Stanislav Jakubec

An elementary proof of the Davenport-Hasse relation

Mathematica Slovaca, Vol. 51 (2001), No. 2, 175--178

Persistent URL: http://dml.cz/dmlcz/136803

Math. Slovaca, **51** (2001), No. 2, 175–178

Mathematica Slovaca

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 χ be a Dirichlet character modulo p. Let $\tau(\chi) = \sum\limits_{x=1}^{p-1} \chi(x)\zeta_p^x$ 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 χ 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 π denotes a suitable element of $\mathbb{Q}(\zeta_p)$ such that $\mathrm{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\pi) = p$.

LEMMA 1. ([4]) *Let p be a prime and $n \neq 1$ be a divisor of $p-1$. There exists a prime divisor $\mathfrak{p}$ of the field $\mathbb{Q}(\zeta_n)$ with $\mathfrak{p} \mid p$ such that for any exponent S there are rational numbers $a_1^*, \dots, a_{n-1}^*$ satisfying*

2000 Mathematics Subject Classification: Primary 11L05.
Key words: Gauss sums.

(i) $a_i^* \equiv \frac{k}{(ki)!} \pmod{p}$,
(ii) $\tau(\chi^i) \equiv n a_i^* \pi^i \pmod{\mathfrak{p}^S}$
for $i = 1, 2, \ldots, n-1$.

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

Proof of the Theorem. Let χ 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:

$$\tau(\chi^i)\tau(\chi^{i+k}) \cdots \tau(\chi^{i+k(l-1)}) = \overline{\chi}^{li}(l)\tau(\chi^k)\tau(\chi^{2k}) \cdots \tau(\chi^{(l-1)k})\tau(\chi^{il}).$$

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 α and its right-hand side by β.

For any positive integer $j < p-1$ relatively prime to $p-1$ let σ_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

$$\sigma_j(\alpha - \beta) = \tau(\chi^{ij})\tau(\chi^{(i+k)j}) \cdots \tau(\chi^{i+(l-1)k)j}) - \overline{\chi}^{ijl}(l)\tau(\chi^{kj})\tau(\chi^{2kj}) \cdots \tau(\chi^{(l-1)kj})\tau(\chi^{ijl}).$$

Let $r = ij - [\frac{ij}{k}]k$, then

$$\sigma_j(\alpha - \beta) = \tau(\chi^r)\tau(\chi^{r+k}) \cdots \tau(\chi^{r+(l-1)}) - \overline{\chi}^{rl}(l)\tau(\chi^{kj})\tau(\chi^{2kj}) \cdots \tau(\chi^{(l-1)kj})\tau(\chi^{rl}).$$

Denote

$$M_j = r + (r+k) + (r+2k) + \cdots + (r+(l-1)k) = rl + (l-1)\frac{p-1}{2}.$$

By Lemma 1, for $n = p-1$ we have

$$\sigma_j(\alpha - \beta) \equiv \pi^{M_j}(p-1)^l (a_r^* a_{r+k}^* \ldots a_{r+(l-1)k}^* - \overline{\chi}^{rl}(l) a_k^* a_{2k}^* a_{(l-1)k}^* a_{rl}^*) \pmod{\mathfrak{p}^S}.$$

We shall prove that

$$a_r^* a_{r+k}^* \cdots a_{r+(l-1)k} \equiv \overline{\chi}^{rl}(l) a_k^* a_{2k}^* \cdots a_{(l-1)k}^* a_{rl}^* \pmod{\mathfrak{p}}.$$

We have mentioned that $\mathfrak{p}$ satisfies

$$\overline{\chi}^{rl}(l) \equiv l^{rl} \pmod{\mathfrak{p}}.$$

From $a_i^* \equiv \frac{1}{i!} \pmod{p}$ it follows that it is enough to prove the congruence

$$\frac{1}{r!}\frac{1}{(r+k)!}\cdots\frac{1}{(r+(l-1)k)!} \equiv l^{rl}\frac{1}{k!}\frac{1}{(2k)!}\cdots\frac{1}{((l-1)k)!}\frac{1}{(rl)!} \pmod{p},$$

