Introduction to Analytic Number Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

Subsection 1

Functions Periodic Modulo k

Functions Periodic Modulo k

- Let k be a positive integer.
- An arithmetical function f is said to be **periodic with period** k (or **periodic modulo** k) if

$$f(n+k) = f(n), \text{ for all integers } n.$$

- If k is a period so is mk, for any integer $m > 0$.
- The smallest positive period of f is called the **fundamental period**.

  Example: The Dirichlet characters mod k are periodic mod k.

  Consider the greatest common divisor (n, k), as a function of n.

  Periodicity enters through the relation

$$(n+k, k) = (n, k).$$

Finite Fourier Series

- Another example is the exponential function
$$f(n) = e^{2\pi imn/k},$$
where m and k are fixed integers.
- The number $e^{2\pi im/k}$ is a k-th root of unity.
- $f(n)$ is its n-th power.
- Any finite linear combination of such functions, say
$$\sum_m c(m) e^{2\pi imn/k}$$
is also periodic mod k, for every choice of coefficients $c(m)$.

The Geometric Sum

- We shall show that every arithmetical function which is periodic mod k can be expressed in the form $\sum_m c(m)e^{2\pi imn/k}$.
- Such sums are called **finite Fourier series**.

Theorem

For fixed $k \geq 1$, let

$$g(n) = \sum_{m=0}^{k-1} e^{2nimn/k}.$$

Then

$$g(n) = \begin{cases} 0, & \text{if } k \nmid n, \\ k, & \text{if } k \mid n. \end{cases}$$

The Geometric Sum (Cont'd)

- By hypothesis, $g(n)$ is the sum of terms in a geometric progression,

$$g(n) = \sum_{m=0}^{k-1} x^m, \quad x = e^{2\pi i n/k}.$$

So we have

$$g(n) = \begin{cases} \frac{x^k-1}{x-1}, & \text{if } x \neq 1 \\ k, & \text{if } x = 1 \end{cases}.$$

If $k \mid n$, then $x = 1$. So $g(n) = k$.

If $k \nmid n$, then $x \neq 1$. But $x^k = 1$. Hence, $g(n) = 0$.

Subsection 2

Existence of Fourier Series for Periodic Arithmetical Functions

Lagrange's Interpolation Theorem

Theorem (Lagrange's Interpolation Theorem)

Let $z_0, z_1, \ldots, z_{k-1}$ be k distinct complex numbers, and let $w_0, w_1, \ldots,$ w_{k-1} be k complex numbers which need not be distinct. Then there is a unique polynomial $P(z)$ of degree $\leq k-1$, such that

$$P(z_m) = w_m, \quad \text{for } m = 0, 1, 2, \ldots, k-1.$$

- The required polynomial $P(z)$, called the **Lagrange interpolation polynomial**, can be constructed explicitly as follows.

  Let

  $$A(z) = (z - z_0)(z - z_1) \cdots (z - z_{k-1}).$$

  Let

  $$A_m(z) = \frac{A(z)}{z - z_m}.$$

Lagrange's Interpolation Theorem (Cont'd)

- $A_m(z) = \frac{A(z)}{z - z_m}$ is a polynomial of degree $k-1$.
  Moreover,
  $$A_m(z_m) \neq 0, \quad A_m(z_j) = 0, \text{ for all } j \neq m.$$
  Hence,
  $$\frac{A_m(z)}{A_m(z_m)}$$
  is a polynomial of degree $k-1$ which:
  - Vanishes at each z_j, for $j \neq m$;
  - Has the value 1 at z_m.

Lagrange's Interpolation Theorem (Cont'd)

- Consider the linear combination

$$P(z) = \sum_{m=0}^{k-1} w_m \frac{A_m(z)}{A_m(z_m)}.$$

It is a polynomial of degree $\leq k-1$, with

$$P(z_j) = w_j, \quad \text{for each } j.$$

Suppose there is another such polynomial $Q(z)$.

The difference $P(z) - Q(z)$ vanishes at k distinct points.

But $P(z) - Q(z)$ has degree $\leq k-1$.

So $P(z) - Q(z) = 0$.

Hence, $P(z) = Q(z)$.

Existence of Fourier Series

Theorem

Given k complex numbers $w_0, w_1, \ldots, w_{k-1}$, there exist k uniquely determined complex numbers $a_0, a_1, \ldots, a_{k-1}$, such that

$$w_m = \sum_{n=0}^{k-1} a_n e^{2\pi imn/k}, \quad m = 0, 1, 2, \ldots, k-1.$$

Moreover, the coefficients a_n are given by the formula

$$a_n = \frac{1}{k} \sum_{m=0}^{k-1} w_m e^{-2\pi imn/k}, \quad m = 0, 1, 2, \ldots, k-1.$$

Existence of Fourier Series (Cont'd)

- Let $z_m = e^{2\pi i m/k}$.

  The numbers $z_0, z_1, \ldots, z_{k-1}$ are distinct.

  So there is a unique Lagrange polynomial

  $$P(z) = \sum_{m=0}^{k-1} a_n z^n,$$

  such that

  $$P(z_m) = w_m, \quad \text{for each } m = 0, 1, 2, \ldots, k-1.$$

  This shows that there are uniquely determined numbers a_n satisfying the first equation.

