Analytic Number Theory in Function Fields (Lecture 2)

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

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

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

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

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

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

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

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 $\|n\|$	norm of a polynomial $\|f\| = q^{\deg(f)}$

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 $\lvert f \rvert = q^{\deg(f)}$
$n = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} P_2^{e_2} \dots P_t^{e_t}$

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 $\lvert f \rvert = q^{\deg(f)}$
$n = p_1^{e_1} p_2^{e_2} \ldots p_t^{e_t}$	$f = \alpha P_1^{e_1} P_2^{e_2} \ldots P_t^{e_t}$
2	q-1

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 $\|n\|$	norm of a polynomial $\|f\| = q^{\deg(f)}$
$n = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} P_2^{e_2} \dots P_t^{e_t}$
2	q-1
$\phi(n) = \sum^{n}{}_{\substack{k=1 \\ (k,n)=1}} 1$	$\Phi(f) = \sum_{\substack{k \text{ monic} \\ \deg(k)<\deg(f) \\ \gcd(f,k)=1}} 1$

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
$\phi(n) = \sum^{n}{}_{\substack{k=1 \\ (k,n)=1}} 1$	$\Phi(f) = \sum_{\substack{k \text{ monic} \\ \deg(k)<\deg(f) \\ \gcd(f,k)=1}} 1$
$n = p_1^{e_1} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} \dots P_t^{e_t}$

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 $\lvert f \rvert = q^{\deg(f)}$
$n = p_1^{e_1} p_2^{e_2} \ldots p_t^{e_t}$	$f = \alpha P_1^{e_1} P_2^{e_2} \ldots P_t^{e_t}$
2	q-1
$\phi(n) = \sum^{n}{}_{\substack{k=1 \\ (k,n)=1}} 1$	$\Phi(f) = \sum_{\substack{k \text{ monic} \\ \deg(k)<\deg(f) \\ \gcd(f,k)=1}} 1$
$n = p_1^{e_1} \ldots p_t^{e_t}$	$f = \alpha P_1^{e_1} \ldots P_t^{e_t}$
$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$	$\zeta_A(s) = \sum_{f \text{ monic}} \frac{1}{\lvert f \rvert^s}$

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 $\|n\|$	norm of a polynomial $\|f\| = q^{\deg(f)}$
$n = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} P_2^{e_2} \dots P_t^{e_t}$
2	q-1
$\phi(n) = \sum^{n}{}_{\substack{k=1 \\ (k,n)=1}} 1$	$\Phi(f) = \sum_{\substack{k \text{ monic} \\ \deg(k)<\deg(f) \\ \gcd(f,k)=1}} 1$
$n = p_1^{e_1} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} \dots P_t^{e_t}$
$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$	$\zeta_A(s) = \sum_{f \text{ monic}} \frac{1}{\|f\|^s}$
$\xi(s) = \pi^{-\frac{s}{2}} \Gamma(\frac{s}{2}) \zeta(s) = \xi(1-s)$	$\xi_A(s) = q^{-s} \Gamma_A(s) \zeta_A(s) = \xi_A(1-s)$

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
$\phi(n) = \sum^{n}{}_{\substack{k=1 \\ (k,n)=1}} 1$	$\Phi(f) = \sum_{\substack{k \text{ monic} \\ \deg(k)<\deg(f) \\ \gcd(f,k)=1}} 1$
$n = p_1^{e_1} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} \dots P_t^{e_t}$
$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$	$\zeta_A(s) = \sum_{f \text{ monic}} \frac{1}{\lvert f \rvert^s}$
$\xi(s) = \pi^{-\frac{s}{2}} \Gamma(\frac{s}{2}) \zeta(s) = \xi(1-s)$	$\xi_A(s) = q^{-s} \Gamma_A(s) \zeta_A(s) = \xi_A(1-s)$
$\zeta(s)$ has analytic continuation	$\zeta_A(s) = (1 - q^{1-s})^{-1}$

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 $\|n\|$	norm of a polynomial $\|f\| = q^{\deg(f)}$
$n = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} P_2^{e_2} \dots P_t^{e_t}$
2	q-1
$\phi(n) = \sum^n{}_{\substack{k=1 \\ (k,n)=1}} 1$	$\Phi(f) = \sum_{\substack{k \text{ monic} \\ \deg(k)<\deg(f) \\ \gcd(f,k)=1}} 1$
$n = p_1^{e_1} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} \dots P_t^{e_t}$
$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$	$\zeta_A(s) = \sum_{f \text{ monic}} \frac{1}{\|f\|^s}$
$\xi(s) = \pi^{-\frac{s}{2}} \Gamma(\frac{s}{2}) \zeta(s) = \xi(1-s)$	$\xi_A(s) = q^{-s} \Gamma_A(s) \zeta_A(s) = \xi_A(1-s)$
$\zeta(s)$ has analytic continuation	$\zeta_A(s) = (1 - q^{1-s})^{-1}$
$\pi(x) \sim \frac{x}{\log(x)}$	$\pi_A(n) = \frac{q^n}{n} + O(\frac{q^{n/2}}{n})$

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 $\|n\|$	norm of a polynomial $\|f\| = q^{\deg(f)}$
$n = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} P_2^{e_2} \dots P_t^{e_t}$
2	q-1
$\phi(n) = \sum^{n}{}_{\substack{k=1 \\ (k,n)=1}} 1$	$\Phi(f) = \sum_{\substack{k \text{ monic} \\ \deg(k)<\deg(f) \\ \gcd(f,k)=1}} 1$
$n = p_1^{e_1} \dots p_t^{e_t}$	$f = \alpha P_1^{e_1} \dots P_t^{e_t}$
$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$	$\zeta_A(s) = \sum_{f \text{ monic}} \frac{1}{\|f\|^s}$
$\xi(s) = \pi^{-\frac{s}{2}} \Gamma(\frac{s}{2}) \zeta(s) = \xi(1-s)$	$\xi_A(s) = q^{-s} \Gamma_A(s) \zeta_A(s) = \xi_A(1-s)$
$\zeta(s)$ has analytic continuation	$\zeta_A(s) = (1 - q^{1-s})^{-1}$
$\pi(x) \sim \frac{x}{\log(x)}$	$\pi_A(n) = \frac{q^n}{n} + O(\frac{q^{n/2}}{n})$
$\mu(n), d_k(n), \varphi(n), \Lambda(n), \lambda(n)$	$\mu(f), d_k(f), \Phi(f), \Lambda(f), \lambda(f)$

We will extend this dictionary in this lecture.

Averages of Arithmetic Functions in $\mathbb{F}_q[T]$

- We introduce the notion of the average values in the context of polynomials.

Averages of Arithmetic Functions in $\mathbb{F}_q[T]$

- We introduce the notion of the average values in the context of polynomials.

Suppose $h(x)$ is a complex valued function on $\mathbb{N}$. Suppose the following limit exists

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} h(n) = \alpha.$$

Averages of Arithmetic Functions in $\mathbb{F}_q[T]$

- We introduce the notion of the average values in the context of polynomials.

Suppose $h(x)$ is a complex valued function on $\mathbb{N}$. Suppose the following limit exists

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} h(n) = \alpha.$$

We then define α to be the **average value** of the function h.

Averages of Arithmetic Functions in $\mathbb{F}_q[T]$

- We introduce the notion of the average values in the context of polynomials.

Suppose $h(x)$ is a complex valued function on $\mathbb{N}$. Suppose the following limit exists

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} h(n) = \alpha.$$

We then define α to be the **average value** of the function h.
In the ring $A = \mathbb{F}_q[T]$ the analogue of the positive integers is the set of monic polynomials. Let $h(x)$ be a function on the set of monic polynomials. For $n > 0$ we define

$$\mathrm{Ave}_n(h) = \frac{1}{q^n} \sum_{\substack{f \text{ monic} \\ \deg(f)=n}} h(f).$$

This is the average value of h on the set of monic polynomials of degree n.

We define the average value of h to be $\lim_{n\to\infty} \text{Ave}_n(h)$ provided this limit exists.

We define the average value of h to be $\lim_{n\to\infty} \mathrm{Ave}_n(h)$ provided this limit exists.
It is an exercise to show that if the average value exists in the sense just given, then it is also equal to the following limit:

$$\lim_{n\to\infty} \frac{1}{1+q+q^2+\cdots+q^n} \sum_{\substack{f \text{ monic} \\ \deg(f)\le n}} h(f).$$

We define the average value of h to be $\lim_{n\to\infty} \mathrm{Ave}_n(h)$ provided this limit exists.
It is an exercise to show that if the average value exists in the sense just given, then it is also equal to the following limit:

$$\lim_{n\to\infty} \frac{1}{1+q+q^2+\cdots+q^n} \sum_{\substack{f \text{ monic} \\ \deg(f)\le n}} h(f).$$

This limit does not always exist. However, even when it doesn't exist, one can speak of the average rate of growth of $h(f)$.

We define the average value of h to be $\lim_{n\to\infty} \mathrm{Ave}_n(h)$ provided this limit exists.

It is an exercise to show that if the average value exists in the sense just given, then it is also equal to the following limit:

$$\lim_{n\to\infty} \frac{1}{1+q+q^2+\cdots+q^n} \sum_{\substack{f \text{ monic} \\ \deg(f)\leq n}} h(f).$$

This limit does not always exist. However, even when it doesn't exist, one can speak of the average rate of growth of $h(f)$. Define

$$H(n) = \sum_{\substack{f \text{ monic} \\ \deg(f)=n}} h(f).$$

We define the average value of h to be $\lim_{n\to\infty} \mathrm{Ave}_n(h)$ provided this limit exists.
It is an exercise to show that if the average value exists in the sense just given, then it is also equal to the following limit:

$$\lim_{n\to\infty} \frac{1}{1+q+q^2+\cdots+q^n} \sum_{\substack{f \text{ monic} \\ \deg(f)\leq n}} h(f).$$

This limit does not always exist. However, even when it doesn't exist, one can speak of the average rate of growth of $h(f)$. Define

$$H(n) = \sum_{\substack{f \text{ monic} \\ \deg(f)=n}} h(f).$$

As we will see, the function $H(n)$ sometimes behaves in a quite regular manner even though the values $h(f)$ vary erratically.

We define the average value of h to be $\lim_{n\to\infty} \mathrm{Ave}_n(h)$ provided this limit exists.

It is an exercise to show that if the average value exists in the sense just given, then it is also equal to the following limit:

$$\lim_{n\to\infty} \frac{1}{1+q+q^2+\cdots+q^n} \sum_{\substack{f \text{ monic} \\ \deg(f)\le n}} h(f).$$

This limit does not always exist. However, even when it doesn't exist, one can speak of the average rate of growth of $h(f)$. Define

$$H(n) = \sum_{\substack{f \text{ monic} \\ \deg(f)=n}} h(f).$$

As we will see, the function $H(n)$ sometimes behaves in a quite regular manner even though the values $h(f)$ vary erratically.

We will use the method of Carlitz which uses Dirichlet series to investigate the mean values of arithmetic functions in $\mathbb{F}_q[T]$.

Given a function h as previously, we define the associated Dirichlet series to be

$$D_h(s) = \sum_{f \text{ monic}} \frac{h(f)}{|f|^s} = \sum_{n=0}^{\infty} \frac{H(n)}{q^{ns}}. \tag{1.1}$$

Given a function h as previously, we define the associated Dirichlet series to be

$$D_h(s) = \sum_{f \text{ monic}} \frac{h(f)}{|f|^s} = \sum_{n=0}^{\infty} \frac{H(n)}{q^{ns}}. \tag{1.1}$$

In what follows, we will work in a formal manner with these series. If one wants to worry about convergence, it is useful to remark that if $|h(f)| = O(|f|^\beta)$, then $D_h(s)$ converges for $\mathfrak{R}(s) > 1 + \beta$. The proof just uses the comparison test and the fact that $\zeta_A(s)$ converges for $\mathfrak{R}(s) > 1$.

Given a function h as previously, we define the associated Dirichlet series to be

$$D_h(s) = \sum_{f \text{ monic}} \frac{h(f)}{|f|^s} = \sum_{n=0}^{\infty} \frac{H(n)}{q^{ns}}. \tag{1.1}$$

In what follows, we will work in a formal manner with these series. If one wants to worry about convergence, it is useful to remark that if $|h(f)| = O(|f|^\beta)$, then $D_h(s)$ converges for $\Re(s) > 1 + \beta$. The proof just uses the comparison test and the fact that $\zeta_A(s)$ converges for $\Re(s) > 1$.

The right hand side of equation above is simply $\sum_{n=0}^{\infty} H(n)u^n$, so the Dirichlet series in s becomes a power series in $u = q^{-s}$ whose coefficients are the averages $H(n)$.

Average value of $d(f)$

Recall the function $d(f)$ which is the number of monic divisors of f.

Average value of $d(f)$

Recall the function $d(f)$ which is the number of monic divisors of f. Let

$$D(n) = \sum_{\substack{f \text{ monic} \\ \deg(f)=n}} d(f).$$

Average value of $d(f)$

Recall the function $d(f)$ which is the number of monic divisors of f. Let

$$D(n) = \sum_{\substack{f \text{ monic} \\ \deg(f)=n}} d(f).$$

Then,

Proposition (2.5)

$D_d(s) = \zeta_A(s)^2 = (1-qu)^{-2}$. Consequently, $D(n) = (n+1)q^n$.

Proof.

$$\zeta_A(s)^2 = \left(\sum_h \frac{1}{|h|^s} \right) \left(\sum_g \frac{1}{|g|^s} \right)$$

Proof.

$$\begin{aligned}\zeta_A(s)^2 &= \left(\sum_h \frac{1}{|h|^s}\right)\left(\sum_g \frac{1}{|g|^s}\right) \\ &= \sum_f \left(\sum_{\substack{h,g \\ hg=f}} 1\right)\frac{1}{|f|^s} = \sum_f \frac{d(f)}{|f|^s} = D_d(s).\end{aligned}$$

Proof.

$$
\begin{aligned}
\zeta_A(s)^2 &= \left(\sum_h \frac{1}{|h|^s}\right)\left(\sum_g \frac{1}{|g|^s}\right) \\
&= \sum_f \left(\sum_{\substack{h,g \\ hg=f}} 1\right)\frac{1}{|f|^s} = \sum_f \frac{d(f)}{|f|^s} = D_d(s).
\end{aligned}
$$

This proves the first assertion.

Proof.

$$\begin{aligned}\zeta_A(s)^2 &= \left(\sum_h \frac{1}{|h|^s}\right)\left(\sum_g \frac{1}{|g|^s}\right)\\ &= \sum_f \left(\sum_{\substack{h,g\\ hg=f}} 1\right)\frac{1}{|f|^s} = \sum_f \frac{d(f)}{|f|^s} = D_d(s).\end{aligned}$$

This proves the first assertion. To prove the second assertion, notice

$$D_d(s) = \sum_{n=0}^{\infty} D(n)u^n = (1-qu)^{-2}.$$

Proof.

$$\begin{aligned}\zeta_A(s)^2 &= \left(\sum_h \frac{1}{|h|^s}\right)\left(\sum_g \frac{1}{|g|^s}\right)\\ &= \sum_f \left(\sum_{\substack{h,g\\ hg=f}} 1\right)\frac{1}{|f|^s} = \sum_f \frac{d(f)}{|f|^s} = D_d(s).\end{aligned}$$

This proves the first assertion. To prove the second assertion, notice

$$D_d(s) = \sum_{n=0}^{\infty} D(n)u^n = (1-qu)^{-2}.$$

It is easily seen that $(1-qu)^{-2} = \sum_{n=0}^{\infty}(n+1)q^n u^n$.

Proof.

$$\begin{aligned}\zeta_A(s)^2 &= \left(\sum_h \frac{1}{|h|^s}\right)\left(\sum_g \frac{1}{|g|^s}\right)\\ &= \sum_f \left(\sum_{\substack{h,g\\ hg=f}} 1\right)\frac{1}{|f|^s} = \sum_f \frac{d(f)}{|f|^s} = D_d(s).\end{aligned}$$

This proves the first assertion. To prove the second assertion, notice

$$D_d(s) = \sum_{n=0}^{\infty} D(n)u^n = (1-qu)^{-2}.$$

It is easily seen that $(1-qu)^{-2} = \sum_{n=0}^{\infty}(n+1)q^n u^n$. Thus, the second assertion follows by comparing the coefficients of u^n on both sides of this identity. $\square$

A Few Remarks

Notice that $\mathrm{Ave}_n(d) = n + 1$ so the average value of $d(f)$ in the way we have defined it doesn't exist. On average, the number of divisors of f grows with the degree.

A Few Remarks

Notice that $\text{Ave}_n(d) = n + 1$ so the average value of $d(f)$ in the way we have defined it doesn't exist. On average, the number of divisors of f grows with the degree.
If we set $x = q^n$ then our result reads $D(n) = x \log_q(x) + x$ which resembles closely the analogues result for the integers

$$\sum_{k=1}^{n} d(k) = x \log(x) + (2\gamma - 1)x + O(\sqrt{x}).$$

A Few Remarks

Notice that $\text{Ave}_n(d) = n + 1$ so the average value of $d(f)$ in the way we have defined it doesn't exist. On average, the number of divisors of f grows with the degree.
If we set $x = q^n$ then our result reads $D(n) = x \log_q(x) + x$ which resembles closely the analogues result for the integers

$$\sum_{k=1}^{n} d(k) = x \log(x) + (2\gamma - 1)x + O(\sqrt{x}).$$

This formula is due to Dirichlet. It is a famous problem in number theory to find the best possible error term. In the polynomial case, there is no error term!

A Few Remarks

Notice that $\text{Ave}_n(d) = n + 1$ so the average value of $d(f)$ in the way we have defined it doesn't exist. On average, the number of divisors of f grows with the degree.
If we set $x = q^n$ then our result reads $D(n) = x \log_q(x) + x$ which resembles closely the analogues result for the integers

$$\sum_{k=1}^{n} d(k) = x \log(x) + (2\gamma - 1)x + O(\sqrt{x}).$$

This formula is due to Dirichlet. It is a famous problem in number theory to find the best possible error term. In the polynomial case, there is no error term!This is because of the very simple nature of the zeta function $\zeta_A(s)$.

A Few Remarks

Notice that $\mathrm{Ave}_n(d) = n + 1$ so the average value of $d(f)$ in the way we have defined it doesn't exist. On average, the number of divisors of f grows with the degree.
If we set $x = q^n$ then our result reads $D(n) = x \log_q(x) + x$ which resembles closely the analogues result for the integers

$$\sum_{k=1}^{n} d(k) = x \log(x) + (2\gamma - 1)x + O(\sqrt{x}).$$

This formula is due to Dirichlet. It is a famous problem in number theory to find the best possible error term. In the polynomial case, there is no error term!This is because of the very simple nature of the zeta function $\zeta_A(s)$.
Similar sums in the general function field context lead to more difficult problems. We shall have more to say later in this course.

Dirichlet Product

It is an interesting fact that many multiplicative functions have corresponding Dirichlet series which can be simply expressed in terms of the zeta function. We have just seen this for $d(f)$.

Dirichlet Product

It is an interesting fact that many multiplicative functions have corresponding Dirichlet series which can be simply expressed in terms of the zeta function. We have just seen this for $d(f)$. More generally, let $h(f)$ be multiplicative. The multiplicativity of $h(f)$ leads to the identity

$$D_h(s) = \prod_P \left(\sum_{k=0}^{\infty} \frac{h(P^k)}{|P|^{ks}} \right).$$

Dirichlet Product

It is an interesting fact that many multiplicative functions have corresponding Dirichlet series which can be simply expressed in terms of the zeta function. We have just seen this for $d(f)$. More generally, let $h(f)$ be multiplicative. The multiplicativity of $h(f)$ leads to the identity

$$D_h(s) = \prod_P \left(\sum_{k=0}^{\infty} \frac{h(P^k)}{|P|^{ks}} \right).$$

As an example, consider the function $\mu(f)$.

Dirichlet Product

It is an interesting fact that many multiplicative functions have corresponding Dirichlet series which can be simply expressed in terms of the zeta function. We have just seen this for $d(f)$. More generally, let $h(f)$ be multiplicative. The multiplicativity of $h(f)$ leads to the identity

$$D_h(s) = \prod_P \left(\sum_{k=0}^{\infty} \frac{h(P^k)}{|P|^{ks}} \right).$$

As an example, consider the function $\mu(f)$. Since $\sum_{k=0}^{\infty} \frac{\mu(P^k)}{|P|^{ks}} = 1 - |P|^{-s}$, we find $D_\mu(s) = \zeta_A(s)^{-1}$.

Dirichlet Product

It is an interesting fact that many multiplicative functions have corresponding Dirichlet series which can be simply expressed in terms of the zeta function. We have just seen this for $d(f)$. More generally, let $h(f)$ be multiplicative. The multiplicativity of $h(f)$ leads to the identity

$$D_h(s) = \prod_P \left(\sum_{k=0}^{\infty} \frac{h(P^k)}{|P|^{ks}} \right).$$

As an example, consider the function $\mu(f)$. Since $\sum_{k=0}^{\infty} \frac{\mu(P^k)}{|P|^{ks}} = 1 - |P|^{-s}$, we find $D_\mu(s) = \zeta_A(s)^{-1}$.
Let λ and ρ be two complex valued functions on the monic polynomials.

Dirichlet Product

It is an interesting fact that many multiplicative functions have corresponding Dirichlet series which can be simply expressed in terms of the zeta function. We have just seen this for $d(f)$. More generally, let $h(f)$ be multiplicative. The multiplicativity of $h(f)$ leads to the identity

$$D_h(s) = \prod_P \left(\sum_{k=0}^{\infty} \frac{h(P^k)}{|P|^{ks}} \right).$$

As an example, consider the function $\mu(f)$. Since $\sum_{k=0}^{\infty} \frac{\mu(P^k)}{|P|^{ks}} = 1 - |P|^{-s}$, we find $D_\mu(s) = \zeta_A(s)^{-1}$.
Let λ and ρ be two complex valued functions on the monic polynomials. We define their Dirichlet product by the following formula (all polynomials involved are assumed to be monic)

$$(\lambda * \rho)(f) = \sum_{\substack{h,g \\ hg=f}} \lambda(h)\rho(g).$$

Proposition

$$D_\lambda(s)D_\rho(s) = D_{\lambda\star\rho}(s).$$

Proposition

$$D_\lambda(s) D_\rho(s) = D_{\lambda \star \rho}(s).$$

Proof.

The calculation is just like in the previous proposition.

$$D_\lambda(s) D_\rho(s) = \left(\sum_h \frac{\lambda(h)}{|h|^s} \right) \left(\sum_g \frac{\rho(g)}{|g|^s} \right)$$

Proposition

$$D_{\lambda}(s)D_{\rho}(s) = D_{\lambda\star\rho}(s).$$

Proof.

