Stanislav Jakubec
An elementary proof of the Davenport-Hasse relation


Persistent URL: [http://dml.cz/dmlcz/136803](http://dml.cz/dmlcz/136803)

Terms of use:

© Mathematical Institute of the Slovak Academy of Sciences, 2001

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these Terms of use.

This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project DML-CZ: The Czech Digital Mathematics Library [http://project.dml.cz](http://project.dml.cz)
AN ELEMENTARY PROOF
OF THE DAVENPORT-HASSE RELATION

STANISLAV JAKUBEC

(Communicated by Pavol Zlatoš)

ABSTRACT. Using a congruence for Gauss period the Davenport-Hasse relation for the Gauss sums is proved.

Let \( p > 3 \) be a prime and \( \chi \) be a Dirichlet character modulo \( p \). Let \( \tau(\chi) = \sum_{x=1}^{p-1} \chi(x)\zeta_p^x \) be a Gauss sum. The following theorem shows a non-trivial multiplicative relations between \( p - 2 \) Gauss sums.

The following Theorem can be found in [3].

THEOREM (DAVENPORT-HASSE RELATION). If \( l \) is a divisor of \( p - 1 \) and \( \chi \) is a Dirichlet character modulo \( p \) satisfying \( \chi^l \neq \varepsilon \), then

\[
\tau(\chi) \prod_{\psi^l = \varepsilon, \psi \neq \varepsilon} \tau(\chi\psi) = \overline{\chi}(l)^l \tau(\chi^l) \prod_{\psi^l = \varepsilon, \psi \neq \varepsilon} \tau(\psi).
\]

For the proof of this theorem, see [2]. An elementary proof is known only in special cases. For \( l = 2^n \) the proof is in [1].

The aim of this paper is to show how this result can be obtained for the fields \( \mathbb{Z}/p\mathbb{Z} \) from the following lemma proved in [4]. Here \( \pi \) denotes a suitable element of \( \mathbb{Q}(\zeta_p) \) such that \( \text{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\pi) = p \).

LEMMA 1. ([4]) Let \( p \) be a prime and \( n \neq 1 \) be a divisor of \( p - 1 \). There exists a prime divisor \( p \) of the field \( \mathbb{Q}(\zeta_n) \) with \( p \mid p \) such that for any exponent \( S \) there are rational numbers \( a^*_1, \ldots, a^*_n \) satisfying

2000 Mathematics Subject Classification: Primary 11L05.
Key words: Gauss sums.
(i) \( a_i^* \equiv \frac{k}{(ki)!} \pmod{p} \),
(ii) \( \tau(\chi^i) \equiv na_i^*\pi^i \pmod{p^S} \)
for \( i = 1, 2, \ldots, n - 1 \).

In [4], the prime divisor \( p \) is chosen to satisfy the congruence \( \bar{\chi}(a) \equiv a \pmod{p} \) for each integer \( a \) relatively prime to \( p \).

Proof of the Theorem. Let \( \chi \) be a generator of the group of Dirichlet characters modulo \( p \). Denote \( k = \frac{p-1}{l} \). Let \( i \) be a positive integer such that \( \chi^il \neq \varepsilon \).

The Davenport-Hasse relation can be rewritten as follows:
\[
\tau(\chi^i)\tau(\chi^{i+k}) \cdots \tau(\chi^{i+k(l-1)}) = \bar{\chi}^{il}(l)\tau(\chi^k)\tau(\chi^{2k}) \cdots \tau(\chi^{(l-1)k})\tau(\chi^{il}).
\]

It is easy to see that both sides of this equality depend only on the residue class of \( i \) modulo \( k \). Let us denote its left-hand side by \( \alpha \) and its right-hand side by \( \beta \).

For any positive integer \( j < p - 1 \) relatively prime to \( p - 1 \) let \( \sigma_j \) be the automorphism of \( \mathbb{Q}(\zeta_{p-1}, \zeta_p) \) such that \( \sigma_j(\zeta_{p-1}) = \zeta_{p-1}^j \) and \( \sigma_j(\zeta_p) = \zeta_p \). Then
\[
\sigma_j(\alpha - \beta) = \tau(\chi^{ij})\tau(\chi^{i+kj}) \cdots \tau(\chi^{i+(l-1)kj})
\]
\[
- \bar{\chi}^{ijl}(l)\tau(\chi^{kj})\tau(\chi^{2kj}) \cdots \tau(\chi^{(l-1)kj})\tau(\chi^{ijl}).
\]
Let \( r = ij - \left[ \frac{ij}{k} \right]k \), then
\[
\sigma_j(\alpha - \beta)
\]
\[
= \tau(\chi^r)\tau(\chi^{r+k}) \cdots \tau(\chi^{r+(l-1)k}) - \bar{\chi}^{rl}(l)\tau(\chi^{kj})\tau(\chi^{2kj}) \cdots \tau(\chi^{(l-1)kj})\tau(\chi^{rl}).
\]

Denote
\[
M_j = r + (r + k) + (r + 2k) + \cdots + (r + (l - 1)k) = rl + (l - 1)^2 + \frac{p - 1}{2}.
\]

