2. Lemmas

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **27 (1981)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **29.05.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

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

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

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

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

Proof: This follows from the relation

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

and Lemma 1 of [2].

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

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

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:

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

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 $a_1, .. a_k$., integers such that*

$$(a_1, a_k, p^m) = \ldots = (a_{k-1}, a_k, p^m) = p^h \qquad 0 \leqslant h < m .$$

Then

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

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

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

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

where

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

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

Now we have the identity