The calculation is just like in the previous proposition.

$$\begin{aligned} D_{\lambda}(s)D_{\rho}(s) &= \left(\sum_{h} \frac{\lambda(h)}{|h|^{s}}\right)\left(\sum_{g} \frac{\rho(g)}{|g|^{s}}\right) \\ &= \sum_{f} \left(\sum_{\substack{h,g \\ hg=f}} \lambda(h)\rho(g)\right)\frac{1}{|f|^{s}} \end{aligned}$$

Proposition

$$D_\lambda(s) D_\rho(s) = D_{\lambda \star \rho}(s).$$

Proof.

The calculation is just like in the previous proposition.

$$\begin{aligned} D_\lambda(s) D_\rho(s) &= \left(\sum_h \frac{\lambda(h)}{|h|^s} \right) \left(\sum_g \frac{\rho(g)}{|g|^s} \right) \\ &= \sum_f \left(\sum_{\substack{h,g \\ hg=f}} \lambda(h)\rho(g) \right) \frac{1}{|f|^s} \\ &= D_{\lambda * \rho}(s). \end{aligned} \tag{1.2}$$

$\square$

We now proceed to calculate the average value of $\Phi(f)$.

We now proceed to calculate the average value of $\Phi(f)$. We have seen that

$$\Phi(f) = |f| \prod_{P|f} (1 - |P|^{-1}).$$

We now proceed to calculate the average value of $\Phi(f)$. We have seen that

$$\Phi(f) = |f| \prod_{P|f} (1 - |P|^{-1}).$$

Define $\lambda(f) = |f|$.

We now proceed to calculate the average value of $\Phi(f)$. We have seen that

$$\Phi(f) = |f| \prod_{P|f} (1 - |P|^{-1}).$$

Define $\lambda(f) = |f|$. A moment's reflection shows that

$$|f| \prod_{P|f} (1 - |P|^{-1}) = \sum_{g|f} \mu(g) |f/g| = (\mu * \lambda)(f).$$

We now proceed to calculate the average value of $\Phi(f)$. We have seen that

$$\Phi(f) = |f| \prod_{P|f} (1 - |P|^{-1}).$$

Define $\lambda(f) = |f|$. A moment's reflection shows that

$$|f| \prod_{P|f} (1 - |P|^{-1}) = \sum_{g|f} \mu(g) |f/g| = (\mu * \lambda)(f).$$

Thus, by the previous proposition we find

We now proceed to calculate the average value of $\Phi(f)$. We have seen that

$$\Phi(f) = |f| \prod_{P|f} (1 - |P|^{-1}).$$

Define $\lambda(f) = |f|$. A moment's reflection shows that

$$|f| \prod_{P|f} (1 - |P|^{-1}) = \sum_{g|f} \mu(g) |f/g| = (\mu * \lambda)(f).$$

Thus, by the previous proposition we find

$$D_\Phi(s) = D_{\mu*\lambda}(s) = D_\mu(s) D_\lambda(s) = \zeta_A(s)^{-1} \zeta_A(s-1). \tag{1.3}$$

We now proceed to calculate the average value of $\Phi(f)$. We have seen that

$$\Phi(f) = |f| \prod_{P|f} (1 - |P|^{-1}).$$

Define $\lambda(f) = |f|$. A moment's reflection shows that

$$|f| \prod_{P|f} (1 - |P|^{-1}) = \sum_{g|f} \mu(g)|f/g| = (\mu * \lambda)(f).$$

Thus, by the previous proposition we find

$$D_{\Phi}(s) = D_{\mu*\lambda}(s) = D_{\mu}(s)D_{\lambda}(s) = \zeta_A(s)^{-1}\zeta_A(s-1). \tag{1.3}$$

Proposition

$$\sum_{\substack{deg(f)=n \\ f \ \ monic}} \Phi(f) = q^{2n}(1 - q^{-1}).$$

Proof of Proposition

Proof.

Let $A(n)$ be the left-hand side of the above equation.

Proof of Proposition

Proof.

Let $A(n)$ be the left-hand side of the above equation. Then, with the usual transformation $u = q^{-s}$, Equation (1.3) becomes

$$\sum_{n=0}^{\infty} A(n)u^n = \frac{1-qu}{1-q^2u}.$$

Proof of Proposition

Proof.

Let $A(n)$ be the left-hand side of the above equation. Then, with the usual transformation $u = q^{-s}$, Equation (1.3) becomes

$$\sum_{n=0}^{\infty} A(n)u^n = \frac{1 - qu}{1 - q^2 u}.$$

Now, expand $(1 - q^2 u)^{-1}$ into a power series using the geometric series, multiply out, and equate the coefficients of u^n on both sides.

Proof of Proposition

Proof.

Let $A(n)$ be the left-hand side of the above equation. Then, with the usual transformation $u = q^{-s}$, Equation (1.3) becomes

$$\sum_{n=0}^{\infty} A(n)u^n = \frac{1 - qu}{1 - q^2 u}.$$

Now, expand $(1 - q^2 u)^{-1}$ into a power series using the geometric series, multiply out, and equate the coefficients of u^n on both sides. One finds $A(n) = q^{2n} - q^{2n-1}$. The result follows. $\square$

We do a similar analysis to the function $\sigma(f)$.

We do a similar analysis to the function $\sigma(f)$. Let $\mathbf{1}(f)$ denote the function which is identically equal to 1 on all monics f.

We do a similar analysis to the function $\sigma(f)$. Let $\mathbf{1}(f)$ denote the function which is identically equal to 1 on all monics f. For any complex valued function λ on monics, we see immediately that $(\mathbf{1} * \lambda)(f) = \sum_{g|f} \lambda(g)$.

We do a similar analysis to the function $\sigma(f)$. Let $\mathbf{1}(f)$ denote the function which is identically equal to 1 on all monics f. For any complex valued function λ on monics, we see immediately that $(\mathbf{1} * \lambda)(f) = \sum_{g|f} \lambda(g)$. In particular, if $\lambda(f) = |f|$, then $(\mathbf{1} * \lambda)(f) = \sigma(f)$.

We do a similar analysis to the function $\sigma(f)$. Let $\mathbf{1}(f)$ denote the function which is identically equal to 1 on all monics f. For any complex valued function λ on monics, we see immediately that $(\mathbf{1} * \lambda)(f) = \sum_{g|f} \lambda(g)$. In particular, if $\lambda(f) = |f|$, then $(\mathbf{1} * \lambda)(f) = \sigma(f)$. Thus,

$$D_\sigma(s) = D_{\mathbf{1}*\lambda}(s) = D_{\mathbf{1}}(s) D_\lambda(s) = \zeta_A(s)\zeta_A(s-1). \tag{1.4}$$

We do a similar analysis to the function $\sigma(f)$. Let $\mathbf{1}(f)$ denote the function which is identically equal to 1 on all monics f. For any complex valued function λ on monics, we see immediately that $(\mathbf{1} * \lambda)(f) = \sum_{g|f} \lambda(g)$. In particular, if $\lambda(f) = |f|$, then $(\mathbf{1} * \lambda)(f) = \sigma(f)$. Thus,

$$D_\sigma(s) = D_{\mathbf{1}*\lambda}(s) = D_{\mathbf{1}}(s) D_\lambda(s) = \zeta_A(s)\zeta_A(s-1). \tag{1.4}$$

Proposition

$$\sum_{\substack{deg(f)=n \\ f \ \ monic}} \sigma(f) = q^{2n} \frac{1 - q^{-n-1}}{1 - q^{-1}}.$$

Proof of Proposition

Proof.

Define $S(n)$ to be the sum on the left hand side of the above equation.

Proof of Proposition

Proof.

Define $S(n)$ to be the sum on the left hand side of the above equation. Then, making the substitution $u = q^{-s}$ in Equation (1.4) we find

$$\sum_{n=0}^{\infty} S(n)u^n = (1 - qu)^{-1}(1 - q^2 u)^{-1}.$$

Proof of Proposition

Proof.

Define $S(n)$ to be the sum on the left hand side of the above equation. Then, making the substitution $u = q^{-s}$ in Equation (1.4) we find

$$\sum_{n=0}^{\infty} S(n)u^n = (1 - qu)^{-1}(1 - q^2 u)^{-1}.$$

Expanding the two terms on the right using the geometric series, multiplying out, and collecting terms, we deduce

$$S(n) = \sum_{k+l=n} q^k q^{2l}.$$

Proof of Proposition

Proof.

Define $S(n)$ to be the sum on the left hand side of the above equation. Then, making the substitution $u = q^{-s}$ in Equation (1.4) we find

$$\sum_{n=0}^{\infty} S(n)u^n = (1 - qu)^{-1}(1 - q^2 u)^{-1}.$$

Expanding the two terms on the right using the geometric series, multiplying out, and collecting terms, we deduce

$$S(n) = \sum_{k+l=n} q^k q^{2l}.$$

The result follows after applying a little algebra. $\square$

The Reciprocity Law

Let $P \in A$ be an irreducible polynomial and d a divisor of $q - 1$ (recall that q is the cardinality of $\mathbb{F}_q$).

The Reciprocity Law

Let $P \in A$ be an irreducible polynomial and d a divisor of $q - 1$ (recall that q is the cardinality of $\mathbb{F}_q$). If $a \in A$ and P does not divide a, then, by Proposition 1.10 from the first lecture, we know $x^d \equiv a (\text{mod } P)$ is solvable if and only if

$$a^{\frac{|P|-1}{d}} \equiv 1 (\text{mod } P).$$

The Reciprocity Law

Let $P \in A$ be an irreducible polynomial and d a divisor of $q - 1$ (recall that q is the cardinality of $\mathbb{F}_q$). If $a \in A$ and P does not divide a, then, by Proposition 1.10 from the first lecture, we know $x^d \equiv a \pmod{P}$ is solvable if and only if

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

The left-hand side of this congruence is, in any case, an element of order dividing d in $(A/PA)^*$.

The Reciprocity Law

Let $P \in A$ be an irreducible polynomial and d a divisor of $q - 1$ (recall that q is the cardinality of $\mathbb{F}_q$). If $a \in A$ and P does not divide a, then, by Proposition 1.10 from the first lecture, we know $x^d \equiv a(\text{mod } P)$ is solvable if and only if

$$a^{\frac{|P|-1}{d}} \equiv 1(\text{mod } P).$$

The left-hand side of this congruence is, in any case, an element of order dividing d in $(A/PA)^*$. Since $\mathbb{F}_q^* \to (A/PA)^*$ is one to one, there is a unique $\alpha \in \mathbb{F}_q^*$ such that

$$a^{\frac{|P|-1}{d}} \equiv \alpha(\text{mod } P).$$

The Reciprocity Law

Let $P \in A$ be an irreducible polynomial and d a divisor of $q - 1$ (recall that q is the cardinality of $\mathbb{F}_q$). If $a \in A$ and P does not divide a, then, by Proposition 1.10 from the first lecture, we know $x^d \equiv a \pmod{P}$ is solvable if and only if

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

The left-hand side of this congruence is, in any case, an element of order dividing d in $(A/PA)^*$. Since $\mathbb{F}_q^* \to (A/PA)^*$ is one to one, there is a unique $\alpha \in \mathbb{F}_q^*$ such that

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

Definition

If P does not divide a, let $(a/P)_d$ be the unique element of $\mathbb{F}_q^*$ such that

$$a^{\frac{|P|-1}{d}} \equiv \left(\frac{a}{P}\right)_d \pmod{P}.$$

The Reciprocity Law

Let $P \in A$ be an irreducible polynomial and d a divisor of $q - 1$ (recall that q is the cardinality of $\mathbb{F}_q$). If $a \in A$ and P does not divide a, then, by Proposition 1.10 from the first lecture, we know $x^d \equiv a \pmod{P}$ is solvable if and only if

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

The left-hand side of this congruence is, in any case, an element of order dividing d in $(A/PA)^*$. Since $\mathbb{F}_q^* \to (A/PA)^*$ is one to one, there is a unique $\alpha \in \mathbb{F}_q^*$ such that

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

Definition

If P does not divide a, let $(a/P)_d$ be the unique element of $\mathbb{F}_q^*$ such that

$$a^{\frac{|P|-1}{d}} \equiv \left(\frac{a}{P}\right)_d \pmod{P}.$$

If $P \mid a$ define $(a/P)_d = 0$.

The Reciprocity Law

Let $P \in A$ be an irreducible polynomial and d a divisor of $q-1$ (recall that q is the cardinality of $\mathbb{F}_q$). If $a \in A$ and P does not divide a, then, by Proposition 1.10 from the first lecture, we know $x^d \equiv a \pmod{P}$ is solvable if and only if

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

The left-hand side of this congruence is, in any case, an element of order dividing d in $(A/PA)^*$. Since $\mathbb{F}_q^* \to (A/PA)^*$ is one to one, there is a unique $\alpha \in \mathbb{F}_q^*$ such that

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

Definition

If P does not divide a, let $(a/P)_d$ be the unique element of $\mathbb{F}_q^*$ such that

$$a^{\frac{|P|-1}{d}} \equiv \left(\frac{a}{P}\right)_d \pmod{P}.$$

*If $P \mid a$ define $(a/P)_d = 0$. The symbol $(a/P)_d$ is called the d-th **power residue symbol**.*

When $d = 2$, the symbol $(a/P)_d$ is just like the Legendre symbol of elementary number theory.

When $d = 2$, the symbol $(a/P)_d$ is just like the Legendre symbol of elementary number theory. The situation is a bit more flexible in A since $A^* = \mathbb{F}_q^*$ is cyclic of order $q - 1$, whereas $\mathbb{Z}^*$ is just $\{\pm 1\}$.

When $d = 2$, the symbol $(a/P)_d$ is just like the Legendre symbol of elementary number theory. The situation is a bit more flexible in A since $A^* = \mathbb{F}_q^*$ is cyclic of order $q - 1$, whereas $\mathbb{Z}^*$ is just $\{\pm 1\}$. Note that the value of the residue symbol is in the finite field $\mathbb{F}_q$ and not in the complex numbers.

When $d = 2$, the symbol $(a/P)_d$ is just like the Legendre symbol of elementary number theory. The situation is a bit more flexible in A since $A^* = \mathbb{F}_q^*$ is cyclic of order $q - 1$, whereas $\mathbb{Z}^*$ is just $\{\pm 1\}$. Note that the value of the residue symbol is in the finite field $\mathbb{F}_q$ and not in the complex numbers.

Proposition

The d-th power residue symbol has the following properties:

When $d = 2$, the symbol $(a/P)_d$ is just like the Legendre symbol of elementary number theory. The situation is a bit more flexible in A since $A^* = \mathbb{F}_q^*$ is cyclic of order $q - 1$, whereas $\mathbb{Z}^*$ is just $\{\pm 1\}$. Note that the value of the residue symbol is in the finite field $\mathbb{F}_q$ and not in the complex numbers.

Proposition

The d-th power residue symbol has the following properties:

1. $\left(\frac{a}{P}\right)_d = \left(\frac{b}{P}\right)_d$ *if* $a \equiv b \pmod{P}$.

When $d = 2$, the symbol $(a/P)_d$ is just like the Legendre symbol of elementary number theory. The situation is a bit more flexible in A since $A^* = \mathbb{F}_q^*$ is cyclic of order $q - 1$, whereas $\mathbb{Z}^*$ is just $\{\pm 1\}$. Note that the value of the residue symbol is in the finite field $\mathbb{F}_q$ and not in the complex numbers.

Proposition

The d-th power residue symbol has the following properties:

1. $\left(\frac{a}{P}\right)_d = \left(\frac{b}{P}\right)_d$ *if* $a \equiv b \pmod{P}$.
2. $\left(\frac{ab}{P}\right)_d = \left(\frac{a}{P}\right)_d \left(\frac{b}{P}\right)_d$.

When $d = 2$, the symbol $(a/P)_d$ is just like the Legendre symbol of elementary number theory. The situation is a bit more flexible in A since $A^* = \mathbb{F}_q^*$ is cyclic of order $q - 1$, whereas $\mathbb{Z}^*$ is just $\{\pm 1\}$. Note that the value of the residue symbol is in the finite field $\mathbb{F}_q$ and not in the complex numbers.

Proposition

The d-th power residue symbol has the following properties:

1. $\left(\frac{a}{P}\right)_d = \left(\frac{b}{P}\right)_d$ *if* $a \equiv b \pmod{P}$.
2. $\left(\frac{ab}{P}\right)_d = \left(\frac{a}{P}\right)_d \left(\frac{b}{P}\right)_d$.
3. $\left(\frac{a}{P}\right)_d = 1$ *iff* $x^d \equiv a \pmod{P}$ *is solvable.*

When $d = 2$, the symbol $(a/P)_d$ is just like the Legendre symbol of elementary number theory. The situation is a bit more flexible in A since $A^* = \mathbb{F}_q^*$ is cyclic of order $q-1$, whereas $\mathbb{Z}^*$ is just $\{\pm 1\}$. Note that the value of the residue symbol is in the finite field $\mathbb{F}_q$ and not in the complex numbers.

Proposition

The d-th power residue symbol has the following properties:

1. $\left(\frac{a}{P}\right)_d = \left(\frac{b}{P}\right)_d$ *if* $a \equiv b \pmod{P}$.
2. $\left(\frac{ab}{P}\right)_d = \left(\frac{a}{P}\right)_d \left(\frac{b}{P}\right)_d$.
3. $\left(\frac{a}{P}\right)_d = 1$ *iff* $x^d \equiv a \pmod{P}$ *is solvable.*
4. *Let* $\zeta \in \mathbb{F}_q^*$ *be an element of order dividing* d. *There exists an* $a \in A$ *such that* $\left(\frac{a}{P}\right)_d = \zeta$.

Proof.

The first assertion follows immediately from the definition.

Proof.

The first assertion follows immediately from the definition. The second follows from the definition and the fact that if two constants are congruent modulo P then they are equal.

Proof.

The first assertion follows immediately from the definition. The second follows from the definition and the fact that if two constants are congruent modulo P then they are equal. The third assertion follows from the definition and Proposition 1.10 (first lecture).

Proof.

The first assertion follows immediately from the definition. The second follows from the definition and the fact that if two constants are congruent modulo P then they are equal. The third assertion follows from the definition and Proposition 1.10 (first lecture). Finally, note that the map from $(A/PA)^* \to \mathbb{F}_q^*$ given by $a \to (a/P)_d$ is a homomorphism whose kernel is the d-th powers in $(A/PA)^*$ by part 3. Since $(A/PA)^*$ is a cyclic group of order $|P| - 1$, the order of the kernel is $(|P| - 1)/d$. Consequently, the image has order d and part 4 follows from this.

Proof.

The first assertion follows immediately from the definition. The second follows from the definition and the fact that if two constants are congruent modulo P then they are equal. The third assertion follows from the definition and Proposition 1.10 (first lecture). Finally, note that the map from $(A/PA)^* \to \mathbb{F}_q^*$ given by $a \to (a/P)_d$ is a homomorphism whose kernel is the d-th powers in $(A/PA)^*$ by part 3. Since $(A/PA)^*$ is a cyclic group of order $|P| - 1$, the order of the kernel is $(|P| - 1)/d$. Consequently, the image has order d and part 4 follows from this. □

It is an easy matter to evaluate the residue symbol on a constant.

Proof.

The first assertion follows immediately from the definition. The second follows from the definition and the fact that if two constants are congruent modulo P then they are equal. The third assertion follows from the definition and Proposition 1.10 (first lecture). Finally, note that the map from $(A/PA)^* \to \mathbb{F}_q^*$ given by $a \to (a/P)_d$ is a homomorphism whose kernel is the d-th powers in $(A/PA)^*$ by part 3. Since $(A/PA)^*$ is a cyclic group of order $|P| - 1$, the order of the kernel is $(|P| - 1)/d$. Consequently, the image has order d and part 4 follows from this. □

It is an easy matter to evaluate the residue symbol on a constant.

Proposition (3.2)

Let $\alpha \in \mathbb{F}_q$. Then,

$$\left(\frac{\alpha}{P}\right)_d = \alpha^{\frac{q-1}{d} deg(P)}.$$

Proof.

The first assertion follows immediately from the definition. The second follows from the definition and the fact that if two constants are congruent modulo P then they are equal. The third assertion follows from the definition and Proposition 1.10 (first lecture). Finally, note that the map from $(A/PA)^* \to \mathbb{F}_q^*$ given by $a \to (a/P)_d$ is a homomorphism whose kernel is the d-th powers in $(A/PA)^*$ by part 3. Since $(A/PA)^*$ is a cyclic group of order $|P| - 1$, the order of the kernel is $(|P| - 1)/d$. Consequently, the image has order d and part 4 follows from this. $\square$

It is an easy matter to evaluate the residue symbol on a constant.

Proposition (3.2)

Let $\alpha \in \mathbb{F}_q$. Then,

$$\left(\frac{\alpha}{P}\right)_d = \alpha^{\frac{q-1}{d} deg(P)}.$$

Proof.

Let $\delta = \deg(P)$.

Proof.

The first assertion follows immediately from the definition. The second follows from the definition and the fact that if two constants are congruent modulo P then they are equal. The third assertion follows from the definition and Proposition 1.10 (first lecture). Finally, note that the map from $(A/PA)^* \to \mathbb{F}_q^*$ given by $a \to (a/P)_d$ is a homomorphism whose kernel is the d-th powers in $(A/PA)^*$ by part 3. Since $(A/PA)^*$ is a cyclic group of order $|P|-1$, the order of the kernel is $(|P|-1)/d$. Consequently, the image has order d and part 4 follows from this. □

It is an easy matter to evaluate the residue symbol on a constant.

Proposition (3.2)

Let $\alpha \in \mathbb{F}_q$. Then,

$$\left(\frac{\alpha}{P}\right)_d = \alpha^{\frac{q-1}{d} deg(P)}.$$

Proof.

Let $\delta = \deg(P)$. Then,

$$\frac{|P|-1}{d} = \frac{q^\delta - 1}{d} = (1 + q + \cdots + q^{\delta-1})\frac{q-1}{d}.$$

Proof.

The first assertion follows immediately from the definition. The second follows from the definition and the fact that if two constants are congruent modulo P then they are equal. The third assertion follows from the definition and Proposition 1.10 (first lecture). Finally, note that the map from $(A/PA)^* \to \mathbb{F}_q^*$ given by $a \to (a/P)_d$ is a homomorphism whose kernel is the d-th powers in $(A/PA)^*$ by part 3. Since $(A/PA)^*$ is a cyclic group of order $|P| - 1$, the order of the kernel is $(|P| - 1)/d$. Consequently, the image has order d and part 4 follows from this. □

It is an easy matter to evaluate the residue symbol on a constant.

Proposition (3.2)

Let $\alpha \in \mathbb{F}_q$. Then,

$$\left(\frac{\alpha}{P}\right)_d = \alpha^{\frac{q-1}{d} deg(P)}.$$

Proof.