Existence of Fourier Series (Coefficients)

- Take $w_m = \sum_{n=0}^{k-1} a_n e^{2\pi imn/k}$.
  Multiply by $e^{-2\pi imr/k}$, where m, r are nonnegative integers $\leq k$.
  Sum on m to get
  $$\sum_{m=0}^{k-1} w_m e^{-2\pi imr/k} = \sum_{n=0}^{k-1} a_n \sum_{m=0}^{k-1} e^{2\pi i(n-r)m/k}.$$
  By a previous theorem, the sum on m is 0 unless $k \mid (n-r)$.
  But $|n-r| \leq k-1$. So $k \mid (n-r)$ if, and only if, $n = r$.
  So the only nonvanishing term on the right occurs when $n = r$,
  $$\sum_{m=0}^{k-1} w_m e^{-2\pi imr/k} = ka_r.$$

Arithmetical Functions and Fourier Series

Theorem

Let f be an arithmetical function which is periodic mod k. Then there is a uniquely determined arithmetical function g, also periodic mod k, such that

$$f(m) = \sum_{m=0}^{k-1} g(n) e^{2\pi imn/k}.$$

In fact, g is given by the formula

$$g(n) = \frac{1}{k} \sum_{m=0}^{k-1} f(m) e^{-2\pi imn/k}.$$

Arithmetical Functions and Fourier Series (Cont'd)

- Let

$$w_m = f(m) = \sum_{m=0}^{k-1} g(n) e^{2\pi i m n/k}, \quad \text{for } m = 0, 1, 2, \ldots, k-1.$$

Apply the preceding theorem to determine the numbers

$$a_0, a_1, \ldots, a_{k-1}.$$

Define the function g by the relations

$$g(m) = a_m, \quad \text{for } m = 0, 1, 2, \ldots, k-1.$$

Extend the definition of $g(m)$ to all integers m by periodicity mod k. Then f is related to g by the equations in the theorem.

Terminology

- Since both f and g are periodic mod k, we can rewrite the sums in the last theorem

$$f(m) = \sum_{n \mod k} g(n) e^{2\pi i mn/k}$$

and

$$g(n) = \frac{1}{k} \sum_{m \mod k} f(m) e^{-2\pi i mn/k}.$$

- In each case the summation can be extended over any complete residue system modulo k.
- The first sum is called the **finite Fourier expansion** of f.
- The numbers $g(n)$ are called the **Fourier coefficients** of f.

Subsection 3

Ramanujan's Sum and Generalizations

Ramanujan's Sum

- Let n be a fixed positive integer.
- The sum of the n-th powers of the primitive k-th roots of unity is
$$c_k(n) = \sum_{\substack{m \bmod k \\ (m,k)=1}} e^{2\pi imn/k}.$$
- It is known as **Ramanujan's sum**.
- Ramanujan showed that $c_k(n)$ is always an integer by proving the relation
$$c_k(n) = \sum_{d|(n,k)} d\mu\left(\frac{k}{d}\right).$$
- This formula suggests that we study general sums of the form
$$s_k(n) = \sum_{d|(n,k)} f(d)g\left(\frac{k}{d}\right).$$

Generalized Ramanujan's Sum and Periodicity

- We study general sums of the form
$$s_k(n) = \sum_{d|(n,k)} f(d)g\left(\frac{k}{d}\right).$$
- These resemble the sums for the Dirichlet convolution $f * g$ except that we sum over a subset of the divisors of k, namely those d which also divide n.
- Since n occurs only in the gcd (n, k), we have
$$s_k(n+k) = s_k(n).$$
- So $s_k(n)$ is a periodic function of n, with period k.
- Hence this sum has a finite Fourier expansion.

Fourier Expansion of Ramanujan's Sum

Theorem

Let

$$s_k(n) = \sum_{d \mid (n,k)} f(d) g\left(\frac{k}{d}\right).$$

Then $s_k(n)$ has the finite Fourier expansion

$$s_k(n) = \sum_{m \mod k} a_k(m) e^{2\pi i m n / k},$$

where

$$a_k(m) = \sum_{d \mid (m,k)} g(d) f\left(\frac{k}{d}\right) \frac{d}{k}.$$

Fourier Expansion of Ramanujan's Sum (Cont'd)

- By the preceding theorem, the coefficients $a_k(m)$ are given by

$$a_k(m) = \frac{1}{k} \sum_{n \bmod k} s_k(n) e^{-2\pi inm/k} = \frac{1}{k} \sum_{n=1}^{k} \sum_{\substack{d \mid n \\ d \mid k}} f(d) g\left(\frac{k}{d}\right) e^{-2\pi inm/k}.$$

  Now we write $n = cd$.

  Note that for each fixed d, c runs from 1 to $\frac{k}{d}$.

