmetic properties of $\mathbb{Z}$ and its field of fractions $\mathbb{Q}$.
- Early on the development of the subject it was noticed that $\mathbb{Z}$ has many properties in common with $A = \mathbb{F}_q[T]$, the ring of polynomials over a finite field.
  - both rings are principal ideal domains.
  - both have the property that the residue class ring of any non-zero ideal is finite.
  - both rings have infinitely many prime elements.
  - both rings have finitely many units.
  - ...

Introduction

What is this course about?

We will study some classical analytic number theory problems and techniques in the context of polynomials over finite fields.

- Elementary number theory is concerned with arithmetic properties of $\mathbb{Z}$ and its field of fractions $\mathbb{Q}$.
- Early on the development of the subject it was noticed that $\mathbb{Z}$ has many properties in common with $A = \mathbb{F}_q[T]$, the ring of polynomials over a finite field.
  - both rings are principal ideal domains.
  - both have the property that the residue class ring of any non-zero ideal is finite.
  - both rings have infinitely many prime elements.
  - both rings have finitely many units.
  - ...
- Thus, one is led to suspect that many results which hold for $\mathbb{Z}$ have analogues of the ring A.

Introduction

What is this course about?

We will study some classical analytic number theory problems and techniques in the context of polynomials over finite fields.

- Elementary number theory is concerned with arithmetic properties of $\mathbb{Z}$ and its field of fractions $\mathbb{Q}$.
- Early on the development of the subject it was noticed that $\mathbb{Z}$ has many properties in common with $A = \mathbb{F}_q[T]$, the ring of polynomials over a finite field.
  - both rings are principal ideal domains.
  - both have the property that the residue class ring of any non-zero ideal is finite.
  - both rings have infinitely many prime elements.
  - both rings have finitely many units.
  - ...
- Thus, one is led to suspect that many results which hold for $\mathbb{Z}$ have analogues of the ring A. This is indeed the case.

Function Fields

Algebraic number theory arises from elementary number theory by considering finite algebraic extensions K of $\mathbb{Q}$, which are called *algebraic number fields*, and investigating properties of the ring of *algebraic integers* $\mathcal{O}_K \subset K$, defined as the integral closure of $\mathbb{Z}$ in K.

Function Fields

Algebraic number theory arises from elementary number theory by considering finite algebraic extensions K of $\mathbb{Q}$, which are called *algebraic number fields*, and investigating properties of the ring of *algebraic integers* $\mathcal{O}_K \subset K$, defined as the integral closure of $\mathbb{Z}$ in K.

Similarly, we can consider $k = \mathbb{F}_q(T)$, the quotient field of A and finite algebraic exstensions L of k. Fields of this type are called *algebraic function fields*. More precisely, an algebraic function field with a finite constant field is called a *global function field*. A global function field is the true analogue of algebraic number field and much of this course will be concerned with investigating properties of global function fields.

Function Fields

Algebraic number theory arises from elementary number theory by considering finite algebraic extensions K of $\mathbb{Q}$, which are called *algebraic number fields*, and investigating properties of the ring of *algebraic integers* $\mathcal{O}_K \subset K$, defined as the integral closure of $\mathbb{Z}$ in K.

Similarly, we can consider $k = \mathbb{F}_q(T)$, the quotient field of A and finite algebraic exstensions L of k. Fields of this type are called *algebraic function fields*. More precisely, an algebraic function field with a finite constant field is called a *global function field*. A global function field is the true analogue of algebraic number field and much of this course will be concerned with investigating properties of global function fields.

The main aim of the course is to study number theory over $A = \mathbb{F}_q[T]$ and $k = \mathbb{F}_q(T)$.

The Plan for the Course

The plan for the course is the following one: (subject to change)

The Plan for the Course

The plan for the course is the following one: (subject to change)

1. Lecture 1 (01/05/2015):
   - Analogies between function fields and number fields.
   - Polynomials over finite fields.
   - Primes and zeta function for $A = \mathbb{F}_q[T]$.
   - Prime Number Theorem for Polynomials.
   - Arithmetic Functions

The Plan for the Course

The plan for the course is the following one: (subject to change)

1. Lecture 1 (01/05/2015):
   - Analogies between function fields and number fields.
   - Polynomials over finite fields.
   - Primes and zeta function for $A = \mathbb{F}_q[T]$.
   - Prime Number Theorem for Polynomials.
   - Arithmetic Functions
2. Lecture 2 (11/05/2015):
   - Arithmetic Functions and Dirichlet Multiplication for $\mathbb{F}_q[T]$.
   - Averages of Arithmetical Functions.
   - Congruences and Reciprocity Law.
   - Dirichlet Characters and L-series for $\mathbb{F}_q(T)$.
   - Dirichlet's Theorem on Primes in Arithmetic Progression in $\mathbb{F}_q[T]$.

The Plan for the Course

3 Lecture 3 (15/05/2015):

- Foundations of the Theory of Algebraic Function Fields and Global Function Fields.

The Plan for the Course

3 Lecture 3 (15/05/2015):

- Foundations of the Theory of Algebraic Function Fields and Global Function Fields.

4 Lecture 4 (22/05/2015):

- Average Value Theorems in Function Fields.
- Tauberian Theorems.
- Some Sieve Methods in Function Fields.

The Plan for the Course

3 Lecture 3 (15/05/2015):
- Foundations of the Theory of Algebraic Function Fields and Global Function Fields.

4 Lecture 4 (22/05/2015):
- Average Value Theorems in Function Fields.
- Tauberian Theorems.
- Some Sieve Methods in Function Fields.

5 Lecture 5 (29/05/2015):
- Selberg's Theorem in Function Fields.
- An Introduction to Katz-Sarnak Philosophy and RMT.
- Traces of the Frobenius class in the hyperelliptic ensemble.

The Plan for the Course

3 Lecture 3 (15/05/2015):
- Foundations of the Theory of Algebraic Function Fields and Global Function Fields.

4 Lecture 4 (22/05/2015):
- Average Value Theorems in Function Fields.
- Tauberian Theorems.
- Some Sieve Methods in Function Fields.

5 Lecture 5 (29/05/2015):
- Selberg's Theorem in Function Fields.
- An Introduction to Katz-Sarnak Philosophy and RMT.
- Traces of the Frobenius class in the hyperelliptic ensemble.

6 Lecture 6 (01/06/2015):
- Moments of L-functions in Function Fields.
- Ratios Conjecture and statistics of zeros of L-functions over $\mathbb{F}_q(T)$.

The Plan for the Course

7 Lecture 7 (05/06/2015):

- Revisiting Mean Values of Arithmetic Functions in $\mathbb{F}_q[T]$.
- Equidistribution theorems, arithmetic statistics and matrix integrals.

The Plan for the Course

7 Lecture 7 (05/06/2015):

- Revisiting Mean Values of Arithmetic Functions in $\mathbb{F}_q[T]$.
- Equidistribution theorems, arithmetic statistics and matrix integrals.

8 Lecture 8 (11/06/2015):

- Overview of a proof of the Function Field Riemann Hypothesis.
- New directions and problems.

The Plan for the Course

7 Lecture 7 (05/06/2015):
- Revisiting Mean Values of Arithmetic Functions in $\mathbb{F}_q[T]$.
- Equidistribution theorems, arithmetic statistics and matrix integrals.

8 Lecture 8 (11/06/2015):
- Overview of a proof of the Function Field Riemann Hypothesis.
- New directions and problems.

Assessment: At the end of the course, participants will choose from a list of topics/original research articles and should write up an exposition of the chosen result. This exposition should place the result in the context of what has been discussed in the course, and should be detailed for other course participants to be able to follow the main steps of the argument.
Problem Sheets: The completion of the weekly problem sheets is optional but strongly encouraged.

Polynomials over Finite Fields

Let $\mathbb{F}_q$ denote a *finite field* with q elements.

Polynomials over Finite Fields

Let $\mathbb{F}_q$ denote a *finite field* with q elements. The model for such a field is $\mathbb{Z}/p\mathbb{Z}$, where p is a prime number. This field has p elements.

Polynomials over Finite Fields

Let $\mathbb{F}_q$ denote a *finite field* with q elements. The model for such a field is $\mathbb{Z}/p\mathbb{Z}$, where p is a prime number. This field has p elements. In general the number of elements in a finite field is a power of a prime, $q = p^a$. Of course, p is the *characteristic* of $\mathbb{F}_q$.

Polynomials over Finite Fields

Let $\mathbb{F}_q$ denote a *finite field* with q elements. The model for such a field is $\mathbb{Z}/p\mathbb{Z}$, where p is a prime number. This field has p elements. In general the number of elements in a finite field is a power of a prime, $q = p^a$. Of course, p is the *characteristic* of $\mathbb{F}_q$. Let $A = \mathbb{F}_q[T]$ be the polynomial ring over $\mathbb{F}_q$. Let $f \in A$, i.e.,

$$f(T) = \alpha_0 T^n + \alpha_1 T^{n-1} + \cdots + \alpha_1 T + \alpha_n,$$

with $\alpha_i \in \mathbb{F}_q$.

Polynomials over Finite Fields

Let $\mathbb{F}_q$ denote a *finite field* with q elements. The model for such a field is $\mathbb{Z}/p\mathbb{Z}$, where p is a prime number. This field has p elements. In general the number of elements in a finite field is a power of a prime, $q = p^a$. Of course, p is the *characteristic* of $\mathbb{F}_q$. Let $A = \mathbb{F}_q[T]$ be the polynomial ring over $\mathbb{F}_q$. Let $f \in A$, i.e.,

$$f(T) = \alpha_0 T^n + \alpha_1 T^{n-1} + \cdots + \alpha_1 T + \alpha_n,$$

with $\alpha_i \in \mathbb{F}_q$.

Definition

*If $\alpha_0 \neq 0$ we say that f has **degree** n, notationally $\deg(f) = n$. In this case we set $\mathrm{sgn}(f) = \alpha_0$ and call this element of $\mathbb{F}_q^*$ the **sign** of f.*

If f and g are non-zero polynomials in A we have

- $\deg(fg) = \deg(f) + \deg(g)$.

If f and g are non-zero polynomials in A we have

- $\deg(fg) = \deg(f) + \deg(g)$.
- $\mathrm{sgn}(fg) = \mathrm{sgn}(f)\mathrm{sgn}(g)$.

If f and g are non-zero polynomials in A we have

- $\deg(fg) = \deg(f) + \deg(g)$.
- $\operatorname{sgn}(fg) = \operatorname{sgn}(f)\operatorname{sgn}(g)$.
- $\deg(f + g) \leq \max(\deg(f), \deg(g))$.
  (equality holds if $\deg(f) \neq \deg(g)$).

If f and g are non-zero polynomials in A we have

- $\deg(fg) = \deg(f) + \deg(g)$.
- $\mathrm{sgn}(fg) = \mathrm{sgn}(f)\mathrm{sgn}(g)$.
- $\deg(f+g) \leq \max(\deg(f), \deg(g))$.
  (equality holds if $\deg(f) \neq \deg(g)$).

Definition

*If $\mathrm{sgn}(f) = 1$ we say that f is a **monic polynomial**.*

If f and g are non-zero polynomials in A we have

- $\deg(fg) = \deg(f) + \deg(g)$.
- $\mathrm{sgn}(fg) = \mathrm{sgn}(f)\mathrm{sgn}(g)$.
- $\deg(f+g) \leq \max(\deg(f), \deg(g))$.
  (equality holds if $\deg(f) \neq \deg(g)$).

Definition

*If $\mathrm{sgn}(f) = 1$ we say that f is a **monic polynomial**.*

Monic polynomials play the role of positive integers.

If f and g are non-zero polynomials in A we have

- $\deg(fg) = \deg(f) + \deg(g)$.
- $\mathrm{sgn}(fg) = \mathrm{sgn}(f)\mathrm{sgn}(g)$.
- $\deg(f+g) \leq \max(\deg(f), \deg(g))$.
  (equality holds if $\deg(f) \neq \deg(g)$).

Definition

*If $\mathrm{sgn}(f) = 1$ we say that f is a **monic polynomial**.*

Monic polynomials play the role of positive integers.
It is sometimes useful to define the sign of the zero polynomial to be 0 and its degree $-\infty$.

A is an unique factorization domain

Proposition (1.1)

Let $f, g \in A$ with $g \neq 0$. Then there exist elements $q, r \in A$ such that $f = qg + r$ and r is either 0 or $\deg(r) < \deg(g)$. Moreover, q and r are uniquely determined by these conditions.

Proof.

Let $n = \deg(f)$, $m = \deg(g)$, $\alpha = \operatorname{sgn}(f)$, $\beta = \operatorname{sgn}(g)$.

A is an unique factorization domain

Proposition (1.1)

Let $f, g \in A$ with $g \neq 0$. Then there exist elements $q, r \in A$ such that $f = qg + r$ and r is either 0 or $deg(r) < deg(g)$. Moreover, q and r are uniquely determined by these conditions.

Proof.

Let $n = \deg(f)$, $m = \deg(g)$, $\alpha = \mathrm{sgn}(f)$, $\beta = \mathrm{sgn}(g)$. We give the proof by induction on $n = \deg(f)$. If $n < m$, set $q = 0$ and $r = f$. If $n \geq m$, we note that $f_1 = f - \alpha\beta^{-1} T^{n-m} g$ has smaller degree than f. By induction, there exist $q_1, r_1 \in A$ such that $f_1 = q_1 g + r_1$ with r_1 being either 0 or with degree less than $\deg(g)$. In this case, set $q = \alpha\beta^{-1} T^{n-m} + q_1$ and $r = r_1$ and we are done.