Let $\delta = \deg(P)$. Then,

$$\frac{|P| - 1}{d} = \frac{q^{\delta} - 1}{d} = (1 + q + \cdots + q^{\delta - 1})\frac{q - 1}{d}.$$

The result now follows from the definition and the fact that for all $\alpha \in \mathbb{F}_q$ we have $\alpha^q = \alpha$.

Proof.

The first assertion follows immediately from the definition. The second follows from the definition and the fact that if two constants are congruent modulo P then they are equal. The third assertion follows from the definition and Proposition 1.10 (first lecture). Finally, note that the map from $(A/PA)^* \to \mathbb{F}_q^*$ given by $a \to (a/P)_d$ is a homomorphism whose kernel is the d-th powers in $(A/PA)^*$ by part 3. Since $(A/PA)^*$ is a cyclic group of order $|P| - 1$, the order of the kernel is $(|P| - 1)/d$. Consequently, the image has order d and part 4 follows from this. □

It is an easy matter to evaluate the residue symbol on a constant.

Proposition (3.2)

Let $\alpha \in \mathbb{F}_q$. Then,

$$\left(\frac{\alpha}{P}\right)_d = \alpha^{\frac{q-1}{d} deg(P)}.$$

Proof.

Let $\delta = \deg(P)$. Then,

$$\frac{|P| - 1}{d} = \frac{q^\delta - 1}{d} = (1 + q + \cdots + q^{\delta - 1})\frac{q - 1}{d}.$$

The result now follows from the definition and the fact that for all $\alpha \in \mathbb{F}_q$ we have $\alpha^q = \alpha$. Notice that if $d \mid \deg(P)$ every constant is automatically a d-th power residue modulo P. □

We are now in a position to state the reciprocity law.

We are now in a position to state the reciprocity law.

Theorem (The d-th power reciprocity law)

Let P and Q be monic irreducible polynomials of degrees δ and ν respectively. Then,

$$\left(\frac{Q}{P}\right)_d = (-1)^{\frac{q-1}{d}\delta\nu}\left(\frac{P}{Q}\right)_d.$$

Proof of the Theorem

Let's define $(a/P) = (a/P)_{q-1}$.

Proof of the Theorem

Let's define $(a/P) = (a/P)_{q-1}$. Then $(a/P)_d = (a/P)^{\frac{q-1}{d}}$.

Proof of the Theorem

Let's define $(a/P) = (a/P)_{q-1}$. Then $(a/P)_d = (a/P)^{\frac{q-1}{d}}$. The theorem would follow in full generality if we could show

$$\left(\frac{Q}{P}\right) = (-1)^{\delta\nu} \left(\frac{P}{Q}\right),$$

since the general result would follow by raising both sides to the $(q-1)/d$ power.

Proof of the Theorem

Let's define $(a/P) = (a/P)_{q-1}$. Then $(a/P)_d = (a/P)^{\frac{q-1}{d}}$. The theorem would follow in full generality if we could show

$$\left(\frac{Q}{P}\right) = (-1)^{\delta\nu}\left(\frac{P}{Q}\right),$$

since the general result would follow by raising both sides to the $(q-1)/d$ power. Let α be a root of P and β a root of Q.

Proof of the Theorem

Let's define $(a/P) = (a/P)_{q-1}$. Then $(a/P)_d = (a/P)^{\frac{q-1}{d}}$. The theorem would follow in full generality if we could show

$$\left(\frac{Q}{P}\right) = (-1)^{\delta\nu}\left(\frac{P}{Q}\right),$$

since the general result would follow by raising both sides to the $(q-1)/d$ power. Let α be a root of P and β a root of Q. Let $\mathbb{F}'$ be a finite field which contains $\mathbb{F}_q$, α, and β.

Proof of the Theorem

Let's define $(a/P) = (a/P)_{q-1}$. Then $(a/P)_d = (a/P)^{\frac{q-1}{d}}$. The theorem would follow in full generality if we could show

$$\left(\frac{Q}{P}\right) = (-1)^{\delta\nu}\left(\frac{P}{Q}\right),$$

since the general result would follow by raising both sides to the $(q-1)/d$ power. Let α be a root of P and β a root of Q. Let $\mathbb{F}'$ be a finite field which contains $\mathbb{F}_q$, α, and β. Using the theory of finite fields we find

$$P(T) = (T-\alpha)(T-\alpha^q)\ldots(T-\alpha^{q^{\delta-1}}) \tag{2.1}$$

Proof of the Theorem

Let's define $(a/P) = (a/P)_{q-1}$. Then $(a/P)_d = (a/P)^{\frac{q-1}{d}}$. The theorem would follow in full generality if we could show

$$\left(\frac{Q}{P}\right) = (-1)^{\delta\nu} \left(\frac{P}{Q}\right),$$

since the general result would follow by raising both sides to the $(q-1)/d$ power. Let α be a root of P and β a root of Q. Let $\mathbb{F}'$ be a finite field which contains $\mathbb{F}_q$, α, and β. Using the theory of finite fields we find

$$P(T) = (T-\alpha)(T-\alpha^q)\ldots(T-\alpha^{q^{\delta-1}}) \tag{2.1}$$

and

$$Q(T) = (T-\beta)(T-\beta^q)\ldots(T-\beta^{q^{\nu-1}}). \tag{2.2}$$

Continuation of Proof

We now take congruences in the ring $A^{'} = \mathbb{F}^{'}[T]$.

Continuation of Proof

We now take congruences in the ring $A^{'} = \mathbb{F}^{'}[T]$. Note that if $f(T) \in A^{'}$ we have $f(T) \equiv f(\alpha) (\text{mod } (T - \alpha))$.

Continuation of Proof

We now take congruences in the ring $A^{'} = \mathbb{F}^{'}[T]$. Note that if $f(T) \in A^{'}$ we have $f(T) \equiv f(\alpha) \pmod{(T - \alpha)}$. Also note that if $g(T) \in A$ then $g(T)^q = g(T^q)$ which follows readily from the fact that the coefficients of $g(T)$ are in $\mathbb{F}_q$.

Continuation of Proof

We now take congruences in the ring $A^{'} = \mathbb{F}^{'}[T]$. Note that if $f(T) \in A^{'}$ we have $f(T) \equiv f(\alpha) (\text{mod } (T - \alpha))$. Also note that if $g(T) \in A$ then $g(T)^q = g(T^q)$ which follows readily from the fact that the coefficients of $g(T)$ are in $\mathbb{F}_q$. From this remark, and the definition, we compute that (Q/P) is congruent to

$$Q(T)^{1+q+\cdots+q^{\delta-1}} \quad \equiv \quad Q(T)Q(T^q)\cdots Q(T^{q^{\delta-1}})$$

Continuation of Proof

We now take congruences in the ring $A^{'} = \mathbb{F}^{'}[T]$. Note that if $f(T) \in A^{'}$ we have $f(T) \equiv f(\alpha)(\bmod\ (T-\alpha))$. Also note that if $g(T) \in A$ then $g(T)^q = g(T^q)$ which follows readily from the fact that the coefficients of $g(T)$ are in $\mathbb{F}_q$. From this remark, and the definition, we compute that (Q/P) is congruent to

$$\begin{aligned} Q(T)^{1+q+\cdots+q^{\delta-1}} &\equiv Q(T)Q(T^q)\cdots Q(T^{q^{\delta-1}}) \\ &\equiv Q(\alpha)Q(\alpha^q)\cdots Q(\alpha^{q^{\delta-1}})(\bmod\ (T-\alpha)). \end{aligned} \quad (2.3)$$

Continuation of Proof

We now take congruences in the ring $A^{'} = \mathbb{F}^{'}[T]$. Note that if $f(T) \in A^{'}$ we have $f(T) \equiv f(\alpha)(\bmod\ (T-\alpha))$. Also note that if $g(T) \in A$ then $g(T)^q = g(T^q)$ which follows readily from the fact that the coefficients of $g(T)$ are in $\mathbb{F}_q$. From this remark, and the definition, we compute that (Q/P) is congruent to

$$\begin{aligned} Q(T)^{1+q+\cdots+q^{\delta-1}} &\equiv Q(T)Q(T^q)\cdots Q(T^{q^{\delta-1}}) \\ &\equiv Q(\alpha)Q(\alpha^q)\cdots Q(\alpha^{q^{\delta-1}})(\bmod\ (T-\alpha)). \end{aligned} \quad (2.3)$$

By symmetry this congruence holds modulo $(T-\alpha^{q^i})$ for all i and it follows that it holds modulo P.

Continuation of Proof

We now take congruences in the ring $A^{'} = \mathbb{F}^{'}[T]$. Note that if $f(T) \in A^{'}$ we have $f(T) \equiv f(\alpha)(\text{mod } (T-\alpha))$. Also note that if $g(T) \in A$ then $g(T)^q = g(T^q)$ which follows readily from the fact that the coefficients of $g(T)$ are in $\mathbb{F}_q$. From this remark, and the definition, we compute that (Q/P) is congruent to

$$\begin{aligned} Q(T)^{1+q+\cdots+q^{\delta-1}} &\equiv Q(T)Q(T^q)\cdots Q(T^{q^{\delta-1}}) \\ &\equiv Q(\alpha)Q(\alpha^q)\cdots Q(\alpha^{q^{\delta-1}})(\text{mod } (T-\alpha)). \quad (2.3) \end{aligned}$$

By symmetry this congruence holds modulo $(T-\alpha^{q^i})$ for all i and it follows that it holds modulo P. Combining this result with equation (2.3) yields the following congruence:

$$\left(\frac{Q}{P}\right) \equiv \prod_{i=0}^{\delta-1}\prod_{j=0}^{\nu-1}(\alpha^{q^i} - \beta^{q^j})(\text{mod } P).$$

Continuation of Proof

We now take congruences in the ring $A^{'} = \mathbb{F}^{'}[T]$. Note that if $f(T) \in A^{'}$ we have $f(T) \equiv f(\alpha)(\text{mod } (T-\alpha))$. Also note that if $g(T) \in A$ then $g(T)^q = g(T^q)$ which follows readily from the fact that the coefficients of $g(T)$ are in $\mathbb{F}_q$. From this remark, and the definition, we compute that (Q/P) is congruent to

$$\begin{aligned} Q(T)^{1+q+\cdots+q^{\delta-1}} &\equiv Q(T)Q(T^q)\cdots Q(T^{q^{\delta-1}}) \\ &\equiv Q(\alpha)Q(\alpha^q)\cdots Q(\alpha^{q^{\delta-1}})(\text{mod } (T-\alpha)). \quad (2.3) \end{aligned}$$

By symmetry this congruence holds modulo $(T-\alpha^{q^i})$ for all i and it follows that it holds modulo P. Combining this result with equation (2.3) yields the following congruence:

$$\left(\frac{Q}{P}\right) \equiv \prod_{i=0}^{\delta-1}\prod_{j=0}^{\nu-1}(\alpha^{q^i} - \beta^{q^j})(\text{mod } P).$$

Both sides of this congruence are in $\mathbb{F}^{'}$ so they must be equal.

Continuation of Proof

We now take congruences in the ring $A^{'} = \mathbb{F}^{'}[T]$. Note that if $f(T) \in A^{'}$ we have $f(T) \equiv f(\alpha)(\text{mod } (T-\alpha))$. Also note that if $g(T) \in A$ then $g(T)^q = g(T^q)$ which follows readily from the fact that the coefficients of $g(T)$ are in $\mathbb{F}_q$. From this remark, and the definition, we compute that (Q/P) is congruent to

$$\begin{aligned} Q(T)^{1+q+\cdots+q^{\delta-1}} &\equiv Q(T)Q(T^q)\cdots Q(T^{q^{\delta-1}}) \\ &\equiv Q(\alpha)Q(\alpha^q)\cdots Q(\alpha^{q^{\delta-1}})(\text{mod } (T-\alpha)). \end{aligned} \quad (2.3)$$

By symmetry this congruence holds modulo $(T-\alpha^{q^i})$ for all i and it follows that it holds modulo P. Combining this result with equation (2.3) yields the following congruence:

$$\left(\frac{Q}{P}\right) \equiv \prod_{i=0}^{\delta-1}\prod_{j=0}^{\nu-1}(\alpha^{q^i} - \beta^{q^j})(\text{mod } P).$$

Both sides of this congruence are in $\mathbb{F}^{'}$ so they must be equal. Thus,

$$\left(\frac{Q}{P}\right) = \prod_{i=0}^{\delta-1}\prod_{j=0}^{\nu-1}(\alpha^{q^i} - \beta^{q^j}) = (-1)^{\delta\nu}\prod_{j=0}^{\nu-1}\prod_{i=0}^{\delta-1}(\beta^{q^j} - \alpha^{q^i}) = (-1)^{\delta\nu}\left(\frac{P}{Q}\right).$$

Continuation of Proof

We now take congruences in the ring $A^{'} = \mathbb{F}^{'}[T]$. Note that if $f(T) \in A^{'}$ we have $f(T) \equiv f(\alpha)(\text{mod } (T-\alpha))$. Also note that if $g(T) \in A$ then $g(T)^q = g(T^q)$ which follows readily from the fact that the coefficients of $g(T)$ are in $\mathbb{F}_q$. From this remark, and the definition, we compute that (Q/P) is congruent to

$$\begin{aligned} Q(T)^{1+q+\cdots+q^{\delta-1}} &\equiv Q(T)Q(T^q)\cdots Q(T^{q^{\delta-1}}) \\ &\equiv Q(\alpha)Q(\alpha^q)\cdots Q(\alpha^{q^{\delta-1}})(\text{mod } (T-\alpha)). \quad (2.3) \end{aligned}$$

By symmetry this congruence holds modulo $(T-\alpha^{q^i})$ for all i and it follows that it holds modulo P. Combining this result with equation (2.3) yields the following congruence:

$$\left(\frac{Q}{P}\right) \equiv \prod_{i=0}^{\delta-1}\prod_{j=0}^{\nu-1}(\alpha^{q^i} - \beta^{q^j})(\text{mod } P).$$

Both sides of this congruence are in $\mathbb{F}^{'}$ so they must be equal. Thus,

$$\left(\frac{Q}{P}\right) = \prod_{i=0}^{\delta-1}\prod_{j=0}^{\nu-1}(\alpha^{q^i} - \beta^{q^j}) = (-1)^{\delta\nu}\prod_{j=0}^{\nu-1}\prod_{i=0}^{\delta-1}(\beta^{q^j} - \alpha^{q^i}) = (-1)^{\delta\nu}\left(\frac{P}{Q}\right).$$

This concludes the proof.

As in the classical theory, it is convenient to extend the definition of the d-th power reciprocity symbol to the case where P is replaced with an arbitrary non-zero element $b \in A$.

As in the classical theory, it is convenient to extend the definition of the d-th power reciprocity symbol to the case where P is replaced with an arbitrary non-zero element $b \in A$.

Definition

Let $b \in A$, $b \neq 0$, and $b = \beta Q_1^{f_1} Q_2^{f_2} \dots Q_s^{f_s}$ be the prime decomposition of b.

As in the classical theory, it is convenient to extend the definition of the d-th power reciprocity symbol to the case where P is replaced with an arbitrary non-zero element $b \in A$.

Definition

Let $b \in A$, $b \neq 0$, and $b = \beta Q_1^{f_1} Q_2^{f_2} \dots Q_s^{f_s}$ be the prime decomposition of b. If $a \in A$, define

$$\left(\frac{a}{b}\right)_d = \prod_{j=1}^{s} \left(\frac{a}{Q_j}\right)_d^{f_j}. \tag{2.4}$$

As in the classical theory, it is convenient to extend the definition of the d-th power reciprocity symbol to the case where P is replaced with an arbitrary non-zero element $b \in A$.

Definition

Let $b \in A$, $b \neq 0$, and $b = \beta Q_1^{f_1} Q_2^{f_2} \dots Q_s^{f_s}$ be the prime decomposition of b. If $a \in A$, define

$$\left(\frac{a}{b}\right)_d = \prod_{j=1}^{s} \left(\frac{a}{Q_j}\right)_d^{f_j}. \tag{2.4}$$

Notice that this definition ignores $\beta = \operatorname{sgn}(b)$ and so the symbol only depends on the principal ideal bA generated by b.

As in the classical theory, it is convenient to extend the definition of the d-th power reciprocity symbol to the case where P is replaced with an arbitrary non-zero element $b \in A$.

Definition

Let $b \in A$, $b \neq 0$, and $b = \beta Q_1^{f_1} Q_2^{f_2} \dots Q_s^{f_s}$ be the prime decomposition of b. If $a \in A$, define

$$\left(\frac{a}{b}\right)_d = \prod_{j=1}^{s} \left(\frac{a}{Q_j}\right)_d^{f_j}. \tag{2.4}$$

Notice that this definition ignores $\beta = \mathrm{sgn}(b)$ and so the symbol only depends on the principal ideal bA generated by b. The basic properties of this extended symbol are easily derived from those of the d-th power residue symbol.

Proposition (3.4)

The symbol $(a/b)_d$ *has the following properties.*

Proposition (3.4)

The symbol $(a/b)_d$ *has the following properties.*

1. *If* $a_1 \equiv a_2 \pmod{b}$ *then* $(a_1/b)_d = (a_2/b)_d$.

Proposition (3.4)

The symbol $(a/b)_d$ has the following properties.

1. *If* $a_1 \equiv a_2 \pmod{b}$ *then* $(a_1/b)_d = (a_2/b)_d$.
2. $(a_1 a_2/b)_d = (a_1/b)_d (a_2/b)_d$.

Proposition (3.4)

The symbol $(a/b)_d$ *has the following properties.*

1. *If* $a_1 \equiv a_2 \pmod{b}$ *then* $(a_1/b)_d = (a_2/b)_d$.
2. $(a_1 a_2/b)_d = (a_1/b)_d (a_2/b)_d$.
3. $(a/b_1 b_2)_d = (a/b_1)_d (a/b_2)_d$.

Proposition (3.4)

The symbol $(a/b)_d$ has the following properties.

1. *If* $a_1 \equiv a_2 (\text{mod } b)$ *then* $(a_1/b)_d = (a_2/b)_d$.
2. $(a_1 a_2/b)_d = (a_1/b)_d (a_2/b)_d$.
3. $(a/b_1 b_2)_d = (a/b_1)_d (a/b_2)_d$.
4. $(a/b)_d \neq 0$ *iff* $(a, b) = 1$ *(a is relatively prime to b).*

Proposition (3.4)

The symbol $(a/b)_d$ has the following properties.

1. *If* $a_1 \equiv a_2 \pmod{b}$ *then* $(a_1/b)_d = (a_2/b)_d$.
2. $(a_1 a_2/b)_d = (a_1/b)_d (a_2/b)_d$.
3. $(a/b_1 b_2)_d = (a/b_1)_d (a/b_2)_d$.
4. $(a/b)_d \neq 0$ *iff* $(a, b) = 1$ *(a is relatively prime to b).*
5. *If* $x^d \equiv a \pmod{b}$ *is solvable, then* $(a/b)_d = 1$*, provided that* $(a, b) = 1$.

Proposition (3.4)

The symbol $(a/b)_d$ has the following properties.

1. *If $a_1 \equiv a_2 \pmod{b}$ then $(a_1/b)_d = (a_2/b)_d$.*
2. $(a_1a_2/b)_d = (a_1/b)_d(a_2/b)_d$.
3. $(a/b_1b_2)_d = (a/b_1)_d(a/b_2)_d$.
4. $(a/b)_d \neq 0$ *iff* $(a,b) = 1$ *(a is relatively prime to b).*
5. *If $x^d \equiv a \pmod{b}$ is solvable, then $(a/b)_d = 1$, provided that $(a,b) = 1$.*

Proof.

Properties 1–4 follow from the definition and the properties of the symbol $(a/P)_d$.

Proposition (3.4)

The symbol $(a/b)_d$ has the following properties.

1. *If $a_1 \equiv a_2 (\bmod\ b)$ then $(a_1/b)_d = (a_2/b)_d$.*
2. $(a_1 a_2/b)_d = (a_1/b)_d (a_2/b)_d$.
3. $(a/b_1 b_2)_d = (a/b_1)_d (a/b_2)_d$.
4. $(a/b)_d \neq 0$ *iff* $(a, b) = 1$ *(a is relatively prime to b).*
5. *If $x^d \equiv a (\bmod\ b)$ is solvable, then $(a/b)_d = 1$, provided that $(a, b) = 1$.*

Proof.

Properties 1–4 follow from the definition and the properties of the symbol $(a/P)_d$. To show property 5, suppose $c^d \equiv a (\bmod\ b)$. Then, by properties 1 and 2, $(a/b)_d = (c^d/b)_d = (c/b)_d^d = 1$. $\square$

It is useful to have a form of the reciprocity law which works for arbitrary (i.e., not necessarily monic or irreducible) elements of A.

It is useful to have a form of the reciprocity law which works for arbitrary (i.e., not necessarily monic or irreducible) elements of A. For $f \in A$, $f \neq 0$, define $\mathrm{sgn}_d(f)$ to be the leading coefficient of f raised to the $\frac{q-1}{d}$ power.

It is useful to have a form of the reciprocity law which works for arbitrary (i.e., not necessarily monic or irreducible) elements of A. For $f \in A$, $f \neq 0$, define $\mathrm{sgn}_d(f)$ to be the leading coefficient of f raised to the $\frac{q-1}{d}$ power.

Theorem (The general reciprocity law)

Let $a, b \in A$ be relatively prime, non-zero elements.

It is useful to have a form of the reciprocity law which works for arbitrary (i.e., not necessarily monic or irreducible) elements of A. For $f \in A$, $f \neq 0$, define $\mathrm{sgn}_d(f)$ to be the leading coefficient of f raised to the $\frac{q-1}{d}$ power.

Theorem (The general reciprocity law)

Let $a, b \in A$ be relatively prime, non-zero elements. Then,

$$\left(\frac{a}{b}\right)_d \left(\frac{b}{a}\right)_d^{-1} = (-1)^{\frac{q-1}{d} deg(a) deg(b)} sgn_d(a)^{deg(b)} sgn_d(b)^{-deg(a)}.$$

It is useful to have a form of the reciprocity law which works for arbitrary (i.e., not necessarily monic or irreducible) elements of A. For $f \in A$, $f \neq 0$, define $\mathrm{sgn}_d(f)$ to be the leading coefficient of f raised to the $\frac{q-1}{d}$ power.

Theorem (The general reciprocity law)

Let $a, b \in A$ be relatively prime, non-zero elements. Then,

$$\left(\frac{a}{b}\right)_d \left(\frac{b}{a}\right)_d^{-1} = (-1)^{\frac{q-1}{d} deg(a) deg(b)} sgn_d(a)^{deg(b)} sgn_d(b)^{-deg(a)}.$$

Proof.

