

## SOME RESULTS ON GAUSS SUMS

For any positive integer  $n$ , let  $(\mathbf{Z}/n\mathbf{Z})^\times$  denote the multiplicative group of integers modulo  $n$ , having order  $\phi(n)$  where  $\phi$  is the Euler totient function.

### 1. DIRICHLET CHARACTERS

**Definition 1.1.** A **Dirichlet character modulo  $n$**  is a homomorphism of multiplicative groups,

$$\chi : (\mathbf{Z}/n\mathbf{Z})^\times \longrightarrow \mathbf{C}^\times.$$

For any two Dirichlet characters  $\chi$  and  $\eta$  modulo  $n$ , the product character defined by the rule

$$(\chi\eta)(x) = \chi(x)\eta(x)$$

is again a Dirichlet character modulo  $n$ . In fact, the set of Dirichlet characters modulo  $n$  is again a multiplicative group, called the **dual group** of  $(\mathbf{Z}/n\mathbf{Z})^\times$  and denoted  $\widehat{(\mathbf{Z}/n\mathbf{Z})^\times}$ . The identity element of the dual group, mapping every element of  $(\mathbf{Z}/n\mathbf{Z})^\times$  to 1, is the **trivial character modulo  $n$** , denoted  $\mathbf{1}_n$  or just  $\mathbf{1}$  when  $n$  is clear,

Since  $(\mathbf{Z}/n\mathbf{Z})^\times$  is a finite group the values taken by any Dirichlet character are complex roots of unity, specifically  $\phi(n)$ th roots of unity. One consequence of this is that there exist only finitely many Dirichlet characters modulo any given positive integer  $n$ . Another consequence is that the inverse of a Dirichlet character is its complex conjugate, defined by the rule

$$\bar{\chi}(x) = \overline{\chi(x)}.$$

A bit surprisingly, for  $n = 1$  we find that  $(\mathbf{Z}/n\mathbf{Z})^\times = \{0\}$ , because 0 is in fact invertible modulo 1. So there is one Dirichlet character modulo 1, the trivial character  $\mathbf{1}_1 : 0 \mapsto 1$ .

For any prime  $p$  the group  $(\mathbf{Z}/p\mathbf{Z})^\times$  is cyclic of order  $p - 1$ . Let  $g$  be a generator and let  $\zeta_{p-1}$  be a primitive  $(p - 1)$ st complex root of unity. Then the group of Dirichlet characters modulo  $p$  is again cyclic of order  $p - 1$ , generated by the character taking  $g$  to  $\zeta_{p-1}$ . In general (see, for example, **A Course in Arithmetic** by Serre),

**Proposition 1.2.** Let  $n$  be a positive integer. The dual group  $\widehat{(\mathbf{Z}/n\mathbf{Z})^\times}$  is isomorphic to the group  $(\mathbf{Z}/n\mathbf{Z})^\times$ . In particular, the number of Dirichlet characters modulo  $n$  is  $\phi(n)$ .

The group  $(\mathbf{Z}/n\mathbf{Z})^\times$  and its dual group are *noncanonically* isomorphic, meaning that constructing an actual isomorphism from  $(\mathbf{Z}/n\mathbf{Z})^\times$  to  $\widehat{(\mathbf{Z}/n\mathbf{Z})^\times}$  involves arbitrary choices of which elements map to which characters.

The groups  $(\mathbf{Z}/n\mathbf{Z})^\times$  and  $\widehat{(\mathbf{Z}/n\mathbf{Z})^\times}$  satisfy the **orthogonality relations** (exercise),

$$\sum_{x \in (\mathbf{Z}/n\mathbf{Z})^\times} \chi(x) = \begin{cases} \phi(n) & \text{if } \chi = \mathbf{1}, \\ 0 & \text{if } \chi \neq \mathbf{1}, \end{cases}$$

and

$$\sum_{\chi \in (\mathbf{Z}/n\mathbf{Z})^\times} \chi(x) = \begin{cases} \phi(n) & \text{if } x = 1, \\ 0 & \text{if } x \neq 1. \end{cases}$$

