

**Zeitschrift:** L'Enseignement Mathématique  
**Herausgeber:** Commission Internationale de l'Enseignement Mathématique  
**Band:** 41 (1995)  
**Heft:** 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

**Artikel:** JACOBI SUMS AND STICKELBERGER'S CONGRUENCE  
**Autor:** Conrad, Keith  
**Kapitel:** Introduction  
**DOI:** <https://doi.org/10.5169/seals-61822>

### **Nutzungsbedingungen**

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

### **Conditions d'utilisation**

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

### **Terms of use**

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

**Download PDF:** 19.08.2025

**ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>**

## JACOBI SUMS AND STICKELBERGER'S CONGRUENCE

by Keith CONRAD<sup>1</sup>

**ABSTRACT.** We present an extension of a classical congruence for Jacobi sums of two characters to a congruence for arbitrary Jacobi sums. This congruence is used to provide what seems to be a new proof of Stickelberger's congruence for Gauss sums, as well as a new explanation for the appearance of base  $p$  digits in Stickelberger's congruence. It is also shown that in fact the Jacobi sum congruence and Stickelberger's congruence are equivalent.

### INTRODUCTION

About a century ago, Stickelberger established a congruence for Gauss sums over a finite field which has had useful implications for the study of cyclotomic fields. A generalized version of a classical congruence for Jacobi sums of two characters will be proven which is ultimately shown to be equivalent to Stickelberger's congruence. In particular, this allows for a new proof of Stickelberger's congruence and a new explanation for the form of the congruence.

Before discussing finite fields, we will need to fix a way of representing these fields and the multiplicative characters on them. Let  $p$  be a positive prime,  $q = p^f$  for  $f$  in  $\mathbf{Z}^+$ . We have the following diagram of number fields and primes, where  $\mathfrak{P}_i$  lies over  $\mathfrak{p}_i$ ,  $g = \varphi(q-1)/f$ , and  $\zeta_p, \zeta_{q-1} \in \mathbf{C}$  denote roots of unity with respective orders  $p$  and  $q-1$ :

$$\begin{array}{ccc}
 \mathbf{Q}(\zeta_{q-1}, \zeta_p) & \mathfrak{P}_1^{p-1} \cdot \dots \cdot \mathfrak{P}_g^{p-1} & \\
 | & | & \\
 \mathbf{Q}(\zeta_{q-1}) & \mathfrak{p}_1 \cdot \dots \cdot \mathfrak{p}_g & \\
 | & | & \\
 \mathbf{Q} & p &
 \end{array}$$

<sup>1</sup>) Supported by an ONR graduate fellowship Mathematics Subject Classification 11L05, 11T24.

Fix any prime  $\mathfrak{p}$  in  $\mathbf{Q}(\zeta_{q-1})$  lying over  $p$  and let  $\mathfrak{P}$  be the unique prime in  $\mathbf{Q}(\zeta_{q-1}, \zeta_p)$  lying over  $\mathfrak{p}$ . Then  $\mathbf{Z}[\zeta_{q-1}]/\mathfrak{p}$  is a field of size  $q$ , and from now on  $\mathbf{F}_q$  denotes this field.

Let  $\omega_{\mathfrak{p}}$  denote the Teichmüller character on  $\mathbf{F}_q$ , i.e. for  $\bar{\alpha}$  in  $\mathbf{F}_q$  ( $\alpha \in \mathbf{Z}[\zeta_{q-1}]$ ),  $\omega_{\mathfrak{p}}(\bar{\alpha})$  is the unique complex root of  $X^q - X$  satisfying  $\omega_{\mathfrak{p}}(\bar{\alpha}) \equiv \alpha \pmod{\mathfrak{p}}$ . Taking  $\alpha = \zeta_{q-1}$ , we see that  $\omega_{\mathfrak{p}}$  has order  $q-1$ , hence generates all multiplicative characters of  $\mathbf{F}_q$ . We will write  $\omega_{\mathfrak{p}}(\alpha)$  instead of  $\omega_{\mathfrak{p}}(\bar{\alpha})$ .

Although  $\mathbf{F}_q$  depends on  $\mathfrak{p}$ , we don't indicate this dependence in the notation. Replacing  $\mathbf{Q}$  by  $\mathbf{Q}_p$  would give only one prime over  $p$  in each extension field, making our representation of  $\mathbf{F}_q$  and definition of  $\omega_{\mathfrak{p}}$  more canonical, but we will not bother with this.

For  $0 \leq a < q-1$ , write the base  $p$  expansion of  $a$  as

$$a = a_0 + \cdots + a_{f-1}p^{f-1},$$

where  $0 \leq a_i \leq p-1$  (not all  $a_i = p-1$ ).