A is an unique factorization domain

Proposition (1.1)

Let $f, g \in A$ with $g \neq 0$. Then there exist elements $q, r \in A$ such that $f = qg + r$ and r is either 0 or $deg(r) < deg(g)$. Moreover, q and r are uniquely determined by these conditions.

Proof.

Let $n = \deg(f)$, $m = \deg(g)$, $\alpha = \text{sgn}(f)$, $\beta = \text{sgn}(g)$. We give the proof by induction on $n = \deg(f)$. If $n < m$, set $q = 0$ and $r = f$. If $n \geq m$, we note that $f_1 = f - \alpha\beta^{-1}T^{n-m}g$ has smaller degree than f. By induction, there exist $q_1, r_1 \in A$ such that $f_1 = q_1 g + r_1$ with r_1 being either 0 or with degree less than $\deg(g)$. In this case, set $q = \alpha\beta^{-1}T^{n-m} + q_1$ and $r = r_1$ and we are done.
If $f = qg + r = q^{'}g + r^{'}$, then g divides $r - r^{'}$ and by degree considerations we see $r = r^{'}$. In this case, $qg = q^{'}g$ so $q = q^{'}$ and the uniqueness is established. □

A is an unique factorization domain

Proposition (1.1)

Let $f, g \in A$ with $g \neq 0$. Then there exist elements $q, r \in A$ such that $f = qg + r$ and r is either 0 or $deg(r) < deg(g)$. Moreover, q and r are uniquely determined by these conditions.

Proof.

Let $n = \deg(f)$, $m = \deg(g)$, $\alpha = \text{sgn}(f)$, $\beta = \text{sgn}(g)$. We give the proof by induction on $n = \deg(f)$. If $n < m$, set $q = 0$ and $r = f$. If $n \geq m$, we note that $f_1 = f - \alpha\beta^{-1}T^{n-m}g$ has smaller degree than f. By induction, there exist $q_1, r_1 \in A$ such that $f_1 = q_1 g + r_1$ with r_1 being either 0 or with degree less than $\deg(g)$. In this case, set $q = \alpha\beta^{-1}T^{n-m} + q_1$ and $r = r_1$ and we are done.
If $f = qg + r = q^{'}g + r^{'}$, then g divides $r - r^{'}$ and by degree considerations we see $r = r^{'}$. In this case, $qg = q^{'}g$ so $q = q^{'}$ and the uniqueness is established. □

This proposition shows that A is an Euclidean domain and thus a principal ideal domain and a unique factorization domain.

A is an unique factorization domain

Proposition (1.1)

Let $f, g \in A$ with $g \neq 0$. Then there exist elements $q, r \in A$ such that $f = qg + r$ and r is either 0 or $deg(r) < deg(g)$. Moreover, q and r are uniquely determined by these conditions.

Proof.

Let $n = \deg(f)$, $m = \deg(g)$, $\alpha = \text{sgn}(f)$, $\beta = \text{sgn}(g)$. We give the proof by induction on $n = \deg(f)$. If $n < m$, set $q = 0$ and $r = f$. If $n \geq m$, we note that $f_1 = f - \alpha\beta^{-1}T^{n-m}g$ has smaller degree than f. By induction, there exist $q_1, r_1 \in A$ such that $f_1 = q_1 g + r_1$ with r_1 being either 0 or with degree less than $\deg(g)$. In this case, set $q = \alpha\beta^{-1}T^{n-m} + q_1$ and $r = r_1$ and we are done.
If $f = qg + r = q^{'}g + r^{'}$, then g divides $r - r^{'}$ and by degree considerations we see $r = r^{'}$. In this case, $qg = q^{'}g$ so $q = q^{'}$ and the uniqueness is established. □

This proposition shows that A is an Euclidean domain and thus a principal ideal domain and a unique factorization domain. It also allows a quick proof of the finiteness of the residue class rings.

Finiteness of the Residue Class Rings

Proposition (1.2)

Suppose $g \in A$ and $g \neq 0$. Then A/gA is a finite ring with $q^{deg(g)}$ elements.

Finiteness of the Residue Class Rings

Proposition (1.2)

Suppose $g \in A$ and $g \neq 0$. Then A/gA is a finite ring with $q^{deg(g)}$ elements.

Proof.

Let $m = \deg(g)$. By Proposition 1.1 one easily verifies that $\{r \in A : \deg(r) < m\}$ is a complete set of representatives for A/gA.

Finiteness of the Residue Class Rings

Proposition (1.2)

Suppose $g \in A$ and $g \neq 0$. Then A/gA is a finite ring with $q^{deg(g)}$ elements.

Proof.

Let $m = \deg(g)$. By Proposition 1.1 one easily verifies that $\{r \in A : \deg(r) < m\}$ is a complete set of representatives for A/gA. Such elements look like

$$r = \alpha_0 T^{m-1} + \alpha_1 T^{m-2} + \cdots + \alpha_{m-1} \qquad \text{with } \alpha_i \in \mathbb{F}_q.$$

Since the α_i vary independently through $\mathbb{F}_q$ there are q^m such polynomials and the result follows. □

Norm of a Polynomial

Definition (Norm of a Polynomial)

Let $g \in A$. If $g \neq 0$, set $|g| = q^{deg(g)}$. If $g = 0$, set $|g| = 0$.

Norm of a Polynomial

Definition (Norm of a Polynomial)

Let $g \in A$. If $g \neq 0$, set $|g| = q^{deg(g)}$. If $g = 0$, set $|g| = 0$.

$|g|$ is a measure of the size of g, the **norm** of g.

Norm of a Polynomial

Definition (Norm of a Polynomial)

Let $g \in A$. If $g \neq 0$, set $|g| = q^{deg(g)}$. If $g = 0$, set $|g| = 0$.

$|g|$ is a measure of the size of g, the **norm** of g. Note that if n is an ordinary integer, then its usual absolute value, $|n|$, is the number of elements in $\mathbb{Z}/n\mathbb{Z}$.

Norm of a Polynomial

Definition (Norm of a Polynomial)

Let $g \in A$. If $g \neq 0$, set $|g| = q^{deg(g)}$. If $g = 0$, set $|g| = 0$.

$|g|$ is a measure of the size of g, the **norm** of g. Note that if n is an ordinary integer, then its usual absolute value, $|n|$, is the number of elements in $\mathbb{Z}/n\mathbb{Z}$. Similarly, $|g|$ is the number of elements in A/gA.

Norm of a Polynomial

Definition (Norm of a Polynomial)

Let $g \in A$. If $g \neq 0$, set $|g| = q^{deg(g)}$. If $g = 0$, set $|g| = 0$.

$|g|$ is a measure of the size of g, the **norm** of g. Note that if n is an ordinary integer, then its usual absolute value, $|n|$, is the number of elements in $\mathbb{Z}/n\mathbb{Z}$. Similarly, $|g|$ is the number of elements in A/gA. It is immediate the following properties:

Norm of a Polynomial

Definition (Norm of a Polynomial)

Let $g \in A$. If $g \neq 0$, set $|g| = q^{deg(g)}$. If $g = 0$, set $|g| = 0$.

$|g|$ is a measure of the size of g, the **norm** of g. Note that if n is an ordinary integer, then its usual absolute value, $|n|$, is the number of elements in $\mathbb{Z}/n\mathbb{Z}$. Similarly, $|g|$ is the number of elements in A/gA. It is immediate the following properties:

- $|fg| = |f||g|$.

Norm of a Polynomial

Definition (Norm of a Polynomial)

Let $g \in A$. If $g \neq 0$, set $|g| = q^{deg(g)}$. If $g = 0$, set $|g| = 0$.

$|g|$ is a measure of the size of g, the **norm** of g. Note that if n is an ordinary integer, then its usual absolute value, $|n|$, is the number of elements in $\mathbb{Z}/n\mathbb{Z}$. Similarly, $|g|$ is the number of elements in A/gA. It is immediate the following properties:

- $|fg| = |f||g|$.
- $|f + g| \leq \max(|f|, |g|)$, with equality holding if $|f| \neq |g|$.

Group of Units

It is a simple matter to determine the *group of units* in A, A^*. If g is a *unit*, then there is an f such that $fg = 1$. Thus,
$0 = \deg(1) = \deg(f) + \deg(g)$ and so $\deg(f) = \deg(g) = 0$.

Group of Units

It is a simple matter to determine the *group of units* in A, A^*. If g is a *unit*, then there is an f such that $fg = 1$. Thus, $0 = \deg(1) = \deg(f) + \deg(g)$ and so $\deg(f) = \deg(g) = 0$. The only units are non-zero constants and each such constant is a unit.

Group of Units

It is a simple matter to determine the *group of units* in A, A^*. If g is a *unit*, then there is an f such that $fg = 1$. Thus, $0 = \deg(1) = \deg(f) + \deg(g)$ and so $\deg(f) = \deg(g) = 0$. The only units are non-zero constants and each such constant is a unit.

Proposition (1.3)

The group of units in A is $\mathbb{F}_q^*$. In particular, it is a finite cyclic group with $q - 1$ elements.

Group of Units

It is a simple matter to determine the *group of units* in A, A^*. If g is a *unit*, then there is an f such that $fg = 1$. Thus, $0 = \deg(1) = \deg(f) + \deg(g)$ and so $\deg(f) = \deg(g) = 0$. The only units are non-zero constants and each such constant is a unit.

Proposition (1.3)

The group of units in A is $\mathbb{F}_q^*$. In particular, it is a finite cyclic group with $q - 1$ elements.

Proof.

The only thing left to prove is the cyclicity of $\mathbb{F}_q^*$. This follows from the very general fact that a finite subgroup of the multiplicative group of a field is cyclic. □

Group of Units

It is a simple matter to determine the *group of units* in A, A^*. If g is a *unit*, then there is an f such that $fg = 1$. Thus, $0 = \deg(1) = \deg(f) + \deg(g)$ and so $\deg(f) = \deg(g) = 0$. The only units are non-zero constants and each such constant is a unit.

Proposition (1.3)

The group of units in A is $\mathbb{F}_q^*$. In particular, it is a finite cyclic group with $q - 1$ elements.

Proof.

The only thing left to prove is the cyclicity of $\mathbb{F}_q^*$. This follows from the very general fact that a finite subgroup of the multiplicative group of a field is cyclic. □

In what follows we will see that the number $q - 1$ often occurs where the number 2 occurs in ordinary number theory. This stems from the fact that the order of $\mathbb{Z}^*$ is 2.

Irreducible Polynomials

Definition (irreducible polynomials)

*A non-constant polynomial $f \in A$ is **irreducible** if it cannot be written as a product of two polynomials, each of positive degree.*

Irreducible Polynomials

Definition (irreducible polynomials)

*A non-constant polynomial $f \in A$ is **irreducible** if it cannot be written as a product of two polynomials, each of positive degree.*

Since every ideal in A is principal, we see that a polynomial is irreducible if and only if it is prime.

Irreducible Polynomials

Definition (irreducible polynomials)

*A non-constant polynomial $f \in A$ is **irreducible** if it cannot be written as a product of two polynomials, each of positive degree.*

Since every ideal in A is principal, we see that a polynomial is irreducible if and only if it is prime. For the definitions of divisibility, prime, irreducible, etc., see the book by Ireland and Rosen *"A Classical Introduction to Modern Number Theory"*.

Irreducible Polynomials

Definition (irreducible polynomials)

*A non-constant polynomial $f \in A$ is **irreducible** if it cannot be written as a product of two polynomials, each of positive degree.*

Since every ideal in A is principal, we see that a polynomial is irreducible if and only if it is prime. For the definitions of divisibility, prime, irreducible, etc., see the book by Ireland and Rosen *"A Classical Introduction to Modern Number Theory"*.
Every non-zero polynomial can be written uniquely as a non-zero constant times a monic polynomial.

Irreducible Polynomials

Definition (irreducible polynomials)

*A non-constant polynomial $f \in A$ is **irreducible** if it cannot be written as a product of two polynomials, each of positive degree.*

Since every ideal in A is principal, we see that a polynomial is irreducible if and only if it is prime. For the definitions of divisibility, prime, irreducible, etc., see the book by Ireland and Rosen *"A Classical Introduction to Modern Number Theory"*.
Every non-zero polynomial can be written uniquely as a non-zero constant times a monic polynomial. Thus, every ideal in A has a unique monic generator. This should be compared with the statement that every non-zero ideal in $\mathbb{Z}$ has a unique positive generator.

Irreducible Polynomials

Definition (irreducible polynomials)

*A non-constant polynomial $f \in A$ is **irreducible** if it cannot be written as a product of two polynomials, each of positive degree.*

Since every ideal in A is principal, we see that a polynomial is irreducible if and only if it is prime. For the definitions of divisibility, prime, irreducible, etc., see the book by Ireland and Rosen *"A Classical Introduction to Modern Number Theory"*.
Every non-zero polynomial can be written uniquely as a non-zero constant times a monic polynomial. Thus, every ideal in A has a unique monic generator. This should be compared with the statement that every non-zero ideal in $\mathbb{Z}$ has a unique positive generator. Finally, the unique factorization property in A can be sharpened to the following statement.

Irreducible Polynomials

Definition (irreducible polynomials)

*A non-constant polynomial $f \in A$ is **irreducible** if it cannot be written as a product of two polynomials, each of positive degree.*

Since every ideal in A is principal, we see that a polynomial is irreducible if and only if it is prime. For the definitions of divisibility, prime, irreducible, etc., see the book by Ireland and Rosen *"A Classical Introduction to Modern Number Theory"*.
Every non-zero polynomial can be written uniquely as a non-zero constant times a monic polynomial. Thus, every ideal in A has a unique monic generator. This should be compared with the statement that every non-zero ideal in $\mathbb{Z}$ has a unique positive generator. Finally, the unique factorization property in A can be sharpened to the following statement. Every $f \in A$, $f \neq 0$, can be written uniquely in the form

$$f = \alpha P_1^{e_1} P_2^{e_2} \cdots P_t^{e_t},$$

where $\alpha \in \mathbb{F}_q^*$, each P_i is a monic irreducible, $P_i \neq P_j$ for $i \neq j$, and each e_i is a non-negative integer.

