ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 25, Number 4, Fall 1995

AN ARITHMETIC APPROACH TO THE DAVENPORT-HASSE RELATION OVER $GF(p)$

JAMES G. HUARD, BLAIR K. SPEARMAN AND KENNETH S. WILLIAMS

ABSTRACT. It is shown how the Davenport-Hasse relation for Gauss sums over $GF(p)$ can be deduced from two simple arithmetic results.

1. Introduction. In this paper we prove two simple arithmetic results and use them to given an elementary proof of the Davenport-Hasse relation (Theorem 3) for Gauss sums over a finite field with p elements, where p is an odd prime. Our first arithmetic result (Theorem 1) gives a congruence $(\bmod p)$ for a certain root of unity modulo p in terms of factorials. Hudson and Williams [**2**] deduced this congruence from the Davenport-Hasse relation [**1**] and a congruence of Yamamoto [**5**] for Gauss sums. Here we take the reverse approach. We prove Theorem 1 by simple arithmetic manipulations and then use it as a key step in a new proof of the Davenport-Hasse relation; specifically, to determine the root of unity appearing in the relation. The second arithmetic result (Theorem 2) compares the number of integers satisfying two inequalities and is used to establish that the quotient of products of Gauss sums in the Davenport-Hasse relation is an algebraic integer. In addition to these two theorems we need only the basic properties of Gauss sums, Jacobi sums, and the ring of integers of a cyclotomic field. After proving the Davenport-Hasse relation we use it to show that the inequality proved in Theorem 2 is actually an equality.

2. Two arithmetic results. In this section we prove the two results discussed in the introduction.

Received by the editors on December 6, 1994.
1991 *Mathematics Subject Classification.* 11L05.
Key words and phrases. Gauss sums, Jacobi sums, Davenport-Hasse relation.
Research of the first author supported by a Canisius College Faculty Fellowship.
Research of the third author supported by a Natural Sciences and Engineering Research Council of Canada Grant A-7233.

Copyright ©1995 Rocky Mountain Mathematics Consortium

Theorem 1. *Let f, m and n be integers with $f \geq 1$, $m \geq 2$, $n \geq 1$, and $p = mnf + 1$ prime. Let t be an integer with $1 \leq t \leq m-1$. Then*

$$(ntf)! \prod_{j=1}^{n-1} (mjf)! \Big/ \prod_{j=0}^{n-1} ((mj+t)f)! \equiv n^{(p-1)t/m} (\operatorname{mod} p).$$

Proof. Consider the first mnf positive integers. Arrange these consecutively in mn rows each of length f. Let A_h, $h = 1, \dots, mn$, be the product of the integers in the hth row, so that

$$(1) \qquad A_h = ((h-1)f+1) \cdots (hf) = (hf)!/(h-1)f!.$$

Next, arrange the first ntf positive integers in tf rows of length n. Let B_l, $l = 1, \dots, n$, be the product of the integers in the lth column, so that

$$B_l = l(l+n) \cdots (l + n(tf-1)).$$

Multiplying each of the f factors of A_{jm+i}, $i = 1, \dots, t$, $j = 1, \dots, n-1$, by n, we have

$$\begin{aligned} n^f A_{jm+i} &= (jmnf + nif - nf + n) \cdots (jmnf + nif) \\ &\equiv (n(if - f + 1) - j) \cdots (nif - j) \quad (\operatorname{mod} p), \end{aligned}$$

so that

$$\prod_{j=1}^{n-1} \prod_{i=1}^{t} n^f A_{jm+i} \equiv \prod_{j=1}^{n-1} B_{n-j} (\operatorname{mod} p).$$

