

# GAUSS AND JACOBI SUMS ON FINITE FIELDS AND $\mathbf{Z}/m\mathbf{Z}$

KEITH CONRAD

## 1. INTRODUCTION

The fields  $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$  for prime  $p$  generalize in two different but analogous ways: to the fields  $\mathbf{F}_q$  where  $q$  is a prime power and to the rings  $\mathbf{Z}/m\mathbf{Z}$  where  $m \geq 2$ . For both  $\mathbf{F}_q$  and  $\mathbf{Z}/m\mathbf{Z}$ , two important sums associated to multiplicative characters on them are Gauss sums and Jacobi sums. After defining these, we will discuss two of their main properties: their absolute value and a formula relating Gauss and Jacobi sums in “nondegenerate” situations. Then we’ll generalize what was done to finite commutative rings.

It is assumed the reader knows about characters on finite abelian groups,<sup>1</sup> especially that the sum of a nontrivial character over a group is 0. We will be working with multiplicative and additive characters on  $\mathbf{F}_q$  and  $\mathbf{Z}/m\mathbf{Z}$ . A multiplicative character is a character  $\chi$  of the unit group  $\mathbf{F}_q^\times$  or  $(\mathbf{Z}/m\mathbf{Z})^\times$ , extended to be 0 on nonunits in order to be defined on the whole ring while preserving the rule  $\chi(ab) = \chi(a)\chi(b)$ . An additive character is a character  $\psi$  of the additive group  $\mathbf{F}_q$  or  $\mathbf{Z}/m\mathbf{Z}$ , so  $\psi(a+b) = \psi(a)\psi(b)$  for all  $a$  and  $b$ .

## 2. GAUSS AND JACOBI SUMS ON FINITE FIELDS

**Definition 2.1.** Let  $\mathbf{F}_q$  be a finite field with characteristic  $p$ . For a multiplicative character  $\chi$  on  $\mathbf{F}_q$ , its *Gauss sum* is

$$G(\chi) = \sum_{a \in \mathbf{F}_q} \chi(a) e^{2\pi i \text{Tr}(a)/p} = \sum_{a \in \mathbf{F}_q} \chi(a) \zeta_p^{\text{Tr}(a)},$$

where  $\zeta_p = e^{2\pi i/p}$  and  $\text{Tr}: \mathbf{F}_q \rightarrow \mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$  is the trace mapping.

For two multiplicative characters  $\chi_1$  and  $\chi_2$  on  $\mathbf{F}_q$ , their *Jacobi sum* is

$$J(\chi_1, \chi_2) = \sum_{a \in \mathbf{F}_q} \chi_1(a) \chi_2(1-a) = \sum_{\substack{a, b \in \mathbf{F}_q \\ a+b=1}} \chi_1(a) \chi_2(b).$$

Each multiplicative character on  $\mathbf{F}_q$ , including the trivial character  $\mathbf{1}_q$ , is set to be 0 at  $a = 0$ ,<sup>2</sup> so we can drop terms in a Gauss or Jacobi sum that make a character 0:

$$G(\chi) = \sum_{a \neq 0} \chi(a) e^{2\pi i \text{Tr}(a)/p} \quad \text{and} \quad J(\chi_1, \chi_2) = \sum_{a \neq 0, 1} \chi_1(a) \chi_2(1-a).$$

Why do we care about these? Gauss used a special case of Gauss sums (where  $\chi$  is the Legendre symbol on  $\mathbf{F}_p$ ) to prove the quadratic reciprocity law [3, Sec. 6.3]. General Gauss and Jacobi sums on  $\mathbf{F}_q$  are used to count solutions to diagonal equations over  $\mathbf{F}_q$  [3, Chap. 8, 11].

**Theorem 2.2.** *Gauss sums on  $\mathbf{F}_q$  never vanish. More precisely,*

<sup>1</sup>For a review, see <https://kconrad.math.uconn.edu/blurbs/grouptheory/charthyshort.pdf>.

<sup>2</sup>Some authors let  $\mathbf{1}_q(0)$  equal 1, not 0, such as [1, p. 9] and [3, p. 88]. Then  $\chi\bar{\chi} \neq \mathbf{1}_q$  at 0 when  $\chi \neq \mathbf{1}_q$ .

- (1)  $G(\mathbf{1}_q) = -1$ ,  
(2) if  $\chi$  is a nontrivial multiplicative character on  $\mathbf{F}_q$ , then  $|G(\chi)| = \sqrt{q}$ .

*Proof.* (1) Since  $\mathbf{1}_q(a) = 1$  for  $a \neq 0$ , while  $\mathbf{1}_q(0) = 0$ ,

$$G(\mathbf{1}_q) = \sum_{a \neq 0} \zeta_p^{\mathrm{Tr}(a)} = \sum_{a \in \mathbf{F}_q} \zeta_p^{\mathrm{Tr}(a)} - 1.$$

Since  $a \mapsto \zeta_p^{\mathrm{Tr}(a)}$  is a nontrivial additive character on  $\mathbf{F}_q$ , the sum of its values over  $\mathbf{F}_q$  is 0 and we're left with  $G(\mathbf{1}_q) = -1$ .<sup>3</sup>

(2) Rewrite  $|G(\chi)| = \sqrt{q}$  as  $|G(\chi)|^2 = q$ , or equivalently  $G(\chi)\overline{G(\chi)} = q$ . That is what we'll verify, using the proof in [6, Lemma 6.1]:

$$G(\chi)\overline{G(\chi)} = \sum_{a \neq 0} \chi(a) \zeta_p^{\mathrm{Tr}(a)} \sum_{b \neq 0} \overline{\chi(b)} \zeta_p^{-\mathrm{Tr}(b)} = \sum_{b \neq 0} \sum_{a \neq 0} \chi(a/b) \zeta_p^{\mathrm{Tr}(a-b)}.$$

In the inner sum (for each nonzero  $b$ ), make the change of variables  $a \mapsto ab$ , so

$$\begin{aligned} G(\chi)\overline{G(\chi)} &= \sum_{b \neq 0} \sum_{a \neq 0} \chi(a) \zeta_p^{\mathrm{Tr}(ab-b)} \\ &= \sum_{b \neq 0} \left( 1 + \sum_{a \neq 0,1} \chi(a) \zeta_p^{\mathrm{Tr}(ab-b)} \right) \\ &= q - 1 + \sum_{a \neq 0,1} \chi(a) \left( \sum_{b \neq 0} \zeta_p^{\mathrm{Tr}(b(a-1))} \right) \\ &= q - 1 + \sum_{a \neq 0,1} \chi(a) \left( \sum_b \zeta_p^{\mathrm{Tr}(b(a-1))} - 1 \right). \end{aligned}$$

When  $a \neq 1$ ,  $a - 1$  is nonzero, so  $b \mapsto \zeta_p^{\mathrm{Tr}(b(a-1))}$  is a nontrivial additive character on  $\mathbf{F}_q$ . Thus the inner sum over all  $b$  in  $\mathbf{F}_q$  is 0, which implies

$$G(\chi)\overline{G(\chi)} = q - 1 - \sum_{a \neq 0,1} \chi(a) = q - 1 - \left( \sum_{a \neq 0} \chi(a) - 1 \right) = q - 1 - (0 - 1) = q. \quad \square$$

A character of  $\mathbf{F}_q^\times$  is called quadratic when it has order 2, which means its values are  $\pm 1$  and not always 1. Since the group  $\mathbf{F}_q^\times$  is cyclic of order  $q - 1$ , its character group is also cyclic of order  $q - 1$ . A cyclic group of even order has a unique element of order 2, so when  $q$  is odd there is a unique quadratic character of  $\mathbf{F}_q^\times$ . When  $q$  is even, there is no quadratic character of  $\mathbf{F}_q^\times$ .

**Corollary 2.3.** *Let  $q$  be an odd prime power and  $\eta$  be the quadratic character of  $\mathbf{F}_q^\times$ . Then  $G(\eta)^2 = \eta(-1)q$ . Thus  $G(\eta) = \pm\sqrt{q}$  when  $-1$  is a square in  $\mathbf{F}_q$  and  $G(\eta) = \pm i\sqrt{q}$  when  $-1$  is not a square in  $\mathbf{F}_q$ .*

<sup>3</sup>If we used the convention that  $\mathbf{1}_q(0) = 1$ , then  $G(\mathbf{1}_q) = \sum_{a \in \mathbf{F}_q} \zeta_p^{\mathrm{Tr}(a)} = 0$  instead, as in [3, Prop. 8.2.1].

*Proof.* Theorem 2.2(2) says  $G(\chi)\overline{G(\chi)} = q$  for every nontrivial character  $\chi$  of  $\mathbf{F}_q^\times$ . We have

$$(2.1) \quad \overline{G(\chi)} = \sum_{a \neq 0} \overline{\chi(a)} \zeta_p^{-\text{Tr}(a)} = \sum_{a \neq 0} \overline{\chi(-a)} \zeta_p^{\text{Tr}(a)} = \overline{\chi(-1)} \sum_{a \neq 0} \overline{\chi(a)} \zeta_p^{\text{Tr}(a)} = \chi(-1)G(\overline{\chi})$$

since  $\chi(-1) = \pm 1$ , so  $\overline{\chi(-1)} = \chi(-1)$ . Thus  $G(\overline{\chi}) = \chi(-1)\overline{G(\chi)}$ , so

$$(2.2) \quad G(\chi)G(\overline{\chi}) = G(\chi)\chi(-1)\overline{G(\chi)} = \chi(-1)q.$$

The quadratic character  $\eta$  of  $\mathbf{F}_q^\times$  has  $\overline{\eta} = \eta$ , so  $G(\eta)^2 = \eta(-1)q$  by (2.2) at  $\chi = \eta$ . The kernel of  $\eta$  is a subgroup of  $\mathbf{F}_q^\times$  with order  $(q-1)/2$ , which has to be the squares in  $\mathbf{F}_q^\times$ , so  $\eta(-1) = 1$  when  $-1$  is a square in  $\mathbf{F}_q$  and  $\eta(-1) = -1$  when  $-1$  is not a square in  $\mathbf{F}_q$ .  $\square$

The next theorem relates Gauss and Jacobi sums most of the time.

**Theorem 2.4.** *Let  $\chi_1$  and  $\chi_2$  be multiplicative characters on  $\mathbf{F}_q$ . If  $\chi_1\chi_2$  is nontrivial then  $G(\chi_1)G(\chi_2) = J(\chi_1, \chi_2)G(\chi_1\chi_2)$ .*

We'll see later that this identity is false when  $\chi_1\chi_2$  is trivial.