Irreducible Polynomials

Definition (irreducible polynomials)

*A non-constant polynomial $f \in A$ is **irreducible** if it cannot be written as a product of two polynomials, each of positive degree.*

Since every ideal in A is principal, we see that a polynomial is irreducible if and only if it is prime. For the definitions of divisibility, prime, irreducible, etc., see the book by Ireland and Rosen *"A Classical Introduction to Modern Number Theory"*.

Every non-zero polynomial can be written uniquely as a non-zero constant times a monic polynomial. Thus, every ideal in A has a unique monic generator. This should be compared with the statement that every non-zero ideal in $\mathbb{Z}$ has a unique positive generator. Finally, the unique factorization property in A can be sharpened to the following statement. Every $f \in A$, $f \neq 0$, can be written uniquely in the form

$$f = \alpha P_1^{e_1} P_2^{e_2} \cdots P_t^{e_t},$$

where $\alpha \in \mathbb{F}_q^*$, each P_i is a monic irreducible, $P_i \neq P_j$ for $i \neq j$, and each e_i is a non-negative integer.

The letter P will often be used for a monic irreducible polynomial in A.

The rings A/fA

The next order of business is to investigate the structure of the rings A/fA and the unit groups $(A/fA)^*$.

The rings A/fA

The next order of business is to investigate the structure of the rings A/fA and the unit groups $(A/fA)^*$.

Proposition (Chinese Remainder Theorem)

Let $m_1, m_2, \ldots, m_t$ be elements of A which are pairwise relatively prime. Let $m = m_1 m_2 \ldots m_t$ and ϕ_i be the natural homomorphism from A/mA to A/m_iA. Then, the map $\phi : A/mA \to A/m_1A \oplus A/m_2A \oplus \cdots \oplus A/m_tA$ given by

$$\phi(a) = (\phi_1(a), \phi_2(a), \ldots, \phi_t(a))$$

is a ring isomorphism.

The rings A/fA

The next order of business is to investigate the structure of the rings A/fA and the unit groups $(A/fA)^*$.

Proposition (Chinese Remainder Theorem)

Let $m_1, m_2, \ldots, m_t$ be elements of A which are pairwise relatively prime. Let $m = m_1 m_2 \ldots m_t$ and ϕ_i be the natural homomorphism from A/mA to A/m_iA. Then, the map $\phi : A/mA \to A/m_1A \oplus A/m_2A \oplus \cdots \oplus A/m_tA$ given by

$$\phi(a) = (\phi_1(a), \phi_2(a), \ldots, \phi_t(a))$$

is a ring isomorphism.

Proof.

This is a standard result which holds in any principal ideal domain (properly formulated it holds in much greater generality). □

The rings A/fA

Corollary

The same map ϕ restricted to the units of A, A^*, gives rise to a group isomorphism

$$(A/mA)^* \simeq (A/m_1A)^* \times (A/m_2A)^* \times \cdots \times (A/m_tA)^*.$$

The rings A/fA

Corollary

The same map ϕ restricted to the units of A, A^*, gives rise to a group isomorphism

$$(A/mA)^* \simeq (A/m_1A)^* \times (A/m_2A)^* \times \cdots \times (A/m_tA)^*.$$

Proof.

This is a standard exercise. See Ireland and Rosen (Proposition 3.4.1). □

Now, let $f \in A$ be non-zero and not a unit and suppose that $f = \alpha P_1^{e_1} P_2^{e_2} \cdots P_t^{e_t}$ is its prime decomposition. From the previous considerations we have

$$(A/fA)^* \simeq (A/P_1^{e_1}A)^* \times (A/P_2^{e_2}A)^* \times \cdots \times (A/P_t^{e_t}A)^*.$$

Now, let $f \in A$ be non-zero and not a unit and suppose that $f = \alpha P_1^{e_1} P_2^{e_2} \cdots P_t^{e_t}$ is its prime decomposition. From the previous considerations we have

$$(A/fA)^* \simeq (A/P_1^{e_1}A)^* \times (A/P_2^{e_2}A)^* \times \cdots \times (A/P_t^{e_t}A)^*.$$

This isomorphism reduces our task to that of determining the structure of the groups $(A/P^eA)^*$ where P is an irreducible polynomial and e is a positive integer. When $e = 1$ the situation is very similar to that in $\mathbb{Z}$.

Now, let $f \in A$ be non-zero and not a unit and suppose that $f = \alpha P_1^{e_1} P_2^{e_2} \cdots P_t^{e_t}$ is its prime decomposition. From the previous considerations we have

$$(A/fA)^* \simeq (A/P_1^{e_1}A)^* \times (A/P_2^{e_2}A)^* \times \cdots \times (A/P_t^{e_t}A)^*.$$

This isomorphism reduces our task to that of determining the structure of the groups $(A/P^eA)^*$ where P is an irreducible polynomial and e is a positive integer. When $e = 1$ the situation is very similar to that in $\mathbb{Z}$.

Proposition (1.5)

Let $P \in A$ be an irreducible polynomial. Then, $(A/PA)^*$ is a cyclic group with $|P| - 1$ elements.

Now, let $f \in A$ be non-zero and not a unit and suppose that $f = \alpha P_1^{e_1} P_2^{e_2} \cdots P_t^{e_t}$ is its prime decomposition. From the previous considerations we have

$$(A/fA)^* \simeq (A/P_1^{e_1}A)^* \times (A/P_2^{e_2}A)^* \times \cdots \times (A/P_t^{e_t}A)^*.$$

This isomorphism reduces our task to that of determining the structure of the groups $(A/P^eA)^*$ where P is an irreducible polynomial and e is a positive integer. When $e = 1$ the situation is very similar to that in $\mathbb{Z}$.

Proposition (1.5)

Let $P \in A$ be an irreducible polynomial. Then, $(A/PA)^*$ is a cyclic group with $|P| - 1$ elements.

Proof.

Since A is a principal ideal domain, PA is a maximal ideal and so A/PA is a field. A finite subgroup of the multiplicative group of a field is cyclic. Thus $(A/PA)^*$ is cyclic.

Now, let $f \in A$ be non-zero and not a unit and suppose that $f = \alpha P_1^{e_1} P_2^{e_2} \cdots P_t^{e_t}$ is its prime decomposition. From the previous considerations we have

$$(A/fA)^* \simeq (A/P_1^{e_1}A)^* \times (A/P_2^{e_2}A)^* \times \cdots \times (A/P_t^{e_t}A)^*.$$

This isomorphism reduces our task to that of determining the structure of the groups $(A/P^eA)^*$ where P is an irreducible polynomial and e is a positive integer. When $e = 1$ the situation is very similar to that in $\mathbb{Z}$.

Proposition (1.5)

Let $P \in A$ be an irreducible polynomial. Then, $(A/PA)^*$ is a cyclic group with $|P| - 1$ elements.

Proof.

Since A is a principal ideal domain, PA is a maximal ideal and so A/PA is a field. A finite subgroup of the multiplicative group of a field is cyclic. Thus $(A/PA)^*$ is cyclic. That the order of this group is $|P| - 1$ is immediate.

Contrast between $A = \mathbb{F}_q[T]$ and $\mathbb{Z}$

We now consider the situation when $e > 1$.

Contrast between $A = \mathbb{F}_q[T]$ and $\mathbb{Z}$

We now consider the situation when $e > 1$. Here we encounter something which is quite different in A from the situation in $\mathbb{Z}$.

Contrast between $A = \mathbb{F}_q[T]$ and $\mathbb{Z}$

We now consider the situation when $e > 1$. Here we encounter something which is quite different in A from the situation in $\mathbb{Z}$. If p is an odd prime number in $\mathbb{Z}$ then it is a standard result that $(\mathbb{Z}/p^e\mathbb{Z})^*$ is cyclic for all positive integers e. If $p = 2$ and $e \geq 3$ then $(\mathbb{Z}/2^e\mathbb{Z})^*$ is the direct product of a cyclic group of order 2 and a cyclic group of order 2^{e-2}. The situation is very different in A.

Contrast between $A = \mathbb{F}_q[T]$ and $\mathbb{Z}$

We now consider the situation when $e > 1$. Here we encounter something which is quite different in A from the situation in $\mathbb{Z}$. If p is an odd prime number in $\mathbb{Z}$ then it is a standard result that $(\mathbb{Z}/p^e\mathbb{Z})^*$ is cyclic for all positive integers e. If $p = 2$ and $e \geq 3$ then $(\mathbb{Z}/2^e\mathbb{Z})^*$ is the direct product of a cyclic group of order 2 and a cyclic group of order 2^{e-2}. The situation is very different in A.

Proposition (1.6)

Let $P \in A$ be an irreducible polynomial and e a positive integer. The order of $(A/P^eA)^*$ is $|P|^{e-1}(|P| - 1)$. Let $(A/P^eA)^{(1)}$ be the kernel of the natural map from $(A/P^eA)^*$ to $(A/PA)^*$. It is a p-group of order $|P|^{e-1}$. As e tends to infinity, the minimal number of generators of $(A/P^eA)^{(1)}$ tends to infinity.

Euler's Φ-function

We have developed more than enough material to enable us to give interesting analogues of the Euler ϕ-function and the little theorems of Euler and Fermat.

Euler's Φ-function

We have developed more than enough material to enable us to give interesting analogues of the Euler ϕ-function and the little theorems of Euler and Fermat.

Definition (Euler's ϕ-function in A)

To begin with, let $f \in A$ be a non-zero polynomial. Define $\Phi(f)$ to be the number of elements in the group $(A/fA)^*$.

Euler's Φ-function

We have developed more than enough material to enable us to give interesting analogues of the Euler ϕ-function and the little theorems of Euler and Fermat.

Definition (Euler's ϕ-function in A)

To begin with, let $f \in A$ be a non-zero polynomial. Define $\Phi(f)$ to be the number of elements in the group $(A/fA)^*$.

We can give another characterization of this number which makes the relation to the Euler ϕ-function even more evident.

Euler's Φ-function

We have developed more than enough material to enable us to give interesting analogues of the Euler ϕ-function and the little theorems of Euler and Fermat.

Definition (Euler's ϕ-function in A)

To begin with, let $f \in A$ be a non-zero polynomial. Define $\Phi(f)$ to be the number of elements in the group $(A/fA)^*$.

We can give another characterization of this number which makes the relation to the Euler ϕ-function even more evident. We have seen that $\{r \in A : \deg(r) < \deg(f)\}$ is a set or representatives for A/fA.

Euler's Φ-function

We have developed more than enough material to enable us to give interesting analogues of the Euler ϕ-function and the little theorems of Euler and Fermat.

Definition (Euler's ϕ-function in A)

To begin with, let $f \in A$ be a non-zero polynomial. Define $\Phi(f)$ to be the number of elements in the group $(A/fA)^*$.

We can give another characterization of this number which makes the relation to the Euler ϕ-function even more evident. We have seen that $\{r \in A : \deg(r) < \deg(f)\}$ is a set or representatives for A/fA. Such an r represents a unit in A/fA if and only if it is relatively prime to f.

Euler's Φ-function

We have developed more than enough material to enable us to give interesting analogues of the Euler ϕ-function and the little theorems of Euler and Fermat.

Definition (Euler's ϕ-function in A)

To begin with, let $f \in A$ be a non-zero polynomial. Define $\Phi(f)$ to be the number of elements in the group $(A/fA)^*$.

We can give another characterization of this number which makes the relation to the Euler ϕ-function even more evident. We have seen that $\{r \in A : \deg(r) < \deg(f)\}$ is a set or representatives for A/fA. Such an r represents a unit in A/fA if and only if it is relatively prime to f. Thus $\Phi(f)$ is the number of non-zero polynomials of degree less than $\deg(f)$ and relatively prime to f, i.e.

$$\Phi(f) = \sum_{\substack{k \text{ monic} \\ \deg(k)<\deg(f) \\ \gcd(f,k)=1}} 1.$$

Proposition (1.7)

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

Proposition (1.7)

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

Proof.

Let $f = \alpha P_1^{e_1} P_2^{e_2} \dots P_t^{e_t}$ be the prime decomposition of f. By the corollary of the Chinese Remainder Theorem and by Proposition 1.6, we see that

$$\Phi(f) = \prod_{i=1}^{t} \Phi(P_i^{e_i}) = \prod_{i=1}^{t} (|P_i|^{e_i} - |P_i|^{e_i - 1}),$$

from which the result follows immediately. □

Proposition (1.7)

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

Proof.

Let $f = \alpha P_1^{e_1} P_2^{e_2} \dots P_t^{e_t}$ be the prime decomposition of f. By the corollary of the Chinese Remainder Theorem and by Proposition 1.6, we see that

$$\Phi(f) = \prod_{i=1}^{t} \Phi(P_i^{e_i}) = \prod_{i=1}^{t} (|P_i|^{e_i} - |P_i|^{e_i - 1}),$$

from which the result follows immediately. □

The similarity of the formula in this proposition to the classical formula $\phi(n) = n \prod_{p|n}(1 - p^{-1})$ is striking.