When a and b are monic irreducibles this reduces to Theorem on the d-th power reciprocity law.

It is useful to have a form of the reciprocity law which works for arbitrary (i.e., not necessarily monic or irreducible) elements of A. For $f \in A$, $f \neq 0$, define $\mathrm{sgn}_d(f)$ to be the leading coefficient of f raised to the $\frac{q-1}{d}$ power.

Theorem (The general reciprocity law)

Let $a, b \in A$ be relatively prime, non-zero elements. Then,

$$\left(\frac{a}{b}\right)_d \left(\frac{b}{a}\right)_d^{-1} = (-1)^{\frac{q-1}{d} deg(a) deg(b)} sgn_d(a)^{deg(b)} sgn_d(b)^{-deg(a)}.$$

Proof.

When a and b are monic irreducibles this reduces to Theorem on the d-th power reciprocity law. In general, the proof proceeds by appealing to Proposition 3.2, the theorem on the d-th power reciprocity law, the definitions, and the fact that the degree of a product of two polynomials is equal to the sum of their degrees. $\square$

A Brief Discussion

The importance of the reciprocity law lies in the fact that it relates two natural questions.

A Brief Discussion

The importance of the reciprocity law lies in the fact that it relates two natural questions. Given a polynomial m of positive degree, what are the d-th powers modulo m?

A Brief Discussion

The importance of the reciprocity law lies in the fact that it relates two natural questions. Given a polynomial m of positive degree, what are the d-th powers modulo m? Since $(A/mA)^*$ is finite, one can answer this question in principle by just writing down the elements of $(A/mA)^*$, raising them to the d-th power, and making a list of the results.

A Brief Discussion

The importance of the reciprocity law lies in the fact that it relates two natural questions. Given a polynomial m of positive degree, what are the d-th powers modulo m? Since $(A/mA)^*$ is finite, one can answer this question in principle by just writing down the elements of $(A/mA)^*$, raising them to the d-th power, and making a list of the results. The answer will be a list of cosets or residue classes modulo m.

A Brief Discussion

The importance of the reciprocity law lies in the fact that it relates two natural questions. Given a polynomial m of positive degree, what are the d-th powers modulo m? Since $(A/mA)^*$ is finite, one can answer this question in principle by just writing down the elements of $(A/mA)^*$, raising them to the d-th power, and making a list of the results. The answer will be a list of cosets or residue classes modulo m. In practice this may be hard because of the amount of calculation involved.

A Brief Discussion

The importance of the reciprocity law lies in the fact that it relates two natural questions. Given a polynomial m of positive degree, what are the d-th powers modulo m? Since $(A/mA)^*$ is finite, one can answer this question in principle by just writing down the elements of $(A/mA)^*$, raising them to the d-th power, and making a list of the results. The answer will be a list of cosets or residue classes modulo m. In practice this may be hard because of the amount of calculation involved. One can appeal to the structure of $(A/mA)^*$ to find shortcuts.

A Brief Discussion

The importance of the reciprocity law lies in the fact that it relates two natural questions. Given a polynomial m of positive degree, what are the d-th powers modulo m? Since $(A/mA)^*$ is finite, one can answer this question in principle by just writing down the elements of $(A/mA)^*$, raising them to the d-th power, and making a list of the results. The answer will be a list of cosets or residue classes modulo m. In practice this may be hard because of the amount of calculation involved. One can appeal to the structure of $(A/mA)^*$ to find shortcuts.

Parenthetically, it is an interesting question to determine the number of d-th powers modulo m.

A Brief Discussion

The importance of the reciprocity law lies in the fact that it relates two natural questions. Given a polynomial m of positive degree, what are the d-th powers modulo m? Since $(A/mA)^*$ is finite, one can answer this question in principle by just writing down the elements of $(A/mA)^*$, raising them to the d-th power, and making a list of the results. The answer will be a list of cosets or residue classes modulo m. In practice this may be hard because of the amount of calculation involved. One can appeal to the structure of $(A/mA)^*$ to find shortcuts.

Parenthetically, it is an interesting question to determine the number of d-th powers modulo m. Recall that we are assuming $d \mid (q-1)$.

A Brief Discussion

The importance of the reciprocity law lies in the fact that it relates two natural questions. Given a polynomial m of positive degree, what are the d-th powers modulo m? Since $(A/mA)^*$ is finite, one can answer this question in principle by just writing down the elements of $(A/mA)^*$, raising them to the d-th power, and making a list of the results. The answer will be a list of cosets or residue classes modulo m. In practice this may be hard because of the amount of calculation involved. One can appeal to the structure of $(A/mA)^*$ to find shortcuts.

Parenthetically, it is an interesting question to determine the number of d-th powers modulo m. Recall that we are assuming $d \mid (q-1)$. Under this assumption, the answer is $\Phi(m)/d^{\lambda(m)}$, where $\lambda(m)$ is the number of distinct monic prime divisors of m.

A Brief Discussion

The importance of the reciprocity law lies in the fact that it relates two natural questions. Given a polynomial m of positive degree, what are the d-th powers modulo m? Since $(A/mA)^*$ is finite, one can answer this question in principle by just writing down the elements of $(A/mA)^*$, raising them to the d-th power, and making a list of the results. The answer will be a list of cosets or residue classes modulo m. In practice this may be hard because of the amount of calculation involved. One can appeal to the structure of $(A/mA)^*$ to find shortcuts.

Parenthetically, it is an interesting question to determine the number of d-th powers modulo m. Recall that we are assuming $d \mid (q-1)$. Under this assumption, the answer is $\Phi(m)/d^{\lambda(m)}$, where $\lambda(m)$ is the number of distinct monic prime divisors of m. This follows from a proposition from last lecture and the Chinese Remainder Theorem.

A Brief Discussion - Continuation

A Brief Discussion - Continuation

Now let's turn things around somewhat.

A Brief Discussion - Continuation

Now let's turn things around somewhat. Given m, find all primes P such that m is a d-th power modulo P.

A Brief Discussion - Continuation

Now let's turn things around somewhat. Given m, find all primes P such that m is a d-th power modulo P. It turns out that there are infinitely many such primes, so that it is not possible to answer the question by making a list.

A Brief Discussion - Continuation

Now let's turn things around somewhat. Given m, find all primes P such that m is a d-th power modulo P. It turns out that there are infinitely many such primes, so that it is not possible to answer the question by making a list. One has to characterize the primes with this property in some natural way.

A Brief Discussion - Continuation

Now let's turn things around somewhat. Given m, find all primes P such that m is a d-th power modulo P. It turns out that there are infinitely many such primes, so that it is not possible to answer the question by making a list. One has to characterize the primes with this property in some natural way. This is what the reciprocity law allows us to do.

A Brief Discussion - Continuation

Now let's turn things around somewhat. Given m, find all primes P such that m is a d-th power modulo P. It turns out that there are infinitely many such primes, so that it is not possible to answer the question by making a list. One has to characterize the primes with this property in some natural way. This is what the reciprocity law allows us to do. For simplicity, we will assume that m is monic.

A Brief Discussion - Continuation

Now let's turn things around somewhat. Given m, find all primes P such that m is a d-th power modulo P. It turns out that there are infinitely many such primes, so that it is not possible to answer the question by making a list. One has to characterize the primes with this property in some natural way. This is what the reciprocity law allows us to do. For simplicity, we will assume that m is monic. It is no loss of generality to assume that all the primes we deal with are monic as well.

A Brief Discussion - Continuation

Now let's turn things around somewhat. Given m, find all primes P such that m is a d-th power modulo P. It turns out that there are infinitely many such primes, so that it is not possible to answer the question by making a list. One has to characterize the primes with this property in some natural way. This is what the reciprocity law allows us to do. For simplicity, we will assume that m is monic. It is no loss of generality to assume that all the primes we deal with are monic as well. Let $\{a_1, a_2, \ldots, a_t\}$ be coset representatives for the classes in $(A/mA)^*$ which have the property $(a/m)_d = 1$.

A Brief Discussion - Continuation

Now let's turn things around somewhat. Given m, find all primes P such that m is a d-th power modulo P. It turns out that there are infinitely many such primes, so that it is not possible to answer the question by making a list. One has to characterize the primes with this property in some natural way. This is what the reciprocity law allows us to do. For simplicity, we will assume that m is monic. It is no loss of generality to assume that all the primes we deal with are monic as well. Let $\{a_1, a_2, \ldots, a_t\}$ be coset representatives for the classes in $(A/mA)^*$ which have the property $(a/m)_d = 1$. If there is a $b \in A$ such that $(b/m)_d = -1$ let $\{b_1, b_2, \ldots, b_t\}$ be coset representatives for all classes with this property.

Proposition (3.6)

With the previous assumptions we have

Proposition (3.6)

With the previous assumptions we have

1. *If* $deg(m)$ *is even,* $(q-1)/d$ *is even, or* $p = char(F) = 2$*,* m *is a* d*-th power modulo* P *iff* $P \equiv a_i (\text{mod } m)$ *for some* $i = 1, 2, \ldots, t$*.*

Proposition (3.6)

With the previous assumptions we have

1. *If* $deg(m)$ *is even,* $(q-1)/d$ *is even, or* $p = char(F) = 2$*,* m *is a* d*-th power modulo* P *iff* $P \equiv a_i \pmod{m}$ *for some* $i = 1, 2, \ldots, t$*.*
2. *If* $deg(m)$ *is odd,* $(q-1)/d$ *is odd, and* $p = char(F)$ *is odd, then* m *is a* d*-th power modulo* P *iff either* $deg(P)$ *is even and* $P \equiv a_i \pmod{m}$ *for some* $i = 1, 2, \ldots, t$ *or* $deg(P)$ *is odd and* $P \equiv b_i \pmod{m}$ *for some* $i = 1, 2, \ldots, t$*.*

A number of interesting number-theoretic questions are of the following form: if a certain property holds modulo all but finitely many primes, does it hold in A?

A number of interesting number-theoretic questions are of the following form: if a certain property holds modulo all but finitely many primes, does it hold in A? One such property is that of being a d-th power.

A number of interesting number-theoretic questions are of the following form: if a certain property holds modulo all but finitely many primes, does it hold in A? One such property is that of being a d-th power. In this case the question has a positive answer.

A number of interesting number-theoretic questions are of the following form: if a certain property holds modulo all but finitely many primes, does it hold in A? One such property is that of being a d-th power. In this case the question has a positive answer. The key to the proof, as we shall see, is the reciprocity law.

A number of interesting number-theoretic questions are of the following form: if a certain property holds modulo all but finitely many primes, does it hold in A? One such property is that of being a d-th power. In this case the question has a positive answer. The key to the proof, as we shall see, is the reciprocity law.

Theorem (3.7)

Let $m \in A$ be a polynomial of positive degree.

A number of interesting number-theoretic questions are of the following form: if a certain property holds modulo all but finitely many primes, does it hold in A? One such property is that of being a d-th power. In this case the question has a positive answer. The key to the proof, as we shall see, is the reciprocity law.

Theorem (3.7)

Let $m \in A$ be a polynomial of positive degree. Let d be an integer dividing $q - 1$.

A number of interesting number-theoretic questions are of the following form: if a certain property holds modulo all but finitely many primes, does it hold in A? One such property is that of being a d-th power. In this case the question has a positive answer. The key to the proof, as we shall see, is the reciprocity law.

Theorem (3.7)

Let $m \in A$ be a polynomial of positive degree. Let d be an integer dividing $q-1$. If $x^d \equiv m \pmod{P}$ is solvable for all but finitely many primes P, then $m = m_0^d$ for some $m_0 \in A$.

Dirichlet L-Series and Primes in Arithmetic Progression

- In this section we will prove the analogue of Dirichlet's famous theorem about primes in arithmetic progression. This was first proved by H. Kornblum and E. Landau.

Dirichlet L-Series and Primes in Arithmetic Progression

- In this section we will prove the analogue of Dirichlet's famous theorem about primes in arithmetic progression. This was first proved by H. Kornblum and E. Landau.
- The proof of the theorem uses the theory of Dirichlet series over $k = \mathbb{F}_q(T)$.

Dirichlet L-Series and Primes in Arithmetic Progression

- In this section we will prove the analogue of Dirichlet's famous theorem about primes in arithmetic progression. This was first proved by H. Kornblum and E. Landau.
- The proof of the theorem uses the theory of Dirichlet series over $k = \mathbb{F}_q(T)$.
- The main difficulty is to proof that $L(1, \chi) \neq 0$ for non-trivial characters χ.

Dirichlet L-Series and Primes in Arithmetic Progression

- In this section we will prove the analogue of Dirichlet's famous theorem about primes in arithmetic progression. This was first proved by H. Kornblum and E. Landau.
- The proof of the theorem uses the theory of Dirichlet series over $k = \mathbb{F}_q(T)$.
- The main difficulty is to proof that $L(1, \chi) \neq 0$ for non-trivial characters χ.
- To conclude we give a refinement of Dirichlet's theorem, which shows that given an arithmetic progression $\{a + mx \mid a, m \in A, (a, m) = 1\}$, then for all sufficiently large integers N, there is a prime P of degree N which lies in this arithmetic progression.

Dirichlet density of primes in A

The Dirichlet density of a set of primes in A gives a quantitative measure how big such a set is.

Dirichlet density of primes in A

The Dirichlet density of a set of primes in A gives a quantitative measure how big such a set is. Let $f(s)$ and $g(s)$ be two complex valued functions of a real variable s both defined on some open interval $(1, b)$.

Dirichlet density of primes in A

The Dirichlet density of a set of primes in A gives a quantitative measure how big such a set is. Let $f(s)$ and $g(s)$ be two complex valued functions of a real variable s both defined on some open interval $(1, b)$. We define $f \approx g$ to mean that $f - g$ remains bounded as $s \to 1$ inside $(1, b)$.

Dirichlet density of primes in A

The Dirichlet density of a set of primes in A gives a quantitative measure how big such a set is. Let $f(s)$ and $g(s)$ be two complex valued functions of a real variable s both defined on some open interval $(1, b)$. We define $f \approx g$ to mean that $f - g$ remains bounded as $s \to 1$ inside $(1, b)$.

Proposition (4.1)

We have

$$\log \zeta_A(s) \approx \log\left(\frac{1}{s-1}\right) \approx \sum_P |P|^{-s},$$

where the sum is over all irreducible monic polynomials P.

Dirichlet density of primes in A

The Dirichlet density of a set of primes in A gives a quantitative measure how big such a set is. Let $f(s)$ and $g(s)$ be two complex valued functions of a real variable s both defined on some open interval $(1, b)$. We define $f \approx g$ to mean that $f - g$ remains bounded as $s \to 1$ inside $(1, b)$.

Proposition (4.1)

We have

$$\log \zeta_A(s) \approx \log\left(\frac{1}{s-1}\right) \approx \sum_P |P|^{-s},$$

where the sum is over all irreducible monic polynomials P.

Proof.

Since $\zeta_A(s) = (1 - q^{1-s})^{-1}$ we see that $\lim_{s\to 1}(s-1)\zeta_A(s) = 1/\log(q)$.

Dirichlet density of primes in A

The Dirichlet density of a set of primes in A gives a quantitative measure how big such a set is. Let $f(s)$ and $g(s)$ be two complex valued functions of a real variable s both defined on some open interval $(1,b)$. We define $f \approx g$ to mean that $f-g$ remains bounded as $s \to 1$ inside $(1,b)$.

Proposition (4.1)

We have

$$\log \zeta_A(s) \approx \log\left(\frac{1}{s-1}\right) \approx \sum_P |P|^{-s},$$

where the sum is over all irreducible monic polynomials P.

Proof.

Since $\zeta_A(s) = (1-q^{1-s})^{-1}$ we see that $\lim_{s\to 1}(s-1)\zeta_A(s) = 1/\log(q)$. Thus, $\log\zeta_A(s) - \log(s-1)^{-1}$ is bounded as $s \to 1$, which establishes the first relation.

Dirichlet density of primes in A

The Dirichlet density of a set of primes in A gives a quantitative measure how big such a set is. Let $f(s)$ and $g(s)$ be two complex valued functions of a real variable s both defined on some open interval $(1, b)$. We define $f \approx g$ to mean that $f - g$ remains bounded as $s \to 1$ inside $(1, b)$.

Proposition (4.1)

We have

$$\log \zeta_A(s) \approx \log\left(\frac{1}{s-1}\right) \approx \sum_P |P|^{-s},$$

where the sum is over all irreducible monic polynomials P.

Proof.

Since $\zeta_A(s) = (1 - q^{1-s})^{-1}$ we see that $\lim_{s\to 1}(s-1)\zeta_A(s) = 1/\log(q)$. Thus, $\log \zeta_A(s) - \log(s-1)^{-1}$ is bounded as $s \to 1$, which establishes the first relation. As for the second relation we see, using the Euler product for $\zeta_A(s)$

$$\log \zeta_A(s) = -\sum_P \log(1 - |P|^{-s}) = \sum_{P,k} \frac{|P|^{-ks}}{k} = \sum_P |P|^{0s} + \sum_{P,k\geq 2} \frac{|P|^{-ks}}{k}.$$

Dirichlet density of primes in A

The Dirichlet density of a set of primes in A gives a quantitative measure how big such a set is. Let $f(s)$ and $g(s)$ be two complex valued functions of a real variable s both defined on some open interval $(1, b)$. We define $f \approx g$ to mean that $f - g$ remains bounded as $s \to 1$ inside $(1, b)$.

Proposition (4.1)

We have

$$\log \zeta_A(s) \approx \log\left(\frac{1}{s-1}\right) \approx \sum_P |P|^{-s},$$

where the sum is over all irreducible monic polynomials P.

Proof.

Since $\zeta_A(s) = (1 - q^{1-s})^{-1}$ we see that $\lim_{s \to 1}(s-1)\zeta_A(s) = 1/\log(q)$. Thus, $\log \zeta_A(s) - \log(s-1)^{-1}$ is bounded as $s \to 1$, which establishes the first relation. As for the second relation we see, using the Euler product for $\zeta_A(s)$

$$\log \zeta_A(s) = -\sum_P \log(1 - |P|^{-s}) = \sum_{P,k} \frac{|P|^{-ks}}{k} = \sum_P |P|^{0s} + \sum_{P,k\geq 2} \frac{|P|^{-ks}}{k}.$$

Now, $\sum_{k\geq 2} |P|^{-ks}/k < \sum_{k\geq 2} |P|^{-ks} = |P|^{-2s}(1 - |P|^{-s})^{-1} < 2|P|^{-2s}$.

Dirichlet density of primes in A

The Dirichlet density of a set of primes in A gives a quantitative measure how big such a set is. Let $f(s)$ and $g(s)$ be two complex valued functions of a real variable s both defined on some open interval $(1,b)$. We define $f \approx g$ to mean that $f-g$ remains bounded as $s \to 1$ inside $(1,b)$.

Proposition (4.1)

We have

$$\log \zeta_A(s) \approx \log\left(\frac{1}{s-1}\right) \approx \sum_P |P|^{-s},$$

where the sum is over all irreducible monic polynomials P.

Proof.

Since $\zeta_A(s) = (1-q^{1-s})^{-1}$ we see that $\lim_{s\to 1}(s-1)\zeta_A(s) = 1/\log(q)$. Thus, $\log \zeta_A(s) - \log(s-1)^{-1}$ is bounded as $s \to 1$, which establishes the first relation. As for the second relation we see, using the Euler product for $\zeta_A(s)$

$$\log \zeta_A(s) = -\sum_P \log(1-|P|^{-s}) = \sum_{P,k} \frac{|P|^{-ks}}{k} = \sum_P |P|^{0s} + \sum_{P,k\geq 2} \frac{|P|^{-ks}}{k}.$$

Now, $\sum_{k\geq 2} |P|^{-ks}/k < \sum_{k\geq 2} |P|^{-ks} = |P|^{-2s}(1-|P|^{-s})^{-1} < 2|P|^{-2s}$. Thus the last sum in the above equation is bounded by $2\zeta_A(2)$.

Dirichlet density of primes in A

The Dirichlet density of a set of primes in A gives a quantitative measure how big such a set is. Let $f(s)$ and $g(s)$ be two complex valued functions of a real variable s both defined on some open interval $(1, b)$. We define $f \approx g$ to mean that $f - g$ remains bounded as $s \to 1$ inside $(1, b)$.

Proposition (4.1)

We have

$$\log \zeta_A(s) \approx \log\left(\frac{1}{s-1}\right) \approx \sum_P |P|^{-s},$$

where the sum is over all irreducible monic polynomials P.

Proof.

Since $\zeta_A(s) = (1 - q^{1-s})^{-1}$ we see that $\lim_{s\to 1}(s-1)\zeta_A(s) = 1/\log(q)$. Thus, $\log \zeta_A(s) - \log(s-1)^{-1}$ is bounded as $s \to 1$, which establishes the first relation. As for the second relation we see, using the Euler product for $\zeta_A(s)$

$$\log \zeta_A(s) = -\sum_P \log(1 - |P|^{-s}) = \sum_{P,k} \frac{|P|^{-ks}}{k} = \sum_P |P|^{0s} + \sum_{P,k\geq 2} \frac{|P|^{-ks}}{k}.$$

Now, $\sum_{k\geq 2} |P|^{-ks}/k < \sum_{k\geq 2} |P|^{-ks} = |P|^{-2s}(1 - |P|^{-s})^{-1} < 2|P|^{-2s}$. Thus the last sum in the above equation is bounded by $2\zeta_A(2)$. This shows that $\log \zeta_A(s) \approx \sum_P |P|^{-s}$ which completes the proof.

Definition

The word "prime" will denote a monic irreducible in A.

Definition

The word "prime" will denote a monic irreducible in A. Let $\mathcal{S}$ be a set of primes in A.

Definition

The word "prime" will denote a monic irreducible in A. Let $\mathcal{S}$ be a set of primes in A. The Dirichlet density of $\mathcal{S}$, $\delta(\mathcal{S})$ is defined to be

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

provided that the limit exists.

Definition

The word "prime" will denote a monic irreducible in A. Let $\mathcal{S}$ be a set of primes in A. The Dirichlet density of $\mathcal{S}$, $\delta(\mathcal{S})$ is defined to be

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

provided that the limit exists. The limit is assumed to be taken over the values of s lying in a real interval $(1, b)$.

Definition

The word "prime" will denote a monic irreducible in A. Let $\mathcal{S}$ be a set of primes in A. The Dirichlet density of $\mathcal{S}$, $\delta(\mathcal{S})$ is defined to be

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

provided that the limit exists. The limit is assumed to be taken over the values of s lying in a real interval $(1, b)$.

Remark

1. $0 \le \delta(\mathcal{S}) \le 1$.