*Proof.* We will multiply out  $G(\chi_1)G(\chi_2)$ :

$$G(\chi_1)G(\chi_2) = \sum_{a \neq 0} \chi_1(a) \zeta_p^{\text{Tr}(a)} \sum_{b \neq 0} \chi_2(b) \zeta_p^{\text{Tr}(b)} = \sum_{a \neq 0} \chi_1(a) \left( \sum_{b \neq 0} \chi_2(b) \zeta_p^{\text{Tr}(a+b)} \right).$$

Replacing  $b$  in the inner sum with  $b-a$ ,

$$\begin{aligned} G(\chi_1)G(\chi_2) &= \sum_{a \neq 0} \chi_1(a) \left( \sum_{b \neq a} \chi_2(b-a) \zeta_p^{\text{Tr}(b)} \right) \\ &= \sum_{a \neq 0} \chi_1(a) \left( \sum_b \chi_2(b-a) \zeta_p^{\text{Tr}(b)} \right) \text{ since } \chi_2(0) = 0. \end{aligned}$$

Split up the inner sum over  $b \neq 0$  and  $b = 0$ :

$$\begin{aligned} G(\chi_1)G(\chi_2) &= \sum_{a \neq 0} \chi_1(a) \left( \sum_{b \neq 0} \chi_2(b-a) \zeta_p^{\text{Tr}(b)} + \chi_2(-a) \right) \\ &= \sum_{b \neq 0} \left( \sum_{a \neq 0} \chi_1(a) \chi_2(b-a) \right) \zeta_p^{\text{Tr}(b)} + \sum_{a \neq 0} \chi_1(a) \chi_2(-a). \end{aligned}$$

The second sum is  $\chi_2(-1) \sum_{a \neq 0} (\chi_1\chi_2)(a)$ , which is 0 since  $\chi_1\chi_2$  is nontrivial. In the first sum, make the change of variables  $c = a/b$  (so  $a = bc$ ) in the inner sum for fixed  $b$ :

$$\sum_{a \neq 0} \chi_1(a) \chi_2(b-a) = \sum_{c \neq 0} \chi_1(bc) \chi_2(b-bc) = (\chi_1\chi_2)(b) \sum_{c \neq 0} \chi_1(c) \chi_2(1-c) = (\chi_1\chi_2)(b) J(\chi_1, \chi_2),$$

so

$$G(\chi_1)G(\chi_2) = \sum_{b \neq 0} (\chi_1\chi_2)(b) J(\chi_1, \chi_2) \zeta_p^{\text{Tr}(b)} = J(\chi_1, \chi_2) G(\chi_1\chi_2). \quad \square$$

**Corollary 2.5.** *When  $\chi_1, \chi_2$ , and  $\chi_1\chi_2$  are all nontrivial,  $|J(\chi_1, \chi_2)| = \sqrt{q}$ .*

*Proof.* Theorem 2.4 lets us express  $J(\chi_1, \chi_2)$  in terms of Gauss sums when  $\chi_1\chi_2$  is nontrivial:

$$J(\chi_1, \chi_2) = \frac{G(\chi_1)G(\chi_2)}{G(\chi_1\chi_2)}.$$

When  $\chi_1, \chi_2$ , and  $\chi_1\chi_2$  are all nontrivial, all three terms on the right side have absolute value  $\sqrt{q}$  by Theorem 2.2(2), so  $|J(\chi_1, \chi_2)| = \sqrt{q}$ .  $\square$

What can we say about  $J(\chi_1, \chi_2)$  when one of  $\chi_1, \chi_2$ , or  $\chi_1\chi_2$  is trivial?

**Theorem 2.6.** *Let  $\chi$  be a nontrivial multiplicative character on  $\mathbf{F}_q$ . Then*

- (1)  $J(\mathbf{1}_q, \mathbf{1}_q) = q - 2$ ,
- (2)  $J(\chi, \mathbf{1}_q) = J(\mathbf{1}_q, \chi) = -1$ ,
- (3)  $J(\chi, \bar{\chi}) = -\chi(-1)$ .

When  $q = 2$ , (1) tells us  $J(\mathbf{1}_q, \mathbf{1}_q)$  vanishes. This is the only case where a Jacobi sum of two multiplicative characters on a finite field vanishes, and  $|J(\mathbf{1}_q, \mathbf{1}_q)| = \sqrt{q}$  only when  $q = 4$ .

*Proof.* (1)  $J(\mathbf{1}_q, \mathbf{1}_q) = \sum_{a \neq 0,1} 1$  is a sum of  $q - 2$  copies of 1.

(2) The sums  $J(\chi, \mathbf{1}_q)$  and  $J(\mathbf{1}_q, \chi)$  are equal since a Jacobi sum is symmetric in its two characters. Using the first sum,  $J(\chi, \mathbf{1}_q) = \sum_{a \neq 0,1} \chi(a) = \sum_{a \neq 0} \chi(a) - 1 = -1$ .

(3) We have

$$J(\chi, \bar{\chi}) = \sum_{a \neq 0,1} \chi(a)\bar{\chi}(1-a) = \sum_{a \neq 0,1} \chi(a/(1-a)).$$

Set  $b = a/(1-a)$ , so  $a \mapsto b$  is a bijection from  $\mathbf{F}_q - \{0, 1\}$  to  $\mathbf{F}_q - \{0, -1\}$  (with  $a = b/(1+b)$ ), so

$$J(\chi, \bar{\chi}) = \sum_{b \neq 0, -1} \chi(b) = \sum_{b \neq 0} \chi(b) - \chi(-1) = -\chi(-1). \quad \square$$

**Remark 2.7.** If we set  $\mathbf{1}_q(0) = 1$  then (1) and (2) change:  $J(\mathbf{1}_q, \mathbf{1}_q) = q$  and  $J(\chi, \mathbf{1}_q) = 0$ .

Let's return to Theorem 2.4 and show in the missing case, when  $\chi_1\chi_2$  is trivial, that the identity there is never true.

**Theorem 2.8.** *For each multiplicative character  $\chi$  on  $\mathbf{F}_q$ ,  $G(\chi)G(\bar{\chi}) \neq J(\chi, \bar{\chi})G(\chi\bar{\chi})$ .*

*Proof.* First assume  $\chi = \mathbf{1}_q$ . Then

$$G(\chi)G(\bar{\chi}) = G(\mathbf{1}_q)^2 = (-1)^2 = 1 \text{ by Theorem 2.2(1),}$$

while  $J(\chi, \bar{\chi})G(\chi\bar{\chi}) = J(\mathbf{1}_q, \mathbf{1}_q)G(\mathbf{1}_q) = -(q-2)$  by Theorem 2.6(1), and  $-(q-2) \neq 1$ .

Now assume  $\chi \neq \mathbf{1}_q$ . We have  $G(\chi)G(\bar{\chi}) = \chi(-1)q$  by (2.1), while  $J(\chi, \bar{\chi})G(\chi\bar{\chi}) = -\chi(-1)G(\mathbf{1}_q) = \chi(-1)$  by Theorems 2.2(1) and 2.6(3), and  $\chi(-1)q \neq \chi(-1)$ .  $\square$

### 3. GAUSS AND JACOBI SUMS ON THE INTEGERS MOD $m$

For  $m \geq 1$ , multiplicative characters on  $\mathbf{Z}/m\mathbf{Z}$  are called *Dirichlet characters mod  $m$* .

**Definition 3.1.** For a Dirichlet character  $\chi$  mod  $m$ , its *Gauss sum* is

$$G(\chi) = \sum_{a \bmod m} \chi(a)e^{2\pi ia/m} = \sum_{a \bmod m} \chi(a)\zeta_m^a,$$

where  $\zeta_m = e^{2\pi i/m}$ . For two Dirichlet characters  $\chi_1, \chi_2 \pmod m$ , their *Jacobi sum* is

$$J(\chi_1, \chi_2) = \sum_{a \pmod m} \chi_1(a)\chi_2(1-a).$$

We set Dirichlet characters mod  $m$  to be 0 on nonunits mod  $m$ , so in a Gauss and Jacobi sum we only need to sum over units mod  $m$ :

$$G(\chi) = \sum_{(a,m)=1} \chi(a)e^{2\pi ia/m} \quad \text{and} \quad J(\chi_1, \chi_2) = \sum_{(a,m)=1} \chi_1(a)\chi_2(1-a).$$

When  $m = p$  is prime, these are the Gauss and Jacobi sums seen before on  $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ , but for composite  $m$  these sums are not special cases of what we already saw.<sup>4</sup> An important application of Gauss sums of Dirichlet characters is their appearance in the constant (“root number”) in the functional equation for Dirichlet  $L$ -functions.

What are Dirichlet characters mod  $m$  when  $m = 1$ ? Since  $\mathbf{Z}/1\mathbf{Z} = \{0 \pmod 1\}$  is the zero ring, which has a trivial unit group (only in the zero ring is 0 invertible, since  $0 = 1$ ), the only Dirichlet character mod 1 is the trivial character  $\mathbf{1}_1$ , where  $\mathbf{1}_1(a \pmod 1) = 1$  for  $a \in \mathbf{Z}$ . Note  $\mathbf{1}_m(0) = 0$  for  $m \geq 2$ , but  $\mathbf{1}_1(0) = 1$ .

Unlike Gauss sums on finite fields, which never vanish, Gauss sums on  $\mathbf{Z}/m\mathbf{Z}$  can vanish.

**Example 3.2.** At the trivial character mod  $m$ ,  $G(\mathbf{1}_m) = \sum_{(a,m)=1} \zeta_m^a$  turns out to be  $\mu(m)$ , where  $\mu$  is the Möbius function. So  $G(\mathbf{1}_m) = 0$  if  $m$  is not squarefree.

While Dirichlet characters can be trivial and nontrivial, just like characters on finite fields, for Dirichlet characters the better analogue of the distinction between trivial and nontrivial characters on a finite field is the distinction between primitive and imprimitive Dirichlet characters:

**Definition 3.3.** Call a Dirichlet character  $\chi \pmod m$  *imprimitive* if there is a proper factor  $m'$  of  $m$  and a Dirichlet character  $\chi' \pmod{m'}$  such that  $\chi$  comes from  $\chi'$ : for all  $a$  in  $(\mathbf{Z}/m\mathbf{Z})^\times$ ,  $\chi(a \pmod m) = \chi'(a \pmod{m'})$ . When  $\chi \pmod m$  is not imprimitive, we call it *primitive*.

**Example 3.4.** Here are the four Dirichlet characters mod 8 (they are 0 at even numbers) and their Gauss sums  $G(\chi) = \sum_{(a,8)=1} \chi(a)e^{2\pi ia/8} = \sum_{(a,8)=1} \chi(a)e^{\pi ia/4}$ .

$a$	1	3	5	7	$G(\chi)$
$\mathbf{1}_8(a)$	1	1	1	1	0
$\chi_8(a)$	1	-1	1	-1	0
$\chi'_8(a)$	1	-1	-1	1	$\sqrt{8}$
$\chi''_8(a)$	1	1	-1	-1	$\sqrt{8}i$

The characters  $\mathbf{1}_8$  and  $\chi_8$  are imprimitive (they both make sense modulo 4) while  $\chi'_8$  and  $\chi''_8$  are primitive (neither one makes sense mod 4).

**Example 3.5.** For prime  $p$ , every nontrivial Dirichlet character modulo  $p$  is primitive while  $\mathbf{1}_p$  is imprimitive.