Euler's little theorem

Proposition (Euler's little theorem)

If $f \in A$, $f \neq 0$, and $a \in A$ is relatively prime to f, i.e., $(a, f) = 1$, then

$$a^{\Phi(f)} \equiv 1 (\mathrm{mod}\, f).$$

Euler's little theorem

Proposition (Euler's little theorem)

If $f \in A$, $f \neq 0$, and $a \in A$ is relatively prime to f, i.e., $(a, f) = 1$, then

$$a^{\Phi(f)} \equiv 1 (\mathrm{mod}\, f).$$

Proof.

The group $(A/fA)^*$ has $\Phi(f)$ elements. The coset of a modulo f, $\overline{a}$, lies in this group. Thus, $\overline{a}^{\Phi(f)} = \overline{1}$ and this is equivalent to the congruence in the proposition. $\square$

Fermat's little theorem

Corollary (Fermat's little theorem)

Let $P \in A$ be irreducible and $a \in A$ be a polynomial not divisible by P. Then,

$$a^{|P|-1} \equiv 1 (\mathrm{mod}\, P).$$

Fermat's little theorem

Corollary (Fermat's little theorem)

Let $P \in A$ be irreducible and $a \in A$ be a polynomial not divisible by P. Then,

$$a^{|P|-1} \equiv 1 (\mathrm{mod}\, P).$$

Proof.

Since P is irreducible, it is relatively prime to a if and only if it does not divide a. The corollary follows from the proposition and the fact that for an irreducible P, $\Phi(P) = |P| - 1$ (Proposition 1.5). □

Fermat's little theorem

Corollary (Fermat's little theorem)

Let $P \in A$ be irreducible and $a \in A$ be a polynomial not divisible by P. Then,

$$a^{|P|-1} \equiv 1 (\mathrm{mod}\, P).$$

Proof.

Since P is irreducible, it is relatively prime to a if and only if it does not divide a. The corollary follows from the proposition and the fact that for an irreducible P, $\Phi(P) = |P| - 1$ (Proposition 1.5). □

The theorems above play the same very important role in this context as they do in elementary number theory.

Fermat's little theorem

Corollary (Fermat's little theorem)

Let $P \in A$ be irreducible and $a \in A$ be a polynomial not divisible by P. Then,

$$a^{|P|-1} \equiv 1 (\mathrm{mod}\, P).$$

Proof.

Since P is irreducible, it is relatively prime to a if and only if it does not divide a. The corollary follows from the proposition and the fact that for an irreducible P, $\Phi(P) = |P| - 1$ (Proposition 1.5). □

The theorems above play the same very important role in this context as they do in elementary number theory. By way of illustration we proceed to the analogue of Wilson's theorem. Recall that this states that $(p-1)! \equiv -1 (\mathrm{mod}\, p)$ where p is a prime number.

Wilson's theorem in $\mathbb{F}_q[T]$

Proposition (1.9)

Let $P \in A$ be irreducible of degree d. Suppose X is an indeterminate. Then,

$$X^{|P|-1} - 1 \equiv \prod_{0 \leq deg(f) < d} (X - f) (\mathrm{mod}\, P).$$

Wilson's theorem in $\mathbb{F}_q[T]$

Proposition (1.9)

Let $P \in A$ be irreducible of degree d. Suppose X is an indeterminate. Then,

$$X^{|P|-1} - 1 \equiv \prod_{0 \leq deg(f) < d} (X - f) (\mathrm{mod}\, P).$$

Corollary (1)

Let d divide $|P| - 1$. The congruence $X^d \equiv 1 (\mathrm{mod}\, P)$ has exactly d solutions. Equivalently, the equation $X^d = \overline{1}$ has exactly d solutions in $(A/PA)^*$.

Wilson's theorem in $\mathbb{F}_q[T]$

Corollary (Wilson's theorem)

With the same notation,

$$\prod_{0 \leq deg(f) < deg(P)} f \equiv -1 (\mathrm{mod}\, P).$$

Wilson's theorem in $\mathbb{F}_q[T]$

Corollary (Wilson's theorem)

With the same notation,

$$\prod_{0 \leq deg(f) < deg(P)} f \equiv -1 (\mathrm{mod}\, P).$$

Proof.

Just set $X = 0$ in the proposition. If the characteristic of $\mathbb{F}_q$ is odd then $|P| - 1$ is even and the result follows.

Wilson's theorem in $\mathbb{F}_q[T]$

Corollary (Wilson's theorem)

With the same notation,

$$\prod_{0 \leq deg(f) < deg(P)} f \equiv -1 (\mathrm{mod}\, P).$$

Proof.

Just set $X = 0$ in the proposition. If the characteristic of $\mathbb{F}_q$ is odd then $|P| - 1$ is even and the result follows. If the characteristic is 2 then the result also follows since in characteristic 2 we have $-1 = 1$. $\square$

d-th power residues

As a final topic in this section we give some theory of d-th power residues.

d-th power residues

As a final topic in this section we give some theory of d-th power residues. This will be of importance for the next class when we will discuss quadratic reciprocity and more general reciprocity laws for A.

d-th power residues

As a final topic in this section we give some theory of d-th power residues. This will be of importance for the next class when we will discuss quadratic reciprocity and more general reciprocity laws for A.

Definition (d-th power residue)

If $f \in A$ is of positive degree and $a \in A$ is relatively prime to f, we say that a is a d-th power residue modulo f if the equation $x^d \equiv a \pmod{f}$ is solvable in A.

d-th power residues

As a final topic in this section we give some theory of d-th power residues. This will be of importance for the next class when we will discuss quadratic reciprocity and more general reciprocity laws for A.

Definition (d-th power residue)

If $f \in A$ is of positive degree and $a \in A$ is relatively prime to f, we say that a is a d-th power residue modulo f if the equation $x^d \equiv a \pmod{f}$ is solvable in A. Equivalently, $\overline{a}$ is a d-th power in $(A/fA)^*$.

d-th power residues

As a final topic in this section we give some theory of d-th power residues. This will be of importance for the next class when we will discuss quadratic reciprocity and more general reciprocity laws for A.

Definition (d-th power residue)

If $f \in A$ is of positive degree and $a \in A$ is relatively prime to f, we say that a is a d-th power residue modulo f if the equation $x^d \equiv a \pmod{f}$ is solvable in A. Equivalently, $\overline{a}$ is a d-th power in $(A/fA)^*$.

Suppose $f = \alpha P_1^{e_1} P_2^{e_2} \cdots P_t^{e_t}$ is the prime decomposition of f. Then it is easy to check that a is a d-th power residue modulo f if and only if a is a d-th power residue modulo $P_i^{e_i}$ for all i between 1 and t. This reduces the problem to the case where the modulus is a prime power.

d-th power residues

As a final topic in this section we give some theory of d-th power residues. This will be of importance for the next class when we will discuss quadratic reciprocity and more general reciprocity laws for A.

Definition (d-th power residue)

If $f \in A$ is of positive degree and $a \in A$ is relatively prime to f, we say that a is a d-th power residue modulo f if the equation $x^d \equiv a \pmod{f}$ is solvable in A. Equivalently, $\overline{a}$ is a d-th power in $(A/fA)^*$.

Suppose $f = \alpha P_1^{e_1} P_2^{e_2} \cdots P_t^{e_t}$ is the prime decomposition of f. Then it is easy to check that a is a d-th power residue modulo f if and only if a is a d-th power residue modulo $P_i^{e_i}$ for all i between 1 and t. This reduces the problem to the case where the modulus is a prime power.

Proposition (1.10)

Let P be irreducible and $a \in A$ not divisible by P. Assume d divides $|P| - 1$. The congruence $X^d \equiv a \pmod{P^e}$ is solvable if and only if

$$a^{\frac{|P|-1}{d}} \equiv 1 \pmod{P}.$$

There are $\frac{\Phi(P^e)}{d}$ d-th power residues modulo P^e.

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

So far we have the following correspondence:

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

So far we have the following correspondence:

Number Fields	Function Fields
$\mathbb{Z}$	$A = \mathbb{F}_q[T]$

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

So far we have the following correspondence:

Number Fields	Function Fields
$\mathbb{Z}$	$A = \mathbb{F}_q[T]$
$\mathbb{Q}$	$k = \mathbb{F}_q(T)$

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

So far we have the following correspondence:

Number Fields	Function Fields
$\mathbb{Z}$	$A = \mathbb{F}_q[T]$
$\mathbb{Q}$	$k = \mathbb{F}_q(T)$
positive integers	A^+ monic polynomials

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

So far we have the following correspondence:

Number Fields	Function Fields
$\mathbb{Z}$	$A = \mathbb{F}_q[T]$
$\mathbb{Q}$	$k = \mathbb{F}_q(T)$
positive integers	A^+ monic polynomials
prime numbers	$\mathcal{P}$ monic irreducible polynomials

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

So far we have the following correspondence:

Number Fields	Function Fields
$\mathbb{Z}$	$A = \mathbb{F}_q[T]$
$\mathbb{Q}$	$k = \mathbb{F}_q(T)$
positive integers	A^+ monic polynomials
prime numbers	$\mathcal{P}$ monic irreducible polynomials
absolute value $\lvert n \rvert$	norm of a polynomial $\lvert f \rvert = q^{\deg(f)}$

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

So far we have the following correspondence:

Number Fields	Function Fields
$\mathbb{Z}$	$A = \mathbb{F}_q[T]$
$\mathbb{Q}$	$k = \mathbb{F}_q(T)$
positive integers	A^+ monic polynomials
prime numbers	$\mathcal{P}$ monic irreducible polynomials
absolute value $\lvert n \rvert$	norm of a polynomial $\lvert f \rvert = q^{\deg(f)}$
$n = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} P_2^{e_2} \dots P_t^{e_t}$

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

So far we have the following correspondence:

Number Fields	Function Fields
$\mathbb{Z}$	$A = \mathbb{F}_q[T]$
$\mathbb{Q}$	$k = \mathbb{F}_q(T)$
positive integers	A^+ monic polynomials
prime numbers	$\mathcal{P}$ monic irreducible polynomials
absolute value $\lvert n \rvert$	norm of a polynomial $\lvert f \rvert = q^{\deg(f)}$
$n = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} P_2^{e_2} \dots P_t^{e_t}$
2	q-1

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

So far we have the following correspondence:

Number Fields	Function Fields
$\mathbb{Z}$	$A = \mathbb{F}_q[T]$
$\mathbb{Q}$	$k = \mathbb{F}_q(T)$
positive integers	A^+ monic polynomials
prime numbers	$\mathcal{P}$ monic irreducible polynomials
absolute value $\lvert n \rvert$	norm of a polynomial $\lvert f \rvert = q^{\deg(f)}$
$n = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} P_2^{e_2} \dots P_t^{e_t}$
2	q-1
$\phi(n) = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} 1$	$\Phi(f) = \sum_{\substack{k \text{ monic} \\ \deg(k)<\deg(f) \\ \gcd(f,k)=1}} 1$

Zeta Function and Primes in $A = \mathbb{F}q[T]$

- We now discuss properties of primes and prime decomposition in A.

Zeta Function and Primes in $A = \mathbb{F}q[T]$

- We now discuss properties of primes and prime decomposition in A.
- The discussion will be facilitated by the use of the zeta function associated to A.

Zeta Function and Primes in $A = \mathbb{F}q[T]$

- We now discuss properties of primes and prime decomposition in A.
- The discussion will be facilitated by the use of the zeta function associated to A.
- This zeta function is an analogue of the classical Riemann zeta function $\zeta(s)$.

Zeta Function and Primes in $A = \mathbb{F}q[T]$

- We now discuss properties of primes and prime decomposition in A.
- The discussion will be facilitated by the use of the zeta function associated to A.
- This zeta function is an analogue of the classical Riemann zeta function $\zeta(s)$.
- In A, the zeta function is is a much simpler object.

Zeta Function and Primes in $A = \mathbb{F}q[T]$

- We now discuss properties of primes and prime decomposition in A.
- The discussion will be facilitated by the use of the zeta function associated to A.
- This zeta function is an analogue of the classical Riemann zeta function $\zeta(s)$.
- In A, the zeta function is is a much simpler object. This will lead us to a sharp version of the prime number theorem.

Zeta Function and Primes in $A = \mathbb{F}q[T]$

- We now discuss properties of primes and prime decomposition in A.
- The discussion will be facilitated by the use of the zeta function associated to A.
- This zeta function is an analogue of the classical Riemann zeta function $\zeta(s)$.
- In A, the zeta function is is a much simpler object. This will lead us to a sharp version of the prime number theorem.
- When we investigate arithmetic in more general function fields than $\mathbb{F}_q(T)$, the corresponding zeta function will turn out to be a much more subtle invariant.

Remembering the Riemann zeta function

The classical Riemann zeta function is defined by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \qquad \Re(s) > 1. \tag{3.1}$$

Some properties:

- analytic continuation to $\mathbb{C}$ except for

Remembering the Riemann zeta function

The classical Riemann zeta function is defined by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \qquad \Re(s) > 1. \tag{3.1}$$

Some properties:

- analytic continuation to $\mathbb{C}$ except for
- simple pole at $s = 1$ with residue 1.

Remembering the Riemann zeta function

The classical Riemann zeta function is defined by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \qquad \Re(s) > 1. \tag{3.1}$$

Some properties:

- analytic continuation to $\mathbb{C}$ except for
- simple pole at $s = 1$ with residue 1.
- **Functional Equation.**

Remembering the Riemann zeta function

The classical Riemann zeta function is defined by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \qquad \Re(s) > 1. \tag{3.1}$$

Some properties:

- analytic continuation to $\mathbb{C}$ except for
- simple pole at $s = 1$ with residue 1.
- **Functional Equation.** If $\xi(s) = \pi^{-s/2}\Gamma(\frac{s}{2})\zeta(s)$.