By Lemma 1, for \( n = p - 1 \) we have
\[
\sigma_j(\alpha - \beta) \equiv \pi^{M_j} (p-1)! \left(a_{r}^*a_{r+k}^* \cdots a_{r+(l-1)k}^* - \bar{\chi}^{rl}(l)a_k^*a_{2k}^*a_{(l-1)k}^*a_{rl}^* \right) \pmod{p^S}.
\]

We shall prove that
\[
a_{r}^*a_{r+k}^* \cdots a_{r+(l-1)k}^* \equiv \bar{\chi}^{rl}(l)a_k^*a_{2k}^*a_{(l-1)k}^*a_{rl}^* \pmod{p}.
\]

We have mentioned that \( p \) satisfies
\[
\bar{\chi}^{rl}(l) \equiv l^{rl} \pmod{p}.
\]
AN ELEMENTARY PROOF OF THE DAVENPORT-HASSE RELATION

From \( a_i^* \equiv \frac{1}{i!} \pmod{p} \) it follows that it is enough to prove the congruence
\[
\frac{1}{r!} \frac{1}{(r + k)!} \cdots \frac{1}{(r + (l - 1)k)!} \equiv \prod_{k=1}^{l} \frac{1}{k!} \frac{1}{(2k)!} \cdots \frac{1}{((l - 1)k)!} \frac{1}{(rl)!} \pmod{p},
\]
for each \( 0 < r < k \).

The last congruence can be easily proved by induction with respect to \( r \).

Thus there is an integer \( \delta \in \mathbb{Q}(\zeta_p, \zeta_{p-1}) \) divisible by \( p \) such that
\[
\sigma_j(\alpha - \beta) \equiv \pi M_j \delta \pmod{p^S}.
\]

Hence there exists an integer \( \delta' \in \mathbb{Q}(\zeta_p, \zeta_{p-1}) \) divisible by \( p^{\varphi(p-1)} \) such that
\[
N_{\mathbb{Q}(\zeta_p, \zeta_{p-1})/\mathbb{Q}(\zeta_p)}(\alpha - \beta) = \prod_{(p-1,j)=1} \sigma_j(\alpha - \beta) \equiv \pi \sum M_j \delta' \pmod{p^S}.
\]

For each automorphism \( \sigma \in \text{Gal}(\mathbb{Q}(\zeta_p, \zeta_{p-1})/\mathbb{Q}(\zeta_{p-1})) \) we have \( \sigma(p) = p \).

Therefore there exists an integer \( \delta'' \in \mathbb{Q}(\zeta_p, \zeta_{p-1}) \) divisible by \( p^{(p-1)\varphi(p-1)} \) such that
\[
N_{\mathbb{Q}(\zeta_p, \zeta_{p-1})/\mathbb{Q}(\zeta_{p-1})}(\alpha - \beta) \equiv p^{\varphi(p)(p-1)^{\frac{l-1}{2}}} \delta'' \pmod{p^S}.
\]

Since \( M_j > (l - 1)^{\frac{p-1}{2}} \), we have
\[
\sum_{(p-1,j)=1} M_j > (l - 1)^{\frac{p-1}{2}} \varphi(p - 1).
\]

Thus there exists an integer \( \delta''' \in \mathbb{Q}(\zeta_p, \zeta_{p-1}) \) divisible by \( p^{(p-1)\varphi(p-1)} \) such that
\[
N_{\mathbb{Q}(\zeta_p, \zeta_{p-1})/\mathbb{Q}(\zeta_{p-1})}(\alpha - \beta) \equiv p^{\varphi(p)(p-1)^{\frac{l-1}{2}}} \delta''' \pmod{p^S}.
\]

Hence the rational integer
\[
N_{\mathbb{Q}(\zeta_p, \zeta_{p-1})/\mathbb{Q}(\zeta_{p-1})/\mathbb{Q}(\zeta_{p-1})}(\alpha - \beta)
\]

is divisible by the divisor
\[
p^{\varphi(p)(p-1)^{\frac{l-1}{2}}} + \varphi(p)(p-1),
\]
and, consequently, also by the integer
\[
p^{\varphi(p)(p-1)^{\frac{l-1}{2}}} + \varphi(p)(p-1).
\]

Since \( \sigma(\alpha - \beta) < 2p^{\frac{l}{2}} \) for any \( \sigma \in \text{Gal}(\mathbb{Q}(\zeta_p, \zeta_{p-1})/\mathbb{Q}) \), we have
\[
|N_{\mathbb{Q}(\zeta_p, \zeta_{p-1})/\mathbb{Q}(\zeta_{p-1})}(\alpha - \beta)| < \left(2p^{\frac{l}{2}}\right)^{\varphi(p)(p-1)}.
\]

It is easy to see that
\[
\left(2p^{\frac{l}{2}}\right)^{\varphi(p)(p-1)} < p^{\varphi(p)(p-1)^{\frac{l-1}{2}}} + \varphi(p)(p-1)
\]
for any \( p \geq 5 \). Hence \( \alpha - \beta = 0 \), and the Theorem is proved. \( \square \)
REFERENCES


Received November 6, 1998
Revised February 22, 2000