**Example 3.6.** For  $m \geq 2$ , the trivial Dirichlet character  $\mathbf{1}_m$  is imprimitive, while  $\mathbf{1}_1$  is primitive.

<sup>4</sup>I thank Darij Grinberg for simplifications to some arguments in this and the next section.

**Example 3.7.** No Dirichlet character mod 10 is primitive: the reduction map  $(\mathbf{Z}/10\mathbf{Z})^\times \rightarrow (\mathbf{Z}/5\mathbf{Z})^\times$  is an isomorphism, so each Dirichlet character mod 10 comes from a Dirichlet character mod 5. (There is no primitive Dirichlet character mod  $m$  if and only if  $m = 2N$  for odd  $N$ .)

**Lemma 3.8.** *Let  $\chi \bmod m$  be primitive and  $m'$  be a proper factor of  $m$ . There are some  $b, c$  relatively prime to  $m$  such that  $b \equiv c \pmod{m'}$  and  $\chi(b) \neq \chi(c)$ .*

*Proof.* Assume the conclusion is false, so for all  $b$  and  $c$  that are relatively prime to  $m$ , if  $b \equiv c \pmod{m'}$  then  $\chi(b) = \chi(c)$ .

In particular, if  $b$  is relatively prime to  $m$  and  $b \equiv 1 \pmod{m'}$  then  $\chi(b) = \chi(1) = 1$ . Such  $b \bmod m$  form the kernel  $K$  of the reduction homomorphism  $(\mathbf{Z}/m\mathbf{Z})^\times \rightarrow (\mathbf{Z}/m'\mathbf{Z})^\times$ , which is onto (by the Chinese remainder theorem). Thus  $\chi: (\mathbf{Z}/m\mathbf{Z})^\times \rightarrow S^1$  induces a group homomorphism  $(\mathbf{Z}/m\mathbf{Z})^\times/K \rightarrow S^1$  where  $(a \bmod m)K \mapsto \chi(a \bmod m)$ , which can be viewed as a Dirichlet character  $\chi': (\mathbf{Z}/m'\mathbf{Z})^\times \rightarrow S^1$  such that  $\chi'(a \bmod m') = \chi(a \bmod m)$  when  $(a, m) = 1$ . This means  $\chi$  is imprimitive, a contradiction.  $\square$

We will calculate  $|G(\chi)|$  when  $\chi$  is a primitive Dirichlet character, and to do that the following modified Gauss sum will be convenient.

**Definition 3.9.** For a Dirichlet character  $\chi \bmod m$  and  $k \in \mathbf{Z}/m\mathbf{Z}$ , set

$$G_k(\chi) := \sum_{a \bmod m} \chi(a) e^{2\pi i k a / m} = \sum_{(a, m) = 1} \chi(a) \zeta_m^{ka}.$$

The Gauss sum  $G(\chi)$  is  $G_1(\chi)$ . In  $G_k(\chi)$ , we don't require  $k$  to be relatively prime to  $m$ , so  $\zeta_m^k$  might have order less than  $m$ . Every  $m$ th root of unity in  $\mathbf{C}$  is a power  $\zeta_m^k$ , so the Gauss sums  $G_k(\chi)$  are what we get by replacing  $\zeta_m$  in the definition of  $G(\chi)$  with all possible  $m$ th roots of unity in  $\mathbf{C}$ .

**Lemma 3.10.** *If  $\chi$  is a primitive Dirichlet character mod  $m$ , then  $G_k(\chi) = \bar{\chi}(k)G(\chi)$  for all  $k \in \mathbf{Z}$ .*

*Proof.* If  $m = 1$  then  $\chi = \mathbf{1}_1$  and  $G_k(\chi) = 1$  and  $\bar{\chi}(k)G(\chi) = 1$ .

When  $m \geq 2$ , we will treat separately the cases when  $(k, m) = 1$  and  $(k, m) > 1$ .

Case 1:  $(k, m) = 1$ .

Since  $k$  is invertible mod  $m$ ,  $\chi(k) \neq 0$ . In the sum  $G_k(\chi) = \sum_{a \bmod m} \chi(a) \zeta_m^{ka}$ , set  $b = ka$ . Since  $k$  is invertible mod  $m$ , the change of variables  $a \mapsto b = ka$  is a bijection on  $\mathbf{Z}/m\mathbf{Z}$ , and from  $\chi(b) = \chi(k)\chi(a)$  we have  $\chi(a) = \bar{\chi}(k)\chi(b)$  since  $\chi(k) \neq 0$ , so

$$G_k(\chi) = \sum_{b \bmod m} \bar{\chi}(k)\chi(b)\zeta_m^b = \bar{\chi}(k)G(\chi).$$

Note this made no use whatsoever of the primitivity assumption: it holds for all Dirichlet characters mod  $m$ .

Case 2:  $(k, m) > 1$ .

Since  $k$  is not invertible mod  $m$ ,  $\chi(k) = 0$ , so we will show  $G_k(\chi) = 0$ .

Let  $\zeta_m^k$  have order  $m'$ , so  $m' \mid m$  and  $m' < m$ . (Explicitly,  $m' = m/(k, m)$ .) Since  $\chi \bmod m$  is primitive, Lemma 3.8 tells us there are some  $b, c$  relatively prime to  $m$  such that  $b \equiv c \pmod{m'}$  and  $\chi(b) \neq \chi(c)$ . Rewrite  $G_k(\chi)$  by the change of variables  $a \mapsto ab$  in  $(\mathbf{Z}/m\mathbf{Z})^\times$ :

$$(3.1) \quad G_k(\chi) = \sum_{a \bmod m} \chi(ab)\zeta_m^{kab} = \chi(b) \sum_{a \bmod m} \chi(a)\zeta_m^{kab}$$

By making the change of variables  $a \mapsto ac$  in  $(\mathbf{Z}/m\mathbf{Z})^\times$  instead, we get in the same way

$$(3.2) \quad G_k(\chi) = \chi(c) \sum_{a \bmod m} \chi(a) \zeta_m^{kac}.$$

Since  $\zeta_m^k$  has order  $m'$  and  $b \equiv c \pmod{m'}$ ,  $\zeta_m^{kb} = \zeta_m^{kc}$ . Thus

$$(3.3) \quad \sum_{a \bmod m} \chi(a) \zeta_m^{kab} = \sum_{a \bmod m} \chi(a) \zeta_m^{kac}.$$

Since  $\chi(b) \neq \chi(c)$ , (3.1) and (3.2) imply the common sum in (3.3) is 0, so  $G_k(\chi) = 0$ .  $\square$

**Example 3.11.** The mod 8 Dirichlet character  $\chi_8$  (see Example 3.4) is not primitive. Check  $G_2(\chi_8) = 4i$ , so the equation  $G_2(\chi_8) = \overline{\chi_8(2)}G(\chi_8)$  is not true since the right side is 0.

Using Lemma 3.10, here is an analogue of Theorem 2.2(2) for Dirichlet characters.

**Theorem 3.12.** *If  $\chi$  is a primitive Dirichlet character mod  $m$ , then  $|G(\chi)| = \sqrt{m}$ .*

*Proof.* This is easy to check when  $m = 1$ , so take  $m \geq 2$ . We will prove this in the equivalent form  $G(\chi)\overline{G(\chi)} = m$  and proceed as in the proof of Theorem 2.2(2):

$$G(\chi)\overline{G(\chi)} = \sum_{a \bmod m} \chi(a) \zeta_m^a \sum_{b \bmod m} \overline{\chi(b)} \zeta_m^{-b} = \sum_{(b,m)=1} \sum_{a \bmod m} \chi(a) \overline{\chi(b)} \zeta_m^{a-b}.$$

In the inner sum on the right (fixed invertible  $b \bmod m$ ), make the change of variables  $a \mapsto ab$ , so

$$G(\chi)\overline{G(\chi)} = \sum_{(b,m)=1} \sum_{a \bmod m} \chi(a) \chi(b) \overline{\chi(b)} \zeta_m^{ab-b} = \sum_{(b,m)=1} \sum_{a \bmod m} \chi(a) \zeta_m^{ab} \zeta_m^{-b}$$

since  $\chi(b)\overline{\chi(b)} = 1$  when  $(b, m) = 1$ . Thus

$$G(\chi)\overline{G(\chi)} = \sum_{(b,m)=1} G_b(\chi) \zeta_m^{-b}.$$

Since  $\chi \bmod m$  is primitive,  $G_b(\chi) = 0$  if  $(b, m) > 1$  by Lemma 3.10, so we can insert these terms into the sum where  $(b, m) > 1$ :

$$\begin{aligned} G(\chi)\overline{G(\chi)} &= \sum_{b \bmod m} G_b(\chi) \zeta_m^{-b} \\ &= \sum_{b \bmod m} \sum_{a \bmod m} \chi(a) \zeta_m^{ab} \zeta_m^{-b} \\ &= \sum_{a \bmod m} \chi(a) \sum_{b \bmod m} \zeta_m^{b(a-1)}. \end{aligned}$$

The inner sum is a sum of the additive character  $b \mapsto \zeta_m^{b(a-1)}$  over the group  $\mathbf{Z}/m\mathbf{Z}$ , so it is 0 unless this character is trivial, which only occurs when  $a \equiv 1 \pmod{m}$  (since  $\zeta_m$  has order  $m$ ), in which case the sum is  $m$ . Thus  $G(\chi)\overline{G(\chi)} = \chi(1)m = m$ .  $\square$

**Remark 3.13.** If  $\chi \bmod m$  is an imprimitive Dirichlet character,  $G(\chi)$  may be 0 (see the table in Example 3.4) or may not, but always  $|G(\chi)| < \sqrt{m}$ , so primitivity of  $\chi$  is equivalent to  $|G(\chi)| = \sqrt{m}$ .

As with characters of finite fields, a Dirichlet character is called quadratic when its values are  $\pm 1$  and not always 1. Since  $(\mathbf{Z}/m\mathbf{Z})^\times$  has order  $\varphi(m)$ , the Dirichlet characters mod  $m$  are also a group with order  $\varphi(m)$ , which is even when  $m \geq 3$ . Thus there are quadratic Dirichlet characters mod  $m$  when  $m \geq 3$ , but they may not be primitive. Unlike with finite fields, there may be multiple elements of order 2 in  $(\mathbf{Z}/m\mathbf{Z})^\times$  and thus there may be multiple quadratic Dirichlet characters mod  $m$ , *e.g.*, in Example 3.4 we saw there are three quadratic Dirichlet characters mod 8, with two primitive and one imprimitive.

**Corollary 3.14.** *Let  $m \geq 3$  and  $\eta$  be a primitive quadratic Dirichlet character mod  $m$ . Then  $G(\eta)^2 = \eta(-1)m$ .*

*Proof.* Adapt the proof of Corollary 2.3, with Theorem 3.12 in place of Theorem 2.2(2).  $\square$

While  $\eta(-1) = \pm 1$ , we usually can't say (unlike with finite fields) that  $\eta(-1) = 1$  only when  $-1 \pmod m$  is a square. For example, the primitive quadratic Dirichlet character  $\chi'_8 \pmod 8$  in Example 3.4 is 1 at  $-1 \pmod 8$  but  $-1 \pmod 8$  is not a square.