Multiplying both sides of this congruence by $B_n = n(2n) \cdots (tfn) = n^{tf}(tf)!$, we obtain

$$n^{tf}(tf)! n^{(n-1)tf} \prod_{j=1}^{n-1} \prod_{i=1}^{t} A_{jm+i} \equiv (ntf)! (\operatorname{mod} p);$$

that is,

$$n^{ntf}(tf)! \prod_{j=1}^{n-1} ((mj+t)f!/(mjf)!) \equiv (ntf)! (\operatorname{mod} p),$$

from which the assertion of the theorem follows. $\square$

Before continuing, we note that since $p = mnf + 1$, we have

$$\begin{aligned} A_{mn-h+1} &= ((mn-h)f+1)\cdots((mn-h+1)f) \\ &\equiv (-hf)\cdots(-hf+f-1) \pmod p, \end{aligned}$$

for $h = 1, \ldots, mn$; that is,

$$A_{mn-h+1} \equiv (-1)^f A_h \pmod p, \tag{2}$$

which we will use later in the proof of Theorem 3.

We also introduce some notation. For a real number x, $[x]$ denotes the greatest integer not exceeding x. For integers $k(\geq 1)$ and a, $[a]_k$ denotes the least nonnegative residue of a modulo k. The following two properties are immediate and will be used extensively in the proof of our next result:

$$[a]_k = a - [a/k]k; \tag{3}$$

$$[ak]_{lk} = k[a]_l, \quad \text{for any positive integer } l. \tag{4}$$

Theorem 2. *Let m and n be integers with $m \geq 2$ and $n \geq 1$. Let l be an integer such that*

$$(l, mn) = 1 \quad \textit{and} \quad 1 \leq l < mn.$$

Let t be an integer such that

$$(t, m) = 1 \quad \textit{and} \quad 1 \leq t < m.$$

Let

$$A(m, n, l, t) = \#\{j = 1, \ldots, n-1 \mid [lmj]_{mn} < mn - [lt]_{mn}\}.$$

For any positive integer λ, let

$$B(m, n, l, t, \lambda) = \#\{j = 1, 2, \ldots, \lambda n - 1 \mid [ltj]_{mn} < mn - [lt]_{mn}\}.$$

Then

(a) $A(m,n,l,t) = n + n[lt/mn] - [lt/m] - 1$;

and

(b) *if* $t|n$, *then* $B(m,n,l,t,1) \leq A(m,n,l,t)$.

Proof. (a) Set $r = [lt/mn]$, so that by (3), $[lt]_{mn} = lt - rmn$. Since lt/m is not an integer, we have

$$\begin{aligned} &[lmj]_{mn} < mn - [lt]_{mn} \\ &\qquad \Longleftrightarrow [lj]_n < n - ((lt/m) - rn) \qquad \text{(by (4))} \\ &\qquad \Longleftrightarrow [lj]_n \leq n + rn - ([lt/m] + 1), \end{aligned}$$

whose right side is less than n. As j runs through $1, \dots, n-1$, so does $[lj]_n$. Hence,

$$\begin{aligned} A(m,n,l,t) &= \#\{j \in \mathbf{Z} \mid 1 \leq j \leq n + rn - [lt/m] - 1\} \\ &= n + n[lt/mn] - [lt/m] - 1, \end{aligned}$$

as required.

(b) Suppose that $t|n$, so that $n_1 = n/t$ is an integer. Let $l_1 = [l]_{mn_1}$. Since, by (4), the inequality $[ltj]_{mn} < mn - [lt]_{mn}$ is equivalent to $[l_1 j]_{mn_1} < mn_1 - l_1$, we have $B(m,n,l,t,1) = B(m,n_1,l_1,1,t)$.

Next define the integers j_w, $w = 1, 2, \dots, [l_1 t/m])$ by $j_w = [wmn_1/l_1]$. Since $mn_1/l_1 > 1$, the j_w's are distinct. The j_w's satisfy the inequalities

$$1 \leq w \leq j_w \leq \frac{wmn_1}{l_1} \leq \left[\frac{l_1 t}{m}\right] \frac{mn_1}{l_1} < \frac{l_1 t}{m} \cdot \frac{mn_1}{l_1} = n_1 t = n.$$

