

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: 2. Lemmas
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>

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].

Lemma 3. Let p be a prime, m, n positive integers, $m = 2n + 1$. Let $y_1, \dots, y_{k-1}, z_1, \dots, z_{k-1}$ be integers; $p \nmid y_1, \dots, p \nmid y_{k-1}$. Then

$$\begin{aligned}
 & [y_1 + p^n z_1, \dots, y_{k-1} + p^n z_{k-1}; p^m] \equiv [y_1, \dots, y_{k-1}; p^m] \\
 & + [y_1; p^m]^3 [y_2; p^m] \dots [y_{k-1}; p^m] p^{2n} z_1^2 \\
 & \cdot \\
 & \cdot \\
 & \cdot \\
 & + [y_1; p^m] \dots [y_{k-2}; p^m] [y_{k-1}; p^m]^3 p^{2n} z_{k-1}^2 \\
 & - [y_1; p^m]^2 [y_2; p^m] \dots [y_{k-1}; p^m] p^n z_1 \\
 & \cdot \\
 & \cdot \\
 & \cdot \\
 & - [y_1; p^m] \dots [y_{k-2}; p^m] [y_{k-1}; p^m]^2 p^n z_{k-1} \\
 & + [y_1; p^m]^2 [y_2; p^m]^2 [y_3; p^m] \dots [y_{k-1}; p^m] p^{2n} z_1 z_2 \\
 & \cdot \\
 & \cdot \\
 & \cdot \\
 & + [y_1; p^m]^2 [y_2; p^m] \dots [y_{k-2}; p^m] [y_{k-1}; p^m]^2 p^{2n} z_1 z_{k-1} \\
 & + [y_1; p^m] [y_2; p^m]^2 [y_3; p^m]^2 [y_4; p^m] \dots [y_{k-1}; p^m] p^{2n} z_2 z_3 \\
 & \cdot \\
 & \cdot \\
 & \cdot \\
 & + [y_1; p^m] [y_2; p^m]^2 [y_3; p^m] \dots [y_{k-2}; p^m] [y_{k-1}; p^m]^2 p^{2n} z_2 z_{k-1} \\
 & \cdot \\
 & \cdot \\
 & \cdot \\
 & + [y_1; p^m] \dots [y_{k-3}; p^m] [y_{k-2}; p^m]^2 [y_{k-1}; p^m]^2 p^{2n} z_{k-2} z_{k-1} \\
 & \pmod{p^m}
 \end{aligned}$$

Proof: This follows from Lemma 5 of [2].

Lemma 4. Let $p > 2$ be a prime, and n a positive integer. Let a, h be integers. Then:

$$\left| \sum_{0 \leq z < p^{n+1}} e(az^2 p^{-1} + hzp^{-n-1}) \right| = \begin{cases} 0 & p^n \nmid h \\ p^{n+\frac{1}{2}} & p^n \mid h, \quad p \nmid a \\ p^{n+1} & p^{n+1} \mid h, \quad p \mid a \\ 0 & p^{n+1} \nmid h, \quad p \mid a. \end{cases}$$

Proof: The first two parts of this lemma are Lemma 5 of [2]. The last two parts are trivial.

3. PROOF OF THEOREMS 1 AND 2

PROPOSITION 1. Let p be a prime, m a positive integer and a_1, \dots, a_k , integers such that

$$(a_1, a_k, p^m) = \dots = (a_{k-1}, a_k, p^m) = p^h \quad 0 \leq h < m.$$

Then

$$S(a_1, \dots, a_k; p^m) = (p^h)^{k-1} S(a_1 p^{-h}, \dots, a_k p^{-h}; p^{m-h})$$

Proof: The proof is similar to that of [2], page 85 bottom.

PROPOSITION 2. Let m, n be positive integers $\frac{1}{2}m \leq n < m$, p a prime, and a_1, \dots, a_k integers such that $(a_1, a_k; p^m) = 1$. Then:

$$|S(a_1, \dots, a_k; p^m)| \leq A(p^n)^{k-1}$$

where

$$A = \begin{cases} k & \text{if } p > 2. \\ 1 & \text{if } p = 2 \text{ and } k \text{ is odd.} \\ \min \{ 2^{r+1}, p^m \} & \text{if } p = 2 \text{ and } k = 2^r l, \\ & r > 1 \text{ and } l \text{ odd.} \end{cases}$$

Proof: Let us assume throughout this proposition that $S(a_1, \dots, a_k; p^m) \neq 0$, or else we are done.

Now we have the identity