  So we get

$$a_k(m) = \frac{1}{k} \sum_{d \mid k} f(d) g\left(\frac{k}{d}\right) \sum_{c=1}^{k/d} e^{-2\pi icdm/k}.$$

Fourier Expansion of Ramanujan's Sum (Cont'd)

- We have
$$a_k(m) = \frac{1}{k} \sum_{d \mid k} f(d) g\left(\frac{k}{d}\right) \sum_{c=1}^{k/d} e^{-2\pi i c d m / k}.$$
Now we replace d by $\frac{k}{d}$ in the sum on the right to get
$$a_k(m) = \frac{1}{k} \sum_{d \mid k} f\left(\frac{k}{d}\right) g(d) \sum_{c=1}^{d} e^{-2\pi i c m / d}.$$
By a previous theorem, the sum on c is 0 unless $d \mid m$ in which case the sum has the value d.
Hence, we get
$$a_k(m) = \frac{1}{k} \sum_{\substack{d \mid k \\ d \mid m}} f\left(\frac{k}{d}\right) g(d) d.$$

Ramanujan's Formula

Theorem

We have

$$c_k(n) = \sum_{d|(n,k)} d\mu\left(\frac{k}{d}\right).$$

- By the preceding theorem, $s_k(n) = \sum_{d|(n,k)} f(d)g\left(\frac{k}{d}\right)$ has the finite Fourier expansion

$$s_k(n) = \sum_{m \mod k} a_k(m)e^{2\pi imn/k},$$

where $a_k(m) = \sum_{d|(m,k)} g(d)f\left(\frac{k}{d}\right)\frac{d}{k}$.

Ramanujan's Formula (Cont'd)

- Take $f(k) = k$ and $g(k) = \mu(k)$.

  We find
  $$\sum_{d|(n,k)} d\mu\left(\frac{k}{d}\right) = \sum_{m \mod k} a_k(m)e^{2\pi imn/k},$$
  where
  $$a_m(k) = \sum_{d|(m,k)} \mu(d) = \left[\frac{1}{(m,k)}\right] = \begin{cases} 1, & \text{if } (m,k) = 1 \\ 0, & \text{if } (m,k) > 1 \end{cases}$$
  Hence
  $$\sum_{d|(n,k)} d\mu\left(\frac{k}{d}\right) = \sum_{\substack{m \mod k \\ (m,k)=1}} e^{2\pi imn/k} = c_k(n).$$

Subsection 4

Multiplicative Properties of the Sums $s_k(n)$

Multiplicative Properties of the Sums $s_k(n)$

Theorem

Let

$$s_k(n) = \sum_{d|(n,k)} f(d) g\left(\frac{k}{d}\right),$$

where f and g are multiplicative. Then we have

$$s_{mk}(ab) = s_m(a) s_k(b), \text{ whenever } (a,k) = (b,m) = 1.$$

In particular, we have

$$s_m(ab) = s_m(a), \text{ if } (b,m) = 1,$$

and

$$s_{mk}(a) = s_m(a) g(k), \text{ if } (a,k) = 1.$$

Multiplicative Properties of the Sums $s_k(n)$ (Cont'd)

- Suppose $(a,k)=(b,m)=1$.
  These imply
  $$(mk,ab)=(a,m)(k,b),$$
  with (a,m) and (b,k) relatively prime.
  Therefore,
  $$s_{mk}(ab)=\sum_{d\mid(mk,ab)} f(d)g\left(\frac{mk}{d}\right)=\sum_{d\mid(a,m)(b,k)} f(d)g\left(\frac{mk}{d}\right).$$
  Writing $d=d_1d_2$ in the last sum, we obtain
  $$\begin{aligned} s_{mk}(ab) &= \textstyle\sum_{d_1\mid(a,m)}\sum_{d_2\mid(b,k)} f(d_1d_2)g(\frac{mk}{d_1d_2}) \\ &= \textstyle\sum_{d_1\mid(a,m)} f(d_1)g(\frac{m}{d_1})\sum_{d_2\mid(b,k)} f(d_2)g(\frac{k}{d_2}) \\ &= s_m(a)s_k(b). \end{aligned}$$

Multiplicative Properties of the Sums $s_k(n)$ (Cont'd)

- We proved that

$$s_{mk}(ab) = s_m(a)s_k(b), \text{ whenever } (a,k) = (b,m) = 1.$$

Now we have $s_1(b) = f(1)g(1) = 1$.

So taking $k = 1$ in the sum, we get

$$s_m(ab) = s_m(a)s_1(b) = s_m(a).$$

Similarly, $s_k(1) = f(1)g(k) = g(k)$.

So taking $b = 1$ in the sum, we find

$$s_{mk}(a) = s_m(a)s_k(1) = s_m(a)g(k).$$

Example

- We proved that Ramanujan's sum is

$$c_k(n) = \sum_{d|(n,k)} d\mu\left(\frac{k}{d}\right).$$

- So applying the theorem, we get the following multiplicative properties

$$\begin{aligned} c_{mk}(ab) &= c_m(a)c_k(b), && \text{whenever } (a,k) = (b,m) = 1; \\ c_m(a,b) &= c_m(a), && \text{whenever } (b,m) = 1; \\ c_{mk}(a) &= c_m(a)\mu(k), && \text{whenever } (a,k) = 1. \end{aligned}$$

Sums $s_k(n)$ and Dirichlet Convolution

Theorem

Let f be completely multiplicative, and let $g(k) = \mu(k)h(k)$, where h is multiplicative. Assume that $f(p) \neq 0$ and $f(p) \neq h(p)$, for all primes p. Let

$$s_k(n) = \sum_{d|(n,k)} f(d) g\left(\frac{k}{d}\right).$$

Then we have

$$s_k(n) = \frac{F(k)g(N)}{F(N)},$$

where $F = f * g$ and $N = \frac{k}{(n,k)}$.