Here is an analogue of Theorem 2.4 for Dirichlet characters.

**Theorem 3.15.** *If the Dirichlet characters  $\chi_1, \chi_2 \pmod m$  have a primitive product, then*

$$G(\chi_1)G(\chi_2) = J(\chi_1, \chi_2)G(\chi_1\chi_2).$$

Most references state this result with an additional assumption that  $\chi_1$  or  $\chi_2$  is primitive. An exception is [2, p. 49], where this result is stated as above, but without proof.

*Proof.* When  $m = 1$ , both sides are 1, so let  $m \geq 2$ .

To begin,

$$G(\chi_1)G(\chi_2) = \sum_{a,b \pmod m} \chi_1(a)\chi_2(b)\zeta_m^{a+b} = \sum_{c \pmod m} \left( \sum_{\substack{a,b \pmod m \\ a+b=c}} \chi_1(a)\chi_2(b) \right) \zeta_m^c.$$

For  $c \in \mathbf{Z}/m\mathbf{Z}$ , set

$$J_c(\chi_1, \chi_2) = \sum_{a \pmod m} \chi_1(a)\chi_2(c-a) = \sum_{\substack{a,b \pmod m \\ a+b=c}} \chi_1(a)\chi_2(b) = \sum_{\substack{a,b \in (\mathbf{Z}/m\mathbf{Z})^\times \\ a+b=c}} \chi_1(a)\chi_2(b).$$

so  $J(\chi_1, \chi_2) = J_1(\chi_1, \chi_2)$  and

$$G(\chi_1)G(\chi_2) = \sum_{c \pmod m} J_c(\chi_1, \chi_2)\zeta_m^c.$$

We'll split up this sum over  $c \pmod m$  into a sum over invertible and noninvertible  $c$ .

When  $(c, m) = 1$ , in  $J_c(\chi_1, \chi_2)$  make the changes of variables  $a \mapsto ac$  and  $b \mapsto bc$  for  $a, b \in (\mathbf{Z}/m\mathbf{Z})^\times$ . Then

$$J_c(\chi_1, \chi_2) = \sum_{\substack{a,b \in (\mathbf{Z}/m\mathbf{Z})^\times \\ ac+bc=c}} \chi_1(ac)\chi_2(bc) = (\chi_1\chi_2)(c) \sum_{\substack{a,b \in (\mathbf{Z}/m\mathbf{Z})^\times \\ a+b=1}} \chi_1(a)\chi_2(b) = (\chi_1\chi_2)(c)J(\chi_1, \chi_2),$$

so

$$\sum_{(c,m)=1} J_c(\chi_1, \chi_2)\zeta_m^c = J(\chi_1, \chi_2) \sum_{(c,m)=1} (\chi_1\chi_2)(c)\zeta_m^c = J(\chi_1, \chi_2)G(\chi_1\chi_2),$$

which is exactly what we want to get. So the sum over noninvertible  $c \bmod m$  must be 0:

$$\sum_{(c,m)>1} J_c(\chi_1, \chi_2) \zeta_m^c \stackrel{?}{=} 0.$$

To prove this, we'll show  $J_c(\chi_1, \chi_2) = 0$  when  $(c, m) > 1$  and  $\chi_1\chi_2$  is primitive.

Write  $J_c(\chi_1, \chi_2)$  as a sum without the restrictions  $a \in (\mathbf{Z}/m\mathbf{Z})^\times$  or  $b \in (\mathbf{Z}/m\mathbf{Z})^\times$ , since  $\chi_1(a)\chi_2(b) = 0$  for other  $a$  and  $b$ :

$$J_c(\chi_1, \chi_2) = \sum_{\substack{a, b \bmod m \\ a+b=c}} \chi_1(a)\chi_2(b).$$

Case 1:  $c = 0$  in  $\mathbf{Z}/m\mathbf{Z}$ . We have

$$J_0(\chi_1, \chi_2) = \sum_{a \bmod m} \chi_1(a)\chi_2(-a) = \chi_2(-1) \sum_{a \bmod m} (\chi_1\chi_2)(a) = \chi_2(-1) \sum_{(a,m)=1} (\chi_1\chi_2)(a).$$

Since  $\chi_1\chi_2$  is primitive, it is nontrivial (the trivial character  $\mathbf{1}_m$  is not primitive when  $m \geq 2$ ) so its sum over  $(\mathbf{Z}/m\mathbf{Z})^\times$  is 0.

Case 2:  $c \neq 0$  in  $\mathbf{Z}/m\mathbf{Z}$  and  $(c, m) > 1$ . Since  $c \notin (\mathbf{Z}/m\mathbf{Z})^\times$  we have  $1 < (c, m) < m$ . Set  $m' = m/(c, m)$ , so  $m'$  is a proper factor of  $m$ .

By primitivity of  $\chi_1\chi_2 \bmod m$  and Lemma 3.8, there are  $u, v$  relatively prime to  $m$  such that  $u \equiv v \bmod m'$  and  $(\chi_1\chi_2)(u) \neq (\chi_1\chi_2)(v)$ . Since  $cm' = (c/(c, m))m$  is a multiple of  $m$ ,  $cu \equiv cv \bmod m$ . Consider

$$J_{cu}(\chi_1, \chi_2) = \sum_{\substack{a, b \bmod m \\ a+b=cu}} \chi_1(a)\chi_2(b)$$

with the change of variables  $a \mapsto au$  and  $b \mapsto bu$ :

$$(3.4) \quad J_{cu}(\chi_1, \chi_2) = \sum_{\substack{a, b \bmod m \\ au+bu=cu}} \chi_1(au)\chi_2(bu) = (\chi_1\chi_2)(u)J_c(\chi_1, \chi_2).$$

By similar reasoning with  $v$  in place of  $u$ ,

$$(3.5) \quad J_{cv}(\chi_1, \chi_2) = (\chi_1\chi_2)(v)J_c(\chi_1, \chi_2).$$

Since  $cu \equiv cv \bmod m$ , comparing (3.4) and (3.5) together with  $(\chi_1\chi_2)(u) \neq (\chi_1\chi_2)(v)$  tells us that  $J_c(\chi_1, \chi_2) = 0$ .  $\square$

Here is an analogue of Corollary 2.5 for Dirichlet characters.

**Corollary 3.16.** *When  $\chi_1, \chi_2$ , and  $\chi_1\chi_2$  are all primitive Dirichlet characters mod  $m$ ,  $|J(\chi_1, \chi_2)| = \sqrt{m}$ .*

*Proof.* By Theorems 3.12 and 3.15,

$$J(\chi_1, \chi_2) = \frac{G(\chi_1)G(\chi_2)}{G(\chi_1\chi_2)}$$

and all terms on the right side have absolute value  $\sqrt{m}$ , so  $|J(\chi_1, \chi_2)| = \sqrt{m}$ .  $\square$

Here is an analogue of Theorem 2.6.

**Theorem 3.17.** *Let  $\chi$  be a primitive character mod  $m$ . Then*

$$(1) \quad J(\mathbf{1}_m, \mathbf{1}_m) = m \prod_{p|m} (1 - 2/p), \text{ where } p \text{ runs over the prime factors of } m,$$

- (2)  $J(\chi, \mathbf{1}_m) = J(\mathbf{1}_m, \chi) = \mu(m)$ ,  
(3)  $J(\chi, \bar{\chi}) = \chi(-1)\mu(m)$ .

*Proof.* If  $m = 1$ , the equations all say  $1 = 1$  (a product over  $p \mid m$  is empty when  $m = 1$  and thus is set equal to 1). Now take  $m \geq 2$ .

Let  $m$  have prime factorization  $p_1^{e_1} \cdots p_r^{e_r}$  where the  $p_i$  are different primes and  $e_i \geq 1$ .

(1) Since  $\mathbf{1}_m$  is 1 at units mod  $m$  and 0 at nonunits,

$$J(\mathbf{1}_m, \mathbf{1}_m) = \sum_{a \bmod m} \mathbf{1}_m(a) \mathbf{1}_m(1-a) = |\{a \in \mathbf{Z}/m\mathbf{Z} : a \text{ and } a-1 \in (\mathbf{Z}/m\mathbf{Z})^\times\}|.$$

Viewing  $\mathbf{Z}/m\mathbf{Z}$  as  $\prod_{i=1}^r \mathbf{Z}/p_i^{e_i}\mathbf{Z}$  by the Chinese remainder theorem,

$$|\{a \in \mathbf{Z}/m\mathbf{Z} : a \text{ and } a-1 \in (\mathbf{Z}/m\mathbf{Z})^\times\}| = \prod_{i=1}^r |\{a_i \in \mathbf{Z}/p_i^{e_i}\mathbf{Z} : a_i \text{ and } a_i-1 \in (\mathbf{Z}/p_i^{e_i}\mathbf{Z})^\times\}|.$$

An integer mod  $p_i^{e_i}$  is *not* a unit exactly when it reduces to 0 modulo  $p_i$ , so

$$\begin{aligned} |\{a_i \in \mathbf{Z}/p_i^{e_i}\mathbf{Z} : a_i \text{ and } a_i-1 \in (\mathbf{Z}/p_i^{e_i}\mathbf{Z})^\times\}| &= p_i^{e_i} - |\{a_i \in \mathbf{Z}/p_i^{e_i}\mathbf{Z} : a_i \equiv 0 \text{ or } 1 \pmod{p_i}\}| \\ &= p_i^{e_i} - 2p_i^{e_i-1} = p_i^{e_i}(1 - 2/p_i). \end{aligned}$$

Thus  $J(\mathbf{1}_m, \mathbf{1}_m) = \prod_{i=1}^r p_i^{e_i}(1 - 2/p_i) = m \prod_{p \mid m} (1 - 2/p)$ .

