

Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 27 (1981)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: THE HYPER-KLOOSTERMAN SUM
Autor: Weinstein, Lenard
Kapitel: 1. Introduction
DOI: <https://doi.org/10.5169/seals-51738>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. 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. [Siehe Rechtliche Hinweise.](#)

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. [Voir Informations légales.](#)

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. [See Legal notice.](#)

Download PDF: 06.02.2025

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

THE HYPER-KLOOSTERMAN SUM

by Lenard WEINSTEIN

1. INTRODUCTION

Deligne, [1], has recently proved the very deep theorem on the bound of the Hyper-Kloosterman sum. His estimate results from his solutions of the strong forms of the Weil conjectures.

The Hyper-Kloosterman sum is defined:

$$S(a_1, \dots, a_k; p) = \sum e\left(\frac{a_1 x_1 + \dots + a_k x_k}{p}\right)$$

where a_1, \dots, a_k, α are non-zero elements of the odd prime field F_p , and the summation runs through the k variables $x_i \in F_p$ with the relation $\prod x_i = \alpha$.

Deligne has shown:

$$|S(a_1, \dots, a_k; p)| \leq k p^{\frac{k-1}{2}}.$$

Here, we prove the following generalization for the bound of the Hyper-Kloosterman sum. Define:

$$S(a_1, \dots, a_k; q) = \sum e\left(\frac{a_1 x_1 + \dots + a_k x_k}{q}\right),$$

where a_1, \dots, a_k are arbitrary integers, q a positive integer, and the summation runs through the k variables $x_i, 0 < x_i \leq q, x_i$ relatively prime to q , with the relation $\prod x_i \equiv 1 \pmod{q}$.

We show:

THEOREM 1. *Let q be an odd positive integer. Then:*

$$|S(a_1, \dots, a_k; q)| \leq k^{v(q)} q^{\frac{k-1}{2}} (a_1, a_k, q)^{\frac{1}{2}} \dots (a_{k-1}, a_k, q)^{\frac{1}{2}}$$

where $v(q)$ is the number of different prime factors of q .

THEOREM 2. Let q be an even positive integer. Then :

$$|S(a_1, \dots, a_k; q)| \leq 2^{\frac{k+1}{2}} k^{v(q)} q^{\frac{k-1}{2}} (a_1, a_k, q)^{\frac{1}{2}} \dots (a_{k-1}, a_k, q)^{\frac{1}{2}}.$$

Estermann, [2], has dealt with the case of the Kloosterman sum.

2. LEMMAS

Lemma 1. Consider the congruence:

$$x^k \equiv a \pmod{p^m}$$

where k, m are positive integers, a is an integer, p a prime and $(a, p) = 1$. Then:

1. If $p > 2$, this congruence has at most k incongruent solutions mod p^m .
2. If $p = 2$ and k is odd, then this congruence has exactly 1 solution mod p^m .
3. If $p = 2$, and $k = 2^r l$, $r > 1$, l odd, then this congruence has at most $\min\{2^{r+1}, p^m\}$ solutions mod p^m .

Proof: This is essentially found on pp. 115, 119 of [3].

Lemma 2. Let p be a prime, and m, n positive integers, $\frac{1}{2}m \leq n < m$. Let $y_1, \dots, y_{k-1}, z_1, \dots, z_{k-1}$ be integers; $p \nmid y_1, \dots, p \nmid y_{k-1}$. Define $[y_1, \dots, y_{k-1}; p^m]$ as that integer y , $0 < y < p^m$ such that $y(y_1 \dots y_{k-1}) \equiv 1 \pmod{p^m}$. Then:

$$\begin{aligned} [y_1 + p^n z_1, \dots, y_{k-1} + p^n z_{k-1}; p^m] &\equiv [y_1, \dots, y_{k-1}; p^m] \\ &\quad - [y_1; p^m]^2 [y_2; p^m] \dots [y_{k-1}; p^m] p^n z_1 \\ &\quad \cdot \\ &\quad \cdot \\ &\quad \cdot \\ &\quad - [y_1; p^m] \dots [y_{k-2}; p^m] [y_{k-1}; p^m]^2 p^n z_{k-1} \pmod{p^m} \end{aligned}$$

Proof: This follows from the relation

$$[y_1; p^m] \dots [y_{k-1}; p^m] \equiv [y_1, \dots, y_{k-1}; p^m] \pmod{p^m}$$

and Lemma 1 of [2].