Let  $n$  be a positive integer and let  $d$  be a positive divisor of  $n$ . Every Dirichlet character  $\chi$  modulo  $d$  lifts to a Dirichlet character  $\chi_n$  modulo  $n$ , defined by the rule

$$\chi_n(x + n\mathbf{Z}) = \chi(x + d\mathbf{Z}) \quad \text{for all } x \in \mathbf{Z} \text{ relatively prime to } n.$$

That is,

$$\chi_n = \chi \circ \pi_{n,d},$$

where

$$\pi_{n,d} : (\mathbf{Z}/n\mathbf{Z})^\times \longrightarrow (\mathbf{Z}/d\mathbf{Z})^\times$$

is natural projection. For example, the Dirichlet character modulo 4 that takes 1 to 1 and 3 to  $-1$  lifts to the Dirichlet character modulo 12 that takes 1 and 5 to 1 and 7 and 11 to  $-1$ .

Going in the other direction, from modulus  $n$  to modulus  $d$  where  $d \mid n$ , isn't always possible. Every Dirichlet character  $\chi$  modulo  $n$  has a **conductor**, the smallest positive divisor  $d$  of  $n$  such that  $\chi = \chi_o \circ \pi_{n,d}$  for some character  $\chi_o$  modulo  $d$ , or, equivalently, the smallest positive divisor  $d$  of  $n$  such that  $\chi$  is trivial on the normal subgroup

$$K_{n,d} = \ker(\pi_{n,d}) = \{n \in (\mathbf{Z}/n\mathbf{Z})^\times : n = 1 \pmod{d}\}.$$

For example, the Dirichlet character modulo 12 taking 1 and 7 to 1 and 5 and 11 to  $-1$  has conductor 3. The only character modulo  $n$  with conductor 1 is the trivial character  $\mathbf{1}_n$ ,

**Definition 1.3.** A Dirichlet character modulo  $n$  is **primitive** if its conductor is  $n$ .

For example, the trivial character  $\mathbf{1}_n$  modulo  $n$  is primitive only for  $n = 1$ .

When  $\chi = \chi_o \circ \pi_{n,d}$  where  $d$  is the conductor of  $\chi$ , so that  $\chi_o$  is primitive, we say that  $\chi$  is **induced** by  $\chi_o$ . Thus every Dirichlet character is induced by a unique primitive Dirichlet character. If  $\chi$  is induced by  $\chi_o$  then

$$\chi_o(x + d\mathbf{Z}) = \chi(x + n\mathbf{Z}) \quad \text{if } \gcd(x, n) = 1,$$

but if  $\gcd(x, d) = 1$  while  $\gcd(x, n) > 1$  then  $\chi_o(x + d\mathbf{Z})$  is defined and nonzero even though  $\chi(x + n\mathbf{Z})$  is undefined.

Associate to any Dirichlet character  $\chi$  modulo  $n$  a corresponding multiplicative function from  $\mathbf{Z}$  to  $\mathbf{C}$ , also called  $\chi$ , by lifting its primitive inducing character,

$$\chi : \mathbf{Z}^+ \longrightarrow \mathbf{C}, \quad \chi(x) = \begin{cases} \chi_o(x + d\mathbf{Z}) & \text{if } \gcd(x, d) = 1, \\ 0 & \text{if } \gcd(x, d) > 1. \end{cases}$$

The following relation, with the new  $\chi$  on the left and the original  $\chi$  on the right,

$$\chi(x) = \chi(x + n\mathbf{Z}) \quad \text{if } \gcd(x, n) = 1,$$

justifies the multiple use of the symbol  $\chi$ . (For example, the orthogonality relations are undisturbed if we apply the new  $\chi$  to coset representatives rather than applying the original  $\chi$  to cosets.) For  $\gcd(x, n) > 1$ ,  $\chi(x)$  is defined and possibly nonzero, while  $\chi(x + n\mathbf{Z})$  is undefined. Often we tacitly pass Dirichlet characters through the process described here, suppressing further reference to the primitive inducing character  $\chi_o$  from the notation.