(2) Since a Jacobi sum is symmetric in its two characters, it suffices to compute

$$J(\chi, \mathbf{1}_m) = \sum_{a \bmod m} \chi(a) \mathbf{1}_m(1-a) = \sum_{\substack{a \bmod m \\ a, a-1 \in (\mathbf{Z}/m\mathbf{Z})^\times}} \chi(a).$$

Viewing  $\mathbf{Z}/m\mathbf{Z}$  as  $\prod_{i=1}^r \mathbf{Z}/p_i^{e_i}\mathbf{Z}$  in the same way as in (1), and  $\chi$  on  $(\mathbf{Z}/m\mathbf{Z})^\times$  as a product of Dirichlet characters  $\chi_i$  on each  $(\mathbf{Z}/p_i^{e_i}\mathbf{Z})^\times$ ,

$$J(\chi, \mathbf{1}_m) = \prod_{i=1}^r \sum_{\substack{a_i \bmod p_i^{e_i} \\ a_i, a_i-1 \in (\mathbf{Z}/p_i^{e_i}\mathbf{Z})^\times}} \chi_i(a_i).$$

The  $i$ th sum on the right omits terms  $a_i \bmod p_i^{e_i}$  such that  $a_i$  or  $a_i - 1$  isn't a unit mod  $p_i^{e_i}$ , which means  $a_i \equiv 0 \pmod{p_i}$  or  $a_i \equiv 1 \pmod{p_i}$ , so

$$\begin{aligned} \sum_{\substack{a_i \bmod p_i^{e_i} \\ a_i, a_i-1 \in (\mathbf{Z}/p_i^{e_i}\mathbf{Z})^\times}} \chi_i(a_i) &= \sum_{a_i \bmod p_i^{e_i}} \chi_i(a_i) - \sum_{\substack{a_i \bmod p_i^{e_i} \\ a_i \equiv 0 \text{ or } 1 \pmod{p_i}}} \chi_i(a_i) \\ &= \sum_{a_i \in (\mathbf{Z}/p_i^{e_i}\mathbf{Z})^\times} \chi_i(a_i) - \sum_{\substack{a_i \in (\mathbf{Z}/p_i^{e_i}\mathbf{Z})^\times \\ a_i \equiv 1 \pmod{p_i}}} \chi_i(a_i). \end{aligned}$$

Since  $\chi \bmod m$  is primitive, each  $\chi_i \bmod p_i^{e_i}$  has to be primitive (why?) and thus nontrivial. That makes the first sum on the right 0. If  $e_i = 1$  then the second sum is  $\chi_i(1) = 1$ , while if  $e_i \geq 2$  then  $\chi_i$  is nontrivial on  $\{a_i \bmod p_i^{e_i} : a_i \equiv 1 \pmod{p_i}\}$ , as otherwise  $\chi_i$  would be a lift of a character mod  $p_i$ , which would contradict primitivity. Thus the left side is  $0 - 1 = -1$  when  $e_i = 1$  and  $0 - 0 = 0$  when  $e_i \geq 2$ , so  $J(\chi, \mathbf{1}_m)$  is  $(-1)^r$  if each  $e_i$  is 1 and is 0 if some  $e_i \geq 2$ , which is the same as  $\mu(m)$  in both cases.

(3) As in (2), view  $\mathbf{Z}/m\mathbf{Z}$  as  $\prod_{i=1}^r \mathbf{Z}/p_i^{e_i}\mathbf{Z}$  and  $\chi$  on  $(\mathbf{Z}/m\mathbf{Z})^\times$  as a product of Dirichlet characters  $\chi_i$  on each  $(\mathbf{Z}/p_i^{e_i}\mathbf{Z})^\times$ , getting  $J(\chi, \bar{\chi}) = \prod_{i=1}^r J(\chi_i, \bar{\chi}_i)$  with each  $\chi_i \bmod p_i^{e_i}$  being primitive. That  $J(\chi, \bar{\chi}) = \chi(-1)\mu(m)$  would follow from the prime-power case:  $J(\chi_i, \bar{\chi}_i) \stackrel{?}{=} \chi_i(-1)\mu(p_i^{e_i})$ . When  $e_i = 1$ , the left side is  $-\chi_i(-1)$  by Theorem 2.6(3) for the finite field  $\mathbf{F}_{p_i}$ . When  $e_i \geq 2$  we want to show  $J(\chi_i, \bar{\chi}_i) = 0$ :

$$J(\chi_i, \bar{\chi}_i) = \sum_{\substack{a \bmod p_i^{e_i} \\ (a, p_i)=1}} \chi_i(a)\bar{\chi}_i(1-a) = \sum_{\substack{a \in (\mathbf{Z}/p_i^{e_i}\mathbf{Z})^\times \\ a \not\equiv 1 \bmod p_i}} \chi_i(a/(1-a))$$

As in the proof of Theorem 2.6(3), the mapping  $a \mapsto b = a/(1-a)$  is a bijection from  $\{a \in (\mathbf{Z}/p_i^{e_i}\mathbf{Z})^\times : a \not\equiv 1 \bmod p_i\}$  to  $\{b \in (\mathbf{Z}/p_i^{e_i}\mathbf{Z})^\times : b \not\equiv -1 \bmod p_i\}$ , so

$$\begin{aligned} J(\chi_i, \bar{\chi}_i) &= \sum_{\substack{b \in (\mathbf{Z}/p_i^{e_i}\mathbf{Z})^\times \\ b \not\equiv -1 \bmod p_i}} \chi_i(b) \\ &= \chi_i(-1) \sum_{\substack{b \in (\mathbf{Z}/p_i^{e_i}\mathbf{Z})^\times \\ b \not\equiv 1 \bmod p_i}} \chi_i(b) \\ &= \chi_i(-1) \sum_{\substack{b \in (\mathbf{Z}/p_i^{e_i}\mathbf{Z})^\times \\ b \equiv 1 \bmod p_i}} \chi_i(b) - \chi_i(-1) \sum_{\substack{b \in (\mathbf{Z}/p_i^{e_i}\mathbf{Z})^\times \\ b \equiv 1 \bmod p_i}} \chi_i(b). \end{aligned}$$

The two sums on the last line are exactly the same as at the end of the proof of (2), so they both vanish when  $e_i \geq 2$ . Thus  $J(\chi_i, \bar{\chi}_i) = 0$  when  $e_i \geq 2$ .  $\square$

Finally, here is an analogue of Theorem 2.8.

**Theorem 3.18.** *If  $\chi \bmod m$  is primitive then  $G(\chi)G(\bar{\chi}) \neq J(\chi, \bar{\chi})G(\chi\bar{\chi})$ .*

*Proof.* The reasoning is just like that in the proof of Theorem 2.8. For the left side,

$$\overline{G(\chi)} = \sum_{a \bmod m} \bar{\chi}(a)\zeta_m^{-a} = \sum_{a \bmod m} \bar{\chi}(-a)\zeta_m^a = \bar{\chi}(-1) \sum_{a \bmod m} \bar{\chi}(a)\zeta_m^a = \chi(-1)G(\bar{\chi})$$

since  $\chi(-1) = \pm 1$ , so  $\bar{\chi}(-1) = \chi(-1)$ . Thus  $G(\bar{\chi}) = \chi(-1)\overline{G(\chi)}$ , so

$$(3.6) \quad G(\chi)G(\bar{\chi}) = G(\chi)\chi(-1)\overline{G(\chi)} = \chi(-1)|G(\chi)|^2 = \chi(-1)m.$$

For the right side, Example 3.2 and Theorem 3.17(3) tell us

$$J(\chi, \bar{\chi})G(\chi\bar{\chi}) = \chi(-1)\mu(m)G(\mathbf{1}_m) = \chi(-1)\mu(m)^2 = \chi(-1)|\mu(m)|,$$

which is 0 or  $\pm 1$ , and thus it is not  $\chi(-1)m$ .  $\square$

#### 4. GAUSS AND JACOBI SUMS ON FINITE COMMUTATIVE RINGS

In this last section, which is based partly on [5, Sect. 5], we will define Gauss and Jacobi sums on certain finite commutative rings. This will include as special cases what we saw previously on  $\mathbf{F}_q$  and  $\mathbf{Z}/m\mathbf{Z}$ . In particular, we'll prove a formula for the absolute value of a Gauss sum and a relation between Gauss and Jacobi sums. Gauss sums on finite commutative rings go back to Lamprecht's 1953 PhD thesis [4].

**Theorem 4.1.** *Let  $R$  be a finite commutative ring. For an additive character  $\psi: R \rightarrow S^1$  and  $r \in R$ , set  $\psi_r: R \rightarrow S^1$  by  $\psi_r(x) = \psi(rx)$ .*

- (1) Each  $\psi_r$  is an additive character on  $R$ .  
(2) The following conditions are equivalent: (i)  $\psi_r$  is the trivial character only when  $r = 0$  and (ii) every additive character of  $R$  is  $\psi_r$  for a unique  $r \in R$ .

*Proof.* (1) It's straightforward to show  $\psi_r$  is an additive character on  $R$ .

(2) Let  $\widehat{R}$  denote the set of additive characters on  $R$ . Since  $\psi_r \cdot \psi_s = \psi_{r+s}$  in  $\widehat{R}$ , we get a group homomorphism  $R \rightarrow \widehat{R}$  by  $r \mapsto \psi_r$ . Condition (i) says this homomorphism is injective and condition (ii) says this homomorphism is bijective. Since  $R$  is finite,  $|\widehat{R}| = |R|$ , so injectivity is equivalent to bijectivity.  $\square$

Since  $r \mapsto \psi_r$  is a group homomorphism, condition (ii) in part (2) of Theorem 4.1 is equivalent to saying  $R$  is isomorphic to its character group by  $r \mapsto \psi_r$ . We'll call such  $\psi$  a *self-dual additive character* on  $R$ .<sup>5</sup>

**Example 4.2.** When  $R = \mathbf{F}_q$  is a finite field of characteristic  $p$ , let  $\psi: R \rightarrow S^1$  by  $\psi(a) = e^{2\pi i \text{Tr}(a)/p}$ . If  $\psi_r$  is trivial then  $\text{Tr}(ra) = 0$  in  $\mathbf{F}_p$  for all  $a \in \mathbf{F}_q$ , so  $\text{Tr}(r\mathbf{F}_q) = 0$ . For nonzero  $r$ ,  $r\mathbf{F}_q = \mathbf{F}_q$ , so  $\text{Tr}(\mathbf{F}_q) = \{0\}$ , which is not true since  $\text{Tr}: \mathbf{F}_q \rightarrow \mathbf{F}_p$  is onto. Thus  $\psi_r$  is trivial only when  $r = 0$ , making  $\psi$  a self-dual additive character on  $\mathbf{F}_q$ .

**Example 4.3.** When  $R = \mathbf{Z}/m\mathbf{Z}$  for some  $m \geq 2$ , let  $\psi: R \rightarrow S^1$  by  $\psi(a) = e^{2\pi i a/m}$ . If  $\psi_r$  is trivial then  $1 = \psi_r(1) = e^{2\pi i r/m}$ , so  $r = 0$  in  $\mathbf{Z}/m$ . Thus  $\psi$  is a self-dual additive character on  $\mathbf{Z}/m\mathbf{Z}$ .

**Theorem 4.4.** *If  $R$  and  $R'$  are finite commutative rings, then  $R \times R'$  has a self-dual additive character if and only if  $R$  and  $R'$  do.*

*Proof.* First we'll assume  $R$  and  $R'$  have self-dual additive characters, say  $\psi$  and  $\psi'$ . Then  $\varphi: R \times R' \rightarrow S^1$  by  $\varphi(x, x') = \psi(x)\psi'(x')$  is an additive character on  $R \times R'$ . For  $(r, r')$  in  $R \times R'$ , assume  $\varphi_{(r, r')}$  is trivial:  $\psi(rx)\psi'(r'x') = 1$  for all  $(x, x') \in R \times R'$ . Setting  $x' = 0$ ,  $\psi(rx) = 0$  for all  $x \in R$ , so  $r = 0$  by the self-duality of  $\psi$ . Similarly,  $r' = 0$ , so  $(r, r') = (0, 0)$ . Thus  $\varphi$  is a self-dual additive character on  $R \times R'$ .