Definition

The word "prime" will denote a monic irreducible in A. Let $\mathcal{S}$ be a set of primes in A. The Dirichlet density of $\mathcal{S}$, $\delta(\mathcal{S})$ is defined to be

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

provided that the limit exists. The limit is assumed to be taken over the values of s lying in a real interval $(1, b)$.

Remark

1. $0 \leq \delta(\mathcal{S}) \leq 1$.
2. *If $\mathcal{S} = \mathcal{S}_1 \cup \mathcal{S}_2$, then $\delta(\mathcal{S}) = \delta(\mathcal{S}_1) + \delta(\mathcal{S}_2)$ provided $\mathcal{S}_1$ and $\mathcal{S}_2$ both have densities and are disjoint.*

Definition

The word "prime" will denote a monic irreducible in A. Let $\mathcal{S}$ be a set of primes in A. The Dirichlet density of $\mathcal{S}$, $\delta(\mathcal{S})$ is defined to be

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

provided that the limit exists. The limit is assumed to be taken over the values of s lying in a real interval $(1, b)$.

Remark

1. $0 \leq \delta(\mathcal{S}) \leq 1$.
2. *If $\mathcal{S} = \mathcal{S}_1 \cup \mathcal{S}_2$, then $\delta(\mathcal{S}) = \delta(\mathcal{S}_1) + \delta(\mathcal{S}_2)$ provided $\mathcal{S}_1$ and $\mathcal{S}_2$ both have densities and are disjoint.*
3. *The Dirichlet density of a finite set is zero.*

Definition

The word "prime" will denote a monic irreducible in A. Let $\mathcal{S}$ be a set of primes in A. The Dirichlet density of $\mathcal{S}$, $\delta(\mathcal{S})$ is defined to be

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

provided that the limit exists. The limit is assumed to be taken over the values of s lying in a real interval $(1, b)$.

Remark

1. $0 \leq \delta(\mathcal{S}) \leq 1$.
2. *If $\mathcal{S} = \mathcal{S}_1 \cup \mathcal{S}_2$, then $\delta(\mathcal{S}) = \delta(\mathcal{S}_1) + \delta(\mathcal{S}_2)$ provided $\mathcal{S}_1$ and $\mathcal{S}_2$ both have densities and are disjoint.*
3. *The Dirichlet density of a finite set is zero.*

Thus, Dirichlet density is something like a probability measure.

If the Dirichlet density of a set exists and is positive, we are assured that the set is infinite.

If the Dirichlet density of a set exists and is positive, we are assured that the set is infinite. One of the two main results in this section asserts that if a and m are relatively prime polynomials, then the Dirichlet density of the set $\mathcal{S} = \{P \in A | P \text{ prime}, P \equiv a (\bmod\ m)\}$ exists and is equal to $1/\Phi(m)$.

If the Dirichlet density of a set exists and is positive, we are assured that the set is infinite. One of the two main results in this section asserts that if a and m are relatively prime polynomials, then the Dirichlet density of the set $\mathcal{S} = \{P \in A | P \text{ prime}, P \equiv a (\bmod\ m)\}$ exists and is equal to $1/\Phi(m)$.

Definition

Let m be an element of A of positive degree.

If the Dirichlet density of a set exists and is positive, we are assured that the set is infinite. One of the two main results in this section asserts that if a and m are relatively prime polynomials, then the Dirichlet density of the set $\mathcal{S} = \{P \in A | P \text{ prime}, P \equiv a (\text{mod } m)\}$ exists and is equal to $1/\Phi(m)$.

Definition

Let m be an element of A of positive degree. A ***Dirichlet character modulo*** *m is a function from $A \to \mathbb{C}$ such that*

(a) $\chi(a + bm) = \chi(a)$ *for all $a, b \in A$.*

If the Dirichlet density of a set exists and is positive, we are assured that the set is infinite. One of the two main results in this section asserts that if a and m are relatively prime polynomials, then the Dirichlet density of the set $\mathcal{S} = \{P \in A | P \text{ prime}, P \equiv a (\text{mod } m)\}$ exists and is equal to $1/\Phi(m)$.

Definition

*Let m be an element of A of positive degree. A **Dirichlet character modulo** m is a function from $A \to \mathbb{C}$ such that*

(a) $\chi(a + bm) = \chi(a)$ *for all* $a, b \in A$.

(b) $\chi(a)\chi(b) = \chi(ab)$ *for all* $a, b \in A$.

If the Dirichlet density of a set exists and is positive, we are assured that the set is infinite. One of the two main results in this section asserts that if a and m are relatively prime polynomials, then the Dirichlet density of the set $\mathcal{S} = \{P \in A | P \text{ prime}, P \equiv a (\text{mod } m)\}$ exists and is equal to $1/\Phi(m)$.

Definition

*Let m be an element of A of positive degree. A **Dirichlet character modulo** m is a function from $A \to \mathbb{C}$ such that*

(a) $\chi(a + bm) = \chi(a)$ *for all* $a, b \in A$.

(b) $\chi(a)\chi(b) = \chi(ab)$ *for all* $a, b \in A$.

(c) $\chi(a) \neq 0$ *if and only if* $(a, m) = 1$.

A Dirichlet character modulo m induces a homomorphism from $(A/mA)^* \to \mathbb{C}$ and conversely, given such a homomorphism there is a uniquely corresponding Dirichlet character.

A Dirichlet character modulo m induces a homomorphism from $(A/mA)^* \to \mathbb{C}$ and conversely, given such a homomorphism there is a uniquely corresponding Dirichlet character. The **trivial Dirichlet character** χ_0 is defined by the property that $\chi_0(a) = 1$ if $(a, m) = 1$ and $\chi_0(a) = 0$ if $(a, m) \neq 1$.

It can be shown that there are exactly $\Phi(m)$ Dirichlet character modulo m which is the same cardinality as that of the group $(A/mA)^*$.

A Dirichlet character modulo m induces a homomorphism from $(A/mA)^* \to \mathbb{C}$ and conversely, given such a homomorphism there is a uniquely corresponding Dirichlet character. The **trivial Dirichlet character** χ_0 is defined by the property that $\chi_0(a) = 1$ if $(a, m) = 1$ and $\chi_0(a) = 0$ if $(a, m) \neq 1$.

It can be shown that there are exactly $\Phi(m)$ Dirichlet character modulo m which is the same cardinality as that of the group $(A/mA)^*$. Let X_m be the set of Dirichlet characters modulo m.

A Dirichlet character modulo m induces a homomorphism from $(A/mA)^* \to \mathbb{C}$ and conversely, given such a homomorphism there is a uniquely corresponding Dirichlet character. The **trivial Dirichlet character** χ_0 is defined by the property that $\chi_0(a) = 1$ if $(a, m) = 1$ and $\chi_0(a) = 0$ if $(a, m) \neq 1$.

It can be shown that there are exactly $\Phi(m)$ Dirichlet character modulo m which is the same cardinality as that of the group $(A/mA)^*$. Let X_m be the set of Dirichlet characters modulo m. If $\chi, \psi \in X_m$ define their product, $\chi\psi$, by the formula $\chi\psi(a) = \chi(a)\psi(a)$.

A Dirichlet character modulo m induces a homomorphism from $(A/mA)^* \to \mathbb{C}$ and conversely, given such a homomorphism there is a uniquely corresponding Dirichlet character. The **trivial Dirichlet character** χ_0 is defined by the property that $\chi_0(a) = 1$ if $(a, m) = 1$ and $\chi_0(a) = 0$ if $(a, m) \neq 1$.

It can be shown that there are exactly $\Phi(m)$ Dirichlet character modulo m which is the same cardinality as that of the group $(A/mA)^*$. Let X_m be the set of Dirichlet characters modulo m. If $\chi, \psi \in X_m$ define their product, $\chi\psi$, by the formula $\chi\psi(a) = \chi(a)\psi(a)$. This makes X_m into a group.

The identity of this group is the trivial character χ_0.

A Dirichlet character modulo m induces a homomorphism from $(A/mA)^* \to \mathbb{C}$ and conversely, given such a homomorphism there is a uniquely corresponding Dirichlet character. The **trivial Dirichlet character** χ_0 is defined by the property that $\chi_0(a) = 1$ if $(a, m) = 1$ and $\chi_0(a) = 0$ if $(a, m) \neq 1$.

It can be shown that there are exactly $\Phi(m)$ Dirichlet character modulo m which is the same cardinality as that of the group $(A/mA)^*$. Let X_m be the set of Dirichlet characters modulo m. If $\chi, \psi \in X_m$ define their product, $\chi\psi$, by the formula $\chi\psi(a) = \chi(a)\psi(a)$. This makes X_m into a group.

The identity of this group is the trivial character χ_0. The inverse of a character is given by $\chi^{-1}(a) = \chi(a)^{-1}$ if $(a, m) = 1$, and $\chi^{-1}(a) = 0$ if $(a, m) \neq 1$.

A Dirichlet character modulo m induces a homomorphism from $(A/mA)^* \to \mathbb{C}$ and conversely, given such a homomorphism there is a uniquely corresponding Dirichlet character. The **trivial Dirichlet character** χ_0 is defined by the property that $\chi_0(a) = 1$ if $(a, m) = 1$ and $\chi_0(a) = 0$ if $(a, m) \neq 1$.

It can be shown that there are exactly $\Phi(m)$ Dirichlet character modulo m which is the same cardinality as that of the group $(A/mA)^*$. Let X_m be the set of Dirichlet characters modulo m. If $\chi, \psi \in X_m$ define their product, $\chi\psi$, by the formula $\chi\psi(a) = \chi(a)\psi(a)$. This makes X_m into a group.

The identity of this group is the trivial character χ_0. The inverse of a character is given by $\chi^{-1}(a) = \chi(a)^{-1}$ if $(a, m) = 1$, and $\chi^{-1}(a) = 0$ if $(a, m) \neq 1$.

It can be shown that X_m is isomorphic to $(A/mA)^*$.

A Dirichlet character modulo m induces a homomorphism from $(A/mA)^* \to \mathbb{C}$ and conversely, given such a homomorphism there is a uniquely corresponding Dirichlet character. The **trivial Dirichlet character** χ_0 is defined by the property that $\chi_0(a) = 1$ if $(a, m) = 1$ and $\chi_0(a) = 0$ if $(a, m) \neq 1$.

It can be shown that there are exactly $\Phi(m)$ Dirichlet character modulo m which is the same cardinality as that of the group $(A/mA)^*$. Let X_m be the set of Dirichlet characters modulo m. If $\chi, \psi \in X_m$ define their product, $\chi\psi$, by the formula $\chi\psi(a) = \chi(a)\psi(a)$. This makes X_m into a group.

The identity of this group is the trivial character χ_0. The inverse of a character is given by $\chi^{-1}(a) = \chi(a)^{-1}$ if $(a, m) = 1$, and $\chi^{-1}(a) = 0$ if $(a, m) \neq 1$.

It can be shown that X_m is isomorphic to $(A/mA)^*$. This is a special case of a general result which asserts that a finite abelian group G is isomorphic to its character group $\hat{G}$, see Lang, "Algebra", Chapter 1, Section 9.

A Dirichlet character modulo m induces a homomorphism from $(A/mA)^* \to \mathbb{C}$ and conversely, given such a homomorphism there is a uniquely corresponding Dirichlet character. The **trivial Dirichlet character** χ_0 is defined by the property that $\chi_0(a) = 1$ if $(a, m) = 1$ and $\chi_0(a) = 0$ if $(a, m) \neq 1$.

It can be shown that there are exactly $\Phi(m)$ Dirichlet character modulo m which is the same cardinality as that of the group $(A/mA)^*$. Let X_m be the set of Dirichlet characters modulo m. If $\chi, \psi \in X_m$ define their product, $\chi\psi$, by the formula $\chi\psi(a) = \chi(a)\psi(a)$. This makes X_m into a group.

The identity of this group is the trivial character χ_0. The inverse of a character is given by $\chi^{-1}(a) = \chi(a)^{-1}$ if $(a, m) = 1$, and $\chi^{-1}(a) = 0$ if $(a, m) \neq 1$.

It can be shown that X_m is isomorphic to $(A/mA)^*$. This is a special case of a general result which asserts that a finite abelian group G is isomorphic to its character group $\hat{G}$, see Lang, "Algebra", Chapter 1, Section 9.

If $\chi \in X_m$ let $\overline{\chi}$ be defined by $\overline{\chi}(a) = \overline{\chi(a)}$ = complex conjugate of $\chi(a)$.

A Dirichlet character modulo m induces a homomorphism from $(A/mA)^* \to \mathbb{C}$ and conversely, given such a homomorphism there is a uniquely corresponding Dirichlet character. The **trivial Dirichlet character** χ_0 is defined by the property that $\chi_0(a) = 1$ if $(a, m) = 1$ and $\chi_0(a) = 0$ if $(a, m) \neq 1$.

It can be shown that there are exactly $\Phi(m)$ Dirichlet character modulo m which is the same cardinality as that of the group $(A/mA)^*$. Let X_m be the set of Dirichlet characters modulo m. If $\chi, \psi \in X_m$ define their product, $\chi\psi$, by the formula $\chi\psi(a) = \chi(a)\psi(a)$. This makes X_m into a group.

The identity of this group is the trivial character χ_0. The inverse of a character is given by $\chi^{-1}(a) = \chi(a)^{-1}$ if $(a, m) = 1$, and $\chi^{-1}(a) = 0$ if $(a, m) \neq 1$.

It can be shown that X_m is isomorphic to $(A/mA)^*$. This is a special case of a general result which asserts that a finite abelian group G is isomorphic to its character group $\hat{G}$, see Lang, "Algebra", Chapter 1, Section 9.

If $\chi \in X_m$ let $\overline{\chi}$ be defined by $\overline{\chi}(a) = \overline{\chi(a)} =$ complex conjugate of $\chi(a)$. Since the value of a character is either zero or a root of unity, it is easy to see that $\overline{\chi} = \chi^{-1}$.

Proposition (4.2)

Let χ and ψ be two Dirichlet characters modulo m and a and b two elements of A relatively prime to m.

Proposition (4.2)

Let χ and ψ be two Dirichlet characters modulo m and a and b two elements of A relatively prime to m. Then

1. $\sum_a \chi(a)\overline{\psi(a)} = \Phi(m)\delta(\chi, \psi)$.

Proposition (4.2)

Let χ and ψ be two Dirichlet characters modulo m and a and b two elements of A relatively prime to m. Then

1. $\sum_a \chi(a)\overline{\psi(a)} = \Phi(m)\delta(\chi, \psi)$.
2. $\sum_\chi \chi(a)\overline{\chi(b)} = \Phi(m)\delta(a, b)$.

Proposition (4.2)

Let χ and ψ be two Dirichlet characters modulo m and a and b two elements of A relatively prime to m. Then

1. $\sum_a \chi(a)\overline{\psi(a)} = \Phi(m)\delta(\chi, \psi)$.
2. $\sum_\chi \chi(a)\overline{\chi(b)} = \Phi(m)\delta(a, b)$.

The first sum is over any set of representatives for A/mA and the second sum is over all Dirichlet characters modulo m.

Proposition (4.2)

Let χ and ψ be two Dirichlet characters modulo m and a and b two elements of A relatively prime to m. Then

1. $\sum_a \chi(a)\overline{\psi(a)} = \Phi(m)\delta(\chi,\psi)$.
2. $\sum_\chi \chi(a)\overline{\chi(b)} = \Phi(m)\delta(a,b)$.

The first sum is over any set of representatives for A/mA and the second sum is over all Dirichlet characters modulo m. By definition, $\delta(\chi,\psi) = 0$ if $\chi \neq \psi$ and 1 if $\chi = \psi$.

Proposition (4.2)

Let χ and ψ be two Dirichlet characters modulo m and a and b two elements of A relatively prime to m. Then

1. $\sum_a \chi(a)\overline{\psi(a)} = \Phi(m)\delta(\chi,\psi)$.
2. $\sum_\chi \chi(a)\overline{\chi(b)} = \Phi(m)\delta(a,b)$.

The first sum is over any set of representatives for A/mA and the second sum is over all Dirichlet characters modulo m. By definition, $\delta(\chi,\psi) = 0$ if $\chi \neq \psi$ and 1 if $\chi = \psi$.

Definition

Let χ be a Dirichlet character modulo m.

Proposition (4.2)

Let χ and ψ be two Dirichlet characters modulo m and a and b two elements of A relatively prime to m. Then

1. $\sum_a \chi(a)\overline{\psi(a)} = \Phi(m)\delta(\chi, \psi)$.
2. $\sum_\chi \chi(a)\overline{\chi(b)} = \Phi(m)\delta(a, b)$.

The first sum is over any set of representatives for A/mA and the second sum is over all Dirichlet characters modulo m. By definition, $\delta(\chi, \psi) = 0$ if $\chi \neq \psi$ and 1 if $\chi = \psi$.

Definition

Let χ be a Dirichlet character modulo m. The Dirichlet L-series corresponding to χ is defined by

$$L(s, \chi) = \sum_{f \text{ monic}} \frac{\chi(f)}{|f|^s}.$$

Proposition (4.2)

Let χ and ψ be two Dirichlet characters modulo m and a and b two elements of A relatively prime to m. Then

1. $\sum_a \chi(a)\overline{\psi(a)} = \Phi(m)\delta(\chi, \psi)$.
2. $\sum_\chi \chi(a)\overline{\chi(b)} = \Phi(m)\delta(a, b)$.

The first sum is over any set of representatives for A/mA and the second sum is over all Dirichlet characters modulo m. By definition, $\delta(\chi, \psi) = 0$ if $\chi \neq \psi$ and 1 if $\chi = \psi$.

Definition

Let χ be a Dirichlet character modulo m. The Dirichlet L-series corresponding to χ is defined by

$$L(s, \chi) = \sum_{f \text{ monic}} \frac{\chi(f)}{|f|^s}.$$

From the definition and by comparison with the zeta function $\zeta_A(s)$ one sees immediately that the series for $L(s, \chi)$ converges absolutely for $\Re(s) > 1$.

Since characters are multiplicative we can deduce that the following Euler products holds for $\Re(s) > 1$.

$$L(s, \chi) = \prod_P \left(1 - \frac{\chi(P)}{|P|^s}\right)^{-1}.$$

Since characters are multiplicative we can deduce that the following Euler products holds for $\Re(s) > 1$.

$$L(s, \chi) = \prod_{P} \left(1 - \frac{\chi(P)}{|P|^s}\right)^{-1}.$$

An immediate consequence of this product decomposition is the fact that the L-series corresponding to the trivial character is almost the same as $\zeta_A(s)$.

Since characters are multiplicative we can deduce that the following Euler products holds for $\Re(s) > 1$.

$$L(s, \chi) = \prod_{P} \left(1 - \frac{\chi(P)}{|P|^s}\right)^{-1}.$$

An immediate consequence of this product decomposition is the fact that the L-series corresponding to the trivial character is almost the same as $\zeta_A(s)$. More precisely,

$$L(s, \chi_0) = \prod_{P|m} \left(1 - \frac{1}{|P|^s}\right) \zeta_A(s).$$

Since characters are multiplicative we can deduce that the following Euler products holds for $\mathfrak{R}(s) > 1$.

$$L(s,\chi) = \prod_{P} \left(1 - \frac{\chi(P)}{|P|^s}\right)^{-1}.$$

An immediate consequence of this product decomposition is the fact that the L-series corresponding to the trivial character is almost the same as $\zeta_A(s)$. More precisely,

$$L(s,\chi_0) = \prod_{P|m} \left(1 - \frac{1}{|P|^s}\right) \zeta_A(s).$$

This shows that $L(s,\chi_0)$ can be analytically continued to all of $\mathbb{C}$ and has a simple pole at $s = 1$ since the same is true of $\zeta_A(s)$.

Since characters are multiplicative we can deduce that the following Euler products holds for $\Re(s) > 1$.

$$L(s, \chi) = \prod_{P} \left(1 - \frac{\chi(P)}{|P|^s}\right)^{-1}.$$

An immediate consequence of this product decomposition is the fact that the L-series corresponding to the trivial character is almost the same as $\zeta_A(s)$. More precisely,

$$L(s, \chi_0) = \prod_{P|m} \left(1 - \frac{1}{|P|^s}\right) \zeta_A(s).$$

This shows that $L(s, \chi_0)$ can be analytically continued to all of $\mathbb{C}$ and has a simple pole at $s = 1$ since the same is true of $\zeta_A(s)$. On the other hand,

Proposition (4.3)

Let χ be a non-trivial Dirichlet character modulo m.

Since characters are multiplicative we can deduce that the following Euler products holds for $\Re(s) > 1$.

$$L(s, \chi) = \prod_P \left(1 - \frac{\chi(P)}{|P|^s}\right)^{-1}.$$

An immediate consequence of this product decomposition is the fact that the L-series corresponding to the trivial character is almost the same as $\zeta_A(s)$. More precisely,

$$L(s, \chi_0) = \prod_{P|m} \left(1 - \frac{1}{|P|^s}\right) \zeta_A(s).$$

This shows that $L(s, \chi_0)$ can be analytically continued to all of $\mathbb{C}$ and has a simple pole at $s = 1$ since the same is true of $\zeta_A(s)$. On the other hand,

Proposition (4.3)

Let χ be a non-trivial Dirichlet character modulo m. Then, $L(s, \chi)$ is a polynomial in q^{-s} of degree at most $deg(m) - 1$.

Proof of Proposition 4.3.

Define

$$A(n,\chi) = \sum_{\substack{\deg(f)=n \\ f \text{ monic}}} \chi(f).$$

Proof of Proposition 4.3.

Define

$$A(n,\chi) = \sum_{\substack{\deg(f)=n \\ f \text{ monic}}} \chi(f).$$

It is clear from the definition of $L(s,\chi)$ that

$$L(s,\chi) = \sum_{n=0}^{\infty} A(n,\chi) q^{-ns}.$$

Proof of Proposition 4.3.

Define

$$A(n, \chi) = \sum_{\substack{\deg(f)=n \\ f \text{ monic}}} \chi(f).$$

It is clear from the definition of $L(s, \chi)$ that

$$L(s, \chi) = \sum_{n=0}^{\infty} A(n, \chi) q^{-ns}.$$

Thus the result will follow if we can show that $A(n, \chi) = 0$ for all $n \geq \deg(m)$.

Proof of Proposition 4.3.

Define

$$A(n, \chi) = \sum_{\substack{\deg(f)=n \\ f \text{ monic}}} \chi(f).$$

It is clear from the definition of $L(s, \chi)$ that

$$L(s, \chi) = \sum_{n=0}^{\infty} A(n, \chi) q^{-ns}.$$

Thus the result will follow if we can show that $A(n, \chi) = 0$ for all $n \geq \deg(m)$.
Let's assume that $n \geq \deg(m)$.

Proof of Proposition 4.3.