Remembering the Riemann zeta function

The classical Riemann zeta function is defined by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \qquad \Re(s) > 1. \tag{3.1}$$

Some properties:

- analytic continuation to $\mathbb{C}$ except for
- simple pole at $s = 1$ with residue 1.
- **Functional Equation.** If $\xi(s) = \pi^{-s/2}\Gamma(\frac{s}{2})\zeta(s)$. Then

$$\xi(s) = \xi(1 - s),$$

where $\Gamma(s)$ is the classical Gamma function.

Remembering the Riemann zeta function

The classical Riemann zeta function is defined by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \qquad \Re(s) > 1. \tag{3.1}$$

Some properties:

- analytic continuation to $\mathbb{C}$ except for
- simple pole at $s = 1$ with residue 1.
- **Functional Equation.** If $\xi(s) = \pi^{-s/2}\Gamma(\frac{s}{2})\zeta(s)$. Then

$$\xi(s) = \xi(1 - s),$$

  where $\Gamma(s)$ is the classical Gamma function.
- $\zeta(-2n) = 0$ for $n \in \mathbb{Z}_+$. (trivial zeros)

Remembering the Riemann zeta function

The classical Riemann zeta function is defined by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \qquad \Re(s) > 1. \tag{3.1}$$

Some properties:

- analytic continuation to $\mathbb{C}$ except for
- simple pole at $s = 1$ with residue 1.
- **Functional Equation.** If $\xi(s) = \pi^{-s/2}\Gamma(\frac{s}{2})\zeta(s)$. Then

$$\xi(s) = \xi(1 - s),$$

  where $\Gamma(s)$ is the classical Gamma function.
- $\zeta(-2n) = 0$ for $n \in \mathbb{Z}_+$. (trivial zeros)

The Riemann Hypothesis: All the non-trivial zeros of $\zeta(s)$ have real part equals $1/2$.

Zeta Function in A

Definition

The zeta function of A, denoted $\zeta_A(s)$, is defined for $\Re(s) > 1$ by the infinite series

Zeta Function in A

Definition

The zeta function of A, denoted $\zeta_A(s)$, is defined for $\Re(s) > 1$ by the infinite series

$$\zeta_A(s) = \sum_{\substack{f \in A \\ f \text{ monic}}} \frac{1}{|f|^s}. \tag{3.2}$$

Zeta Function in A

Definition

The zeta function of A, denoted $\zeta_A(s)$, is defined for $\Re(s) > 1$ by the infinite series

$$\zeta_A(s) = \sum_{\substack{f \in A \\ f \text{ monic}}} \frac{1}{|f|^s}. \tag{3.2}$$

There are exactly q^d monic polynomials of degree d in A, so one has

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

Zeta Function in A

Definition

The zeta function of A, denoted $\zeta_A(s)$, is defined for $\Re(s) > 1$ by the infinite series

$$\zeta_A(s) = \sum_{\substack{f \in A \\ f \text{ monic}}} \frac{1}{|f|^s}. \tag{3.2}$$

There are exactly q^d monic polynomials of degree d in A, so one has

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

and consequently

$$\zeta_A(s) = \frac{1}{1 - q^{1-s}}. \tag{3.3}$$

Properties of $\zeta_A(s)$

- Analytic continuation. By equation (3.3), $\zeta_A(s)$ is well defined for the whole complex plane $\mathbb{C}$ except for

Properties of $\zeta_A(s)$

- Analytic continuation. By equation (3.3), $\zeta_A(s)$ is well defined for the whole complex plane $\mathbb{C}$ except for
- Simple pole at $s = 1$ with residue $\frac{1}{\log(q)}$.

Properties of $\zeta_A(s)$

- Analytic continuation. By equation (3.3), $\zeta_A(s)$ is well defined for the whole complex plane $\mathbb{C}$ except for
- Simple pole at $s = 1$ with residue $\frac{1}{\log(q)}$.
- **Functional Equation.** Let $\Gamma_A(s) = (1 - q^{-s})^{-1}$ be the Gamma function over A.

Properties of $\zeta_A(s)$

- Analytic continuation. By equation (3.3), $\zeta_A(s)$ is well defined for the whole complex plane $\mathbb{C}$ except for
- Simple pole at $s = 1$ with residue $\frac{1}{\log(q)}$.
- **Functional Equation.** Let $\Gamma_A(s) = (1 - q^{-s})^{-1}$ be the Gamma function over A. Set $\xi_A(s) = q^{-s}\Gamma_A(s)\zeta_A(s)$.

Properties of $\zeta_A(s)$

- Analytic continuation. By equation (3.3), $\zeta_A(s)$ is well defined for the whole complex plane $\mathbb{C}$ except for
- Simple pole at $s = 1$ with residue $\frac{1}{\log(q)}$.
- **Functional Equation.** Let $\Gamma_A(s) = (1 - q^{-s})^{-1}$ be the Gamma function over A. Set $\xi_A(s) = q^{-s}\Gamma_A(s)\zeta_A(s)$. Then it is easy to check that

$$\xi_A(s) = \xi_A(1 - s).$$

Properties of $\zeta_A(s)$

- Analytic continuation. By equation (3.3), $\zeta_A(s)$ is well defined for the whole complex plane $\mathbb{C}$ except for
- Simple pole at $s = 1$ with residue $\frac{1}{\log(q)}$.
- **Functional Equation.** Let $\Gamma_A(s) = (1 - q^{-s})^{-1}$ be the Gamma function over A. Set $\xi_A(s) = q^{-s}\Gamma_A(s)\zeta_A(s)$. Then it is easy to check that

$$\xi_A(s) = \xi_A(1 - s).$$

As opposed to the case of the classical zeta-function, the proofs are very easy for $\zeta_A(s)$.

Properties of $\zeta_A(s)$

- Analytic continuation. By equation (3.3), $\zeta_A(s)$ is well defined for the whole complex plane $\mathbb{C}$ except for
- Simple pole at $s = 1$ with residue $\frac{1}{\log(q)}$.
- **Functional Equation.** Let $\Gamma_A(s) = (1 - q^{-s})^{-1}$ be the Gamma function over A. Set $\xi_A(s) = q^{-s}\Gamma_A(s)\zeta_A(s)$. Then it is easy to check that

$$\xi_A(s) = \xi_A(1 - s).$$

As opposed to the case of the classical zeta-function, the proofs are very easy for $\zeta_A(s)$. Later we will consider generalizations of $\zeta_A(s)$ in the context of function fields over finite fields.

Properties of $\zeta_A(s)$

- Analytic continuation. By equation (3.3), $\zeta_A(s)$ is well defined for the whole complex plane $\mathbb{C}$ except for
- Simple pole at $s = 1$ with residue $\frac{1}{\log(q)}$.
- **Functional Equation.** Let $\Gamma_A(s) = (1 - q^{-s})^{-1}$ be the Gamma function over A. Set $\xi_A(s) = q^{-s}\Gamma_A(s)\zeta_A(s)$. Then it is easy to check that

$$\xi_A(s) = \xi_A(1 - s).$$

As opposed to the case of the classical zeta-function, the proofs are very easy for $\zeta_A(s)$. Later we will consider generalizations of $\zeta_A(s)$ in the context of function fields over finite fields. Similar statements will hold, but the proofs will be more difficult and will be based on the Riemann-Roch theorem for algebraic curves.

Euler Product

Euler noted that the unique decomposition of integers into products of primes leads to the following identity for the Riemann zeta-function:

$$\zeta(s) = \prod_{\substack{p \text{ prime} \\ p>0}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Euler Product

Euler noted that the unique decomposition of integers into products of primes leads to the following identity for the Riemann zeta-function:

$$\zeta(s) = \prod_{\substack{p \text{ prime} \\ p>0}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

This is valid for $\Re(s) > 1$. The exact same reasoning (which we won't repeat here) leads to the following identity:

$$\zeta_A(s) = \prod_{\substack{P \text{ monic} \\ \text{irreducible}}} \left(1 - \frac{1}{|P|^s}\right)^{-1}. \tag{3.4}$$

Euler Product

Euler noted that the unique decomposition of integers into products of primes leads to the following identity for the Riemann zeta-function:

$$\zeta(s) = \prod_{\substack{p \text{ prime} \\ p>0}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

This is valid for $\Re(s) > 1$. The exact same reasoning (which we won't repeat here) leads to the following identity:

$$\zeta_A(s) = \prod_{\substack{P \text{ monic} \\ \text{irreducible}}} \left(1 - \frac{1}{|P|^s}\right)^{-1}. \tag{3.4}$$

One can immediately put this Equation in use.

Primes in $\mathbb{F}_q[T]$

Proposition

There are infinitely many monic irreducibles in $\mathbb{F}_q[T]$.

Primes in $\mathbb{F}_q[T]$

Proposition

There are infinitely many monic irreducibles in $\mathbb{F}_q[T]$.

Proof.

Suppose there were only finitely many irreducible polynomials in A. The right-hand side of the Euler product would then be defined at $s = 1$ and even have a non-zero value there. On the other hand, the left hand side has a pole at $s = 1$. This shows there are infinitely many irreducibles in A. □

Primes in $\mathbb{F}_q[T]$

Proposition

There are infinitely many monic irreducibles in $\mathbb{F}_q[T]$.

Proof.

Suppose there were only finitely many irreducible polynomials in A. The right-hand side of the Euler product would then be defined at $s = 1$ and even have a non-zero value there. On the other hand, the left hand side has a pole at $s = 1$. This shows there are infinitely many irreducibles in A. □

One doesn't need the zeta function to show this. Euclid's proof that there are infinitely many prime integers works equally well in A.

Prime Number Theorem

Let x be a real number and $\pi(x)$ be the number of prime numbers less than or equal to x.

Prime Number Theorem

Let x be a real number and $\pi(x)$ be the number of prime numbers less than or equal to x.

Theorem (Prime Number Theorem (1896) - Hadamard and de la Vallée-Poussin)

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

Prime Number Theorem

Let x be a real number and $\pi(x)$ be the number of prime numbers less than or equal to x.

Theorem (Prime Number Theorem (1896) - Hadamard and de la Vallée-Poussin)

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

Let d be a positive integer and $x = q^d$.

Prime Number Theorem

Let x be a real number and $\pi(x)$ be the number of prime numbers less than or equal to x.

Theorem (Prime Number Theorem (1896) - Hadamard and de la Vallée-Poussin)

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

Let d be a positive integer and $x = q^d$. We will show that the number of monic irreducibles P such that $|P| = x$ is asymptotic to $x/\log_q(x)$ which is clearly in the spirit of the classical result above.

Prime Number Theorem

Let x be a real number and $\pi(x)$ be the number of prime numbers less than or equal to x.

Theorem (Prime Number Theorem (1896) - Hadamard and de la Vallée-Poussin)

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

Let d be a positive integer and $x = q^d$. We will show that the number of monic irreducibles P such that $|P| = x$ is asymptotic to $x/\log_q(x)$ which is clearly in the spirit of the classical result above.

Proposition (Gauss)

Let a_d be the number of monic irreducibles of degree d. Then

$$\sum_{d|n} d a_d = q^n \tag{3.5}$$

Proof.

Define a_d to be the number of monic irreducibles of degree d.

Proof.

Define a_d to be the number of monic irreducibles of degree d. Then, from the equation defining $\zeta_A(s)$ we find

$$\zeta_A(s) = \prod_{d=1}^{\infty} (1 - q^{-ds})^{-a_d}.$$

Proof.

Define a_d to be the number of monic irreducibles of degree d. Then, from the equation defining $\zeta_A(s)$ we find

$$\zeta_A(s) = \prod_{d=1}^{\infty} (1 - q^{-ds})^{-a_d}.$$

If we recall that $\zeta_A(s) = (1 - q^{1-s})^{-1}$ and substitute $u = q^{-s}$

Proof.

Define a_d to be the number of monic irreducibles of degree d. Then, from the equation defining $\zeta_A(s)$ we find

$$\zeta_A(s) = \prod_{d=1}^{\infty} (1 - q^{-ds})^{-a_d}.$$

If we recall that $\zeta_A(s) = (1 - q^{1-s})^{-1}$ and substitute $u = q^{-s}$ (note that $|u| < 1$ if and only if $\Re(s) > 1$)

Proof.

Define a_d to be the number of monic irreducibles of degree d. Then, from the equation defining $\zeta_A(s)$ we find

$$\zeta_A(s) = \prod_{d=1}^{\infty} (1 - q^{-ds})^{-a_d}.$$

If we recall that $\zeta_A(s) = (1 - q^{1-s})^{-1}$ and substitute $u = q^{-s}$ (note that $|u| < 1$ if and only if $\Re(s) > 1$) we obtain the identity

Proof.

Define a_d to be the number of monic irreducibles of degree d. Then, from the equation defining $\zeta_A(s)$ we find

$$\zeta_A(s) = \prod_{d=1}^{\infty} (1 - q^{-ds})^{-a_d}.$$

If we recall that $\zeta_A(s) = (1 - q^{1-s})^{-1}$ and substitute $u = q^{-s}$ (note that $|u| < 1$ if and only if $\Re(s) > 1$) we obtain the identity

$$\frac{1}{1 - qu} = \prod_{d=1}^{\infty} (1 - u^d)^{-a_d}.$$

Proof.

