PURE GAUSS SUMS OVER FINITE FIELDS

RONALD J. EVANS

Abstract. New classes of pairs e, p are presented for which the Gauss sums corresponding to characters of order e over finite fields of characteristic p are pure, *i.e.*, have a real power. Certain pure Gauss sums are explicitly evaluated.

§1. *Introduction.* Stickelberger [7] showed in 1890 that if -1 is a power of p (mod e), then all Gauss sums over finite fields of characteristic p corresponding to characters of all orders dividing e are real. Baumert, Mills and Ward [**1**, Theorems 1 and 4] recently proved the converse, using the theory of cyclotomic periods. In §3, we give a short variant of their proof, via Jacobi sums.

Call a Gauss or Jacobi sum *pure* if some non-zero, integral power of it is real. The main purpose of this paper is to present (see §4) classes of pairs e, p for which -1 is not a power of p (mod e) but the Gauss sums of order e over finite fields of characteristic p are pure. Such pairs do not exist when e is a prime power (see Theorem 2), but they exist for example when e is twice a power of a prime congruent to 7 (mod 8). Some pure Gauss sums are explicitly evaluated in §5.

Chowla and Mordell each showed in 1962 that Gauss sums (mod p) of order $e > 2$ are never pure. For some more recent papers dealing with pure Gauss sums, see Evans [3] and Kubert and Lang [**6**, §3].

§2. *Preliminaries.* In the sequel, fix $e > 2$, let p be prime, $r \geqslant 1$, and $e \mid (p^r - 1)$. Write $q = p^r$.

The finite field $GF(q)$ contains an element g_r of multiplicative order $q-1$. Let $\zeta_n = \exp(2\pi i/n)$. Define a character $\chi = \chi_r$ on $GF(q)$ by $\chi(g_r) = \zeta_e$. Define Gauss and Jacobi sums over $GF(q)$ of orders dividing e as follows.

$$G(\chi^j) = G_r(\chi^j) = \sum_{\substack{\alpha \in GF(q) \\ \alpha \neq 0}} \chi^j(\alpha)\zeta_p^{T(\alpha)},$$

where $T(\alpha) = \alpha^p + \alpha^{p^2} + \ldots + \alpha^{p^r}$, and

$$J(u, v) = J_r(u, v) = \sum_{\substack{\alpha \in GF(q) \\ \alpha \neq 0, 1}} \chi^u(\alpha)\chi^v(1-\alpha).$$

The following formulae are well known [**5**, pp. 91–93, 132–133]. For $j \not\equiv 0 \pmod{e}$,

$$G(\chi^j)G(\bar{\chi}^j) = \chi^j(-1)q, \quad |q^{-1/2}G(\chi^j)| = 1; \tag{1}$$

$$J(0,0) = q-2, \quad J(j,-j) = -\chi^j(-1), \quad J(0,j) = J(j,0) = -1; \tag{2}$$

and

$$J(u, v) = \frac{G(\chi^u)G(\chi^v)}{G(\chi^{u+v})}, \quad \text{if } u+v \not\equiv 0 \pmod{e}. \tag{3}$$

[MATHEMATIKA, **28** (1981), 239–248]

It follows from (1) and (3) that

$$G^e(\chi) = \chi(-1)q \prod_{v=1}^{e-2} J(1,v). \tag{4}$$

We shall use the Hasse–Davenport theorem [5, p. 147] which states that, if $n \mid r$, $e \mid (p^n - 1)$, and $g_n = g_r^{(p^r-1)/(p^n-1)}$, then

$$G_r(\chi_r) = -(-G_n(\chi_n))^{r/n}. \tag{5}$$

We have

$$G_r(\chi) = -(-i_p p^{1/2})^r \text{ when } e = 2, \text{ where } i_p = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4, \\ i, & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{6}$$

In particular, Gauss sums of order $\leqslant 2$ are pure. Formula (6) was proved by Gauss for $r = 1$, and it follows for general r by (5).

