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
Kurzfassung
DOI: https://doi.org/10.5169/seals-61822

L'Enseignement Mathématique, t. 41 (1995), p. 141-153

JACOBI SUMS AND STICKELBERGER'S CONGRUENCE

by Keith CONRAD[1]

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 $q-1$:

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

[1]) Supported by an ONR graduate fellowship Mathematics Subject Classification 11L05, 11T24.