Define a_d to be the number of monic irreducibles of degree d. Then, from the equation defining $\zeta_A(s)$ we find

$$\zeta_A(s) = \prod_{d=1}^{\infty} (1 - q^{-ds})^{-a_d}.$$

If we recall that $\zeta_A(s) = (1 - q^{1-s})^{-1}$ and substitute $u = q^{-s}$ (note that $|u| < 1$ if and only if $\Re(s) > 1$) we obtain the identity

$$\frac{1}{1 - qu} = \prod_{d=1}^{\infty} (1 - u^d)^{-a_d}.$$

Taking the logarithmic derivative of both sides and multiplying the result by u yields

Proof.

Define a_d to be the number of monic irreducibles of degree d. Then, from the equation defining $\zeta_A(s)$ we find

$$\zeta_A(s) = \prod_{d=1}^{\infty} (1 - q^{-ds})^{-a_d}.$$

If we recall that $\zeta_A(s) = (1 - q^{1-s})^{-1}$ and substitute $u = q^{-s}$ (note that $|u| < 1$ if and only if $\Re(s) > 1$) we obtain the identity

$$\frac{1}{1 - qu} = \prod_{d=1}^{\infty} (1 - u^d)^{-a_d}.$$

Taking the logarithmic derivative of both sides and multiplying the result by u yields

$$\frac{qu}{1 - qu} = \sum_{d=1}^{\infty} \frac{d a_d u^d}{1 - u^d}.$$

Proof.

Define a_d to be the number of monic irreducibles of degree d. Then, from the equation defining $\zeta_A(s)$ we find

$$\zeta_A(s) = \prod_{d=1}^{\infty} (1 - q^{-ds})^{-a_d}.$$

If we recall that $\zeta_A(s) = (1 - q^{1-s})^{-1}$ and substitute $u = q^{-s}$ (note that $|u| < 1$ if and only if $\Re(s) > 1$) we obtain the identity

$$\frac{1}{1 - qu} = \prod_{d=1}^{\infty} (1 - u^d)^{-a_d}.$$

Taking the logarithmic derivative of both sides and multiplying the result by u yields

$$\frac{qu}{1 - qu} = \sum_{d=1}^{\infty} \frac{d a_d u^d}{1 - u^d}.$$

Finally, expand both sides into power series using the geometric series and compare coefficients of u^n.

Prime Number Theorem for Polynomials

Theorem

Let $\pi_A(n)$ denote the number of monic irreducible polynomials in $A = \mathbb{F}_q[T]$ of degree n. Then,

$$\pi_A(n) = \frac{q^n}{n} + O(\frac{q^{n/2}}{n}). \tag{3.6}$$

Prime Number Theorem for Polynomials

Theorem

Let $\pi_A(n)$ denote the number of monic irreducible polynomials in $A = \mathbb{F}_q[T]$ of degree n. Then,

$$\pi_A(n) = \frac{q^n}{n} + O(\frac{q^{n/2}}{n}). \tag{3.6}$$

Proof.

We apply the Möbius inversion formula to the formula given in the proposition to obtain that

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

Prime Number Theorem for Polynomials

Theorem

Let $\pi_A(n)$ denote the number of monic irreducible polynomials in $A = \mathbb{F}_q[T]$ of degree n. Then,

$$\pi_A(n) = \frac{q^n}{n} + O(\frac{q^{n/2}}{n}). \tag{3.6}$$

Proof.

We apply the Möbius inversion formula to the formula given in the proposition to obtain that

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

From equation above we see that the highest power of q that occurs is q^n and the next highest power that may occur is $q^{n/2}$

Prime Number Theorem for Polynomials

Theorem

Let $\pi_A(n)$ denote the number of monic irreducible polynomials in $A = \mathbb{F}_q[T]$ of degree n. Then,

$$\pi_A(n) = \frac{q^n}{n} + O(\frac{q^{n/2}}{n}). \tag{3.6}$$

Proof.

We apply the Möbius inversion formula to the formula given in the proposition to obtain that

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

From equation above we see that the highest power of q that occurs is q^n and the next highest power that may occur is $q^{n/2}$ (this occurs if and only if $2 \mid n$). All the other terms have the form $\pm q^m$ where $m \leq \frac{n}{3}$.

Prime Number Theorem for Polynomials

Theorem

Let $\pi_A(n)$ denote the number of monic irreducible polynomials in $A = \mathbb{F}_q[T]$ of degree n. Then,

$$\pi_A(n) = \frac{q^n}{n} + O(\frac{q^{n/2}}{n}). \tag{3.6}$$

Proof.

We apply the Möbius inversion formula to the formula given in the proposition to obtain that

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

From equation above we see that the highest power of q that occurs is q^n and the next highest power that may occur is $q^{n/2}$ (this occurs if and only if $2 \mid n$). All the other terms have the form $\pm q^m$ where $m \leq \frac{n}{3}$. The total number of terms is $\sum_{d|n} |\mu(d)|$, which is easily seen to be 2^t, where t is the number of distinct prime divisors of n.

Prime Number Theorem for Polynomials

Theorem

Let $\pi_A(n)$ denote the number of monic irreducible polynomials in $A = \mathbb{F}_q[T]$ of degree n. Then,

$$\pi_A(n) = \frac{q^n}{n} + O(\frac{q^{n/2}}{n}). \tag{3.6}$$

Proof.

We apply the Möbius inversion formula to the formula given in the proposition to obtain that

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

From equation above we see that the highest power of q that occurs is q^n and the next highest power that may occur is $q^{n/2}$ (this occurs if and only if $2 \mid n$). All the other terms have the form $\pm q^m$ where $m \leq \frac{n}{3}$. The total number of terms is $\sum_{d|n} |\mu(d)|$, which is easily seen to be 2^t, where t is the number of distinct prime divisors of n. . Let $p_1, p_2, \ldots, p_t$ be the distinct primes dividing n.

Prime Number Theorem for Polynomials

Theorem

Let $\pi_A(n)$ denote the number of monic irreducible polynomials in $A = \mathbb{F}_q[T]$ of degree n. Then,

$$\pi_A(n) = \frac{q^n}{n} + O(\frac{q^{n/2}}{n}). \tag{3.6}$$

Proof.

We apply the Möbius inversion formula to the formula given in the proposition to obtain that

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

From equation above we see that the highest power of q that occurs is q^n and the next highest power that may occur is $q^{n/2}$ (this occurs if and only if $2 \mid n$). All the other terms have the form $\pm q^m$ where $m \leq \frac{n}{3}$. The total number of terms is $\sum_{d|n} |\mu(d)|$, which is easily seen to be 2^t, where t is the number of distinct prime divisors of n. . Let $p_1, p_2, \ldots, p_t$ be the distinct primes dividing n. Then, $2^t \leq p_1 p_2 \ldots p_t \leq n$.

Prime Number Theorem for Polynomials

Theorem

Let $\pi_A(n)$ denote the number of monic irreducible polynomials in $A = \mathbb{F}_q[T]$ of degree n. Then,

$$\pi_A(n) = \frac{q^n}{n} + O(\frac{q^{n/2}}{n}). \tag{3.6}$$

Proof.

We apply the Möbius inversion formula to the formula given in the proposition to obtain that

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

From equation above we see that the highest power of q that occurs is q^n and the next highest power that may occur is $q^{n/2}$ (this occurs if and only if $2 \mid n$). All the other terms have the form $\pm q^m$ where $m \leq \frac{n}{3}$. The total number of terms is $\sum_{d|n} |\mu(d)|$, which is easily seen to be 2^t, where t is the number of distinct prime divisors of n. . Let $p_1, p_2, \ldots, p_t$ be the distinct primes dividing n. Then, $2^t \leq p_1 p_2 \ldots p_t \leq n$. Thus, we have the following estimate:

$$\left| a_n - \frac{q^n}{n} \right| \leq \frac{q^{n/2}}{n} + q^{n/3}.$$

Noting that $a_n = \pi_A(n)$ this establishes the theorem.

Prime Number Theorem for Polynomials

We have that

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

Prime Number Theorem for Polynomials

We have that

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

Note that if we set $x = q^n$ the right-hand side of this equation is $x/\log_q(x) + O(\sqrt{x}/\log_q(x))$ which looks like the conjectured precise form of the classical prime number theorem.

Prime Number Theorem for Polynomials

We have that

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

Note that if we set $x = q^n$ the right-hand side of this equation is $x/\log_q(x) + O(\sqrt{x}/\log_q(x))$ which looks like the conjectured precise form of the classical prime number theorem. This still not proven. It depends on the truth of the Riemann hypothesis.

The number of square-free polynomials

We will use the zeta function for other counting problems.

The number of square-free polynomials

We will use the zeta function for other counting problems. What is the number of square-free monics of degree n?

The number of square-free polynomials

We will use the zeta function for other counting problems. What is the number of square-free monics of degree n?

Proposition

Let $b_n = \#\{f \in A, \text{monic}, \deg(f) = n, f \text{ square-free}\}$. *Then* $b_1 = q$ *and for* $n > 1$, $b_n = q^n(1 - q^{-1})$.

The number of square-free polynomials

We will use the zeta function for other counting problems. What is the number of square-free monics of degree n?

Proposition

Let $b_n = \#\{f \in A, \text{monic}, \deg(f) = n, f \text{ square-free}\}$. *Then* $b_1 = q$ *and for* $n > 1$, $b_n = q^n(1 - q^{-1})$.

Proof.

Consider the product

$$\prod_P \left(1 + \frac{1}{|P|^s}\right) = \sum \frac{\delta(f)}{|f|^s}.$$

The number of square-free polynomials

We will use the zeta function for other counting problems. What is the number of square-free monics of degree n?

Proposition

Let $b_n = \#\{f \in A, \text{monic}, \deg(f) = n, f \text{ square-free}\}$. *Then* $b_1 = q$ *and for* $n > 1$, $b_n = q^n(1 - q^{-1})$.

Proof.

Consider the product

$$\prod_P \left(1 + \frac{1}{|P|^s}\right) = \sum \frac{\delta(f)}{|f|^s}.$$

As usual, the product is over all monic irreducibles P and the sum is over all monics f.

The number of square-free polynomials

We will use the zeta function for other counting problems. What is the number of square-free monics of degree n?

Proposition

Let $b_n = \#\{f \in A, \text{monic}, \deg(f) = n, f \text{ square-free}\}$. *Then* $b_1 = q$ *and for* $n > 1$, $b_n = q^n(1 - q^{-1})$.

Proof.

Consider the product

$$\prod_P \left(1 + \frac{1}{|P|^s}\right) = \sum \frac{\delta(f)}{|f|^s}.$$

As usual, the product is over all monic irreducibles P and the sum is over all monics f. The function $\delta(f)$ is 1 when f is square-free, and 0 otherwise.

The number of square-free polynomials

We will use the zeta function for other counting problems. What is the number of square-free monics of degree n?

Proposition

Let $b_n = \#\{f \in A, \text{monic}, \deg(f) = n, f \text{ square-free}\}$. Then $b_1 = q$ and for $n > 1$, $b_n = q^n(1 - q^{-1})$.

Proof.

Consider the product

$$\prod_P \left(1 + \frac{1}{|P|^s}\right) = \sum \frac{\delta(f)}{|f|^s}.$$

As usual, the product is over all monic irreducibles P and the sum is over all monics f. The function $\delta(f)$ is 1 when f is square-free, and 0 otherwise. This is an easy consequence of unique factorization in A and the definition of square-free.

The number of square-free polynomials

We will use the zeta function for other counting problems. What is the number of square-free monics of degree n?

Proposition

Let $b_n = \#\{f \in A, \text{monic}, \deg(f) = n, f \text{ square-free}\}$. *Then* $b_1 = q$ *and for* $n > 1$, $b_n = q^n(1 - q^{-1})$.

Proof.

Consider the product

$$\prod_P \left(1 + \frac{1}{|P|^s}\right) = \sum \frac{\delta(f)}{|f|^s}.$$

As usual, the product is over all monic irreducibles P and the sum is over all monics f. The function $\delta(f)$ is 1 when f is square-free, and 0 otherwise. This is an easy consequence of unique factorization in A and the definition of square-free. Making the substitution $u = q^{-s}$, the right-hand side of equation above becomes $\sum_{n=0}^{\infty} b_n u^n$.

The number of square-free polynomials

We will use the zeta function for other counting problems. What is the number of square-free monics of degree n?

Proposition

Let $b_n = \#\{f \in A, \text{monic}, \deg(f) = n, f \text{ square-free}\}$. Then $b_1 = q$ and for $n > 1$, $b_n = q^n(1 - q^{-1})$.

Proof.

Consider the product

$$\prod_P \left(1 + \frac{1}{|P|^s}\right) = \sum \frac{\delta(f)}{|f|^s}.$$

As usual, the product is over all monic irreducibles P and the sum is over all monics f. The function $\delta(f)$ is 1 when f is square-free, and 0 otherwise. This is an easy consequence of unique factorization in A and the definition of square-free. Making the substitution $u = q^{-s}$, the right-hand side of equation above becomes $\sum_{n=0}^{\infty} b_n u^n$. Consider the identity $1 + w = (1 - w^2)/(1 - w)$.

The number of square-free polynomials

We will use the zeta function for other counting problems. What is the number of square-free monics of degree n?

Proposition

Let $b_n = \#\{f \in A, \text{monic}, \deg(f) = n, f \text{ square-free}\}$. Then $b_1 = q$ and for $n > 1$, $b_n = q^n(1 - q^{-1})$.

Proof.