By (1), $G(\chi)$ is pure, if, and only if, $q^{-1/2}G(\chi)$ is a root of unity. Thus, by [3, Theorem 4],

$$G(\chi) \text{ is pure, if, and only if, for each } b \text{ prime to } e, \quad \sum_{v=1}^{r} ((bp^v/e)) = 0, \tag{7}$$

where, as usual,

$$((x)) = \begin{cases} x - [x] - 1/2, & \text{if } x \notin \mathbb{Z}, \\ 0, & \text{otherwise}, \end{cases}$$

and where $[x]$ denotes the greatest integer $\leqslant x$. Taking $b = 1$ in (7), we see that

$$\frac{q-1}{(p-1)e} \equiv r/2 \pmod 1, \quad \text{if } G(\chi) \text{ is pure}. \tag{8}$$

For an elementary proof of (8), see [3, p. 345], but please correct the misprint "$2 \nmid r$" on the first line of [3, Cor. 3] to read "$2 \mid r$". It follows from (8) that

$$\chi|_{GF(p)} \text{ has order } \begin{cases} 2, & \text{if } 2 \nmid r, \\ 1, & \text{if } 2 \mid r, \end{cases}, \quad \text{if } G(\chi) \text{ is pure}, \tag{9}$$

where $\chi|_{GF(p)}$ denotes the restriction of χ to $GF(p)$.

The cyclotomic number $(h, k)_r$ of order e over $GF(q)$ is defined to be the number of α in $GF(q)$ such that $\chi(\alpha/g_r^h) = \chi((\alpha+1)/g_r^k) = 1$. The numbers $(h, k)_r$ are related to Jacobi sums by the following easily proved double finite Fourier series relations [4, p. 324]:

$$\chi^u(-1)J(u, v) = \sum_{h=0}^{e-1} \sum_{k=0}^{e-1} (h, k)_r \zeta_e^{hu+kv}, \tag{10}$$

and

$$e^2(h, k)_r = \sum_{u=0}^{e-1} \sum_{v=0}^{e-1} \chi^u(-1)J(u, v)\zeta_e^{-hu-kv}. \tag{11}$$

§3. *Real Gauss sums of all orders dividing e.*

THEOREM 1. *Given e, p and r, with $e > 2$, $e \mid (p^r - 1)$, the following are equivalent.*

$$-1 \text{ is a power of } p \pmod{e}. \tag{12}$$

-1 *is a power* $p^t \pmod{e}$, *and for minimal such $t > 0$ and $s = r/2t$,*

$$p^{-r/2} G_r(\chi^j) = \begin{cases} (-1)^{js+s+1}, & \text{if } 2 \mid e,\ 2 \nmid (p^t+1)/e, \\ (-1)^{s+1}, & \text{otherwise}, \end{cases}$$

$$\text{for all } j \not\equiv 0 \pmod{e}. \tag{13}$$

$$\sum_{v=1}^{r} ((bp^v/e)) = 0 \text{ for all } b \in \mathbb{Z}. \tag{14}$$

$$G_r(\chi^j) \text{ is pure for all } j \in \mathbb{Z}. \tag{15}$$

$$J_r(u, v) \text{ is pure for all } u, v \in \mathbb{Z}. \tag{16}$$

Proof. The equivalence of (12) and (13) is well known [7, §§3.6, 3.10]. The equivalence of (14) and (15) follows easily from (7). The equivalence of (15) and (16) follows from (2)–(4). Trivially (13) implies (15). It remains to show that (16) implies (12).

Define the following sets of ordered pairs with entries $\pmod{e}$:

$$L = \{(u, v) : u, v, u+v \not\equiv 0 \pmod{e}\};$$

$$M = \{(h, k) : h, k, h-k \not\equiv 0 \pmod{e}\}; \quad \text{and}$$

$$N = \{(h, k) : (h, k) \notin M \cup (0, 0)\}.$$

Assume that (16) holds. Without loss of generality, there exists $\theta = \pm 1$ independent of u, v such that

$$J_r(u, v) = \theta p^{r/2}, \quad \text{for all } (u, v) \in L, \tag{17}$$

otherwise replace r by an appropriate multiple of r and employ the Hasse–Davenport theorem. We may assume r is minimal such that (17) holds for some $\theta = \pm 1$. Assume that (12) is false. We shall show that there exist $n \in \mathbb{Z}$ and $\theta_1 = \pm 1$ such that $r = 2n$, $e \mid (p^n - 1)$, and $J_n(u, v) = \theta_1 p^{n/2}$ for all $(u, v) \in L$. This will contradict the minimality of r.

By (17), $p^{r/2} \in \mathbb{Q}(\zeta_e) \cap \mathbb{Q}(\zeta_{4p}) \subset \mathbb{Q}(i)$, so $p^{r/2} \in \mathbb{Z}$ and $r = 2n$. By (2), (11) and (17),

$$e^2(1, 2)_r = p^r + 1 + 2\theta p^{r/2}.$$

Therefore $(1, 2)_r = (p^n + \theta)^2/e^2$ and, since (12) is false, $\theta = -1$ and $e \mid (p^n - 1)$. By (17) and the Hasse–Davenport theorem, $J_n^2(u, v) = p^n$ for all $(u, v) \in L$, so

$$J_n(u, v) = \varepsilon(u, v) p^{n/2} \quad \text{for all } (u, v) \in L, \text{ where } \varepsilon(u, v) = \pm 1. \tag{18}$$

It remains to show that all $J_n(u, v)$ in (18) are equal.