Sums $s_k(n)$ and Dirichlet Convolution (Cont'd)

- First we note that
$$\begin{array}{rcl} F(k) & = & \sum_{d|k} f(d)\mu(\frac{k}{d})h(\frac{k}{d}) \\ & = & \sum_{d|k} f(\frac{k}{d})\mu(d)h(d) \\ & = & f(k)\sum_{d|k}\mu(d)\frac{h(d)}{f(d)} \\ & = & f(k)\prod_{p|k}\left(1-\frac{h(p)}{f(p)}\right), \end{array}$$
where the last equation follows from the fact that, if a function f is multiplicative, then $\sum_{d|n}\mu(d)f(d)=\prod_{p|n}(1-f(p))$.
Next, we write $a=(n,k)$, so that $k=aN$.
Then we have
$$\begin{array}{rcl} s_k(n) & = & \sum_{d|a} f(d)\mu(\frac{k}{d})h(\frac{k}{d}) \\ & = & \sum_{d|a} f(d)\mu(\frac{aN}{d})h(\frac{aN}{d}) \\ & = & \sum_{d|a} f(\frac{a}{d})\mu(Nd)h(Nd). \end{array}$$

Sums $s_k(n)$ and Dirichlet Convolution

- We wrote $a=(n,k)$, so that $k=aN$, and we have:
  - $\mu(Nd)=\mu(N)\mu(d)$ if $(N,d)=1$;
  - $\mu(Nd)=0$, if $(N,d)>1$.

  So the last equation gives us

$$\begin{aligned}
s_k(n) &= \mu(N)h(N)\sum_{\substack{d\mid a\\(N,d)=1}} f\left(\tfrac{a}{d}\right)\mu(d)h(d)\\
&= f(a)\mu(N)h(N)\sum_{\substack{d\mid a\\(N,d)=1}} \mu(d)\frac{h(d)}{f(d)}\\
&= f(a)\mu(N)h(N)\prod_{\substack{p\mid a\\p\nmid N}}\left(1-\frac{h(p)}{f(p)}\right)\\
&= f(a)\mu(N)h(N)\frac{\prod_{p\mid aN}\left(1-\frac{h(p)}{f(p)}\right)}{\prod_{p\mid N}\left(1-\frac{h(p)}{f(p)}\right)}\\
&= f(a)\mu(N)h(N)\frac{F(k)}{f(k)}\frac{f(N)}{F(N)} \quad (g=\mu h, F=f*g)\\
&= \frac{F(k)\mu(N)h(N)}{F(N)}=\frac{F(k)g(N)}{F(N)}.
\end{aligned}$$

Example

- Ramanujan's sum is
$$c_k(n) = \sum_{d|(n,k)} d\mu\left(\frac{k}{d}\right).$$
- By the theorem,
$$s_k(n) = \sum_{d|(n,k)} f(d)g\left(\frac{k}{d}\right).$$
- Set:
    - f the identity, which is completely multiplicative;
    - $g = \mu$, which is multiplicative.
- Recall that $\varphi(k) = \sum_{d|k} d\mu(\frac{k}{d})$.
- Therefore, we have
$$c_k(n) = \frac{\varphi(k)\mu(N)}{\varphi(N)} = \frac{\varphi(k)\mu\left(\frac{k}{(n,k)}\right)}{\varphi\left(\frac{k}{(n,k)}\right)}.$$

Subsection 5

Gauss Sums Associated with Dirichlet Characters

Gauss Sums Associated with Dirichlet Characters

Definition

For any Dirichlet character χ mod k the sum

$$G(n,\chi) = \sum_{m=1}^{k} \chi(m) e^{2\pi i m n/k}$$

is called the **Gauss sum associated with** χ.

Gauss Sums and Ramanujan's Sum

- Let $\chi = \chi_1$ be the principal character mod k.
- We then have
$$\chi_1(m) = \begin{cases} 1, & \text{if } (m,k) = 1, \\ 0, & \text{otherwise.} \end{cases}$$
- In this case the Gauss sum
$$G(n,\chi) = \sum_{m=1}^{k} \chi(m) e^{2\pi i m n/k}$$
reduces to Ramanujan's sum,
$$G(n,\chi_1) = \sum_{\substack{m=1 \\ (m,k)=1}}^{k} e^{2\pi i m n/k} = c_k(n).$$
- Thus, the Gauss sums $G(n,\chi)$ can be regarded as generalizations of Ramanujan's sum.

A Factorization Property

Theorem

If χ is any Dirichlet character mod k, then

$$G(n,\chi) = \overline{\chi}(n)G(1,\chi), \text{ whenever } (n,k) = 1.$$

- When $(n,k) = 1$ the numbers nr run through a complete residue system mod k with r. Also, $|\chi(n)|^2 = \chi(n)\overline{\chi}(n) = 1$. So

  $$\chi(r) = \overline{\chi}(n)\chi(n)\chi(r) = \overline{\chi}(n)\chi(nr).$$

  Therefore, the sum defining $G(n,\chi)$ can be written as follows:

  $$\begin{array}{rcl} G(n,\chi) & = & \sum_{r \bmod k} \chi(r)e^{2\pi inr/k} \\ & = & \overline{\chi}(n)\sum_{r \bmod k} \chi(nr)e^{2\pi inr/k} \\ & = & \overline{\chi}(n)\sum_{m \bmod k} \chi(m)e^{2\pi im/k} \\ & = & \overline{\chi}(n)G(1,\chi). \end{array}$$

Separable Gauss Sums

Definition

The Gauss sum $G(n,\chi)$ is said to be **separable** if

$$G(n,\chi)=\overline{\chi}(n)G(1,\chi).$$

- By the preceding theorem, $G(n,\chi)$ is separable whenever n is relatively prime to the modulus k.
- A characterization of separability for those integers n not relatively prime to k is given in the next slide.