Consider the product

$$\prod_P \left(1 + \frac{1}{|P|^s}\right) = \sum \frac{\delta(f)}{|f|^s}.$$

As usual, the product is over all monic irreducibles P and the sum is over all monics f. The function $\delta(f)$ is 1 when f is square-free, and 0 otherwise. This is an easy consequence of unique factorization in A and the definition of square-free. Making the substitution $u = q^{-s}$, the right-hand side of equation above becomes $\sum_{n=0}^{\infty} b_n u^n$. Consider the identity $1 + w = (1 - w^2)/(1 - w)$. If we substitute $w = |P|^{-s}$ and then take the product over all monic irreducibles P, we see that the left-hand side is equal to $\zeta_A(s)/\zeta_A(2s) = (1 - q^{1-2s})/(1 - q^{1-s})$.

The number of square-free polynomials

We will use the zeta function for other counting problems. What is the number of square-free monics of degree n?

Proposition

Let $b_n = \#\{f \in A, \text{monic}, \deg(f) = n, f \text{ square-free}\}$. Then $b_1 = q$ and for $n > 1$, $b_n = q^n(1 - q^{-1})$.

Proof.

Consider the product

$$\prod_P \left(1 + \frac{1}{|P|^s}\right) = \sum \frac{\delta(f)}{|f|^s}.$$

As usual, the product is over all monic irreducibles P and the sum is over all monics f. The function $\delta(f)$ is 1 when f is square-free, and 0 otherwise. This is an easy consequence of unique factorization in A and the definition of square-free. Making the substitution $u = q^{-s}$, the right-hand side of equation above becomes $\sum_{n=0}^{\infty} b_n u^n$. Consider the identity $1 + w = (1 - w^2)/(1 - w)$. If we substitute $w = |P|^{-s}$ and then take the product over all monic irreducibles P, we see that the left-hand side is equal to $\zeta_A(s)/\zeta_A(2s) = (1 - q^{1-2s})/(1 - q^{1-s})$. Putting everything in terms of u leads to the identity

$$\frac{1 - qu^2}{1 - qu} = \sum_{n=0}^{\infty} b_n u^n.$$

The number of square-free polynomials

We will use the zeta function for other counting problems. What is the number of square-free monics of degree n?

Proposition

Let $b_n = \#\{f \in A, \text{monic}, \deg(f) = n, f \text{ square-free}\}$. Then $b_1 = q$ and for $n > 1$, $b_n = q^n(1 - q^{-1})$.

Proof.

Consider the product

$$\prod_P \left(1 + \frac{1}{|P|^s}\right) = \sum \frac{\delta(f)}{|f|^s}.$$

As usual, the product is over all monic irreducibles P and the sum is over all monics f. The function $\delta(f)$ is 1 when f is square-free, and 0 otherwise. This is an easy consequence of unique factorization in A and the definition of square-free. Making the substitution $u = q^{-s}$, the right-hand side of equation above becomes $\sum_{n=0}^{\infty} b_n u^n$. Consider the identity $1 + w = (1 - w^2)/(1 - w)$. If we substitute $w = |P|^{-s}$ and then take the product over all monic irreducibles P, we see that the left-hand side is equal to $\zeta_A(s)/\zeta_A(2s) = (1 - q^{1-2s})/(1 - q^{1-s})$. Putting everything in terms of u leads to the identity

$$\frac{1 - qu^2}{1 - qu} = \sum_{n=0}^{\infty} b_n u^n.$$

Expand the left-hand side in a geometric series and compare the coefficients of u^n. □

Let us compare the previous result with what is known to be true in $\mathbb{Z}$.

Let us compare the previous result with what is known to be true in $\mathbb{Z}$.

- Let B_n be the number of positive square-free integers less than or equal to n. Then,

$$\lim_{n\to\infty} \frac{B_n}{n} = \frac{6}{\pi^2}.$$

Let us compare the previous result with what is known to be true in $\mathbb{Z}$.

- Let B_n be the number of positive square-free integers less than or equal to n. Then,

$$\lim_{n\to\infty} \frac{B_n}{n} = \frac{6}{\pi^2}.$$

- The probability that a positive integer is square-free is $6/\pi^2$.

Let us compare the previous result with what is known to be true in $\mathbb{Z}$.

- Let B_n be the number of positive square-free integers less than or equal to n. Then,

$$\lim_{n\to\infty} \frac{B_n}{n} = \frac{6}{\pi^2}.$$

- The probability that a positive integer is square-free is $6/\pi^2$.
- Now the probability that a monic polynomial of degree n is square-free is b_n/q^n, and this is equals to $(1 - q^{-1})$ for $n > 1$.

Let us compare the previous result with what is known to be true in $\mathbb{Z}$.

- Let B_n be the number of positive square-free integers less than or equal to n. Then,

$$\lim_{n\to\infty} \frac{B_n}{n} = \frac{6}{\pi^2}.$$

- The probability that a positive integer is square-free is $6/\pi^2$.
- Now the probability that a monic polynomial of degree n is square-free is b_n/q^n, and this is equals to $(1 - q^{-1})$ for $n > 1$.
- Thus the probability that a monic polynomial in A is square-free is $(1 - q^{-1}) = \frac{1}{\zeta_A(2)}$.

Let us compare the previous result with what is known to be true in $\mathbb{Z}$.

- Let B_n be the number of positive square-free integers less than or equal to n. Then,

$$\lim_{n\to\infty} \frac{B_n}{n} = \frac{6}{\pi^2}.$$

- The probability that a positive integer is square-free is $6/\pi^2$.
- Now the probability that a monic polynomial of degree n is square-free is b_n/q^n, and this is equals to $(1 - q^{-1})$ for $n > 1$.
- Thus the probability that a monic polynomial in A is square-free is $(1 - q^{-1}) = \frac{1}{\zeta_A(2)}$.
- Note that $6/\pi^2 = \frac{1}{\zeta(2)}$

Arithmetic Functions

Our goal now is to introduce analogues of some well-known number-theoretic functions and to discuss their properties.

Arithmetic Functions

Our goal now is to introduce analogues of some well-known number-theoretic functions and to discuss their properties. We have already introduced the Euler's $\Phi(f)$ function.

Arithmetic Functions

Our goal now is to introduce analogues of some well-known number-theoretic functions and to discuss their properties. We have already introduced the Euler's $\Phi(f)$ function.

Definition (Möbius Function)

$$\mu(f) = \begin{cases} 0 & \text{if } f \text{ is not square-free} \\ (-1)^t & \text{if } f = \alpha P_1 P_2 \dots P_t. \end{cases} \tag{3.7}$$

Arithmetic Functions

Our goal now is to introduce analogues of some well-known number-theoretic functions and to discuss their properties. We have already introduced the Euler's $\Phi(f)$ function.

Definition (Möbius Function)

$$\mu(f) = \begin{cases} 0 & \text{if } f \text{ is not square-free} \\ (-1)^t & \text{if } f = \alpha P_1 P_2 \dots P_t. \end{cases} \tag{3.7}$$

Definition (Divisor Functions)

Let $d_k(f)$ denote the k-fold divisor function.

Arithmetic Functions

Our goal now is to introduce analogues of some well-known number-theoretic functions and to discuss their properties. We have already introduced the Euler's $\Phi(f)$ function.

Definition (Möbius Function)

$$\mu(f) = \begin{cases} 0 & \text{if } f \text{ is not square-free} \\ (-1)^t & \text{if } f = \alpha P_1 P_2 \dots P_t. \end{cases} \tag{3.7}$$

Definition (Divisor Functions)

Let $d_k(f)$ denote the k-fold divisor function.

$$d_k(f) = \sum_{f_1 \dots f_k = f} 1,$$

Arithmetic Functions

Our goal now is to introduce analogues of some well-known number-theoretic functions and to discuss their properties. We have already introduced the Euler's $\Phi(f)$ function.

Definition (Möbius Function)

$$\mu(f) = \begin{cases} 0 & \text{if } f \text{ is not square-free} \\ (-1)^t & \text{if } f = \alpha P_1 P_2 \dots P_t. \end{cases} \tag{3.7}$$

Definition (Divisor Functions)

Let $d_k(f)$ denote the k-fold divisor function.

$$d_k(f) = \sum_{f_1 \dots f_k = f} 1,$$

i.e., $d_k(f)$ is the number of ways to express f as a product of k factors.

Arithmetic Functions

Our goal now is to introduce analogues of some well-known number-theoretic functions and to discuss their properties. We have already introduced the Euler's $\Phi(f)$ function.

Definition (Möbius Function)

$$\mu(f) = \begin{cases} 0 & \text{if } f \text{ is not square-free} \\ (-1)^t & \text{if } f = \alpha P_1 P_2 \dots P_t. \end{cases} \tag{3.7}$$

Definition (Divisor Functions)

Let $d_k(f)$ denote the k-fold divisor function.

$$d_k(f) = \sum_{f_1 \dots f_k = f} 1,$$

i.e., $d_k(f)$ is the number of ways to express f as a product of k factors.

If $k = 2$ then $d_2(f) = d(f)$ is the usual **divisor function**.

Arithmetic Functions

Definition (Sum of Divisors)

$$\sigma(f) = \sum_{g|f} |g|,$$

where the sum is over all monic divisors of f.

Definition (Sum of Divisors)

$$\sigma(f) = \sum_{g|f} |g|,$$

where the sum is over all monic divisors of f.

Definition (Liouville function)

$$\lambda(f) = \begin{cases} 1 & \text{if } f = \alpha,\ \alpha \in \mathbb{F}_q^* \\ (-1)^{a_1+\cdots+a_k} & \text{if } f = \alpha P_1^{a_1} P_2^{a_2} \dots P_k^{a_k}. \end{cases} \tag{3.8}$$

Definition (Sum of Divisors)

$$\sigma(f) = \sum_{g|f} |g|,$$

where the sum is over all monic divisors of f.

Definition (Liouville function)

$$\lambda(f) = \begin{cases} 1 & \text{if } f = \alpha,\ \alpha \in \mathbb{F}_q^* \\ (-1)^{a_1+\cdots+a_k} & \text{if } f = \alpha P_1^{a_1} P_2^{a_2} \dots P_k^{a_k}. \end{cases} \tag{3.8}$$

Note that $\lambda(\alpha f) = \lambda(f)$.

Definition (Sum of Divisors)

$$\sigma(f) = \sum_{g|f} |g|,$$

where the sum is over all monic divisors of f.

Definition (Liouville function)

$$\lambda(f) = \begin{cases} 1 & \text{if } f = \alpha,\ \alpha \in \mathbb{F}_q^* \\ (-1)^{a_1+\cdots+a_k} & \text{if } f = \alpha P_1^{a_1} P_2^{a_2} \dots P_k^{a_k}. \end{cases} \tag{3.8}$$

Note that $\lambda(\alpha f) = \lambda(f)$.

Definition (von Mangoldt function)

$$\Lambda(f) = \begin{cases} \log_q |P| = deg(P) & \text{if } f = P^k \\ 0 & \text{otherwise.} \end{cases} \tag{3.9}$$

Multiplicative Functions

Some of these functions, like their counterparts, have the property of being multiplicative.

Multiplicative Functions

Some of these functions, like their counterparts, have the property of being multiplicative.

Definition

A complex valued function F on $A - \{0\}$ is called ***multiplicative*** *if $F(fg) = F(f)F(g)$ whenever f and g are relatively prime. We assume F is 1 on $\mathbb{F}_q^*$.*

Multiplicative Functions

Some of these functions, like their counterparts, have the property of being multiplicative.

Definition

A complex valued function F on $A - \{0\}$ is called ***multiplicative*** *if $F(fg) = F(f)F(g)$ whenever f and g are relatively prime. We assume F is 1 on $\mathbb{F}_q^*$.*

Let

$$f = \alpha P_1^{e_1} P_2^{e_2} \dots P_t^{e_t}$$

be the prime decomposition of f.

Multiplicative Functions

Some of these functions, like their counterparts, have the property of being multiplicative.

Definition

A complex valued function F on $A - \{0\}$ is called ***multiplicative*** *if $F(fg) = F(f)F(g)$ whenever f and g are relatively prime. We assume F is 1 on $\mathbb{F}_q^*$.*

Let

$$f = \alpha P_1^{e_1} P_2^{e_2} \dots P_t^{e_t}$$

be the prime decomposition of f. If F is multiplicative,

$$F(f) = F(P_1^{e_1})F(P_2^{e_2}) \dots F(P_t^{e_t}).$$

Multiplicative Functions

Some of these functions, like their counterparts, have the property of being multiplicative.

Definition

A complex valued function F on $A - \{0\}$ is called ***multiplicative*** *if $F(fg) = F(f)F(g)$ whenever f and g are relatively prime. We assume F is 1 on $\mathbb{F}_q^*$.*

Let

$$f = \alpha P_1^{e_1} P_2^{e_2} \dots P_t^{e_t}$$

be the prime decomposition of f. If F is multiplicative,

$$F(f) = F(P_1^{e_1})F(P_2^{e_2}) \dots F(P_t^{e_t}).$$

Thus, a multiplicative function is completely determined by its values on prime powers.

Multiplicative Functions

Some of these functions, like their counterparts, have the property of being multiplicative.

Definition

A complex valued function F on $A - \{0\}$ is called ***multiplicative*** *if $F(fg) = F(f)F(g)$ whenever f and g are relatively prime. We assume F is 1 on $\mathbb{F}_q^*$.*

Let

$$f = \alpha P_1^{e_1} P_2^{e_2} \dots P_t^{e_t}$$

be the prime decomposition of f. If F is multiplicative,

$$F(f) = F(P_1^{e_1})F(P_2^{e_2}) \dots F(P_t^{e_t}).$$

Thus, a multiplicative function is completely determined by its values on prime powers. Using multiplicativity, one can derive the following formulas

Multiplicative Functions

Some of these functions, like their counterparts, have the property of being multiplicative.