Define

$$A(n,\chi) = \sum_{\substack{\deg(f)=n \\ f \text{ monic}}} \chi(f).$$

It is clear from the definition of $L(s,\chi)$ that

$$L(s,\chi) = \sum_{n=0}^{\infty} A(n,\chi) q^{-ns}.$$

Thus the result will follow if we can show that $A(n,\chi) = 0$ for all $n \geq \deg(m)$. Let's assume that $n \geq \deg(m)$. If $\deg(f) = n$, we can write $f = hm + r$, where r is a polynomial of degree less than $\deg(m)$ or $r = 0$.

Proof of Proposition 4.3.

Define

$$A(n,\chi) = \sum_{\substack{\deg(f)=n \\ f \text{ monic}}} \chi(f).$$

It is clear from the definition of $L(s,\chi)$ that

$$L(s,\chi) = \sum_{n=0}^{\infty} A(n,\chi) q^{-ns}.$$

Thus the result will follow if we can show that $A(n,\chi) = 0$ for all $n \geq \deg(m)$. Let's assume that $n \geq \deg(m)$. If $\deg(f) = n$, we can write $f = hm + r$, where r is a polynomial of degree less than $\deg(m)$ or $r = 0$. Here, h is a polynomial of degree $n - \deg(m) \geq 0$, whose leading coefficient is $\operatorname{sgn}(m)^{-1}$ (since f is monic).

Proof of Proposition 4.3.

Define

$$A(n,\chi) = \sum_{\substack{\deg(f)=n \\ f \text{ monic}}} \chi(f).$$

It is clear from the definition of $L(s,\chi)$ that

$$L(s,\chi) = \sum_{n=0}^{\infty} A(n,\chi) q^{-ns}.$$

Thus the result will follow if we can show that $A(n,\chi) = 0$ for all $n \geq \deg(m)$. Let's assume that $n \geq \deg(m)$. If $\deg(f) = n$, we can write $f = hm + r$, where r is a polynomial of degree less than $\deg(m)$ or $r = 0$. Here, h is a polynomial of degree $n - \deg(m) \geq 0$, whose leading coefficient is $\operatorname{sgn}(m)^{-1}$ (since f is monic). Conversely, all monic polynomials of degree $n \geq \deg(m)$ can be uniquely written in this fashion.

Proof of Proposition 4.3.

Define

$$A(n,\chi) = \sum_{\substack{\deg(f)=n \\ f \ \text{monic}}} \chi(f).$$

It is clear from the definition of $L(s,\chi)$ that

$$L(s,\chi) = \sum_{n=0}^{\infty} A(n,\chi) q^{-ns}.$$

Thus the result will follow if we can show that $A(n,\chi) = 0$ for all $n \geq \deg(m)$. Let's assume that $n \geq \deg(m)$. If $\deg(f) = n$, we can write $f = hm + r$, where r is a polynomial of degree less than $\deg(m)$ or $r = 0$. Here, h is a polynomial of degree $n - \deg(m) \geq 0$, whose leading coefficient is $\mathrm{sgn}(m)^{-1}$ (since f is monic). Conversely, all monic polynomials of degree $n \geq \deg(m)$ can be uniquely written in this fashion. Since χ is periodic modulo m and since h can be chosen in $q^{n-\deg(m)}$ ways, we have

$$A(n,\chi) = q^{n-\deg(m)} \sum_{r} \chi(r) = 0,$$

by the first orthogonality relation since $\chi \neq \chi_0$, and the sum is over all r with $\deg(r) < \deg(m)$, which is a set of representatives for A/mA. □

The previous proposition shows that if χ is non-trivial, then $L(s, \chi)$ which was initially defined for $\Re(s) > 1$ can be analytically continued to an entire function on all of $\mathbb{C}$.

The previous proposition shows that if χ is non-trivial, then $L(s, \chi)$ which was initially defined for $\Re(s) > 1$ can be analytically continued to an entire function on all of $\mathbb{C}$. We have already seen that $L(s, \chi_0)$ can be analytically continued to all of $\mathbb{C}$ with a simple pole at $s = 1$.

The previous proposition shows that if χ is non-trivial, then $L(s, \chi)$ which was initially defined for $\Re(s) > 1$ can be analytically continued to an entire function on all of $\mathbb{C}$. We have already seen that $L(s, \chi_0)$ can be analytically continued to all of $\mathbb{C}$ with a simple pole at $s = 1$. These facts are much harder to establish when working over $\mathbb{Z}$ rather than A.

The previous proposition shows that if χ is non-trivial, then $L(s, \chi)$ which was initially defined for $\Re(s) > 1$ can be analytically continued to an entire function on all of $\mathbb{C}$. We have already seen that $L(s, \chi_0)$ can be analytically continued to all of $\mathbb{C}$ with a simple pole at $s = 1$. These facts are much harder to establish when working over $\mathbb{Z}$ rather than A.

In the proof of Dirichlet's theorem on primes in arithmetic progressions the most difficult part is the proof that $L(1, \chi) \neq 0$ if χ is non-trivial.

The previous proposition shows that if χ is non-trivial, then $L(s, \chi)$ which was initially defined for $\Re(s) > 1$ can be analytically continued to an entire function on all of $\mathbb{C}$. We have already seen that $L(s, \chi_0)$ can be analytically continued to all of $\mathbb{C}$ with a simple pole at $s = 1$. These facts are much harder to establish when working over $\mathbb{Z}$ rather than A.

In the proof of Dirichlet's theorem on primes in arithmetic progressions the most difficult part is the proof that $L(1, \chi) \neq 0$ if χ is non-trivial. This turns out to be substantially easier in function fields because the L-series are essentially polynomials.

The previous proposition shows that if χ is non-trivial, then $L(s, \chi)$ which was initially defined for $\Re(s) > 1$ can be analytically continued to an entire function on all of $\mathbb{C}$. We have already seen that $L(s, \chi_0)$ can be analytically continued to all of $\mathbb{C}$ with a simple pole at $s = 1$. These facts are much harder to establish when working over $\mathbb{Z}$ rather than A.

In the proof of Dirichlet's theorem on primes in arithmetic progressions the most difficult part is the proof that $L(1, \chi) \neq 0$ if χ is non-trivial. This turns out to be substantially easier in function fields because the L-series are essentially polynomials. We begin with a lemma.

The previous proposition shows that if χ is non-trivial, then $L(s, \chi)$ which was initially defined for $\mathfrak{R}(s) > 1$ can be analytically continued to an entire function on all of $\mathbb{C}$. We have already seen that $L(s, \chi_0)$ can be analytically continued to all of $\mathbb{C}$ with a simple pole at $s = 1$. These facts are much harder to establish when working over $\mathbb{Z}$ rather than A.
In the proof of Dirichlet's theorem on primes in arithmetic progressions the most difficult part is the proof that $L(1, \chi) \neq 0$ if χ is non-trivial. This turns out to be substantially easier in function fields because the L-series are essentially polynomials. We begin with a lemma.

Lema (4.4)

Let χ vary over all Dirichlet characters modulo m.

The previous proposition shows that if χ is non-trivial, then $L(s,\chi)$ which was initially defined for $\Re(s) > 1$ can be analytically continued to an entire function on all of $\mathbb{C}$. We have already seen that $L(s,\chi_0)$ can be analytically continued to all of $\mathbb{C}$ with a simple pole at $s = 1$. These facts are much harder to establish when working over $\mathbb{Z}$ rather than A.

In the proof of Dirichlet's theorem on primes in arithmetic progressions the most difficult part is the proof that $L(1,\chi) \neq 0$ if χ is non-trivial. This turns out to be substantially easier in function fields because the L-series are essentially polynomials. We begin with a lemma.

Lema (4.4)

Let χ vary over all Dirichlet characters modulo m. Then, for each prime P not dividing m, there exist positive integers f_P and g_P such that $f_P g_P = \Phi(m)$

The previous proposition shows that if χ is non-trivial, then $L(s,\chi)$ which was initially defined for $\mathfrak{R}(s) > 1$ can be analytically continued to an entire function on all of $\mathbb{C}$. We have already seen that $L(s,\chi_0)$ can be analytically continued to all of $\mathbb{C}$ with a simple pole at $s = 1$. These facts are much harder to establish when working over $\mathbb{Z}$ rather than A.

In the proof of Dirichlet's theorem on primes in arithmetic progressions the most difficult part is the proof that $L(1,\chi) \neq 0$ if χ is non-trivial. This turns out to be substantially easier in function fields because the L-series are essentially polynomials. We begin with a lemma.

Lema (4.4)

Let χ vary over all Dirichlet characters modulo m. Then, for each prime P not dividing m, there exist positive integers f_P and g_P such that $f_P g_P = \Phi(m)$ and

$$\prod_{\chi} L(s,\chi) = \prod_{P \nmid m} (1 - |P|^{-f_P s})^{-g_P}.$$

Proof of Lemma 4.4.

For a fixed prime P not dividing m, the map $\chi \to \chi(P)$ is a homomorphism from the group $X_m \to \mathbb{C}^*$.

Proof of Lemma 4.4.

For a fixed prime P not dividing m, the map $\chi \to \chi(P)$ is a homomorphism from the group $X_m \to \mathbb{C}^*$. The image must be a cyclic group of order f_P, say, generated by ζ_{f_P}.

Proof of Lemma 4.4.

For a fixed prime P not dividing m, the map $\chi \to \chi(P)$ is a homomorphism from the group $X_m \to \mathbb{C}^*$. The image must be a cyclic group of order f_P, say, generated by ζ_{f_P}. If g_P is the order of the kernel, clearly $f_P g_P = \Phi(m)$.

Proof of Lemma 4.4.

For a fixed prime P not dividing m, the map $\chi \to \chi(P)$ is a homomorphism from the group $X_m \to \mathbb{C}^*$. The image must be a cyclic group of order f_P, say, generated by ζ_{f_P}. If g_P is the order of the kernel, clearly $f_P g_P = \Phi(m)$. With these preliminaries, we can calculate for fixed P.

$$\prod_{\chi}(1 - \chi(P)|P|^{-s}) = \prod_{i=0}^{f_P - 1}(1 - \zeta_{f_P}^i |P|^{-s})^{g_P} = (1 - |P|^{-f_P s})^{g_P}.$$

Proof of Lemma 4.4.

For a fixed prime P not dividing m, the map $\chi \to \chi(P)$ is a homomorphism from the group $X_m \to \mathbb{C}^*$. The image must be a cyclic group of order f_P, say, generated by ζ_{f_P}. If g_P is the order of the kernel, clearly $f_P g_P = \Phi(m)$. With these preliminaries, we can calculate for fixed P.

$$\prod_{\chi}(1-\chi(P)|P|^{-s}) = \prod_{i=0}^{f_P-1}(1-\zeta_{f_P}^{i}|P|^{-s})^{g_P} = (1-|P|^{-f_P s})^{g_P}.$$

Now take the inverse of both sides, multiply over all P, and the lemma follows. $\square$

Lema (4.5)

Suppose χ *is a complex Dirichlet character modulo m, i.e.* $\overline{\chi} \neq \chi$.

Lema (4.5)

Suppose χ is a complex Dirichlet character modulo m, i.e. $\overline{\chi} \neq \chi$. Then, $L(1, \chi) \neq 0$.

Proof.

The right-hand side of the equation in the statement of Lemma 4.4 is equal to a Dirichlet series with positive coefficients and constant term 1.

Lema (4.5)

Suppose χ is a complex Dirichlet character modulo m, i.e. $\overline{\chi} \neq \chi$. Then, $L(1, \chi) \neq 0$.

Proof.

The right-hand side of the equation in the statement of Lemma 4.4 is equal to a Dirichlet series with positive coefficients and constant term 1. Consequently, its value at real numbers s such that $s > 1$ is a real number greater than 1.

Lema (4.5)

Suppose χ is a complex Dirichlet character modulo m, i.e. $\overline{\chi} \neq \chi$. Then, $L(1, \chi) \neq 0$.

Proof.

The right-hand side of the equation in the statement of Lemma 4.4 is equal to a Dirichlet series with positive coefficients and constant term 1. Consequently, its value at real numbers s such that $s > 1$ is a real number greater than 1. Suppose χ is a complex Dirichlet character and that $L(1, \chi) = 0$.

Lema (4.5)

Suppose χ is a complex Dirichlet character modulo m, i.e. $\overline{\chi} \neq \chi$. Then, $L(1, \chi) \neq 0$.

Proof.

The right-hand side of the equation in the statement of Lemma 4.4 is equal to a Dirichlet series with positive coefficients and constant term 1. Consequently, its value at real numbers s such that $s > 1$ is a real number greater than 1. Suppose χ is a complex Dirichlet character and that $L(1, \chi) = 0$. Then, by complex conjugation we see $L(1, \overline{\chi}) = 0$ as well.

Lema (4.5)

Suppose χ is a complex Dirichlet character modulo m, i.e. $\overline{\chi} \neq \chi$. Then, $L(1, \chi) \neq 0$.

Proof.

The right-hand side of the equation in the statement of Lemma 4.4 is equal to a Dirichlet series with positive coefficients and constant term 1. Consequently, its value at real numbers s such that $s > 1$ is a real number greater than 1. Suppose χ is a complex Dirichlet character and that $L(1, \chi) = 0$. Then, by complex conjugation we see $L(1, \overline{\chi}) = 0$ as well. In the product $\prod_{\chi} L(s, \chi)$ the term corresponding to the trivial character has a simple pole at $s = 1$.

Lema (4.5)

Suppose χ is a complex Dirichlet character modulo m, i.e. $\overline{\chi} \neq \chi$. Then, $L(1, \chi) \neq 0$.

Proof.

The right-hand side of the equation in the statement of Lemma 4.4 is equal to a Dirichlet series with positive coefficients and constant term 1. Consequently, its value at real numbers s such that $s > 1$ is a real number greater than 1. Suppose χ is a complex Dirichlet character and that $L(1, \chi) = 0$. Then, by complex conjugation we see $L(1, \overline{\chi}) = 0$ as well. In the product $\prod_{\chi} L(s, \chi)$ the term corresponding to the trivial character has a simple pole at $s = 1$. All the other terms are regular there and two of them have zeros.

Lema (4.5)

Suppose χ is a complex Dirichlet character modulo m, i.e. $\overline{\chi} \neq \chi$. Then, $L(1, \chi) \neq 0$.

Proof.

The right-hand side of the equation in the statement of Lemma 4.4 is equal to a Dirichlet series with positive coefficients and constant term 1. Consequently, its value at real numbers s such that $s > 1$ is a real number greater than 1. Suppose χ is a complex Dirichlet character and that $L(1, \chi) = 0$. Then, by complex conjugation we see $L(1, \overline{\chi}) = 0$ as well. In the product $\prod_{\chi} L(s, \chi)$ the term corresponding to the trivial character has a simple pole at $s = 1$. All the other terms are regular there and two of them have zeros. Thus, the product is zero at $s = 1$.

Lema (4.5)

Suppose χ is a complex Dirichlet character modulo m, i.e. $\overline{\chi} \neq \chi$. Then, $L(1, \chi) \neq 0$.

Proof.

The right-hand side of the equation in the statement of Lemma 4.4 is equal to a Dirichlet series with positive coefficients and constant term 1. Consequently, its value at real numbers s such that $s > 1$ is a real number greater than 1. Suppose χ is a complex Dirichlet character and that $L(1, \chi) = 0$. Then, by complex conjugation we see $L(1, \overline{\chi}) = 0$ as well. In the product $\prod_{\chi} L(s, \chi)$ the term corresponding to the trivial character has a simple pole at $s = 1$. All the other terms are regular there and two of them have zeros. Thus, the product is zero at $s = 1$. This contradicts the fact, established above, that for all $s > 1$ the value of the product is greater than 1.

Lema (4.5)

Suppose χ is a complex Dirichlet character modulo m, i.e. $\overline{\chi} \neq \chi$. Then, $L(1, \chi) \neq 0$.

Proof.

The right-hand side of the equation in the statement of Lemma 4.4 is equal to a Dirichlet series with positive coefficients and constant term 1. Consequently, its value at real numbers s such that $s > 1$ is a real number greater than 1. Suppose χ is a complex Dirichlet character and that $L(1, \chi) = 0$. Then, by complex conjugation we see $L(1, \overline{\chi}) = 0$ as well. In the product $\prod_{\chi} L(s, \chi)$ the term corresponding to the trivial character has a simple pole at $s = 1$. All the other terms are regular there and two of them have zeros. Thus, the product is zero at $s = 1$. This contradicts the fact, established above, that for all $s > 1$ the value of the product is greater than 1. Thus, $L(1, \chi) \neq 0$, as asserted. $\square$

The next step is to deal with real-valued characters.

The next step is to deal with real-valued characters. It is not hard to see that these coincide with characters of order 2.

The next step is to deal with real-valued characters. It is not hard to see that these coincide with characters of order 2. The proof for such characters will be a modification of a proof of the classical case due to de la Vallée Poussin.

The next step is to deal with real-valued characters. It is not hard to see that these coincide with characters of order 2. The proof for such characters will be a modification of a proof of the classical case due to de la Vallée Poussin. Assume now that χ has order 2 and consider the function

$$G(s) = \frac{L(s, \chi_0)L(s, \chi)}{L(2s, \chi_0)}.$$

The next step is to deal with real-valued characters. It is not hard to see that these coincide with characters of order 2. The proof for such characters will be a modification of a proof of the classical case due to de la Vallée Poussin. Assume now that χ has order 2 and consider the function

$$G(s) = \frac{L(s,\chi_0)L(s,\chi)}{L(2s,\chi_0)}.$$

This can be written as a product over all monic irreducibles not dividing m.

The next step is to deal with real-valued characters. It is not hard to see that these coincide with characters of order 2. The proof for such characters will be a modification of a proof of the classical case due to de la Vallée Poussin. Assume now that χ has order 2 and consider the function

$$G(s) = \frac{L(s, \chi_0)L(s, \chi)}{L(2s, \chi_0)}.$$

This can be written as a product over all monic irreducibles not dividing m. Let P be such a prime.

The next step is to deal with real-valued characters. It is not hard to see that these coincide with characters of order 2. The proof for such characters will be a modification of a proof of the classical case due to de la Vallée Poussin. Assume now that χ has order 2 and consider the function

$$G(s) = \frac{L(s, \chi_0)L(s, \chi)}{L(2s, \chi_0)}.$$

This can be written as a product over all monic irreducibles not dividing m. Let P be such a prime. Then $\chi(P) = \pm 1$.

The next step is to deal with real-valued characters. It is not hard to see that these coincide with characters of order 2. The proof for such characters will be a modification of a proof of the classical case due to de la Vallée Poussin. Assume now that χ has order 2 and consider the function

$$G(s) = \frac{L(s,\chi_0)L(s,\chi)}{L(2s,\chi_0)}.$$

This can be written as a product over all monic irreducibles not dividing m. Let P be such a prime. Then $\chi(P) = \pm 1$. The factor of the above series corresponding to P is

$$\frac{(1-|P|^{-s})^{-1}(1-\chi(P)|P|^{-s})^{-1}}{(1-|P|^{-2s})^{-1}}.$$

The next step is to deal with real-valued characters. It is not hard to see that these coincide with characters of order 2. The proof for such characters will be a modification of a proof of the classical case due to de la Vallée Poussin. Assume now that χ has order 2 and consider the function

$$G(s) = \frac{L(s, \chi_0)L(s, \chi)}{L(2s, \chi_0)}.$$

This can be written as a product over all monic irreducibles not dividing m. Let P be such a prime. Then $\chi(P) = \pm 1$. The factor of the above series corresponding to P is

$$\frac{(1 - |P|^{-s})^{-1}(1 - \chi(P)|P|^{-s})^{-1}}{(1 - |P|^{-2s})^{-1}}.$$

If $\chi(P) = -1$ this whole factor reduces to 1.

The next step is to deal with real-valued characters. It is not hard to see that these coincide with characters of order 2. The proof for such characters will be a modification of a proof of the classical case due to de la Vallée Poussin. Assume now that χ has order 2 and consider the function

$$G(s) = \frac{L(s,\chi_0)L(s,\chi)}{L(2s,\chi_0)}.$$

This can be written as a product over all monic irreducibles not dividing m. Let P be such a prime. Then $\chi(P) = \pm 1$. The factor of the above series corresponding to P is

$$\frac{(1-|P|^{-s})^{-1}(1-\chi(P)|P|^{-s})^{-1}}{(1-|P|^{-2s})^{-1}}.$$

If $\chi(P) = -1$ this whole factor reduces to 1. If $\chi(P) = 1$ it simplifies to

$$\frac{(1+|P|^{-s})}{(1-|P|^{-s})} = 1 + 2\sum_{k=1}^{\infty} |P|^{-ks}.$$

The next step is to deal with real-valued characters. It is not hard to see that these coincide with characters of order 2. The proof for such characters will be a modification of a proof of the classical case due to de la Vallée Poussin. Assume now that χ has order 2 and consider the function

$$G(s) = \frac{L(s, \chi_0) L(s, \chi)}{L(2s, \chi_0)}.$$

This can be written as a product over all monic irreducibles not dividing m. Let P be such a prime. Then $\chi(P) = \pm 1$. The factor of the above series corresponding to P is

$$\frac{(1 - |P|^{-s})^{-1}(1 - \chi(P)|P|^{-s})^{-1}}{(1 - |P|^{-2s})^{-1}}.$$

If $\chi(P) = -1$ this whole factor reduces to 1. If $\chi(P) = 1$ it simplifies to

$$\frac{(1 + |P|^{-s})}{(1 - |P|^{-s})} = 1 + 2 \sum_{k=1}^{\infty} |P|^{-ks}.$$

It follows from these remarks that $G(s)$ is a Dirichlet series with non-negative coefficients.

The next step is to deal with real-valued characters. It is not hard to see that these coincide with characters of order 2. The proof for such characters will be a modification of a proof of the classical case due to de la Vallée Poussin. Assume now that χ has order 2 and consider the function

$$G(s) = \frac{L(s,\chi_0)L(s,\chi)}{L(2s,\chi_0)}.$$

This can be written as a product over all monic irreducibles not dividing m. Let P be such a prime. Then $\chi(P) = \pm 1$. The factor of the above series corresponding to P is

$$\frac{(1-|P|^{-s})^{-1}(1-\chi(P)|P|^{-s})^{-1}}{(1-|P|^{-2s})^{-1}}.$$

If $\chi(P) = -1$ this whole factor reduces to 1. If $\chi(P) = 1$ it simplifies to

$$\frac{(1+|P|^{-s})}{(1-|P|^{-s})} = 1 + 2\sum_{k=1}^{\infty} |P|^{-ks}.$$

It follows from these remarks that $G(s)$ is a Dirichlet series with non-negative coefficients. This will shortly play a crucial role.

First, we look more carefully at $L(s, \chi_0)/L(2s, \chi_0)$.