Characterization of Separable Gauss Sums

Theorem

If χ is a character mod k the Gauss sum $G(n,\chi)$ is separable for every n if, and only if

$$G(n,\chi)=0 \quad \text{whenever } (n,k)>1.$$

- Separability always holds if $(n,k)=1$.

  If $(n,k)>1$ we have $\overline{\chi}(n)=0$.

  So the equation holds if and only if $G(n,\chi)=0$.

Consequence of Separability

Theorem

If $G(n,\chi)$ is separable for every n, then

$$|G(1,\chi)|^2 = k.$$

- We have

$$\begin{array}{rcl}
|G(1,\chi)|^2 & = & G(1,\chi)\overline{G(1,\chi)} \\
& = & G(1,\chi)\sum_{m=1}^{k}\overline{\chi}(m)e^{-2\pi im/k} \\
& = & \sum_{m=1}^{k}G(m,\chi)e^{-2\pi im/k} \\
& = & \sum_{m=1}^{k}\sum_{r=1}^{k}\chi(r)e^{2\pi imr/k}e^{-2\pi im/k} \\
& = & \sum_{r=1}^{k}\chi(r)\sum_{m=1}^{k}e^{2\pi im(r-1)/k} \\
& \stackrel{\text{geometric}}{=} & k\chi(1) \\
& = & k.
\end{array}$$

Subsection 6

Dirichlet Characters with Nonvanishing Gauss Sums

Dirichlet Characters with Nonzero Gauss Sums

- The next theorem gives a necessary condition for $G(n,\chi)$ to be nonzero for $(n,k) > 1$.

Theorem

Let χ be a Dirichlet character mod k. Assume that $G(n,\chi) \neq 0$, for some n satisfying $(n,k) > 1$. Then there exists a divisor d of k, $d < k$, such that

$$\chi(a) = 1 \text{ whenever } (a,k) = 1 \text{ and } a \equiv 1 \pmod{d}.$$

- For the given n, let $q = (n,k)$ and let $d = k/q$.

  Then $d \mid k$ and, since $q > 1$, we have $d < k$.

  Choose any a satisfying $(a,k) = 1$ and $a \equiv 1 \pmod{d}$.

  We will prove that $\chi(a) = 1$.

Dirichlet Characters with Nonzero Gauss Sums (Cont'd)

- Since $(a, k) = 1$, in the sum defining $G(n, \chi)$ we can replace the index of summation m by am. Then we find

$$\begin{array}{rcl} G(n,\chi) & = & \sum_{m \bmod k} \chi(m) e^{2\pi i n m/k} \\ & = & \sum_{m \bmod k} \chi(am) e^{2\pi i n a m/k} \\ & = & \chi(a) \sum_{m \bmod k} \chi(m) e^{2\pi i n a m/k}. \end{array}$$

  Now $a \equiv 1 \pmod{d}$ and $d = \frac{k}{q}$.

  So, for some integer b,

$$a = 1 + \frac{bk}{q}.$$

Dirichlet Characters with Nonzero Gauss Sums (Cont'd)

- We wrote $a = 1 + \frac{bk}{q}$.
  Since $q \mid n$, we have
  $$\frac{anm}{k} = \frac{nm}{k} + \frac{bknm}{qk} = \frac{nm}{k} + \frac{bnm}{q} \equiv \frac{nm}{k} \pmod{1}.$$
  Hence,
  $$e^{2\pi i nam/k} = e^{2\pi i nm/k}.$$
  So the sum for $G(n, \chi)$ becomes
  $$G(n, \chi) = \chi(a) \sum_{m \mod k} \chi(m) e^{2\pi i nm/k} = \chi(a) G(n, \chi).$$
  Since $G(n, \chi) \neq 0$, this implies $\chi(a) = 1$, as asserted.
- The theorem points towards characters χ mod k for which there is a divisor $d < k$, satisfying $\chi(a) = 1$, if $(a, k) = 1$ and $a \equiv 1 \pmod{d}$.

Subsection 7

Induced Moduli and Primitive Characters

Induced Moduli

Definition of Induced Modulus

Let χ be a Dirichlet character mod k and let d be any positive divisor of k. The number d is called an **induced modulus for** χ if we have

$$\chi(a) = 1 \text{ whenever } (a,k) = 1 \text{ and } a \equiv 1 \pmod{d}.$$

- Note d is an induced modulus if the character χ mod k acts like a character mod d on the representatives of the residue class $\widehat{1}$ mod d which are relatively prime to k.
- Note also that k itself is always an induced modulus for χ.

Condition for 1 to be an Induced Modulus

Theorem

Let χ be a Dirichlet character mod k. Then 1 is an induced modulus for χ if, and only if, $\chi = \chi_1$.

- If $\chi = \chi_1$, then $\chi(a) = 1$, for all a relatively prime to k.

  But every a satisfies $a \equiv 1 \pmod{1}$.

  So the number 1 is an induced modulus.

  Conversely, suppose 1 is an induced modulus.

  Then $\chi(a) = 1$, whenever $(a, k) = 1$.

  Also, χ vanishes on the numbers not prime to k.

  It follows that $\chi = \chi_1$.

Primitive Characters

- For any Dirichlet character mod k, k itself is an induced modulus.
- If there are no others we call the character primitive.