Furthermore, as wmn_1/l_1 is not an integer, we have $(wmn_1/l_1) - 1 < j_w < wmn_1/l_1$, from which we obtain

$$0 < mn_1 - l_1 < l_1 j_w - (w-1)mn_1 < mn_1.$$

Thus we have shown that the j_w's, $w = 1, \dots, [l_1 t/m]$, belong to the set $\{j = 1, \dots, n-1 \mid [l_1 j]_{mn_1} \not< mn_1 - [l_1]_{mn_1}\}$. Hence,

$$\begin{aligned} B(m,n,l,t,1) &= B(m,n_1,l_1,1,t) \\ &\leq n - 1 - [l_1 t/m] \\ &= n - 1 - [(l - [l/mn_1]mn_1)t/m] \qquad \text{(by (3))} \\ &= n - 1 - [lt/m] + [l/mn_1]n \\ &= n - 1 - [lt/m] + n[lt/mn] \\ &= A(m,n,l,t) \qquad \text{(by (a))}. \qquad \square \end{aligned}$$

In fact, we will see later from the Davenport-Hasse relation that $B(m,n,l,t,1) = A(m,n,l,t)$, where the condition $t|n$ in (b) has been removed.

3. Jacobi sums and Gauss sums. For any positive integer k, set $\beta_k = \exp(2\pi i/k)$. Let K denote the cyclotomic field $\mathbf{Q}(\beta_{mn})$, where $m(\geq 2)$ and $n(\geq 1)$ are integers. Let p be a prime with $p \equiv 1 (\operatorname{mod} mn)$ and set $f = (p-1)/mn$. Let O_K denote the ring of integers of K and let P be a prime ideal of O_K dividing the prime p. Choose a primitive root g modulo p so that $g^f \equiv \beta_{mn} (\operatorname{mod} P)$. For any integer $l \not\equiv 0 (\operatorname{mod} p)$, let $\operatorname{ind}_g(l)$ be the least nonnegative integer for which $g^{\operatorname{ind}_g(l)} \equiv l (\operatorname{mod} p)$. Then define the character $\chi (\operatorname{mod} p)$ of order mn by $\chi(g) = \beta_{mn}$, so that $\chi(l) \equiv l^f (\operatorname{mod} P)$. The Jacobi sum $J(\chi^r, \chi^s)$ is defined for integers r and s by

$$J(\chi^r, \chi^s) = \sum_{x=2}^{p-1} \chi^r(x)\chi^s(1-x), \tag{5}$$

and is in O_K. The Gauss sum $G(\chi^r)$ is defined for an integer r by

$$G(\chi^r) = \sum_{x=1}^{p-1} \chi^r(x)\beta_p^x,$$

which is an integer of $\mathbf{Q}(\beta_{mnp})$. The basic formula relating Jacobi sums and Gauss sums is

$$J(\chi^r, \chi^s) = \frac{G(\chi^r)G(\chi^s)}{G(\chi^{r+s})}, \quad \text{if } r, s, r+s \not\equiv 0 (\operatorname{mod} mn). \tag{6}$$

Let σ_a be the automorphism of K given by $\sigma_a(\beta_{mn}) = \beta_{mn}^a$, where $a = 1, \dots, mn$, $(a, mn) = 1$, and set $P_a = \sigma_a(P)$, so that pO_K is the product of the P_a's. If $r, s, r+s \not\equiv 0 (\operatorname{mod} mn)$, then $J(\chi^r, \chi^s)\overline{J(\chi^r, \chi^s)} = p$, so that $J(\chi^r, \chi^s)O_K$ is a squarefree product of some of the P_a's. The congruence

(7)

$$J(\chi^r, \chi^s) \equiv \begin{cases} 0 (\operatorname{mod} P_{k^{-1}}), & \text{if } [kr]_{mn} + [ks]_{mn} < mn, \\ (-1)^{ksf+1} \dbinom{[kr]_{mn} f}{(mn - [ks]_{mn}) f} (\operatorname{mod} P_{k^{-1}}), & \text{otherwise}, \end{cases}$$

(where k^{-1} denotes the inverse of k modulo mn) follows from (5) by means of the binomial theorem. The argument is a straightforward modification of that given in [**2**] for Theorem 5.1. From (7), we see that

$$J(\chi^r,\chi^s)O_K = \prod_{\substack{k=1\\(k,mn)=1\\ [kr]_{mn}+[ks]_{mn}<mn}}^{mn} P_{k^{-1}}. \tag{8}$$

A full discussion of Jacobi sums can be found, for example, in [**3**].