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 $\mathfrak{p}$ such that

$$\sigma_j(\alpha - \beta) \equiv \pi^{M_j}\delta \pmod{\mathfrak{p}^S}.$$

Hence there exists an integer $\delta' \in \mathbb{Q}(\zeta_p, \zeta_{p-1})$ divisible by $\mathfrak{p}^{\varphi(p-1)}$ such that

$$\mathrm{N}_{\mathbb{Q}(\zeta_p,\zeta_{p-1})/\mathbb{Q}(\zeta_p)}(\alpha - \beta) = \prod_{(p-1,j)=1} \sigma_j(\alpha - \beta) \equiv \pi^{\sum M_j}\delta' \pmod{\mathfrak{p}^S}.$$

For each automorphism $\sigma \in \mathrm{Gal}\big(\mathbb{Q}(\zeta_p, \zeta_{p-1})/\mathbb{Q}(\zeta_{p-1})\big)$ we have $\sigma(\mathfrak{p}) = \mathfrak{p}$. Therefore there exists an integer $\delta'' \in \mathbb{Q}(\zeta_p, \zeta_{p-1})$ divisible by $\mathfrak{p}^{(p-1)\varphi(p-1)}$ such that

$$\mathrm{N}_{\mathbb{Q}(\zeta_p,\zeta_{p-1})/\mathbb{Q}}(\alpha - \beta) \equiv p^{\sum M_j}\delta'' \pmod{\mathfrak{p}^S}.$$

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 $\mathfrak{p}^{(p-1)\varphi(p-1)}$ such that

$$\mathrm{N}_{\mathbb{Q}(\zeta_p,\zeta_{p-1})/\mathbb{Q}}(\alpha - \beta) \equiv p^{\varphi(p)\varphi(p-1)\frac{l-1}{2}}\delta''' \pmod{\mathfrak{p}^S}.$$

Hence the rational integer

$$\mathrm{N}_{\mathbb{Q}(\zeta_p,\zeta_{p-1})/\mathbb{Q}}(\alpha - \beta)$$

is divisible by the divisor

$$\mathfrak{p}^{\varphi(p)\varphi(p-1)\frac{l-1}{2}+\varphi(p)\varphi(p-1)},$$

and, consequently, also by the integer

$$p^{\varphi(p)\varphi(p-1)\frac{l-1}{2}+\varphi(p)\varphi(p-1)}.$$

Since $\sigma(\alpha - \beta) < 2p^{\frac{l}{2}}$ for any $\sigma \in \mathrm{Gal}\big(\mathbb{Q}(\zeta_p, \zeta_{p-1})/\mathbb{Q}\big)$, we have

$$|\mathrm{N}_{\mathbb{Q}(\zeta_p,\zeta_{p-1})/\mathbb{Q}}(\alpha - \beta)| < \big(2p^{\frac{l}{2}}\big)^{\varphi(p)\varphi(p-1)}.$$

It is easy to see that

$$\big(2p^{\frac{l}{2}}\big)^{\varphi(p)\varphi(p-1)} < p^{\varphi(p)\varphi(p-1)\frac{l-1}{2}+\varphi(p)\varphi(p-1)}$$

for any $p \geq 5$. Hence $\alpha - \beta = 0$, and the Theorem is proved. □

REFERENCES

[1] BERNDT, B. C.—EVANS, R. J.: *Sums of Gauss, Eisenstein, Jacobi, Jacobsthal and Brewer*, Illinois. J. Math. **23** (1979), 374–437.

[2] DAVENPORT, H.—HASSE, H.: *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fallen*, J. Reine Angew. Math. **172** (1934), 151–182.

[3] HASSE, H.: *Vorlesungen über Zahlentheorie*, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1950.

[4] JAKUBEC, S.: *Note on the congruence of Ankeny-Artin-Chowla type modulo* p^2, Acta Arith. **85** (1998), 377–388.

Received November 6, 1998
Revised February 22, 2000

Matematický ústav SAV
Štefánikova 49
SK-814 37 Bratislava
SLOVAKIA
E-mail: jakubec@mat.savba.sk