Definition of Primitive Characters

A Dirichlet character χ mod k is said to be **primitive** mod k if it has no induced modulus $d < k$.
In other words, χ is primitive mod k if, and only if, for every divisor d of k, $0 < d < k$, there exists an integer $a \equiv 1 \pmod{d}$, $(a, k) = 1$, such that $\chi(a) \neq 1$.

- If $k > 1$, the principal character χ_1 is not primitive since it has 1 as an induced modulus.

Primitivity of all Characters Modulo a Prime

- If the modulus is prime, every non principal character is primitive.

Theorem

Every non principal character χ modulo a prime p is a primitive character mod p.

- The only divisors of p are 1 and p.

  So these are the only candidates for induced moduli.

  By the preceding theorem, if $\chi \neq \chi_1$, the divisor 1 is not an induced modulus.

  So χ has no induced modulus $< p$.

  Hence, χ is primitive.

Properties of Primitive Characters

Theorem

Let χ be a primitive Dirichlet character mod k. Then we have:

(a) $G(n,\chi) = 0$, for every n with $(n,k) > 1$.

(b) $G(n,\chi)$ is separable for every n.

(c) $|G(1,\chi)|^2 = k$.

(a) Suppose $G(n,\chi) \neq 0$, for some n with $(n,k) > 1$.
By a previous theorem, χ has an induced modulus $d < k$.
So, in this case, χ cannot be primitive.

(b) By Part (a) and the characterization of separability.

(c) By Part (b), $G(n,\chi)$ is separable, for every n.
By a previous theorem, $|G(1,\chi)|^2 = k$.

Comments

- By Part (b) of the theorem, if χ is primitive, the Gauss sum $G(n,\chi)$ is separable.
- Later we prove the converse.
- That is, we shall show that, if $G(n,\chi)$ is separable, for every n, then χ is primitive.

Subsection 8

Further Properties of Induced Moduli

Numbers Congruent Modulo an Induced Modulus

Theorem

Let χ he a Dirichlet character mod k. Assume $d \mid k$, $d > 0$. Then d is an induced modulus for χ if and only if

$$\chi(a) = \chi(b) \text{ whenever } (a, k) = (b, k) = 1 \text{ and } a \equiv b \pmod{d}.$$

- Suppose the stated condition holds.

  With $b = 1$, we get that, for all a, such that $(a, k) = 1$ and $a \equiv 1 \pmod{d}$, $\chi(a) = \chi(1) = 1$.

  Therefore, by definition, χ is an induced modulus.

  Conversely, let a, b such that $(a, k) = (b, k) = 1$ and $a \equiv b \pmod{d}$.

  We will show that $\chi(a) = \chi(b)$.

  Since $(a, k) = 1$, a mod k has a reciprocal a'.

Numbers Congruent Modulo an Induced Modulus (Cont'd)

- We chose a, b, with $(a, k) = (b, k) = 1$ and $a \equiv b \pmod{d}$.
  Also, there exists a', such that $aa' \equiv 1 \pmod{k}$.
  Now $aa' \equiv 1 \pmod{d}$ since $d \mid k$.
  Hence $\chi(aa') = 1$, since d is an induced modulus.
  But $aa' \equiv ba' \equiv 1 \pmod{d}$ because $a \equiv b \pmod{d}$.
  Hence, $\chi(aa') = \chi(ba')$.
  So $\chi(a)\chi(a') = \chi(b)\chi(a')$.
  But $\chi(a') \neq 0$, since $\chi(a)\chi(a') = 1$.
  Canceling $\chi(a')$, we find $\chi(a) = \chi(b)$.
- So, χ is periodic mod d on those integers relatively prime to k.
- Thus, χ acts very much like a character mod d.

Example

- The following table describes one of the characters χ mod 9.

n	1	2	3	4	5	6	7	8	9
$\chi(n)$	1	-1	0	1	-1	0	1	-1	0

  The table is periodic modulo 3.

  So 3 is an induced modulus for χ.

  In fact, χ acts like the following character ψ modulo 3:

n	1	2	3
$\psi(n)$	1	-1	0

  Since $\chi(n) = \psi(n)$, for all n, we call χ an **extension** of ψ.
- It is clear that whenever χ is an extension of a character ψ modulo d, then d will be an induced modulus for χ.

Example

- Now we examine one of the characters χ modulo 6:

n	1	2	3	4	5	6
$\chi(n)$	1	0	0	0	-1	0

For all $n \equiv 1 \pmod 3$ with $(n, 6) = 1$ (i.e., $n = 1$), $\chi(n) = 1$.

So the number 3 is an induced modulus.

However, χ is not an extension of any character 0 modulo 3.

The only characters modulo 3 are the characters ψ_1 and ψ,

n	1	2	3
$\psi_1(n)$	1	1	0
$\psi(n)$	1	-1	0

Since $\chi(2) = 0$, it cannot be an extension of either ψ or ψ_1.

Induced Moduli and Characters

Theorem

Let χ be a Dirichlet character modulo k. Assume $d \mid k$, $d > 0$. Then the following two statements are equivalent:

(a) d is an induced modulus for χ.

(b) There is a character ψ modulo d, such that

$$\chi(n) = \psi(n)\chi_1(n), \quad \text{for all } n,$$

where χ_1 is the principal character modulo k.

- Assume Condition (b) holds.