Throughout this paper,  $\zeta_p$  is fixed. The (normalized) Gauss sum of a multiplicative character  $\chi$  of  $\mathbf{F}_q$  is defined by

$$G(\chi) \stackrel{\text{def}}{=} - \sum_{x \in \mathbf{F}_q} \chi(x) \zeta_p^{\text{Tr}_{\mathbf{F}_q/\mathbf{F}_p}(x)}.$$

The (normalized) Jacobi sum of the multiplicative characters  $\chi_1, \dots, \chi_r$  of  $\mathbf{F}_q$  is defined by

$$J(\chi_1, \dots, \chi_r) \stackrel{\text{def}}{=} (-1)^{r-1} \sum_{\substack{x_1, \dots, x_r \in \mathbf{F}_q \\ x_1 + \cdots + x_r = 1}} \chi_1(x_1) \cdots \chi_r(x_r).$$

For basic properties of Gauss and Jacobi sums see [6, Chapters 8 and 10]. (Note: We always take  $\chi(0) = 0$ . In contrast to the definitions above, Gauss and Jacobi sums in [6] are *not* normalized by a power of  $-1$ , and the trivial multiplicative character is set equal to 1 at 0. These differences affect no results we use from [6] in any essential way. Actually, our normalizations make some formulas from [6] which we won't use look cleaner.) Using Jacobi sums we will prove

**THEOREM 1** (Stickelberger). *Using the same notation as above,*

$$G(\omega_{\mathfrak{p}}^{-a}) \equiv \frac{(\zeta_p - 1)^{a_0 + \cdots + a_{f-1}}}{a_0! \cdots a_{f-1}!} \pmod{\mathfrak{P}^{a_0 + \cdots + a_{f-1} + 1}}.$$

The original proof of this congruence is in [10, Section 6]. A modern reference for a proof is [7, Chapter 1]. In our proof, we use the following

relation between Gauss sums and Jacobi sums in order to introduce the factorials of the base  $p$  digits into Stickelberger's congruence in (essentially) one step:

LEMMA 1. *If  $\chi_1, \dots, \chi_r$  are multiplicative characters on  $\mathbf{F}_q$  with nontrivial product  $\chi_1 \cdot \dots \cdot \chi_r$ , then*

$$G(\chi_1 \cdot \dots \cdot \chi_r) = \frac{G(\chi_1) \cdot \dots \cdot G(\chi_r)}{J(\chi_1, \dots, \chi_r)}.$$

*Proof.* See [6, Chapter 8, Theorem 3], noting that our weaker hypotheses than those of [6] are sufficient since we assume the trivial character vanishes at 0.  $\square$

#### PROOF OF STICKELBERGER'S CONGRUENCE VIA JACOBI SUMS

For  $\chi_1, \dots, \chi_r$  multiplicative characters on  $\mathbf{F}_q = \mathbf{Z}[\zeta_{q-1}]/\mathfrak{p}$ , it is easy to check that

$$J(\chi_1, \dots, \chi_r)^p \equiv J(\chi_1, \dots, \chi_r) \pmod{\mathfrak{p}},$$

so  $J(\chi_1, \dots, \chi_r) \equiv$  rational integer  $\pmod{\mathfrak{p}}$ . We will show below (Theorem 2) that when some  $\chi_i$  is nontrivial, as an integer representative one can take a certain  $r$ -fold multinomial coefficient.

In the case  $r = 2$  there is the following classical congruence: if  $0 \leq k_1, k_2 < q - 1$  and not both  $k_1, k_2$  are zero, then

$$J(\omega_{\mathfrak{p}}^{-k_1}, \omega_{\mathfrak{p}}^{-k_2}) \equiv \frac{(k_1 + k_2)!}{k_1! k_2!} \pmod{\mathfrak{p}}.$$

References for this congruence are given in the Notes in [6, Chapter 14]. We shall extend this congruence to Jacobi sums of any number of multiplicative characters of  $\mathbf{F}_q$  as follows:

THEOREM 2. *For  $r \geq 1$  and  $0 \leq k_1, \dots, k_r < q - 1$  with some  $k_j > 0$ ,*

$$J(\omega_{\mathfrak{p}}^{-k_1}, \dots, \omega_{\mathfrak{p}}^{-k_r}) \equiv \frac{(k_1 + \dots + k_r)!}{k_1! \cdot \dots \cdot k_r!} \pmod{\mathfrak{p}}.$$

The simplicity of the statement of this generalization makes it somewhat surprising that it does not seem to appear in the literature (such as that which is mentioned in the Notes in [8, Chapter 5]).