First, we look more carefully at $L(s,\chi_0)/L(2s,\chi_0)$. As we have already seen,

$$L(s,\chi_0) = \prod_{P|m}(1-|P|^{-s})\zeta_A(s) = \prod_{P|m}(1-|P|^{-s})\frac{1}{1-q^{1-s}}.$$

First, we look more carefully at $L(s, \chi_0)/L(2s, \chi_0)$. As we have already seen,

$$L(s, \chi_0) = \prod_{P|m}(1 - |P|^{-s})\zeta_A(s) = \prod_{P|m}(1 - |P|^{-s})\frac{1}{1 - q^{1-s}}.$$

A short calculation shows

$$\frac{L(s, \chi_0)}{L(2s, \chi_0)} = \prod_{P|m}(1 + |P|^{-s})^{-1}\frac{1 - q^{1-2s}}{1 - q^{1-s}}.$$

First, we look more carefully at $L(s, \chi_0)/L(2s, \chi_0)$. As we have already seen,

$$L(s, \chi_0) = \prod_{P|m} (1 - |P|^{-s}) \zeta_A(s) = \prod_{P|m} (1 - |P|^{-s}) \frac{1}{1 - q^{1-s}}.$$

A short calculation shows

$$\frac{L(s, \chi_0)}{L(2s, \chi_0)} = \prod_{P|m} (1 + |P|^{-s})^{-1} \frac{1 - q^{1-2s}}{1 - q^{1-s}}.$$

From this identity and what we have already proven about $G(s)$ we deduce that

$$\frac{(1 - q^{1-2s}) L(s, \chi)}{(1 - q^{1-s})} = \sum_n \frac{a(n)}{|n|^s},$$

a Dirichlet series with non-negative coefficients.

First, we look more carefully at $L(s, \chi_0)/L(2s, \chi_0)$. As we have already seen,

$$L(s, \chi_0) = \prod_{P|m} (1 - |P|^{-s}) \zeta_A(s) = \prod_{P|m} (1 - |P|^{-s}) \frac{1}{1 - q^{1-s}}.$$

A short calculation shows

$$\frac{L(s, \chi_0)}{L(2s, \chi_0)} = \prod_{P|m} (1 + |P|^{-s})^{-1} \frac{1 - q^{1-2s}}{1 - q^{1-s}}.$$

From this identity and what we have already proven about $G(s)$ we deduce that

$$\frac{(1 - q^{1-2s}) L(s, \chi)}{(1 - q^{1-s})} = \sum_n \frac{a(n)}{|n|^s},$$

a Dirichlet series with non-negative coefficients.

It is now convenient to switch to a new variable, $u = q^{-s}$.

It is now convenient to switch to a new variable, $u = q^{-s}$. The previous equation becomes

$$\frac{(1 - qu^2)L^*(u, \chi)}{1 - qu} = \sum_d A(d)u^d,$$

where $L^*(u, \chi)$ is a polynomial in u by Proposition 4.3, and

$$A(d) = \sum_{n,\ \deg(n)=d} a(n)$$

is non-negative for all $d \geq 0$ and $A(0) = 1$.

It is now convenient to switch to a new variable, $u = q^{-s}$. The previous equation becomes

$$\frac{(1 - qu^2)L^*(u, \chi)}{1 - qu} = \sum_d A(d)u^d,$$

where $L^*(u, \chi)$ is a polynomial in u by Proposition 4.3, and

$$A(d) = \sum_{n,\ \deg(n)=d} a(n)$$

is non-negative for all $d \geq 0$ and $A(0) = 1$. The Dirichlet series converges for $\Re(s) > 1$ which implies the power series in u converges for $|u| < q^{-1}$.

It is now convenient to switch to a new variable, $u = q^{-s}$. The previous equation becomes

$$\frac{(1-qu^2)L^*(u,\chi)}{1-qu} = \sum_d A(d)u^d,$$

where $L^*(u,\chi)$ is a polynomial in u by Proposition 4.3, and

$$A(d) = \sum_{n,\ \deg(n)=d} a(n)$$

is non-negative for all $d \geq 0$ and $A(0) = 1$. The Dirichlet series converges for $\Re(s) > 1$ which implies the power series in u converges for $|u| < q^{-1}$. Finally, notice that $s = 1$ corresponds to q^{-1} so what we are trying to prove is that $L^*(q^{-1},\chi) \neq 0$.

It is now convenient to switch to a new variable, $u = q^{-s}$. The previous equation becomes

$$\frac{(1-qu^2)L^*(u,\chi)}{1-qu} = \sum_d A(d)u^d,$$

where $L^*(u,\chi)$ is a polynomial in u by Proposition 4.3, and

$$A(d) = \sum_{n,\ \deg(n)=d} a(n)$$

is non-negative for all $d \geq 0$ and $A(0) = 1$. The Dirichlet series converges for $\Re(s) > 1$ which implies the power series in u converges for $|u| < q^{-1}$. Finally, notice that $s = 1$ corresponds to q^{-1} so what we are trying to prove is that $L^*(q^{-1},\chi) \neq 0$. We now have developed everything we need to give a quick proof of this.

We argue by contradiction.

We argue by contradiction. Suppose $L^*(q^{-1}, \chi) = 0$.

We argue by contradiction. Suppose $L^*(q^{-1}, \chi) = 0$. Then $(1 - qu)$ divides $L^*(u, \chi)$ and the left-hand side of the above equation is a polynomial in u.

We argue by contradiction. Suppose $L^*(q^{-1}, \chi) = 0$. Then $(1 - qu)$ divides $L^*(u, \chi)$ and the left-hand side of the above equation is a polynomial in u. It follows that the right-hand side is a polynomial in u with non-negative coefficients and constant term 1.

We argue by contradiction. Suppose $L^*(q^{-1}, \chi) = 0$. Then $(1 - qu)$ divides $L^*(u, \chi)$ and the left-hand side of the above equation is a polynomial in u. It follows that the right-hand side is a polynomial in u with non-negative coefficients and constant term 1. It therefore cannot have a positive root.

We argue by contradiction. Suppose $L^*(q^{-1}, \chi) = 0$. Then $(1 - qu)$ divides $L^*(u, \chi)$ and the left-hand side of the above equation is a polynomial in u. It follows that the right-hand side is a polynomial in u with non-negative coefficients and constant term 1. It therefore cannot have a positive root. However, the left-hand side vanishes when $u = 1/\sqrt{q}$.

We argue by contradiction. Suppose $L^*(q^{-1},\chi) = 0$. Then $(1 - qu)$ divides $L^*(u,\chi)$ and the left-hand side of the above equation is a polynomial in u. It follows that the right-hand side is a polynomial in u with non-negative coefficients and constant term 1. It therefore cannot have a positive root. However, the left-hand side vanishes when $u = 1/\sqrt{q}$. This is a contradiction, so $L^*(q^{-1},\chi) \neq 0$ and thus, $L(1,\chi) \neq 0$.

We argue by contradiction. Suppose $L^*(q^{-1}, \chi) = 0$. Then $(1 - qu)$ divides $L^*(u, \chi)$ and the left-hand side of the above equation is a polynomial in u. It follows that the right-hand side is a polynomial in u with non-negative coefficients and constant term 1. It therefore cannot have a positive root. However, the left-hand side vanishes when $u = 1/\sqrt{q}$. This is a contradiction, so $L^*(q^{-1}, \chi) \neq 0$ and thus, $L(1, \chi) \neq 0$. We have proven the following key result.

We argue by contradiction. Suppose $L^*(q^{-1}, \chi) = 0$. Then $(1 - qu)$ divides $L^*(u, \chi)$ and the left-hand side of the above equation is a polynomial in u. It follows that the right-hand side is a polynomial in u with non-negative coefficients and constant term 1. It therefore cannot have a positive root. However, the left-hand side vanishes when $u = 1/\sqrt{q}$. This is a contradiction, so $L^*(q^{-1}, \chi) \neq 0$ and thus, $L(1, \chi) \neq 0$. We have proven the following key result.

Proposition (4.6)

Let χ be a non-trivial Dirichlet character modulo m.

We argue by contradiction. Suppose $L^*(q^{-1}, \chi) = 0$. Then $(1 - qu)$ divides $L^*(u, \chi)$ and the left-hand side of the above equation is a polynomial in u. It follows that the right-hand side is a polynomial in u with non-negative coefficients and constant term 1. It therefore cannot have a positive root. However, the left-hand side vanishes when $u = 1/\sqrt{q}$. This is a contradiction, so $L^*(q^{-1}, \chi) \neq 0$ and thus, $L(1, \chi) \neq 0$. We have proven the following key result.

Proposition (4.6)

Let χ be a non-trivial Dirichlet character modulo m. Then, $L(1, \chi) \neq 0$.

We argue by contradiction. Suppose $L^*(q^{-1},\chi)=0$. Then $(1-qu)$ divides $L^*(u,\chi)$ and the left-hand side of the above equation is a polynomial in u. It follows that the right-hand side is a polynomial in u with non-negative coefficients and constant term 1. It therefore cannot have a positive root. However, the left-hand side vanishes when $u=1/\sqrt{q}$. This is a contradiction, so $L^*(q^{-1},\chi)\neq 0$ and thus, $L(1,\chi)\neq 0$. We have proven the following key result.

Proposition (4.6)

Let χ be a non-trivial Dirichlet character modulo m. Then, $L(1,\chi)\neq 0$.

From Proposition 4.6 and previous remarks we see that as $s\to 1$ with s real and greater than 1 we have

$$\lim_{s\to 1}\log L(s,\chi_0)=\infty \qquad \lim_{s\to 1}\log L(s,\chi)$$

exists for $\chi\neq\chi_0$.

We argue by contradiction. Suppose $L^*(q^{-1}, \chi) = 0$. Then $(1 - qu)$ divides $L^*(u, \chi)$ and the left-hand side of the above equation is a polynomial in u. It follows that the right-hand side is a polynomial in u with non-negative coefficients and constant term 1. It therefore cannot have a positive root. However, the left-hand side vanishes when $u = 1/\sqrt{q}$. This is a contradiction, so $L^*(q^{-1}, \chi) \neq 0$ and thus, $L(1, \chi) \neq 0$. We have proven the following key result.

Proposition (4.6)

Let χ be a non-trivial Dirichlet character modulo m. Then, $L(1, \chi) \neq 0$.

From Proposition 4.6 and previous remarks we see that as $s \to 1$ with s real and greater than 1 we have

$$\lim_{s \to 1} \log L(s, \chi_0) = \infty \qquad \lim_{s \to 1} \log L(s, \chi)$$

exists for $\chi \neq \chi_0$. Here, and in what follows we take for $\log(z)$ the principal branch of the logarithm.

Theorem (4.7)

Let $a, m \in A$ be two relatively prime polynomials with m of positive degree.

Theorem (4.7)

Let $a, m \in A$ be two relatively prime polynomials with m of positive degree. Consider the set of primes, $\mathcal{S} = \{P \in A | P \equiv a \pmod{m}\}$.

Theorem (4.7)

Let $a, m \in A$ be two relatively prime polynomials with m of positive degree. Consider the set of primes, $\mathcal{S} = \{P \in A | P \equiv a \pmod{m}\}$. Then, $\delta(\mathcal{S}) = 1/\Phi(m)$.

Theorem (4.7)

Let $a, m \in A$ *be two relatively prime polynomials with* m *of positive degree. Consider the set of primes,* $\mathcal{S} = \{P \in A | P \equiv a \pmod{m}\}$*. Then,* $\delta(\mathcal{S}) = 1/\Phi(m)$*. In particular,* $\mathcal{S}$ *is an infinite set.*

Proof.

Using the product formula for $L(s, \chi)$ and the same technique used in the proof of Proposition 4.1, one finds

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

where the function $R(s, \chi)$ is bounded as s tends to 1 from above.

Proof.

Using the product formula for $L(s, \chi)$ and the same technique used in the proof of Proposition 4.1, one finds

$$\log L(s, \chi) = \sum_{P} \frac{\chi(P)}{|P|^{s}} + R(s, \chi),$$

where the function $R(s, \chi)$ is bounded as s tends to 1 from above. Multiply both sides by $\overline{\chi}(a)$ and sum over all χ.

Proof.

Using the product formula for $L(s,\chi)$ and the same technique used in the proof of Proposition 4.1, one finds

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

where the function $R(s,\chi)$ is bounded as s tends to 1 from above. Multiply both sides by $\overline{\chi}(a)$ and sum over all χ. Using the orthogonality relation for Dirichlet characters, Proposition 4.2, part (2), we obtain

$$\sum_\chi \overline{\chi}(a) \log L(s,\chi) = \Phi(m) \sum_{P \equiv a (\mod m)} \frac{1}{|P|^s} + R(s),$$

where $R(s)$ is a function which remains bounded as $s \to 1$.

Proof.

Using the product formula for $L(s,\chi)$ and the same technique used in the proof of Proposition 4.1, one finds

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

where the function $R(s,\chi)$ is bounded as s tends to 1 from above. Multiply both sides by $\overline{\chi}(a)$ and sum over all χ. Using the orthogonality relation for Dirichlet characters, Proposition 4.2, part (2), we obtain

$$\sum_\chi \overline{\chi}(a) \log L(s,\chi) = \Phi(m) \sum_{P \equiv a \pmod{m}} \frac{1}{|P|^s} + R(s),$$

where $R(s)$ is a function which remains bounded as $s \to 1$.
Divide each summand on the left-hand side of the above equation by $\sum_P |P|^{-s}$ and let s tend to 1 from above.

Proof.

Using the product formula for $L(s,\chi)$ and the same technique used in the proof of Proposition 4.1, one finds

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

where the function $R(s,\chi)$ is bounded as s tends to 1 from above. Multiply both sides by $\overline{\chi}(a)$ and sum over all χ. Using the orthogonality relation for Dirichlet characters, Proposition 4.2, part (2), we obtain

$$\sum_\chi \overline{\chi}(a) \log L(s,\chi) = \Phi(m) \sum_{P \equiv a \pmod{m}} \frac{1}{|P|^s} + R(s),$$

where $R(s)$ is a function which remains bounded as $s \to 1$.
Divide each summand on the left-hand side of the above equation by $\sum_P |P|^{-s}$ and let s tend to 1 from above. By Proposition 4.1 and the remarks preceding the theorem, the summand corresponding to the trivial character tends to 1, while each summand corresponding to a non-trivial character tends to zero.

Proof.

Using the product formula for $L(s,\chi)$ and the same technique used in the proof of Proposition 4.1, one finds

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

where the function $R(s,\chi)$ is bounded as s tends to 1 from above. Multiply both sides by $\overline{\chi}(a)$ and sum over all χ. Using the orthogonality relation for Dirichlet characters, Proposition 4.2, part (2), we obtain

$$\sum_\chi \overline{\chi}(a) \log L(s,\chi) = \Phi(m) \sum_{P \equiv a (\mod m)} \frac{1}{|P|^s} + R(s),$$

where $R(s)$ is a function which remains bounded as $s \to 1$.
Divide each summand on the left-hand side of the above equation by $\sum_P |P|^{-s}$ and let s tend to 1 from above. By Proposition 4.1 and the remarks preceding the theorem, the summand corresponding to the trivial character tends to 1, while each summand corresponding to a non-trivial character tends to zero. If we divide the right-hand side by $\sum_P |P|^{-s}$ and let s tend to 1 from above, we get $\Phi(m)\delta(\mathcal{S})$.

Proof.

Using the product formula for $L(s,\chi)$ and the same technique used in the proof of Proposition 4.1, one finds

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

where the function $R(s,\chi)$ is bounded as s tends to 1 from above. Multiply both sides by $\overline{\chi}(a)$ and sum over all χ. Using the orthogonality relation for Dirichlet characters, Proposition 4.2, part (2), we obtain

$$\sum_\chi \overline{\chi}(a) \log L(s,\chi) = \Phi(m) \sum_{P \equiv a \pmod{m}} \frac{1}{|P|^s} + R(s),$$

where $R(s)$ is a function which remains bounded as $s \to 1$.
Divide each summand on the left-hand side of the above equation by $\sum_P |P|^{-s}$ and let s tend to 1 from above. By Proposition 4.1 and the remarks preceding the theorem, the summand corresponding to the trivial character tends to 1, while each summand corresponding to a non-trivial character tends to zero. If we divide the right-hand side by $\sum_P |P|^{-s}$ and let s tend to 1 from above, we get $\Phi(m)\delta(\mathcal{S})$. The result follows. $\square$

The previous theorem is the original form of Dirichlet's theorem.

The previous theorem is the original form of Dirichlet's theorem. It is possible, with more work, to prove a much stronger form of the theorem.

The previous theorem is the original form of Dirichlet's theorem. It is possible, with more work, to prove a much stronger form of the theorem. Suppose $a, m \in A$ are relatively prime and that m has positive degree.

The previous theorem is the original form of Dirichlet's theorem. It is possible, with more work, to prove a much stronger form of the theorem. Suppose $a, m \in A$ are relatively prime and that m has positive degree. Consider the set of primes

$$S_N(a,m) = \{P \in A | P \equiv a (\text{mod } m), \deg(P) = N\}.$$

The previous theorem is the original form of Dirichlet's theorem. It is possible, with more work, to prove a much stronger form of the theorem. Suppose $a, m \in A$ are relatively prime and that m has positive degree. Consider the set of primes

$$S_N(a, m) = \{P \in A | P \equiv a (\text{mod } m), \deg(P) = N\}.$$

We claim that for all large integers N this set is not empty.

The previous theorem is the original form of Dirichlet's theorem. It is possible, with more work, to prove a much stronger form of the theorem. Suppose $a, m \in A$ are relatively prime and that m has positive degree. Consider the set of primes

$$S_N(a, m) = \{P \in A | P \equiv a (\mathrm{mod}\ m), \deg(P) = N\}.$$

We claim that for all large integers N this set is not empty. The following theorem proves this and more.

Theorem (4.8)

$$\# S_N(a, m) = \frac{1}{\Phi(m)} \frac{q^N}{N} + O\left(\frac{q^{N/2}}{N}\right).$$

The previous theorem is the original form of Dirichlet's theorem. It is possible, with more work, to prove a much stronger form of the theorem. Suppose $a, m \in A$ are relatively prime and that m has positive degree. Consider the set of primes

$$S_N(a,m) = \{P \in A | P \equiv a (\text{mod } m), \deg(P) = N\} .$$

We claim that for all large integers N this set is not empty. The following theorem proves this and more.

Theorem (4.8)

$$\# S_N(a,m) = \frac{1}{\Phi(m)} \frac{q^N}{N} + O\left(\frac{q^{N/2}}{N} \right) .$$

Let S_N be the set of primes of degree N.

The previous theorem is the original form of Dirichlet's theorem. It is possible, with more work, to prove a much stronger form of the theorem. Suppose $a, m \in A$ are relatively prime and that m has positive degree. Consider the set of primes

$$S_N(a,m) = \{P \in A | P \equiv a (\bmod\ m), \deg(P) = N\}.$$

We claim that for all large integers N this set is not empty. The following theorem proves this and more.

Theorem (4.8)

$$\#S_N(a,m) = \frac{1}{\Phi(m)} \frac{q^N}{N} + O\left(\frac{q^{N/2}}{N}\right).$$

Let S_N be the set of primes of degree N. We have seen on the first lecture that

$$\#S_N = \frac{q^N}{N} + O\left(\frac{q^{N/2}}{N}\right).$$

The previous theorem is the original form of Dirichlet's theorem. It is possible, with more work, to prove a much stronger form of the theorem. Suppose $a, m \in A$ are relatively prime and that m has positive degree. Consider the set of primes

$$S_N(a, m) = \{P \in A | P \equiv a (\mathrm{mod}\ m), \deg(P) = N\} .$$

We claim that for all large integers N this set is not empty. The following theorem proves this and more.

Theorem (4.8)

$$\# S_N(a, m) = \frac{1}{\Phi(m)} \frac{q^N}{N} + O\left(\frac{q^{N/2}}{N}\right) .$$

Let S_N be the set of primes of degree N. We have seen on the first lecture that

$$\# S_N = \frac{q^N}{N} + O\left(\frac{q^{N/2}}{N}\right) .$$

Putting this together with the statement of the theorem we find

$$\lim_{N \to \infty} \frac{\# S_N(a, m)}{\# S_N} = \frac{1}{\Phi(m)} .$$

The previous theorem is the original form of Dirichlet's theorem. It is possible, with more work, to prove a much stronger form of the theorem. Suppose $a, m \in A$ are relatively prime and that m has positive degree. Consider the set of primes

$$S_N(a, m) = \{P \in A | P \equiv a (\text{mod } m), \deg(P) = N\}.$$

We claim that for all large integers N this set is not empty. The following theorem proves this and more.

Theorem (4.8)

$$\#S_N(a, m) = \frac{1}{\Phi(m)} \frac{q^N}{N} + O\left(\frac{q^{N/2}}{N}\right).$$

Let S_N be the set of primes of degree N. We have seen on the first lecture that

$$\#S_N = \frac{q^N}{N} + O\left(\frac{q^{N/2}}{N}\right).$$

Putting this together with the statement of the theorem we find

$$\lim_{N \to \infty} \frac{\#S_N(a, m)}{\#S_N} = \frac{1}{\Phi(m)}.$$

This is a natural density analogue to the Dirichlet density form of the main theorem.

Proof of Theorem 4.8

The idea of the proof is to realize that the L-function $L(s, \chi)$ can be expressed as a product in two ways.

Proof of Theorem 4.8

The idea of the proof is to realize that the L-function $L(s, \chi)$ can be expressed as a product in two ways. One way, which we have already considered, is as an Euler product.

Proof of Theorem 4.8

The idea of the proof is to realize that the L-function $L(s, \chi)$ can be expressed as a product in two ways. One way, which we have already considered, is as an Euler product. The other is as a product over its complex zeros.

Proof of Theorem 4.8

The idea of the proof is to realize that the L-function $L(s, \chi)$ can be expressed as a product in two ways. One way, which we have already considered, is as an Euler product. The other is as a product over its complex zeros. This is made easier by rewriting, as we have done before, everything in terms of the variable $u = q^{-s}$.

Proof of Theorem 4.8

The idea of the proof is to realize that the L-function $L(s, \chi)$ can be expressed as a product in two ways. One way, which we have already considered, is as an Euler product. The other is as a product over its complex zeros. This is made easier by rewriting, as we have done before, everything in terms of the variable $u = q^{-s}$. If χ is not trivial, then by Proposition 4.3, $L(s, \chi)$ is a polynomial in q^{-s} of degree at most $M - 1$ where $M = \deg(m)$.