Definition

A complex valued function F on $A - \{0\}$ is called ***multiplicative*** *if $F(fg) = F(f)F(g)$ whenever f and g are relatively prime. We assume F is 1 on $\mathbb{F}_q^*$.*

Let

$$f = \alpha P_1^{e_1} P_2^{e_2} \dots P_t^{e_t}$$

be the prime decomposition of f. If F is multiplicative,

$$F(f) = F(P_1^{e_1})F(P_2^{e_2}) \dots F(P_t^{e_t}).$$

Thus, a multiplicative function is completely determined by its values on prime powers. Using multiplicativity, one can derive the following formulas

Proposition

Let the prime decomposition of f be given as above. Then,

Multiplicative Functions

Some of these functions, like their counterparts, have the property of being multiplicative.

Definition

A complex valued function F on $A - \{0\}$ is called ***multiplicative*** *if $F(fg) = F(f)F(g)$ whenever f and g are relatively prime. We assume F is 1 on $\mathbb{F}_q^*$.*

Let

$$f = \alpha P_1^{e_1} P_2^{e_2} \dots P_t^{e_t}$$

be the prime decomposition of f. If F is multiplicative,

$$F(f) = F(P_1^{e_1})F(P_2^{e_2}) \dots F(P_t^{e_t}).$$

Thus, a multiplicative function is completely determined by its values on prime powers. Using multiplicativity, one can derive the following formulas

Proposition

Let the prime decomposition of f be given as above. Then,

1. $d(f) = (e_1 + 1)(e_2 + 1) \dots (e_t + 1)$.

Multiplicative Functions

Some of these functions, like their counterparts, have the property of being multiplicative.

Definition

A complex valued function F on $A - \{0\}$ is called ***multiplicative*** *if $F(fg) = F(f)F(g)$ whenever f and g are relatively prime. We assume F is 1 on $\mathbb{F}_q^*$.*

Let

$$f = \alpha P_1^{e_1} P_2^{e_2} \dots P_t^{e_t}$$

be the prime decomposition of f. If F is multiplicative,

$$F(f) = F(P_1^{e_1})F(P_2^{e_2}) \dots F(P_t^{e_t}).$$

Thus, a multiplicative function is completely determined by its values on prime powers. Using multiplicativity, one can derive the following formulas

Proposition

Let the prime decomposition of f be given as above. Then,

1. $d(f) = (e_1 + 1)(e_2 + 1) \dots (e_t + 1)$.
2. $$\sigma(f) = \frac{|P_1|^{e_1+1} - 1}{|P_1| - 1} \frac{|P_2|^{e_2+1} - 1}{|P_2| - 1} \cdots \frac{|P_t|^{e_t+1} - 1}{|P_t| - 1}.$$

Reviewing the Dictionary between $\mathbb{F}_q[T]$ and $\mathbb{Z}$

Number Fields	Function Fields
$\mathbb{Z}$	$A = \mathbb{F}_q[T]$

Reviewing the Dictionary between $\mathbb{F}_q[T]$ and $\mathbb{Z}$

Number Fields	Function Fields
$\mathbb{Z}$	$A = \mathbb{F}_q[T]$
$\mathbb{Q}$	$k = \mathbb{F}_q(T)$

Reviewing the Dictionary between $\mathbb{F}_q[T]$ and $\mathbb{Z}$

Number Fields	Function Fields
$\mathbb{Z}$	$A = \mathbb{F}_q[T]$
$\mathbb{Q}$	$k = \mathbb{F}_q(T)$
positive integers	A^+ monic polynomials

Reviewing the Dictionary between $\mathbb{F}_q[T]$ and $\mathbb{Z}$

Number Fields	Function Fields
$\mathbb{Z}$	$A = \mathbb{F}_q[T]$
$\mathbb{Q}$	$k = \mathbb{F}_q(T)$
positive integers	A^+ monic polynomials
prime numbers	$\mathcal{P}$ monic irreducible polynomials

Reviewing the Dictionary between $\mathbb{F}_q[T]$ and $\mathbb{Z}$

Number Fields	Function Fields
$\mathbb{Z}$	$A = \mathbb{F}_q[T]$
$\mathbb{Q}$	$k = \mathbb{F}_q(T)$
positive integers	A^+ monic polynomials
prime numbers	$\mathcal{P}$ monic irreducible polynomials
absolute value $\lvert n \rvert$	norm of a polynomial $\lvert f \rvert = q^{\deg(f)}$

Reviewing the Dictionary between $\mathbb{F}_q[T]$ and $\mathbb{Z}$

Number Fields	Function Fields
$\mathbb{Z}$	$A = \mathbb{F}_q[T]$
$\mathbb{Q}$	$k = \mathbb{F}_q(T)$
positive integers	A^+ monic polynomials
prime numbers	$\mathcal{P}$ monic irreducible polynomials
absolute value $\lvert n \rvert$	norm of a polynomial $\lvert f \rvert = q^{\deg(f)}$
$n = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} P_2^{e_2 \dots P_t^{e_t}}$

Reviewing the Dictionary between $\mathbb{F}_q[T]$ and $\mathbb{Z}$

Number Fields	Function Fields
$\mathbb{Z}$	$A = \mathbb{F}_q[T]$
$\mathbb{Q}$	$k = \mathbb{F}_q(T)$
positive integers	A^+ monic polynomials
prime numbers	$\mathcal{P}$ monic irreducible polynomials
absolute value $\lvert n \rvert$	norm of a polynomial $\lvert f \rvert = q^{\deg(f)}$
$n = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} P_2^{e_2 \dots P_t^{e_t}}$
2	q-1

Reviewing the Dictionary between $\mathbb{F}_q[T]$ and $\mathbb{Z}$

Number Fields	Function Fields
$\mathbb{Z}$	$A = \mathbb{F}_q[T]$
$\mathbb{Q}$	$k = \mathbb{F}_q(T)$
positive integers	A^+ monic polynomials
prime numbers	$\mathcal{P}$ monic irreducible polynomials
absolute value $\lvert n \rvert$	norm of a polynomial $\lvert f \rvert = q^{\deg(f)}$
$n = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} P_2^{e_2 \dots} P_t^{e_t}$
2	q-1
$\phi(n) = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} 1$	$\Phi(f) = \sum_{\substack{k \text{ monic} \\ \deg(k)<\deg(f) \\ \gcd(f,k)=1}} 1$

Reviewing the Dictionary between $\mathbb{F}_q[T]$ and $\mathbb{Z}$

Number Fields	Function Fields
$\mathbb{Z}$	$A = \mathbb{F}_q[T]$
$\mathbb{Q}$	$k = \mathbb{F}_q(T)$
positive integers	A^+ monic polynomials
prime numbers	$\mathcal{P}$ monic irreducible polynomials
absolute value $\lvert n\rvert$	norm of a polynomial $\lvert f\rvert = q^{\deg(f)}$
$n = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} P_2^{e_2 \dots} P_t^{e_t}$
2	q-1
$\phi(n) = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} 1$	$\Phi(f) = \sum_{\substack{k \text{ monic} \\ \deg(k)<\deg(f) \\ \gcd(f,k)=1}} 1$
$n = p_1^{e_1} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} \dots P_t^{e_t}$

Reviewing the Dictionary between $\mathbb{F}_q[T]$ and $\mathbb{Z}$

Number Fields	Function Fields
$\mathbb{Z}$	$A = \mathbb{F}_q[T]$
$\mathbb{Q}$	$k = \mathbb{F}_q(T)$
positive integers	A^+ monic polynomials
prime numbers	$\mathcal{P}$ monic irreducible polynomials
absolute value $\lvert n\rvert$	norm of a polynomial $\lvert f\rvert = q^{\deg(f)}$
$n = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} P_2^{e_2 \dots} P_t^{e_t}$
2	q-1
$\phi(n) = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} 1$	$\Phi(f) = \sum_{\substack{k \text{ monic} \\ \deg(k)<\deg(f) \\ \gcd(f,k)=1}} 1$
$n = p_1^{e_1} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} \dots P_t^{e_t}$
$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$	$\zeta_A(s) = \sum_{f \text{ monic}} \frac{1}{\lvert f\rvert^s}$

Reviewing the Dictionary between $\mathbb{F}_q[T]$ and $\mathbb{Z}$

Number Fields	Function Fields
$\mathbb{Z}$	$A = \mathbb{F}_q[T]$
$\mathbb{Q}$	$k = \mathbb{F}_q(T)$
positive integers	A^+ monic polynomials
prime numbers	$\mathcal{P}$ monic irreducible polynomials
absolute value $\lvert n\rvert$	norm of a polynomial $\lvert f\rvert = q^{\deg(f)}$
$n = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} P_2^{e_2 \dots} P_t^{e_t}$
2	q-1
$\phi(n) = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} 1$	$\Phi(f) = \sum_{\substack{k \text{ monic} \\ \deg(k)<\deg(f) \\ \gcd(f,k)=1}} 1$
$n = p_1^{e_1} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} \dots P_t^{e_t}$
$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$	$\zeta_A(s) = \sum_{f \text{ monic}} \frac{1}{\lvert f\rvert^s}$
$\xi(s) = \pi^{-\frac{s}{2}} \Gamma(\frac{s}{2}) \zeta(s) = \xi(1-s)$	$\xi_A(s) = q^{-s} \Gamma_A(s) \zeta_A(s) = \xi_A(1-s)$

Reviewing the Dictionary between $\mathbb{F}_q[T]$ and $\mathbb{Z}$

Number Fields	Function Fields
$\mathbb{Z}$	$A = \mathbb{F}_q[T]$
$\mathbb{Q}$	$k = \mathbb{F}_q(T)$
positive integers	A^+ monic polynomials
prime numbers	$\mathcal{P}$ monic irreducible polynomials
absolute value $\lvert n\rvert$	norm of a polynomial $\lvert f\rvert = q^{\deg(f)}$
$n = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} P_2^{e_2 \dots} P_t^{e_t}$
2	q-1
$\phi(n) = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} 1$	$\Phi(f) = \sum_{\substack{k \text{ monic} \\ \deg(k)<\deg(f) \\ \gcd(f,k)=1}} 1$
$n = p_1^{e_1} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} \dots P_t^{e_t}$
$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$	$\zeta_A(s) = \sum_{f \text{ monic}} \frac{1}{\lvert f\rvert^s}$
$\xi(s) = \pi^{-\frac{s}{2}} \Gamma(\frac{s}{2}) \zeta(s) = \xi(1-s)$	$\xi_A(s) = q^{-s} \Gamma_A(s) \zeta_A(s) = \xi_A(1-s)$
$\zeta(s)$ has analytic continuation	$\zeta_A(s) = (1 - q^{1-s})^{-1}$

Reviewing the Dictionary between $\mathbb{F}_q[T]$ and $\mathbb{Z}$

Number Fields	Function Fields
$\mathbb{Z}$	$A = \mathbb{F}_q[T]$
$\mathbb{Q}$	$k = \mathbb{F}_q(T)$
positive integers	A^+ monic polynomials
prime numbers	$\mathcal{P}$ monic irreducible polynomials
absolute value $\lvert n\rvert$	norm of a polynomial $\lvert f\rvert = q^{\deg(f)}$
$n = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} P_2^{e_2 \dots} P_t^{e_t}$
2	q-1
$\phi(n) = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} 1$	$\Phi(f) = \sum_{\substack{k \text{ monic} \\ \deg(k)<\deg(f) \\ \gcd(f,k)=1}} 1$
$n = p_1^{e_1} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} \dots P_t^{e_t}$
$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$	$\zeta_A(s) = \sum_{f \text{ monic}} \frac{1}{\lvert f\rvert^s}$
$\xi(s) = \pi^{-\frac{s}{2}} \Gamma(\frac{s}{2}) \zeta(s) = \xi(1-s)$	$\xi_A(s) = q^{-s} \Gamma_A(s) \zeta_A(s) = \xi_A(1-s)$
$\zeta(s)$ has analytic continuation	$\zeta_A(s) = (1 - q^{1-s})^{-1}$
$\pi(x) \sim \frac{x}{\log(x)}$	$\pi_A(n) = \frac{q^n}{n} + O(\frac{q^{n/2}}{n})$

Reviewing the Dictionary between $\mathbb{F}_q[T]$ and $\mathbb{Z}$

Number Fields	Function Fields
$\mathbb{Z}$	$A = \mathbb{F}_q[T]$
$\mathbb{Q}$	$k = \mathbb{F}_q(T)$
positive integers	A^+ monic polynomials
prime numbers	$\mathcal{P}$ monic irreducible polynomials
absolute value $\lvert n\rvert$	norm of a polynomial $\lvert f\rvert = q^{\deg(f)}$
$n = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} P_2^{e_2 \dots} P_t^{e_t}$
2	q-1
$\phi(n) = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} 1$	$\Phi(f) = \sum_{\substack{k \text{ monic} \\ \deg(k)<\deg(f) \\ \gcd(f,k)=1}} 1$
$n = p_1^{e_1} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} \dots P_t^{e_t}$
$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$	$\zeta_A(s) = \sum_{f \text{ monic}} \frac{1}{\lvert f\rvert^s}$
$\xi(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s) = \xi(1-s)$	$\xi_A(s) = q^{-s}\Gamma_A(s)\zeta_A(s) = \xi_A(1-s)$
$\zeta(s)$ has analytic continuation	$\zeta_A(s) = (1-q^{1-s})^{-1}$
$\pi(x) \sim \frac{x}{\log(x)}$	$\pi_A(n) = \frac{q^n}{n} + O(\frac{q^{n/2}}{n})$
$\mu(n), d_k(n), \varphi(n), \Lambda(n), \lambda(n)$	$\mu(f), d_k(f), \Phi(f), \Lambda(f), \lambda(f)$