In particular, if  $n > 1$  then the trivial character modulo  $n$  does not extend directly to the constant function 1 on the positive integers. However,  $1_n$  has conductor  $d = 1$ , and the primitive trivial character  $1_o$  modulo 1 is identically 1 on  $(\mathbf{Z}/1\mathbf{Z})^\times = \{\bar{0}\}$ . The primitive trivial character lifts to the constant function  $1(x) = 1$  for all  $x \in \mathbf{Z}$ .

## 2. PRIMITIVE GAUSS SUMS

**Definition 2.1.** The **Gauss sum** of a Dirichlet character  $\chi$  modulo  $n$  is

$$\tau(\chi) = \sum_{t=0}^{n-1} \chi(t)\zeta_n^t, \quad \zeta_n = e^{2\pi i/n}.$$

For any integer  $m$  the  **$m$ th variant Gauss sum** is

$$\tau_m(\chi) = \sum_{t=0}^{n-1} \chi(t)\zeta_n^{mt}, \quad \zeta_n = e^{2\pi i/n}.$$

**Proposition 2.2.** If  $\chi$  is primitive modulo  $n$  then for any integer  $m$ ,

$$\tau_m(\chi) = \bar{\chi}(m)\tau(\chi).$$

*Proof.* First assume that  $\gcd(m, n) = 1$ . The fact that  $\bar{\chi}(m)\chi(m) = 1$  quickly proves the formula,

$$\begin{aligned} \tau_m(\chi) &= \sum_{t=0}^{n-1} \chi(t)\zeta_n^{mt} = \bar{\chi}(m) \sum_{t=0}^{n-1} \chi(mt)\zeta_n^{mt} \\ &= \bar{\chi}(m) \sum_{t=0}^{n-1} \chi(t)\zeta_n^t = \bar{\chi}(m)\tau(\chi). \end{aligned}$$

Now assume that  $\gcd(m, n) > 1$ . Let  $g = \gcd(m, n)$ , so that  $m = m'g$  for some integer  $m'$  and  $n = n'g$  for some positive integer  $n'$ . Then

$$(1) \quad \sum_{t=0}^{n-1} \chi(t)\zeta_n^{mt} = \sum_{s=0}^{n'-1} \left( \sum_{\substack{t=0 \\ t=s(n')}}^{n-1} \chi(t) \right) \zeta_n^{m's}.$$

Recall the  $\pi_{n,n'}$ -kernel subgroup of  $(\mathbf{Z}/n\mathbf{Z})^\times$ ,

$$K = K_{n,n'} = \{k \in (\mathbf{Z}/n\mathbf{Z})^\times : k \equiv 1 \pmod{n'}\}.$$

Because  $\chi$  is primitive,

$$\sum_{k \in K} \chi(k) = 0.$$

Since  $(\mathbf{Z}/n\mathbf{Z})^\times = \bigcup_s sK$  where the coset representatives  $s$  taken modulo  $n'$  run through  $(\mathbf{Z}/n'\mathbf{Z})^\times$ , the inner sum in (1) is  $\sum_{t \in sK} \chi(t)$ , and this is 0. The result follows.  $\square$

Let  $\chi$  be a primitive Dirichlet character modulo  $n$ . Then the square of the absolute value of its Gauss sum is

$$\begin{aligned} \tau(\chi)\overline{\tau(\chi)} &= \sum_{m=0}^{n-1} \bar{\chi}(m)\tau(\chi)\zeta_n^{-m} = \sum_{m=0}^{n-1} \sum_{t=0}^{n-1} \chi(t)\zeta_n^{mt}\zeta_n^{-m} \quad \text{by the proposition} \\ &= \sum_{t=0}^{n-1} \chi(t) \sum_{m=0}^{n-1} \zeta_n^{(t-1)m} = n, \end{aligned}$$

the last equality holding because the inner sum is  $n$  when  $t = 1$  and 0 otherwise. In particular, the Gauss sum is nonzero.