4. The Davenport-Hasse relation.

We now give our new proof of the relation [**1**]. We state the relation in two equivalent forms, first using Gauss sums and then using Jacobi sums.

Theorem 3 (Davenport-Hasse relation). *Using the notation of Section* 3, *for* $t = 1,\dots,m-1$,

$$G(\chi^{tn})\prod_{j=1}^{n-1}G(\chi^{mj})\Big/\prod_{j=0}^{n-1}G(\chi^{mj+t}) = \beta_{mn}^{nt\,\mathrm{ind}_g(n)}, \tag{9}$$

equivalently,

$$\prod_{j=1}^{n-1}(J(\chi^{mj},\chi^t)/J(\chi^{tj},\chi^t)) = \beta_{mn}^{nt\,\mathrm{ind}_g(n)}. \tag{10}$$

Proof. We first prove that equations (9) and (10) are equivalent by expressing the left side of (9) in terms of Jacobi sums:

$$\begin{aligned}
\frac{G(\chi^{tn})\prod_{j=1}^{n-1}G(\chi^{mj})}{\prod_{j=0}^{n-1}G(\chi^{mj+t})} &= \frac{G(\chi^{tn})}{G(\chi^t)}\cdot\prod_{j=1}^{n-1}\frac{G(\chi^{mj})}{G(\chi^{mj+t})}\\
&= \prod_{j=1}^{n-1}\frac{G(\chi^{t(j+1)})}{G(\chi^{tj})}\cdot\prod_{j=1}^{n-1}\frac{G(\chi^{mj})}{G(\chi^{mj+t})}\\
&= \prod_{j=1}^{n-1}\left(\frac{G(\chi^{tj+t})}{G(\chi^{tj})G(\chi^t)}\cdot\frac{G(\chi^{mj})G(\chi^t)}{G(\chi^{mj+t})}\right)\\
&= \prod_{j=1}^{n-1}(J(\chi^{mj},\chi^t)/J(\chi^{tj},\chi^t)) \quad \text{(by (6))}.
\end{aligned}$$

We define $\rho(m,n,t,\chi)$ in K by

$$\rho(m,n,t,\chi)=\prod_{j=1}^{n-1}(J(\chi^{mj},\chi^{t})/J(\chi^{tj},\chi^{t})). \tag{11}$$

It suffices to prove (10) under the assumption that $(t,m)=1$, for if $(t,m)=e$, then $t=et_1$, $m=em_1$, $(t_1,m_1)=1$ for some integers t_1 and m_1, and so (10) becomes $\rho(m_1,n,t_1,\chi^e)=\beta_{m_1n}^{nt_1\operatorname{ind}_g(n)}$, where $\chi^e(g)=\beta_{mn}^e=\beta_{m_1n}$.

Assume now that $(t,m)=1$. We show that we may also suppose that $t|n$. To see this, let $t'=(t,n)$, and let c be such that $tc\equiv t'\pmod{mn}$. As c is coprime with mn/t', there is an integer x such that $a=c+(mn/t')x$ is coprime with mn. Now apply the automorphism σ_a to (10) to obtain

$$\prod_{j=1}^{n-1}J(\chi^{amj},\chi^{at})/J(\chi^{atj},\chi^{at})=\beta_{mn}^{ant\operatorname{ind}_g(n)}.$$

In the numerator of the left side we may change the product index j to aj. After relabelling and using (11) we obtain $\rho(m,n,t',\chi)=\beta_{mn}^{nt'\operatorname{ind}_g(n)}$.