Next assume  $R \times R'$  has a self-dual additive character, say  $\varphi$ . Every character on a direct product of finite abelian groups is a product of characters on the factors, so there are additive characters  $\psi$  and  $\psi'$  on  $R$  and  $R'$ , respectively, such that  $\varphi(x, x') = \psi(x)\psi'(x')$  for all  $x \in R$  and  $x' \in R'$ . For  $r \in R$ , if  $\psi(rx) = 0$  for all  $x \in R$  then  $\varphi_{(r, 0)}(x, x') = \psi(rx)\psi'(0) = 1$  for all  $(x, x') \in R \times R'$ , so  $(r, 0) = (0, 0)$  by self-duality of  $\varphi$ . Thus  $r = 0$ , so  $\psi$  is self-dual on  $R$ . Similarly,  $\psi'$  is self-dual on  $R'$ .  $\square$

**Remark 4.5.** Every finite commutative ring  $R$  is a direct product of local rings, so Theorem 4.4 tells us that  $R$  has a self-dual additive character if and only if its local pieces do.

**Remark 4.6.** A finite commutative ring that does *not* have a self-dual additive character is  $R = \mathbf{F}_p[u, v]/(u, v)^2 = \{a + bu + cv : a, b, c \in \mathbf{F}_p, u^2 = uv = v^2 = 0\}$ . We'll show for each additive character  $\psi: R \rightarrow S^1$  that there is a nonzero  $r$  in  $R$  such that  $\psi_r$  is trivial.

The values of  $\psi$  are  $p$ th roots of unity, so  $\psi(ax) = \psi(x)^a$  for all  $a \in \mathbf{F}_p$  and  $x \in R$ . Letting  $r = Bu + Cv$  for unknown  $B$  and  $C$ ,

$$\psi_r(a + bu + cv) = \psi((Bu + Cv)(a + bu + cv)) = \psi(a(Bu + Cv)) = (\psi(u)^B \psi(v)^C)^a,$$

<sup>5</sup>Lamprecht [4, p. 154] called such additive characters “echt,” which is German for “genuine” (translating it as “real” in math could be misleading).

so we'll find  $B$  and  $C$  in  $\mathbf{F}_p$  not both 0 such that  $\psi(u)^B \psi(v)^C = 1$ . If  $\psi(u) = 1$  then use  $B = 1$  and  $C = 0$  (so  $r = u$ ). If  $\psi(u) \neq 1$  then  $\psi(u)$  has order  $p$ , so  $\psi(v) = \psi(u)^k$  for some  $k \in \mathbf{F}_p$ . Use  $B = -k$  and  $C = 1$  (so  $r = -ku + v$ ).

From now on we will work with a finite commutative ring  $R$  that has a self-dual additive character  $\psi$ . A *multiplicative character* on  $R$  is a character on the unit group  $R^\times$ , which is extended to a function on  $R$  by setting it equal to 0 on the nonunits (including for the trivial multiplicative character on  $R$ ).

**Definition 4.7.** For a multiplicative character  $\chi$  on  $R$ , its *Gauss sum* is

$$G(\chi) = \sum_{a \in R} \chi(a) \psi(a).$$

For two multiplicative characters  $\chi_1$  and  $\chi_2$  on  $R$ , their *Jacobi sum* is

$$J(\chi_1, \chi_2) = \sum_{a \in R} \chi_1(a) \chi_2(1 - a).$$

The Gauss sum  $G(\chi)$  depends on the choice of self-dual additive character  $\psi$  on  $R$ , but we don't include  $\psi$  in the notation.

Since multiplicative characters are 0 on nonunits, we only need to sum over the units of  $R$  in Gauss and Jacobi sums:

$$G(\chi) = \sum_{a \in R^\times} \chi(a) \psi(a) \quad \text{and} \quad J(\chi_1, \chi_2) = \sum_{a \in R^\times} \chi_1(a) \chi_2(1 - a).$$

**Definition 4.8.** A multiplicative character  $\chi$  on  $R$  is called *imprimitive* if there is a nonzero ideal  $I$  in  $R$  such that whenever  $a, b \in R^\times$  satisfy  $a \equiv b \pmod{I}$ ,  $\chi(a) = \chi(b)$ . A multiplicative character on  $R$  that is not imprimitive is called *primitive*.

**Example 4.9.** When  $R \neq 0$ , the trivial multiplicative character on  $R$  is imprimitive, using  $I = R$ , so primitive characters on  $R$  are nontrivial.

**Example 4.10.** The trivial multiplicative character on the zero ring is primitive.

**Example 4.11.** When  $R = \mathbf{F}_q$ , its only nonzero ideal is  $R$ , so an imprimitive multiplicative character on  $\mathbf{F}_q$  is trivial. Thus the primitive multiplicative characters on a finite field are its nontrivial multiplicative characters.

**Example 4.12.** When  $R = \mathbf{Z}/m\mathbf{Z}$  for  $m \geq 1$ , its ideals are  $m'\mathbf{Z}/m\mathbf{Z}$  where  $m' \mid m$  and a primitive multiplicative character on  $\mathbf{Z}/m\mathbf{Z}$  is exactly the same thing as a primitive Dirichlet character mod  $m$ .

**Definition 4.13.** For a multiplicative character  $\chi$  on  $R$  and  $r \in R$ , set

$$G_r(\chi) = \sum_{a \in R} \chi(a) \psi_r(a) = \sum_{a \in R} \chi(a) \psi(ra) = \sum_{a \in R^\times} \chi(a) \psi(ra).$$

Since all additive characters on  $R$  have the form  $\psi_r$  for some  $r$ , the sums  $G_r(\chi)$  as  $r$  varies are just the usual Gauss sums  $G(\chi)$  with  $\psi$  in its definition replaced by the other additive characters on  $R$ .

**Lemma 4.14.** *When  $R$  is a finite commutative ring and  $I$  is an ideal in  $R$ , the reduction mapping  $R^\times \rightarrow (R/I)^\times$  is surjective.*

*Proof.* This is true when  $R$  is the zero ring, so we can assume now that  $R \neq 0$ .

Every nonzero finite ring is a direct product of local rings:  $R \cong R_1 \times \cdots \times R_k$  where each  $R_j$  is a local ring. The ideals in a product ring are products of ideals, so that ring isomorphism identifies  $I$  in  $R$  with  $I_1 \times \cdots \times I_k$  where  $I_j$  is an ideal in  $R_j$ . The surjectivity of  $R^\times \rightarrow (R/I)^\times$  would be a consequence of surjectivity of  $R_j^\times \rightarrow (R_j/I_j)^\times$  for all  $j$ , where  $R_j$  is a local ring.

That  $R_j^\times \rightarrow (R_j/I_j)^\times$  is surjective for a local ring  $R_j$  is clear if  $I_j = R_j$ , so we may assume  $I_j \neq R_j$ . Then  $I_j \subset M_j$  where  $M_j$  is the unique maximal ideal of  $R_j$ . For  $\bar{a} \in (R_j/I_j)^\times$ ,  $ab \equiv 1 \pmod{I_j}$  for some  $b \in R_j$ , so  $ab$  is in  $1 + I_j$ , which is disjoint from  $M_j$ . Thus  $1 + I_j \subset R_j^\times$  (nonunits in  $R_j$  are contained in  $M_j$ ), so  $ab \in R_j^\times$ , which implies  $a \in R_j^\times$ .<sup>6</sup>  $\square$

**Lemma 4.15.** *If  $\chi$  is a primitive multiplicative character on  $R$ , then for each nonzero ideal  $I$  in  $R$ , there are some  $b, c$  in  $R^\times$  such that  $b \equiv c \pmod{I}$  and  $\chi(b) \neq \chi(c)$ .*

*Proof.* The argument will be like that for Lemma 3.8, using contradiction.

If the result is false then there is a nonzero ideal  $I$  in  $R$  such that for all  $b, c$  in  $R^\times$ , if  $b \equiv c \pmod{I}$  then  $\chi(b) = \chi(c)$ .

Thus if  $b \in R^\times$  and  $b \equiv 1 \pmod{I}$ , then  $\chi(b) = \chi(1) = 1$ . These  $b$  form the kernel  $K$  of the natural homomorphism  $R^\times \rightarrow (R/I)^\times$ , which is onto by Lemma 4.14. Thus  $\chi: R^\times \rightarrow S^1$  induces a group homomorphism  $R^\times/K \rightarrow S^1$  where  $aK \mapsto \chi(a)$ , which can be viewed as a multiplicative character  $\chi': (R/I)^\times \rightarrow S^1$  such that  $\chi'(a \pmod{I}) = \chi(a)$  for all  $a \in R^\times$ . This means  $\chi$  is imprimitive, a contradiction.  $\square$

**Lemma 4.16.** *If  $\chi$  is a primitive multiplicative character on  $R$  then  $G_r(\chi) = \bar{\chi}(r)G(\chi)$  for all  $r \in R$ .*

*Proof.* When  $R = 0$ , both sides of the equation are 1, so now let  $R \neq 0$ . As in the proof of Lemma 3.10, we will consider separately  $r \in R^\times$  and  $r \notin R^\times$ .

Case 1:  $r \in R^\times$ .

The argument is identical to that of Case 1 in the proof of Lemma 3.10.

Case 2:  $r \notin R^\times$ .

If  $r = 0$  then  $G_r(\chi) = \sum_{a \in R^\times} \chi(a) = 0$  since primitive multiplicative characters on  $R$  are nontrivial. Now let  $r \neq 0$ .

The rest of the argument is like that of Case 2 in the proof of Lemma 3.10. Since  $r \notin R^\times$ , the mapping  $f: R \rightarrow R$  where  $f(x) = rx$  is not surjective, so it's not injective: there is some nonzero  $s \in R$  such that  $rs = 0$ . Then the ideal  $I = Rs$  is nonzero (since  $s \neq 0$ ).

Since  $\chi$  is primitive, by Lemma 4.15 there are some  $b, c$  in  $R^\times$  such that  $b \equiv c \pmod{I}$  and  $\chi(b) \neq \chi(c)$ . Making the change of variables  $a \mapsto ab$  in  $R$ ,

$$(4.1) \quad G_r(\chi) = \sum_{a \in R} \chi(ab)\psi(rab) = \chi(b) \sum_{a \in R} \chi(a)\psi(rab).$$

Using the change of variables  $a \mapsto ac$  on  $R$ , we similarly get

$$(4.2) \quad G_r(\chi) = \chi(c) \sum_{a \in R} \chi(a)\psi(rac).$$

---

<sup>6</sup>This result is easy to see in the special case  $R_j = \mathbf{Z}/p^n\mathbf{Z}$  for prime  $p$  and  $n \geq 2$ : a unit mod  $p^n$  is a congruence class not divisible by  $p$ , so  $(\mathbf{Z}/p^n\mathbf{Z})^\times \rightarrow (\mathbf{Z}/p^{n'}\mathbf{Z})^\times$  is onto for  $1 \leq n' < n$  because when  $a \pmod{p^{n'}}$  is a unit,  $p \nmid a$ , so  $a \pmod{p^n}$  is a unit.