**Proposition 2.3.** *Let  $n$  be a positive integer. If  $n = 1$  or  $n = 2$  then every Dirichlet character  $\chi$  modulo  $n$  satisfies  $\chi(-1) = 1$ . If  $n > 2$  then the number of Dirichlet characters modulo  $n$  is even, half of them satisfying  $\chi(-1) = 1$  and the other half satisfying  $\chi(-1) = -1$ .*

*Proof.* The result for  $n = 1$  and  $n = 2$  is clear. If  $n > 2$  then  $4 \mid n$  or  $p \mid n$  for some odd prime  $p$ . The nontrivial character modulo 4 takes  $-1 \pmod{4}$  to  $-1$ , and for every odd prime  $p$  the character modulo  $p$  taking a generator  $g$  of  $(\mathbf{Z}/p\mathbf{Z})^\times$  to a primitive  $(p-1)$ st complex root of unity takes  $-1 \pmod{p}$  to  $-1$  since  $-1 = g^{(p-1)/2} \pmod{p}$ . In either case the character lifts to a character modulo  $n$  taking  $-1 \pmod{n}$  to  $-1$ .

Let  $(\widehat{\mathbf{Z}/n\mathbf{Z}})^\times$  denote the group of Dirichlet characters modulo  $n$ . The map  $(\widehat{\mathbf{Z}/n\mathbf{Z}})^\times \rightarrow \{\pm 1\}$  taking each character  $\chi$  to  $\chi(-1)$  is a homomorphism. We have just seen that the homomorphism surjects if  $n > 2$ , and so the result follows from the First Isomorphism Theorem of group theory.  $\square$

### 3. DECOMPOSITION OF PRIMITIVE GAUSS SUMS

Consider a positive integer

$$n = \prod_p p^{e_p},$$

and consider the Gauss sum of a primitive Dirichlet character modulo  $n$ ,

$$\tau(\chi) = \sum_{t \in \mathbf{Z}/n\mathbf{Z}} \chi(t)\zeta_n^t.$$

Recall that the Sun-Ze Theorem gives a ring isomorphism

$$\prod_p \mathbf{Z}/p^{e_p}\mathbf{Z} \xrightarrow{\sim} \mathbf{Z}/n\mathbf{Z}, \quad (t_p) \mapsto \sum_p u_p t_p,$$

where each  $u_p = \delta_{p,q} \pmod{q^{e_q}}$  for all  $q$ . Thus we may identify the primitive Dirichlet character modulo  $n$  with a product of primitive Dirichlet characters modulo the prime-power divisors of  $n$ ,

$$\chi \longleftrightarrow \bigotimes_p \chi_p, \quad \chi\left(\sum_p u_p t_p\right) = \prod_p \chi_p(t_p).$$

**Proposition 3.1.** *Let  $n$  be a positive integer and let  $\chi$  be a primitive Dirichlet character modulo  $n$ . Then the Gauss sum factors over the prime divisors of  $n$ ,*

$$\tau(\chi) = \prod_p \chi_p(n/p^{e_p})\tau(\chi_p).$$

*Proof.* For each  $t = \sum_p u_p t_p \in \mathbf{Z}/n\mathbf{Z}$  we have

$$\zeta_n^t = \prod_p \zeta_n^{u_p t_p} = \prod_p \zeta_{p^{e_p}}^{m_p t_p} \quad \text{where } m_p = (n/p^{e_p})^{-1} \pmod{p^{e_p}}.$$

Thus the Gauss sum is in fact a product of variant Gauss sums of characters modulo the prime-power divisors of  $n$ ,

$$\tau(\chi) = \sum_{(t_p) \in \prod_p \mathbf{Z}/p^{e_p}\mathbf{Z}} \prod_p \chi_p(t_p) \zeta_{p^{e_p}}^{m_p t_p} = \prod_p \sum_{t_p \in \mathbf{Z}/p^{e_p}\mathbf{Z}} \chi_p(t_p) \zeta_{p^{e_p}}^{m_p t_p} = \prod_p \tau_{m_p}(\chi_p).$$

For each  $p$  we have by Proposition 2.2 since  $\chi_p$  is primitive modulo  $p^{e_p}$ ,

$$\tau_{m_p}(\chi_p) = \bar{\chi}_p(m_p) \tau(\chi_p) = \chi_p(n/p^{e_p}) \tau(\chi_p).$$

The previous two displays combine to give the result.  $\square$