The next step is to show that $\rho=\rho(m,n,t,\chi)$ is a root of unity for $t=1,\ldots,m-1$, with $(t,m)=1$ and $t|n$. Now, by (8),

$$\rho O_K=\prod_{j=1}^{n-1}\left(\prod_{\substack{k=1\\(k,mn)=1\\ [kmj]_{mn}+[kt]_{mn}<mn}}^{mn}P_{k^{-1}}\Bigg/\sum_{\substack{k=1\\(k,mn)=1\\ [ktj]_{mn}+[kt]_{mn}<mn}}^{mn}P_{k^{-1}}\right); \tag{12}$$

that is, using the notation of Theorem 2,

$$\rho O_K=\prod_{\substack{k=1\\(k,mn)=1}}^{mn}(P_{k^{-1}}^{A(m,n,k,t)}/P_{k^{-1}}^{B(m,n,k,t,1)}), \tag{13}$$

which is an integral ideal by Theorem 2(b). Hence, $\rho\in O_K$. The conjugates of ρ are given by $\sigma_a(\rho)$, where $a=1,\ldots,mn$, with $(a,mn)=1$.

A typical conjugate has modulus

$$\begin{aligned}|\sigma_a(\rho)| &= \prod_{j=1}^{n-1}(|J(\chi^{amj},\chi^{at})|/|J(\chi^{atj},\chi^{at})|)\\ &= \prod_{j=1}^{n-1}(\sqrt{p}/\sqrt{p}) = 1.\end{aligned}$$

Since ρ and all of its conjugates have modulus 1, by a classical result (see, for example, Lemma 11.6 in [4]), ρ is a root of unity in O_K, so that $\rho = \beta_{mn}^u$ for some integer u.

In order to determine the value of u, we need a prime ideal P_{k-1} that does not divide any of the Jacobi sums occurring in ρ. By (12), $k = mn-1$ satisfies these conditions since $(k,mn) = 1$, $[kmj]_{mn} + [kt]_{mn} = mn - mj + (mn-t) \geq m + mn - t > mn$, and $[ktj]_{mn} + [kt]_{mn} = (mn-tj) + (mn-t) = 2mn - (j+1)t > mn$. We next use Theorem 1 and the properties of the A_h's introduced in its proof to compute $\rho \pmod{P_{k-1}}$. Using (7) and (11), we see that

$$\begin{aligned}\rho &\equiv \prod_{j=1}^{n-1}\left((-1)^{ktf+1}\binom{[kmj]_{mn}f}{(mn-[kt]_{mn})f}\Bigg/ (-1)^{ktf+1}\binom{[ktj]_{mn}f}{(mn-[kt]_{mn})f}\right) \pmod{P_{k-1}}\\
&\equiv \prod_{j=1}^{n-1}\left(\binom{(mn-mj)f}{tf}\Bigg/\binom{(mn-tj)f}{tf}\right) \pmod{P_{k-1}}\\
&\equiv \prod_{j=1}^{n-1}\frac{((mn-mj)f)!((mn-tj-t)f)!}{((mn-mj-t)f)!((mn-tj)f)!} \pmod{P_{k-1}}\\
&\equiv \prod_{j=1}^{n-1}\frac{A_{mn-mj}A_{mn-mj-1}\cdots A_{mn-mj-t+1}}{A_{mn-tj}A_{mn-tj-1}\cdots A_{mn-tj-t+1}} \pmod{P_{k-1}} \qquad \text{(by (1))}\\
&\equiv \prod_{j=1}^{n-1}\frac{(-1)^{tf}A_{mj+1}A_{mj+2}\cdots A_{mj+t}}{(-1)^{tf}A_{tj+1}A_{tj+2}\cdots A_{tj+t}} \pmod{P_{k-1}} \qquad \text{(by (2))}\\
&\equiv \prod_{j=1}^{n-1}\frac{((mj+t)f)!(tjf)!}{(mjf)!((tj+t)f)!} \pmod{P_{k-1}} \qquad \text{(by (1))}\end{aligned}$$

$$\equiv \frac{(tf)!}{(ntf)!} \prod_{j=1}^{n-1} \frac{((mj+t)f)!}{(mjf)!} (\operatorname{mod} P_{k-1})$$

$$\equiv n^{-(p-1)t/m} (\operatorname{mod} P_{k-1}) \qquad \text{(by Theorem 1).}$$