  Choose n satisfying $(n, k) = 1$, $n \equiv 1 \pmod{d}$.

  Then $\chi_1(n) = \psi(n) = 1$. So $\chi(n) = 1$.

  Hence, d is an induced modulus.

Induced Moduli and Characters (Converse)

- Assume Condition (a) holds.

  We exhibit a character ψ modulo d for which Condition (b) holds.

  We define $\psi(n)$ as follows.

  - If $(n, d) > 1$, let $\psi(n) = 0$.
    In this case we also have $(n, k) > 1$.
    So we obtain

    $$\chi(n) = 0 = 0 \cdot \chi_1(n) = \psi(n)\chi_1(n).$$

    So Condition (b) holds.

Induced Moduli and Characters (Converse Cont'd)

- Suppose $(n, d) = 1$.
  By Dirichlet's Theorem, there exists m, such that:
  - $m \equiv n \pmod{d}$;
  - $(m, k) = 1$.

  The arithmetic progression $xd + n$ contains infinitely many primes.
  We choose one that does not divide k and call this m.
  Having chosen m, which is unique modulo d, define

  $$\psi(n) = \chi(m).$$

  The number $\psi(n)$ is well-defined because χ takes equal values at numbers which are congruent modulo d and relatively prime to k.
  We can verify that ψ is a character mod d.
  - If $(n, k) = 1$, then $(n, d) = 1$.
    So $\psi(n) = \chi(m)$, for some $m \equiv n \pmod{d}$.
    Hence, by a previous theorem,

    $$\chi(n) = \chi(m) = \psi(n) \stackrel{\chi_1(n) = 1}{=} \psi(n)\chi_1(n).$$
  - If $(n, k) > 1$, then $\chi(n) = \chi_1(n) = 0$. So Condition (b) holds.

Subsection 9

The Conductor of a Character

The Conductor of a Character

Definition

Let χ be a Dirichlet character mod k. The smallest induced modulus d for χ is called the **conductor** of χ.

Theorem

Every Dirichlet character χ mod k can be expressed as a product,

$$\chi(n) = \psi(n)\chi_1(n), \text{ for all } n,$$

where χ_1 is the principal character mod k and ψ is a primitive character modulo the conductor of ψ.

- Let d be the conductor of χ.
  By the preceding theorem, χ can be expressed as a product of the given form, where ψ is a character mod d.
  We prove that ψ is primitive mod d.

The Conductor of a Character (Cont'd)

- Suppose that ψ is not primitive mod d.

  There is a divisor q of d, $q < d$, which is an induced modulus for ψ.

  We show that q, which divides k, is also an induced modulus for χ.

  This contradicts the fact that d is the smallest induced modulus for χ.

  Choose $n \equiv 1 \pmod{q}$, $(n, k) = 1$.

  Now q is an induced modulus for ψ.

  So we have
  $$\chi(n) = \psi(n)\chi_1(n) = \psi(n) = 1.$$

  Hence q is also an induced modulus for χ.

Subsection 10

Primitive Characters and Separable Gauss Sums

Alternate Description of Primitive Characters

Theorem

Let χ be a character mod k. Then χ is primitive mod k if, and only if, the Gauss sum

$$G(n,\chi) = \sum_{m \mod k} \chi(m) e^{2\pi imn/k}$$

is separable for every n.

- If χ is primitive, then $G(n,\chi)$ is separable by a previous theorem.

  For the converse, by previous theorems, we must show that, if χ is not primitive mod k, then for some r satisfying $(r,k) > 1$ we have $G(r,\chi) \neq 0$.

  Suppose, then, that χ is not primitive mod k. This implies $k > 1$. Then χ has a conductor $d < k$. Let $r = \frac{k}{d}$. Then $(r,k) > 1$.

  We prove that $G(r,\chi) \neq 0$ for this r.

Alternate Description of Primitive Characters (Cont'd)

- By the preceding theorem, there exists a primitive character ψ mod d, such that $\chi(n) = \psi(n)\chi_1(n)$, for all n. Hence we can write

$$\begin{array}{rcl} G(r,\chi) & = & \sum_{m \bmod k} \psi(m)\chi_1(m)e^{2\pi irm/k} \\ & = & \sum_{\substack{m \bmod k \\ (m,k)=1}} \psi(m)e^{2\pi irm/k} \\ & = & \sum_{\substack{m \bmod k \\ (m,k)=1}} \psi(m)e^{2\pi im/d} \\ & = & \frac{\varphi(k)}{\varphi(d)} \sum_{\substack{m \bmod d \\ (m,d)=1}} \psi(m)e^{2\pi im/d}. \end{array}$$

Therefore, we have

$$G(r,\chi) = \frac{\varphi(k)}{\varphi(d)} G(1,\psi).$$

But $|G(1,\psi)|^2 = d$ by a previous theorem (ψ primitive mod d). Hence $G(r,\chi) \neq 0$.