Proof of Theorem 4.8

The idea of the proof is to realize that the L-function $L(s, \chi)$ can be expressed as a product in two ways. One way, which we have already considered, is as an Euler product. The other is as a product over its complex zeros. This is made easier by rewriting, as we have done before, everything in terms of the variable $u = q^{-s}$. If χ is not trivial, then by Proposition 4.3, $L(s, \chi)$ is a polynomial in q^{-s} of degree at most $M - 1$ where $M = \deg(m)$. We have

$$L^*(u, \chi) = \sum_{k=0}^{M-1} a_k(\chi) u^k = \prod_{i=1}^{M-1} (1 - \alpha_i(\chi) u). \tag{3.1}$$

Proof of Theorem 4.8

The idea of the proof is to realize that the L-function $L(s, \chi)$ can be expressed as a product in two ways. One way, which we have already considered, is as an Euler product. The other is as a product over its complex zeros. This is made easier by rewriting, as we have done before, everything in terms of the variable $u = q^{-s}$. If χ is not trivial, then by Proposition 4.3, $L(s, \chi)$ is a polynomial in q^{-s} of degree at most $M - 1$ where $M = \deg(m)$. We have

$$L^*(u, \chi) = \sum_{k=0}^{M-1} a_k(\chi) u^k = \prod_{i=1}^{M-1} (1 - \alpha_i(\chi) u). \tag{3.1}$$

The second expression for $L^*(u, \chi)$ comes from rewriting the Euler product for $L(s, \chi)$ in terms of u.

Proof of Theorem 4.8

The idea of the proof is to realize that the L-function $L(s,\chi)$ can be expressed as a product in two ways. One way, which we have already considered, is as an Euler product. The other is as a product over its complex zeros. This is made easier by rewriting, as we have done before, everything in terms of the variable $u = q^{-s}$. If χ is not trivial, then by Proposition 4.3, $L(s,\chi)$ is a polynomial in q^{-s} of degree at most $M-1$ where $M = \deg(m)$. We have

$$L^*(u,\chi) = \sum_{k=0}^{M-1} a_k(\chi)u^k = \prod_{i=1}^{M-1}(1-\alpha_i(\chi)u). \tag{3.1}$$

The second expression for $L^*(u,\chi)$ comes from rewriting the Euler product for $L(s,\chi)$ in terms of u. We first regroup the terms in the Euler product.

$$L(s,\chi) = \prod_{P\nmid m}(1-\chi(P)|P|^{-s})^{-1} = \prod_{d=1}^{\infty}\prod_{\substack{P\nmid m\\ \deg(P)=d}}(1-\chi(P)q^{-ds})^{-1}.$$

Proof of Theorem 4.8

The idea of the proof is to realize that the L-function $L(s,\chi)$ can be expressed as a product in two ways. One way, which we have already considered, is as an Euler product. The other is as a product over its complex zeros. This is made easier by rewriting, as we have done before, everything in terms of the variable $u = q^{-s}$. If χ is not trivial, then by Proposition 4.3, $L(s,\chi)$ is a polynomial in q^{-s} of degree at most $M-1$ where $M = \deg(m)$. We have

$$L^*(u,\chi) = \sum_{k=0}^{M-1} a_k(\chi)u^k = \prod_{i=1}^{M-1}(1-\alpha_i(\chi)u). \tag{3.1}$$

The second expression for $L^*(u,\chi)$ comes from rewriting the Euler product for $L(s,\chi)$ in terms of u. We first regroup the terms in the Euler product.

$$L(s,\chi) = \prod_{P \nmid m}(1-\chi(P)|P|^{-s})^{-1} = \prod_{d=1}^{\infty} \prod_{\substack{P \nmid m \\ \deg(P)=d}} (1-\chi(P)q^{-ds})^{-1}.$$

Now, make the substitution $u = q^{-s}$.

Proof of Theorem 4.8

The idea of the proof is to realize that the L-function $L(s, \chi)$ can be expressed as a product in two ways. One way, which we have already considered, is as an Euler product. The other is as a product over its complex zeros. This is made easier by rewriting, as we have done before, everything in terms of the variable $u = q^{-s}$. If χ is not trivial, then by Proposition 4.3, $L(s, \chi)$ is a polynomial in q^{-s} of degree at most $M - 1$ where $M = \deg(m)$. We have

$$L^*(u, \chi) = \sum_{k=0}^{M-1} a_k(\chi) u^k = \prod_{i=1}^{M-1} (1 - \alpha_i(\chi) u). \tag{3.1}$$

The second expression for $L^*(u, \chi)$ comes from rewriting the Euler product for $L(s, \chi)$ in terms of u. We first regroup the terms in the Euler product.

$$L(s, \chi) = \prod_{P \nmid m} (1 - \chi(P)|P|^{-s})^{-1} = \prod_{d=1}^{\infty} \prod_{\substack{P \nmid m \\ \deg(P) = d}} (1 - \chi(P) q^{-ds})^{-1}.$$

Now, make the substitution $u = q^{-s}$. We obtain the expression

$$L^*(u, \chi) = \prod_{d=1}^{\infty} \prod_{\substack{P \nmid m \\ \deg(P) = d}} (1 - \chi(P) u^d)^{-1}.$$

Our intention is to take the logarithmic derivative of both expressions, write the results as power series in u and compare coefficients.

Our intention is to take the logarithmic derivative of both expressions, write the results as power series in u and compare coefficients. Afterwards we apply the orthogonality relations to isolate the primes congruent to a modulo m.

Our intention is to take the logarithmic derivative of both expressions, write the results as power series in u and compare coefficients. Afterwards we apply the orthogonality relations to isolate the primes congruent to a modulo m. However, in addition to the algebra involved, we will have to do a number of estimates.

Our intention is to take the logarithmic derivative of both expressions, write the results as power series in u and compare coefficients. Afterwards we apply the orthogonality relations to isolate the primes congruent to a modulo m. However, in addition to the algebra involved, we will have to do a number of estimates. One of these estimates will involve invoking a deep result of A. Weil. The others are more elementary.

Our intention is to take the logarithmic derivative of both expressions, write the results as power series in u and compare coefficients. Afterwards we apply the orthogonality relations to isolate the primes congruent to a modulo m.
However, in addition to the algebra involved, we will have to do a number of estimates. One of these estimates will involve invoking a deep result of A. Weil. The others are more elementary.
We begin by writing down an identity which will be used repeatedly. Namely,

$$u\frac{d}{du}(\log(1-\alpha u)^{-1}) = \sum_{k=1}^{\infty} \alpha^k u^k. \tag{3.2}$$

Our intention is to take the logarithmic derivative of both expressions, write the results as power series in u and compare coefficients. Afterwards we apply the orthogonality relations to isolate the primes congruent to a modulo m.
However, in addition to the algebra involved, we will have to do a number of estimates. One of these estimates will involve invoking a deep result of A. Weil. The others are more elementary.
We begin by writing down an identity which will be used repeatedly. Namely,

$$u\frac{d}{du}(\log(1-\alpha u)^{-1}) = \sum_{k=1}^{\infty} \alpha^k u^k. \tag{3.2}$$

Here α is a complex number.

Our intention is to take the logarithmic derivative of both expressions, write the results as power series in u and compare coefficients. Afterwards we apply the orthogonality relations to isolate the primes congruent to a modulo m. However, in addition to the algebra involved, we will have to do a number of estimates. One of these estimates will involve invoking a deep result of A. Weil. The others are more elementary.
We begin by writing down an identity which will be used repeatedly. Namely,

$$u\frac{d}{du}(\log(1-\alpha u)^{-1}) = \sum_{k=1}^{\infty} \alpha^k u^k. \tag{3.2}$$

Here α is a complex number. The sum converges for all u such that $|u| < |\alpha|^{-1}$.

Our intention is to take the logarithmic derivative of both expressions, write the results as power series in u and compare coefficients. Afterwards we apply the orthogonality relations to isolate the primes congruent to a modulo m.
However, in addition to the algebra involved, we will have to do a number of estimates. One of these estimates will involve invoking a deep result of A. Weil. The others are more elementary.
We begin by writing down an identity which will be used repeatedly. Namely,

$$u\frac{d}{du}(\log(1-\alpha u)^{-1}) = \sum_{k=1}^{\infty} \alpha^k u^k. \tag{3.2}$$

Here α is a complex number. The sum converges for all u such that $|u| < |\alpha|^{-1}$. The proof of this identity is a simple exercise using geometric series.
For each character χ modulo m define the numbers $c_N(\chi)$ by

$$u\frac{d}{du}\log(L^*(u,\chi)) = \sum_{N=1}^{\infty} c_N(\chi)u^N.$$

Our intention is to take the logarithmic derivative of both expressions, write the results as power series in u and compare coefficients. Afterwards we apply the orthogonality relations to isolate the primes congruent to a modulo m.
However, in addition to the algebra involved, we will have to do a number of estimates. One of these estimates will involve invoking a deep result of A. Weil. The others are more elementary.
We begin by writing down an identity which will be used repeatedly. Namely,

$$u\frac{d}{du}(\log(1-\alpha u)^{-1}) = \sum_{k=1}^{\infty} \alpha^k u^k. \tag{3.2}$$

Here α is a complex number. The sum converges for all u such that $|u| < |\alpha|^{-1}$. The proof of this identity is a simple exercise using geometric series.
For each character χ modulo m define the numbers $c_N(\chi)$ by

$$u\frac{d}{du}\log(L^*(u,\chi)) = \sum_{N=1}^{\infty} c_N(\chi)u^N.$$

We claim that

$$c_N(\chi_0) = q^N + O(1) \quad \text{and that} \quad c_N(\chi) = O(q^{N/2}) \quad \text{if } \chi \neq \chi_0. \tag{3.3}$$

The easy case is when $\chi = \chi_0$.

The easy case is when $\chi = \chi_0$. Recall that

$$L(s, \chi_0) = \prod_{P|m}(1 - |P|^{-s})\zeta_A(s).$$

The easy case is when $\chi = \chi_0$. Recall that

$$L(s, \chi_0) = \prod_{P|m} (1 - |P|^{-s}) \zeta_A(s).$$

Thus,

$$L^*(u, \chi_0) = \prod_{P|m} (1 - u^{\deg(P)}) \frac{1}{1 - qu}.$$

The easy case is when $\chi = \chi_0$. Recall that

$$L(s, \chi_0) = \prod_{P|m} (1 - |P|^{-s}) \zeta_A(s).$$

Thus,

$$L^*(u, \chi_0) = \prod_{P|m} (1 - u^{\deg(P)}) \frac{1}{1 - qu}.$$

It now follows immediately, using Equation (3.2) and the additivity of the logarithmic derivative, that $c_N(\chi_0) = q^N + O(1)$.

The easy case is when $\chi = \chi_0$. Recall that

$$L(s, \chi_0) = \prod_{P|m}(1 - |P|^{-s})\zeta_A(s).$$

Thus,

$$L^*(u, \chi_0) = \prod_{P|m}(1 - u^{\deg(P)})\frac{1}{1 - qu}.$$

It now follows immediately, using Equation (3.2) and the additivity of the logarithmic derivative, that $c_N(\chi_0) = q^N + O(1)$. For $\chi \neq \chi_0$, by combining Equation (3.1) with Equation (3.2) we find

$$c_N(\chi) = -\sum_{k=1}^{M-1} \alpha_k(\chi)^N.$$

The easy case is when $\chi = \chi_0$. Recall that

$$L(s, \chi_0) = \prod_{P|m} (1 - |P|^{-s}) \zeta_A(s).$$

Thus,

$$L^*(u, \chi_0) = \prod_{P|m} (1 - u^{\deg(P)}) \frac{1}{1 - qu}.$$

It now follows immediately, using Equation (3.2) and the additivity of the logarithmic derivative, that $c_N(\chi_0) = q^N + O(1)$. For $\chi \neq \chi_0$, by combining Equation (3.1) with Equation (3.2) we find

$$c_N(\chi) = -\sum_{k=1}^{M-1} \alpha_k(\chi)^N.$$

It follows from the analogue of the Riemann hypothesis for function fields over a finite field that each of the roots $\alpha_k(\chi)$ has absolute value either 1 or $\sqrt{q}$.

The easy case is when $\chi = \chi_0$. Recall that

$$L(s, \chi_0) = \prod_{P|m} (1 - |P|^{-s}) \zeta_A(s).$$

Thus,

$$L^*(u, \chi_0) = \prod_{P|m} (1 - u^{\deg(P)}) \frac{1}{1 - qu}.$$

It now follows immediately, using Equation (3.2) and the additivity of the logarithmic derivative, that $c_N(\chi_0) = q^N + O(1)$. For $\chi \neq \chi_0$, by combining Equation (3.1) with Equation (3.2) we find

$$c_N(\chi) = -\sum_{k=1}^{M-1} \alpha_k(\chi)^N.$$

It follows from the analogue of the Riemann hypothesis for function fields over a finite field that each of the roots $\alpha_k(\chi)$ has absolute value either 1 or $\sqrt{q}$. This is the deepest part of the proof and is due to A. Weil.

The easy case is when $\chi = \chi_0$. Recall that

$$L(s, \chi_0) = \prod_{P|m} (1 - |P|^{-s}) \zeta_A(s).$$

Thus,

$$L^*(u, \chi_0) = \prod_{P|m} (1 - u^{\deg(P)}) \frac{1}{1 - qu}.$$

It now follows immediately, using Equation (3.2) and the additivity of the logarithmic derivative, that $c_N(\chi_0) = q^N + O(1)$. For $\chi \neq \chi_0$, by combining Equation (3.1) with Equation (3.2) we find

$$c_N(\chi) = -\sum_{k=1}^{M-1} \alpha_k(\chi)^N.$$

It follows from the analogue of the Riemann hypothesis for function fields over a finite field that each of the roots $\alpha_k(\chi)$ has absolute value either 1 or $\sqrt{q}$. This is the deepest part of the proof and is due to A. Weil. We will discuss it in some detail in the next lectures.

The easy case is when $\chi = \chi_0$. Recall that

$$L(s, \chi_0) = \prod_{P|m} (1 - |P|^{-s}) \zeta_A(s).$$

Thus,

$$L^*(u, \chi_0) = \prod_{P|m} (1 - u^{\deg(P)}) \frac{1}{1 - qu}.$$

It now follows immediately, using Equation (3.2) and the additivity of the logarithmic derivative, that $c_N(\chi_0) = q^N + O(1)$. For $\chi \neq \chi_0$, by combining Equation (3.1) with Equation (3.2) we find

$$c_N(\chi) = -\sum_{k=1}^{M-1} \alpha_k(\chi)^N.$$

It follows from the analogue of the Riemann hypothesis for function fields over a finite field that each of the roots $\alpha_k(\chi)$ has absolute value either 1 or $\sqrt{q}$. This is the deepest part of the proof and is due to A. Weil. We will discuss it in some detail in the next lectures. Assuming it for now, we see immediately from the last equation that $c_N(\chi) = O(q^{N/2})$.

Thus, we have verified both assertions of Equation (3.3) from the previous slide.

Thus, we have verified both assertions of Equation (3.3) from the previous slide. It should be remarked that one can prove much more easily, a weaker result than the Riemann hypothesis which has the effect of replacing the error term in the theorem with $O(q^{\theta N})$ where θ is some real number less than 1.

Thus, we have verified both assertions of Equation (3.3) from the previous slide. It should be remarked that one can prove much more easily, a weaker result than the Riemann hypothesis which has the effect of replacing the error term in the theorem with $O(q^{\theta N})$ where θ is some real number less than 1. This still gives the corollary that the set $S_N(a, m)$ is non-empty for all large N.

Thus, we have verified both assertions of Equation (3.3) from the previous slide. It should be remarked that one can prove much more easily, a weaker result than the Riemann hypothesis which has the effect of replacing the error term in the theorem with $O(q^{\theta N})$ where θ is some real number less than 1. This still gives the corollary that the set $S_N(a, m)$ is non-empty for all large N. We will indicate how to prove this in the next lecture.

We now continue with the proof of the theorem.

We now continue with the proof of the theorem. Consider the Euler product expansion of $L^*(u, \chi)$ given previously.

We now continue with the proof of the theorem. Consider the Euler product expansion of $L^*(u, \chi)$ given previously. Take the logarithmic derivative of both sides and multiply both sides of the resulting equation by u.

We now continue with the proof of the theorem. Consider the Euler product expansion of $L^*(u, \chi)$ given previously. Take the logarithmic derivative of both sides and multiply both sides of the resulting equation by u. Again using Equation (3.2) we find

$$c_N(\chi) = \sum_{\substack{k,P \\ k\deg(P)=N}} \deg(P)\chi(P)^k.$$

We now continue with the proof of the theorem. Consider the Euler product expansion of $L^*(u, \chi)$ given previously. Take the logarithmic derivative of both sides and multiply both sides of the resulting equation by u. Again using Equation (3.2) we find

$$c_N(\chi) = \sum_{\substack{k,P \\ k\deg(P)=N}} \deg(P)\chi(P)^k.$$

In the sum on the right-hand side separate out the terms corresponding to $k = 1$.

We now continue with the proof of the theorem. Consider the Euler product expansion of $L^*(u,\chi)$ given previously. Take the logarithmic derivative of both sides and multiply both sides of the resulting equation by u. Again using Equation (3.2) we find

$$c_N(\chi) = \sum_{\substack{k,P \\ k\deg(P)=N}} \deg(P)\chi(P)^k.$$

In the sum on the right-hand side separate out the terms corresponding to $k=1$. The result is $N\sum_{\deg(P)=N}\chi(P)$.

We now continue with the proof of the theorem. Consider the Euler product expansion of $L^*(u, \chi)$ given previously. Take the logarithmic derivative of both sides and multiply both sides of the resulting equation by u. Again using Equation (3.2) we find

$$c_N(\chi) = \sum_{\substack{k,P \\ k\deg(P)=N}} \deg(P)\chi(P)^k.$$

In the sum on the right-hand side separate out the terms corresponding to $k = 1$. The result is $N \sum_{\deg(P)=N} \chi(P)$. The rest of the terms can be written as follows:

$$\sum_{\substack{d|N \\ d \le N/2}} d \sum_{\deg(P)=d} \chi(P)^{N/d}.$$

We now continue with the proof of the theorem. Consider the Euler product expansion of $L^*(u,\chi)$ given previously. Take the logarithmic derivative of both sides and multiply both sides of the resulting equation by u. Again using Equation (3.2) we find

$$c_N(\chi) = \sum_{\substack{k,P \\ k\deg(P)=N}} \deg(P)\chi(P)^k.$$

In the sum on the right-hand side separate out the terms corresponding to $k=1$. The result is $N\sum_{\deg(P)=N}\chi(P)$. The rest of the terms can be written as follows:

$$\sum_{\substack{d|N \\ d\le N/2}} d \sum_{\deg(P)=d} \chi(P)^{N/d}.$$

The inner sum in absolute value is less than or equal to $\#\{P\in A|\deg(P)=d\} = q^d/d + O(q^{d/2}/d)$ by the Prime Number Theorem for Polynomials.

We now continue with the proof of the theorem. Consider the Euler product expansion of $L^*(u,\chi)$ given previously. Take the logarithmic derivative of both sides and multiply both sides of the resulting equation by u. Again using Equation (3.2) we find

$$c_N(\chi) = \sum_{\substack{k,P \\ k\deg(P)=N}} \deg(P)\chi(P)^k.$$

In the sum on the right-hand side separate out the terms corresponding to $k=1$. The result is $N\sum_{\deg(P)=N}\chi(P)$. The rest of the terms can be written as follows:

$$\sum_{\substack{d|N \\ d\leq N/2}} d \sum_{\deg(P)=d} \chi(P)^{N/d}.$$

The inner sum in absolute value is less than or equal to $\#\{P\in A|\deg(P)=d\} = q^d/d + O(q^{d/2}/d)$ by the Prime Number Theorem for Polynomials. Thus the double sum is bounded by

$$1+q+q^2+\cdots+q^{[N/2]} + O(1+q+q^2+\cdots+q^{[N/4]}) = O(q^{N/2}).$$

We now continue with the proof of the theorem. Consider the Euler product expansion of $L^*(u,\chi)$ given previously. Take the logarithmic derivative of both sides and multiply both sides of the resulting equation by u. Again using Equation (3.2) we find

$$c_N(\chi) = \sum_{\substack{k,P \\ k\deg(P)=N}} \deg(P)\chi(P)^k.$$

In the sum on the right-hand side separate out the terms corresponding to $k=1$. The result is $N\sum_{\deg(P)=N}\chi(P)$. The rest of the terms can be written as follows:

$$\sum_{\substack{d|N \\ d\leq N/2}} d \sum_{\deg(P)=d} \chi(P)^{N/d}.$$

The inner sum in absolute value is less than or equal to $\#\{P\in A|\deg(P)=d\} = q^d/d + O(q^{d/2}/d)$ by the Prime Number Theorem for Polynomials. Thus the double sum is bounded by

$$1+q+q^2+\cdots+q^{[N/2]} + O(1+q+q^2+\cdots+q^{[N/4]}) = O(q^{N/2}).$$

We have proven

$$c_N(\chi) = N\sum_{\deg(P)=N} \chi(P) + O(q^{N/2}). \tag{3.4}$$

Finally we compute the expression $\sum_\chi \overline{\chi}(a) c_N(\chi)$ in two ways.

Finally we compute the expression $\sum_{\chi} \overline{\chi}(a) c_N(\chi)$ in two ways. First we use Equation (3.4) and then we use Equation (3.3).

Finally we compute the expression $\sum_\chi \overline{\chi}(a)c_N(\chi)$ in two ways. First we use Equation (3.4) and then we use Equation (3.3). From the orthogonality relations and Equation (3.4) we find

$$\frac{1}{\Phi(m)} \sum_\chi \overline{\chi}(a)c_N(\chi) = N\#S_N(a, m) + O(q^{N/2}).$$

Finally we compute the expression $\sum_\chi \overline{\chi}(a) c_N(\chi)$ in two ways. First we use Equation (3.4) and then we use Equation (3.3). From the orthogonality relations and Equation (3.4) we find

$$\frac{1}{\Phi(m)} \sum_\chi \overline{\chi}(a) c_N(\chi) = N \# S_N(a, m) + O(q^{N/2}).$$

Next, from Equation (3.3) we see

$$\sum_\chi \overline{\chi}(a) c_N(\chi) = q^N + O(q^{N/2}).$$

Finally we compute the expression $\sum_\chi \overline{\chi}(a)c_N(\chi)$ in two ways. First we use Equation (3.4) and then we use Equation (3.3). From the orthogonality relations and Equation (3.4) we find

$$\frac{1}{\Phi(m)} \sum_\chi \overline{\chi}(a)c_N(\chi) = N\#S_N(a,m) + O(q^{N/2}).$$

Next, from Equation (3.3) we see

$$\sum_\chi \overline{\chi}(a)c_N(\chi) = q^N + O(q^{N/2}).$$

So, we finally arrive at the main result:

$$\#S_N(a,m) = \frac{1}{\Phi(m)} \frac{q^N}{N} + O(q^{N/2}/N).$$

□