Therefore,

$$\rho \equiv n^{-ntf} \equiv n^{nktf} \equiv g^{nktf \operatorname{ind}_g(n)} \equiv \beta_{mn}^{nt \operatorname{ind}_g(n)} (\operatorname{mod} P_{k-1}).$$

But we also have $\rho = \beta_{mn}^{u} \equiv g^{kfu} (\operatorname{mod} P_{k-1})$, so that $g^{kfu} \equiv g^{nktf \operatorname{ind}_g(n)} (\operatorname{mod} p)$. This can occur only if $kfu \equiv nktf \operatorname{ind}_g(n))$ $(\operatorname{mod}(p-1))$; that is, $u \equiv nt \operatorname{ind}_g(n) (\operatorname{mod} mn)$. Finally, we have $\rho = \beta_{mn}^{nt \operatorname{ind}_g(n)}$ as required. □

Using Theorem 3, we may remove the condition $t|n$ in Theorem 2(b) and replace the inequality by an equality.

Theorem 4. *Using the notation of Theorem 2, we have*

$$B(m,n,l,t,1) = A(m,n,l,t). \tag{14}$$

Proof. By (13), since ρ is a unit, we have (14). □

We have been unable to prove (14) in a purely arithmetic manner.

5. Final remarks. The impediment to extending our method to prove the Davenport-Hasse relation for Gauss sums over an arbitrary finite field is that it is not always possible to find a prime ideal of O_K that divides p but does not divide any of the Jacobi sums occurring in ρ. For example, consider $m = 2$, $n = 2$, $K = \mathbf{Q}(\beta_4) = \mathbf{Q}(i)$, $q = 3^2 \equiv 1 (\operatorname{mod} 4)$, where $f = (q-1)/mn = 2$ and $3O_K$ is a prime ideal. The group of units of the field $GF(3^2) = \{x + iy | x, y \in GF(3)\}$ is generated by $\gamma = 1 + 2i$, where $\gamma^f = (1+2i)^2 \equiv i (\operatorname{mod} 3O_K)$. We define the character χ by $\chi(\gamma) = i$ and the Jacobi sum by $J(\chi^r, \chi^s) = \sum_{X \in GF(3^2), X \neq 0,1} \chi^r(X) \chi^s(1-X)$. For $t = 1$, we have $\rho = J(\chi^2, \chi)/J(\chi, \chi) = 3/3 = 1$, so that the only prime ideal dividing 3 also divides each Jacobi sum occurring in ρ.

REFERENCES

1. H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunctionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. **172** (1934), 151–182.

2. R.H. Hudson and K.S. Williams, *Binomial coefficients and Jacobi sums*, Trans. Amer. Math. Soc. **281** (1984), 431–505.

3. R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications, Vol. 20, Addison-Wesley Publ. Co., Reading, MA, 1983.

4. I.N. Stewart and D.O. Tall, *Algebraic number theory*, Second edition, Chapman and Hall, London, 1987.

5. K. Yamamoto, *On a conjecture of Hasse concerning multiplicative relations of Gaussian sums*, J. Combin. Theory **1** (1966), 476–489.

DEPARTMENT OF MATHEMATICS, CANISIUS COLLEGE, BUFFALO, NY 14208

DEPARTMENT OF MATHEMATICS AND STATISTICS, OKANAGAN UNIVERSITY COLLEGE, KELOWNA, B.C. V1V 1V7, CANADA

DEPARTMENT OF MATHEMATICS AND STATISTICS, CARLETON UNIVERSITY, OTTAWA, ONTARIO K1S 5B6, CANADA