Subsection 11

The Finite Fourier Series of the Dirichlet Characters

Fourier Series and Dirichlet Characters

- Since each Dirichlet character χ mod k is periodic mod k, it has a finite Fourier expansion

$$\chi(m) = \sum_{n=1}^{k} a_k(n) e^{2\pi i m n / k}.$$

A previous theorem tells us that its coefficients are given by the formula

$$a_k(n) = \frac{1}{k} \sum_{m=1}^{k} \chi(m) e^{-2\pi i m n / k}.$$

The sum on the right is a Gauss sum $G(-n, \chi)$. So we have

$$a_k(n) = \frac{1}{k} G(-n, x).$$

Fourier Expansion of Primitive Characters

Theorem

The finite Fourier expansion of a primitive Dirichlet character χ mod k has the form

$$\chi(m) = \frac{\tau_k(\chi)}{\sqrt{k}} \sum_{m=1}^{k} \overline{\chi}(n) e^{-2\pi imn/k},$$

where

$$\tau_k(\chi) = \frac{G(1,\chi)}{\sqrt{k}} = \frac{1}{\sqrt{k}} \sum_{m=1}^{k} \chi(m) e^{2\pi im/k}.$$

The numbers $\tau_k(\chi)$ have absolute value 1.

Fourier Expansion of Primitive Characters (Cont'd)

- Since χ is primitive, we have

$$G(-n,\chi) = \chi(-n)G(1,\chi).$$

So the general form $a_k(n) = \frac{1}{k}G(-n,\chi)$ yields

$$a_k(n) = \frac{1}{k}\overline{\chi}(-n)G(1,\chi).$$

Therefore, $\chi(m) = \sum_{n=1}^{k} a_k(n)e^{2\pi imn/k}$ can be written as

$$\begin{aligned}\chi(m) &= \tfrac{G(1,\chi)}{k}\textstyle\sum_{m=1}^{k}\overline{\chi}(-n)e^{2\pi imn/k}\\ &= \tfrac{G(1,\chi)}{k}\textstyle\sum_{m=1}^{k}\overline{\chi}(n)e^{-2\pi imn/k}.\end{aligned}$$

A previous theorem shows that the $\tau_k(x)$ have absolute value 1.

Subsection 12

Pólya's Inequality for the Partial Sums of Primitive Characters

Pólya's Inequality

Theorem (Pólya's Inequality)

If χ is any primitive character mod k, then, for all $x \geq 1$, we have

$$\left|\sum_{m \leq x} \chi(m)\right| < \sqrt{k} \log k.$$

- Express $\chi(m)$ by its Fourier expansion, as given in the theorem

$$\chi(m) = \frac{\tau_k(\chi)}{\sqrt{k}} \sum_{n=1}^{k} \overline{\chi}(n) e^{-2\pi imn/k}.$$

Sum over all $m \leq x$, taking into account $\chi(k) = 0$, to get

$$\sum_{m \leq x} \chi(m) = \frac{\tau_k(\chi)}{\sqrt{k}} \sum_{n=1}^{k-1} \overline{\chi}(n) \sum_{m \leq x} e^{-2\pi imn/k}.$$

Pólya's Inequality (Cont'd)

- Take absolute values and multiply by $\sqrt{k}$ to get

$$\sqrt{k}\left|\sum_{m\leq x}\chi(m)\right| \leq \sum_{n=1}^{k-1}\left|\sum_{m\leq x}e^{-2\pi imn/k}\right| = \sum_{n=1}^{k-1}|f(n)|,$$

say, where $f(n)=\sum_{m\leq x}e^{-2\pi imn/k}$.
Now

$$f(k-n)=\sum_{m\leq x}e^{-2\pi im(k-n)/k}=\sum_{m\leq x}e^{2\pi imn/k}=\overline{f(n)}.$$

So $|f(k-n)|=|f(n)|$. Hence

$$\sqrt{k}\left|\sum_{m\leq x}\chi(m)\right|\leq 2\sum_{n\leq k/2}|f(n)|.$$

Pólya's Inequality (Cont'd)

- Now $f(n)$ is a geometric sum of the form

$$f(n) = \sum_{m=1}^{r} y^m,$$

where $r = [x]$ and $y = e^{-2\pi in/k}$.
Moreover, since $1 \leq n \leq k-1$, $y \neq 1$.
Writing $z = e^{-\pi in/k}$, we have $y = z^2$.
Moreover, $z^2 \neq 1$, since $n \leq \frac{k}{2}$.
Hence,

$$f(n) = y\frac{y^r - 1}{y - 1} = z^2 \frac{z^{2r} - 1}{z^2 - 1} = z^{r+1}\frac{z^r - z^{-r}}{z - z^{-1}}.$$

So we get

$$|f(n)| = \left|\frac{z^r - z^{-r}}{z - z^{-1}}\right| = \left|\frac{e^{-\pi irn/k} - e^{\pi irn/k}}{e^{-\pi in/k} - e^{\pi in/k}}\right| = \frac{|\sin \frac{\pi rn}{k}|}{|\sin \frac{\pi n}{k}|} \leq \frac{1}{\sin \frac{\pi n}{k}}.$$

Pólya's Inequality (Cont'd)

- We obtained
$$|f(n)| \leq \frac{1}{\sin \frac{\pi n}{k}}.$$
For or $0 \leq t \leq \frac{\pi}{2}$, we have the inequality
$$\sin t \geq \frac{2t}{\pi}.$$
Set $t = \frac{\pi n}{k}$ to get
$$|f(n)| \leq \frac{1}{\sin \frac{\pi n}{k}} \leq \frac{1}{\frac{2}{\pi} \frac{\pi n}{k}} = \frac{k}{2n}.$$
Hence
$$\sqrt{k} \left| \sum_{m \leq x} \chi(m) \right| \leq 2 \sum_{n \leq k/2} |f(n)| \leq k \sum_{n \leq k/2} \frac{1}{n} < k \log k.$$