Since  $b \equiv c \pmod{I}$  and  $rI = rsR = \{0\}$ , we have  $rb = rc$ , so  $\psi(rab) = \psi(rac)$  for all  $a \in R$ . Thus

$$(4.3) \quad \sum_{a \in R} \chi(a)\psi(rab) = \sum_{a \in R} \chi(a)\psi(rac).$$

Using (4.1), (4.2), and  $\chi(b) \neq \chi(c)$ , the common sum in (4.3) is 0, so  $G_r(\chi) = 0$ .  $\square$

**Theorem 4.17.** *If  $\chi$  is a primitive multiplicative character on  $R$  then  $|G(\chi)| = \sqrt{|R|}$ .*

*Proof.* If  $R = 0$  then  $\chi = \mathbf{1}_R$  is 1 on  $R$  and  $G(\chi) = 1$ , so we're done. Now take  $R \neq 0$ .

We will prove  $|G(\chi)| = \sqrt{|R|}$  in the equivalent form  $G(\chi)\overline{G(\chi)} = |R|$  by modifying the proof of Theorem 3.12:

$$\begin{aligned} G(\chi)\overline{G(\chi)} &= \sum_{a \in R} \chi(a)\psi(a) \sum_{b \in R} \overline{\chi}(b)\psi(-b) \\ &= \sum_{a, b \in R} \chi(a)\overline{\chi}(b)\psi(a)\psi(-b) \\ &= \sum_{b \in R^\times} \sum_{a \in R} \chi(a/b)\psi(a)\psi(-b). \end{aligned}$$

In the inner sum, make the change of variables  $a \mapsto ab$ :

$$G(\chi)\overline{G(\chi)} = \sum_{b \in R^\times} \sum_{a \in R} \chi(a)\psi(ab)\psi(-b) = \sum_{b \in R^\times} \left( \sum_{a \in R} \chi(a)\psi(ab) \right) \psi(-b),$$

so

$$G(\chi)\overline{G(\chi)} = \sum_{b \in R^\times} G_b(\chi)\psi(-b).$$

Since  $\chi$  is primitive,  $G_b(\chi) = 0$  if  $b \notin R^\times$  by Lemma 4.16, so terms at  $b \notin R^\times$  can be put in the sum:

$$\begin{aligned} G(\chi)\overline{G(\chi)} &= \sum_{b \in R} G_b(\chi)\psi(-b) \\ &= \sum_{b \in R} \sum_{a \pmod{m}} \chi(a)\psi(ab)\psi(-b) \\ &= \sum_{a \in R} \chi(a) \sum_{b \in R} \psi((a-1)b). \end{aligned}$$

When  $a \neq 1$ , the additive character  $x \mapsto \psi((a-1)x)$  on  $R$  is nontrivial (since  $\psi$  is self-dual), so the inner sum is 0. At  $a = 1$ , the inner sum is  $|R|$ , so  $G(\chi)\overline{G(\chi)} = \chi(1)|R| = |R|$ .  $\square$

**Remark 4.18.** Since  $\overline{G(\chi)} = \sum_{a \in R} \overline{\chi}(a)\psi(-a) = \chi(-1)G(\overline{\chi})$ , the relation  $G(\chi)\overline{G(\chi)} = |R|$  for primitive  $\chi$  is equivalent to  $G(\chi)G(\overline{\chi}) = \chi(-1)|R|$ , which has (2.2) and (3.6) as special cases. In particular, if  $R^\times$  has a primitive quadratic character  $\eta$ , then  $G(\eta)^2 = \eta(-1)|R|$ .

**Theorem 4.19.** *If  $\chi_1$  and  $\chi_2$  are multiplicative characters on  $R$  whose product  $\chi_1\chi_2$  is primitive, then*

$$G(\chi_1)G(\chi_2) = J(\chi_1, \chi_2)G(\chi_1\chi_2).$$

*Proof.* When  $R = 0$ , both sides are 1. When  $R \neq 0$ , we'll modify the proof of Theorem 3.15, starting with

$$G(\chi_1)G(\chi_2) = \sum_{a,b \in R} \chi_1(a)\chi_2(b)\psi(a+b) = \sum_{c \in R} \left( \sum_{\substack{a,b \in R \\ a+b=c}} \chi_1(a)\chi_2(b) \right) \psi(c).$$

For  $c \in R$ , set

$$J_c(\chi_1, \chi_2) = \sum_{a \in R} \chi_1(a)\chi_2(c-a) = \sum_{\substack{a,b \in R \\ a+b=c}} \chi_1(a)\chi_2(b) = \sum_{\substack{a,b \in R^\times \\ a+b=c}} \chi_1(a)\chi_2(b).$$

Then

$$G(\chi_1)G(\chi_2) = \sum_{c \in R} J_c(\chi_1, \chi_2)\psi(c).$$

For  $c \in R^\times$ , the changes of variables  $a \mapsto ac$  and  $b \mapsto bc$  for  $a, b \in R^\times$  makes

$$J_c(\chi_1, \chi_2) = \sum_{\substack{a,b \in R^\times \\ ac+bc=c}} \chi_1(ac)\chi_2(bc) = (\chi_1\chi_2)(c) \sum_{\substack{a,b \in R^\times \\ a+b=1}} \chi_1(a)\chi_2(b) = (\chi_1\chi_2)(c)J(\chi_1, \chi_2),$$

so

$$\sum_{c \in R^\times} J_c(\chi_1, \chi_2)\zeta_m^c = J(\chi_1, \chi_2) \sum_{c \in R^\times} (\chi_1\chi_2)(c)\psi(c) = J(\chi_1, \chi_2)G(\chi_1\chi_2).$$

It remains to show  $J_c(\chi_1, \chi_2) = 0$  when  $c \notin R^\times$  and  $\chi_1\chi_2$  is primitive.

Since  $\chi_1(a)\chi_2(b) = 0$  when  $a$  or  $b$  is not in  $R^\times$ ,

$$J_c(\chi_1, \chi_2) = \sum_{\substack{a,b \in R \\ a+b=c}} \chi_1(a)\chi_2(b).$$

Case 1:  $c = 0$ . We have

$$J_0(\chi_1, \chi_2) = \sum_{a \in R} \chi_1(a)\chi_2(-a) = \chi_2(-1) \sum_{a \in R} (\chi_1\chi_2)(a) = \chi_2(-1) \sum_{a \in R^\times} (\chi_1\chi_2)(a).$$

Since  $\chi_1\chi_2$  is primitive, it is nontrivial (see Example 4.9), so its sum over  $R^\times$  is 0.

Case 2:  $c \neq 0$  and  $c \notin R^\times$ .

As in the proof of Case 2 of Lemma 4.16, there is a nonzero ideal  $I$  in  $R$  such that  $cI = \{0\}$ . By primitivity of  $\chi_1\chi_2$  and Lemma 4.15, there are  $u, v$  in  $R^\times$  such that  $u \equiv v \pmod{I}$  and  $(\chi_1\chi_2)(u) \neq (\chi_1\chi_2)(v)$ . Since  $cI = \{0\}$ ,  $cu = cv$ . Consider

$$J_{cu}(\chi_1, \chi_2) = \sum_{\substack{a,b \in R \\ a+b=cu}} \chi_1(a)\chi_2(b)$$

with the change of variables  $a \mapsto au$  and  $b \mapsto bu$ :

$$(4.4) \quad J_{cu}(\chi_1, \chi_2) = \sum_{\substack{a,b \in R \\ au+bu=cu}} \chi_1(au)\chi_2(bu) = (\chi_1\chi_2)(u)J_c(\chi_1, \chi_2).$$

Using  $v$  in place of  $u$ ,

$$(4.5) \quad J_{cv}(\chi_1, \chi_2) = (\chi_1\chi_2)(v)J_c(\chi_1, \chi_2).$$

Since  $cu = cv$ , comparing (4.4) and (4.5) together with  $(\chi_1\chi_2)(u) \neq (\chi_1\chi_2)(v)$  tells us that  $J_c(\chi_1, \chi_2) = 0$ .  $\square$

**Corollary 4.20.** *If  $\chi_1$  and  $\chi_2$  are multiplicative characters on  $R$  such that  $\chi_1, \chi_2$ , and  $\chi_1\chi_2$  are all primitive, then  $|J(\chi_1, \chi_2)| = \sqrt{|R|}$ .*

*Proof.* We have  $J(\chi_1, \chi_2) = G(\chi_1)G(\chi_2)/G(\chi_1\chi_2)$  by Theorem 4.19, and all three terms on the right have absolute value  $\sqrt{|R|}$  by Theorem 4.17.  $\square$

A question we have not addressed is: why should we care about Gauss and Jacobi sums on a finite commutative ring  $R$ ? Here are two constructions on  $R$  that are related to classical Fourier analysis, and lead in special cases to Gauss and Jacobi sums.

Let  $A$  be a finite abelian group (written additively) with character group  $\widehat{A}$ . For a function  $f: A \rightarrow \mathbf{C}$ , its *Fourier transform* is the function  $\widehat{f}: \widehat{A} \rightarrow \mathbf{C}$  where

$$\widehat{f}(\chi) = \sum_{a \in A} f(a)\overline{\chi}(a).$$

For two functions  $f_1, f_2: A \rightarrow \mathbf{C}$ , their *convolution* is the function  $f_1 * f_2: A \rightarrow \mathbf{C}$  where

$$(f_1 * f_2)(x) = \sum_{a \in A} f_1(a)f_2(x - a).$$

Let's look at the Fourier transform and convolution of primitive multiplicative characters on  $R$ , viewed as functions on  $R$  by setting them to be 0 on the nonunits.

**Theorem 4.21.** *Let  $\chi$  be a primitive multiplicative character on  $R$  with self-dual additive character  $\psi$ . Viewing  $\chi$  as a function on  $R$ ,  $\widehat{\chi}(\psi_r) = \chi(-1)G(\chi)\overline{\chi}(r)$  for all  $r \in R$ .*

*Proof.* We have

$$\widehat{\chi}(\psi_r) = \sum_{a \in R} \chi(a)\overline{\psi_r}(a) = \sum_{a \in R} \chi(a)\psi(-ra) = \chi(-1) \sum_{a \in R} \chi(a)\psi(ra) = \chi(-1)G_r(\chi).$$

By Lemma 4.16,  $G_r(\chi) = G(\chi)\overline{\chi}(r)$  for all  $r \in R$ , so  $\widehat{\chi}(\psi_r) = \chi(-1)G(\chi)\overline{\chi}(r)$ .  $\square$

**Theorem 4.22.** *Let  $\chi_1$  and  $\chi_2$  be multiplicative characters on  $R$  whose product is primitive. Viewing  $\chi_1$  and  $\chi_2$  as functions on  $R$ ,  $(\chi_1 * \chi_2)(r) = J(\chi_1, \chi_2)(\chi_1\chi_2)(r)$  for all  $r \in R$ .*

*Proof.* We have

$$(\chi_1 * \chi_2)(r) = \sum_{a \in R} \chi_1(a)\chi_2(r - a) = J_r(\chi_1, \chi_2),$$

and by the proof of Theorem 4.19,  $J_r(\chi_1, \chi_2) = J(\chi_1, \chi_2)(\chi_1\chi_2)(r)$  when  $r \in R^\times$  and  $J_r(\chi_1, \chi_2) = 0$  when  $r \notin R^\times$  because  $\chi_1\chi_2$  is primitive. Since  $(\chi_1\chi_2)(r) = 0$  when  $r \notin R^\times$ ,  $J_r(\chi_1, \chi_2) = J(\chi_1, \chi_2)(\chi_1\chi_2)(r)$  for all  $r \in R$ .  $\square$

## APPENDIX A. ANALOGIES WITH INTEGRALS

It was noticed long ago that Gauss and Jacobi sums are discrete analogues of two functions defined by integrals in analysis: the Gamma function  $\Gamma(s)$  and the Beta function  $B(s, t)$ , where

$$\Gamma(s) = \int_0^\infty x^{s-1}e^{-x} dx = \int_0^\infty x^s e^{-x} \frac{dx}{x}, \quad B(s, t) = \int_0^1 x^{s-1}(1-x)^{t-1} dx$$

for  $s, t > 0$ . (These integrals make sense for complex  $s$  and  $t$  with positive imaginary parts, but for simplicity we just use real variables.) The Gamma function satisfies several analytic identities, such as the reflection formula<sup>7</sup>

$$(A.1) \quad \Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}$$

for  $0 < s < 1$  and the duplication formula

$$(A.2) \quad \Gamma(2s) = \frac{2^{2s-1}}{\sqrt{\pi}} \Gamma(s)\Gamma\left(s + \frac{1}{2}\right),$$

which is the special case  $n = 2$  of the multiplication formula

$$(A.3) \quad \Gamma(ns) = \frac{n^{ns-1/2}}{(2\pi)^{(n-1)/2}} \Gamma(s)\Gamma\left(s + \frac{1}{n}\right)\Gamma\left(s + \frac{2}{n}\right)\cdots\Gamma\left(s + \frac{n-1}{n}\right)$$

for  $n \in \mathbf{Z}^+$ .

How does  $G(\chi) = \sum_{a \in R} \chi(a)\psi(a)$  resemble  $\Gamma(s) = \int_0^\infty x^{s-1}e^{-x} dx$ ? In  $G(\chi)$  we have a multiplicative character  $\chi$  on  $R^\times$  and an additive character  $\psi$  on  $R$ . These are analogous to  $x \mapsto x^{s-1}$  (or  $x \mapsto x^s$ ) and  $x \mapsto e^{-x}$  in the Gamma integral since  $\chi(ab) = \chi(a)\chi(b)$  is like  $(xy)^{s-1} = x^{s-1}y^{s-1}$  and  $\psi(a+b) = \psi(a)\psi(b)$  is like  $e^{-(x+y)} = e^{-x}e^{-y}$ . The terms  $\chi_1(a)\chi_2(1-a)$  in  $J(\chi_1, \chi_2)$  resemble the integrand  $x^{s-1}(1-x)^{t-1}$  in  $B(s, t)$ . The formula  $J(\chi_1, \chi_2) = G(\chi_1)G(\chi_2)/G(\chi_1\chi_2)$  (when  $\chi_1\chi_2$  is primitive) resembles the following relation between the Beta and Gamma functions:

$$B(s, t) = \frac{\Gamma(s)\Gamma(t)}{\Gamma(s+t)}.$$

Reflection formula. The Gauss sum analogue of (A.1) is  $G(\chi)G(\bar{\chi}) = \chi(-1)|R|$  for primitive  $\chi$ . Taking  $s = 1/2$  in the reflection formula, we get  $\Gamma(1/2)^2 = \pi$ , so

$$(A.4) \quad \Gamma(1/2) = \sqrt{\pi}$$

since  $\Gamma(1/2) > 0$ . Since  $x \mapsto x^{1/2} = \sqrt{x}$  is a multiplicative function that squares to the identity function  $x \mapsto x$ , its analogue on  $R$  is a quadratic multiplicative character  $\eta$  (so  $\eta^2 = \mathbf{1}_R$  and  $\eta \neq \mathbf{1}_R$ ). When  $\eta$  is primitive quadratic, we saw in Remark 4.18 that  $G(\eta)^2 = \eta(-1)|R|$ , so the Gauss sum analogue of (A.4) is

$$\eta \text{ primitive quadratic} \implies G(\eta) = \pm\sqrt{\eta(-1)|R|}.$$

We can't say for sure which sign on the right side is correct:  $G(\eta)$  depends implicitly on a self-dual additive character  $\psi$  and changing this to another self-dual character could change  $G(\eta)$  by a sign. Consider the special case where  $R = \mathbf{F}_p$  is a field with odd prime order, whose only quadratic character is the Legendre symbol  $\eta = \left(\frac{\cdot}{p}\right)$ , so  $\eta(-1) = \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ . Using as  $\psi$  the standard additive character  $a \mapsto e^{2\pi ia/p}$ ,  $G(\eta) = \sum_{a \bmod p} \left(\frac{a}{p}\right) e^{2\pi ia/p}$  is  $\pm\sqrt{p}$  if  $p \equiv 1 \pmod{4}$  and is  $\pm i\sqrt{p}$  if  $p \equiv 3 \pmod{4}$ . With this specific choice of  $\psi$  in the sum, Gauss conjectured by numerical data that the sign is  $+$  in both cases, and it took him *four years* to prove that:

$$\sum_{a \bmod p} \left(\frac{a}{p}\right) e^{2\pi ia/p} = \begin{cases} \sqrt{p}, & \text{if } p \equiv 1 \pmod{4}, \\ i\sqrt{p}, & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

<sup>7</sup>When  $\Gamma(s)$  is extended to the whole real line or complex plane using integration by parts, the reflection formula holds for  $s$  outside the interval  $(0, 1)$ .

When  $q = p^f$  is an odd prime power, the quadratic character of  $\mathbf{F}_q^\times$  is  $\eta(a) = \left(\frac{N_{\mathbf{F}_q/\mathbf{F}_p}(a)}{p}\right)$ . Using  $\psi(a) = e^{2\pi i \text{Tr}_{\mathbf{F}_q/\mathbf{F}_p}(a)/p}$  as the self-dual additive character of  $\mathbf{F}_q$ , the Hasse–Davenport relation for Gauss sums of liftings of characters from  $\mathbf{F}_p$  to  $\mathbf{F}_q$  [3, Theorem 1, p. 162] says

$$\begin{aligned} -G(\eta) &= - \sum_{a \in \mathbf{F}_q} \left(\frac{N_{\mathbf{F}_q/\mathbf{F}_p}(a)}{p}\right) e^{2\pi i \text{Tr}_{\mathbf{F}_q/\mathbf{F}_p}(a)/p} = \left( - \sum_{a \bmod p} \left(\frac{a}{p}\right) e^{2\pi i a/p} \right)^f \\ &= \begin{cases} (-1)^f \sqrt{q}, & \text{if } p \equiv 1 \pmod{4}, \\ (-1)^f i^f \sqrt{q}, & \text{if } p \equiv 3 \pmod{4}. \end{cases} \end{aligned}$$

Duplication and multiplication formulas. For an odd prime power  $q$ , let  $\eta$  be the unique quadratic character on  $\mathbf{F}_q^\times$ :  $\eta(a) = \left(\frac{N_{\mathbf{F}_q/\mathbf{F}_p}(a)}{p}\right)$ . A Gauss sum analogue of (A.2) is

$$(A.5) \quad G(\chi^2) = \frac{\chi(2)^2}{G(\eta)} G(\chi) G(\chi\eta).$$

where  $\chi$  is a nontrivial multiplicative character on  $\mathbf{F}_q$ .<sup>8</sup> The role of  $\sqrt{\pi}$  in the denominator in (A.2) is played by  $G(\eta)$  in (A.5), and we already pointed out how  $G(\eta)$  is like  $\sqrt{\pi}$  when  $\eta$  is quadratic. I am unaware of a generalization of (A.5) to Gauss sums on other finite commutative rings: they could have more than one (primitive) quadratic multiplicative character.

There is a generalization of (A.5) to  $G(\chi^n)$  when  $n \mid (q-1)$ : there is a multiplicative character  $\lambda$  on  $\mathbf{F}_q$  with order  $n$ , all the multiplicative characters on  $\mathbf{F}_q$  with order dividing  $n$  are  $\{\lambda^j : j = 0, \dots, n-1\}$ , and

$$(A.6) \quad G(\chi^n) = \frac{\chi(n)^n}{\prod_{j=1}^{n-1} G(\lambda^j)} \prod_{j=0}^{n-1} G(\chi\lambda^j).$$

This analogue of (A.3) is called the Hasse–Davenport product relation<sup>9</sup> for Gauss sums [1, Sect. 11.3] and its proof uses algebraic number theory (Stickelberger’s congruence for Gauss sums on finite fields). If you want the product in the denominator of (A.6) to include a term at  $j = 0$ , then you need to multiply the right side of the formula by  $-1$  since  $G(\mathbf{1}_q) = -1$ . I do not know a generalization of (A.6) to Gauss sums on other finite commutative rings. Even a generalization to the rings  $\mathbf{Z}/m\mathbf{Z}$  for composite  $m$  looks tricky since  $G(\mathbf{1}_m) = \mu(m)$ , which is often 0.

## REFERENCES

- [1] B. C. Berndt, R. J. Evans, and K. S. Williams “Gauss and Jacobi sums,” Wiley, New York, 1998.
- [2] H. Iwaniec and E. Kowalski, “Analytic Number Theory,” Amer. Math. Soc., Providence, 2004.
- [3] K. Ireland and M. Rosen, “A Classical Introduction to Modern Number Theory,” 2nd ed., Springer-Verlag, New York, 1990.
- [4] E. Lamprecht, Allgemeine Theorie der Gaußschen Summen in endlichen kommutativen Ringen, *Math. Nachr.* 9 (1953), 149–196.
- [5] B. Nica, Kloosterman sums over finite Frobenius rings, *Acta Arith.* 201 (2021), 391–420. URL <https://arxiv.org/pdf/1910.00165.pdf>.
- [6] L. Washington, “Introduction to Cyclotomic Fields,” 2nd ed., Springer-Verlag, New York, 1996.

<sup>8</sup>When  $\chi = \eta$ ,  $\chi\eta = \eta^2$  and both sides of (A.5) are  $G(\mathbf{1}_q)$  since  $\eta(4) = 1$ .

<sup>9</sup>When  $\chi = \lambda$ , both sides of (A.6) are  $G(\mathbf{1}_q)$ .