By (18), $p^{n/2} \in \mathbb{Q}(\zeta_e) \cap \mathbb{Q}(\zeta_{4p}) \subset \mathbb{Q}(i)$, so n is even. By (18) and (4) with n in place of r, $G_n(\chi_n)$ is pure. Thus by (9), $\chi_n(-1) = 1$. Now from (2), (11) and (18),

$$e^2(h,k)_n = p^n + 1 + p^{n/2}\, Y(h,k) \quad \text{for all } (h,k) \in M \tag{19}$$

and

$$e^2(h,k)_n = p^n + 1 - e + p^{n/2}\, Y(h,k) \quad \text{for all } (h,k) \in N\,, \tag{20}$$

where

$$Y(h,k) = \sum_{(u,v)\in L} \varepsilon(u,v)\zeta_e^{-hu-kv}\,. \tag{21}$$

By (19)–(21), the algebraic integers $Y(h,k)$ are in fact rational integers satisfying $|Y(h,k)| < e^2$.

First consider the $Y(h,k)$ with $(h,k) \in M$. By (19), they are all congruent to each other $(\operatorname{mod} e^2)$. Moreover, they are all even, since

$$Y(h,k) \equiv \sum_{(u,v)\in L} \zeta_e^{-hu-kv} = 2 \pmod 2\,.$$

Thus if e is odd, these $Y(h,k)$ are congruent to each other $(\operatorname{mod} 2e^2)$, so they are all equal. Suppose now that e is even. As $(h,k) \in M$, one of $(h+e/2, k)$, $(h, k+e/2)$ and $(h+e/2, k+e/2)$ is in M. Say the latter is in M; the argument proceeds similarly in the other cases. Then

$$\sum_{\substack{(u,v)\in L\\ 2\mid(u+v)}} \varepsilon(u,v)\zeta_e^{-hu-kv} = \tfrac{1}{2}\big(Y(h,k) - Y(h+e/2, k+e/2)\big) \equiv 0 \,(\operatorname{mod} e^2/2)\,,$$

and the left sum has fewer than $e^2/2$ terms, so it vanishes. Thus

$$|Y(h,k)| = \left| \sum_{\substack{(u,v)\in L\\ 2\nmid(u+v)}} \varepsilon(u,v)\zeta_e^{-hu-kv} \right| < e^2/2\,.$$

Therefore, all the $Y(h,k)$ with $(h,k) \in M$ are equal.

Similarly, we see that all $Y(h,k)$ with $(h,k) \in N$ are equal. It then follows from (19) and (20) that all $(h,k)_n$ with $(h,k) \in M$ are equal, and all $(h,k)_n$ with $(h,k) \in N$ are equal. Therefore, by (10), all $J_n(u,v)$ with $(u,v) \in L$ are equal.

It would be nice to have an elementary proof of the equivalence of (12) and (14). Of course (12) trivially implies (14) since $((-x)) = -((x))$.

§4. *Pure Gauss sums of order e.* Theorem 1 showed that -1 is a power of $p \,(\operatorname{mod} e)$, if, and only if, $G(\chi^j)$ is pure for all j. Theorem 2 below shows that, if e is a prime power, then in fact -1 is a power of p $(\operatorname{mod} e)$, if, and only if, $G(\chi)$ is pure.

THEOREM 2. *Suppose that e is a prime power and that $G(\chi)$ is pure. Then -1 is a power of p* $(\operatorname{mod} e)$.

Proof. By the Hasse–Davenport theorem, we may assume that r is the order of p $(\operatorname{mod} e)$. We have $2 \mid r$, otherwise (8) yields the contradiction $2 \,\|\, e$. If $2 \nmid e$, then

$e \mid (p^{r/2}+1)$, since $e \mid (p^r-1)$ and $e \nmid (p^{r/2}-1)$. Finally, suppose that e is a power of 2. By (8), $e \mid (p^{r/2}+1)W$, where $W = (p^{r/2}-1)/(p-1)$. We must have $e \mid (p^{r/2}+1)$; otherwise $2 \mid W$, so $4 \mid (p^{r/2}-1)$, so $2 \parallel (p^{r/2}+1)$, so $e/2 \mid W$, so $e \mid (p^{r/2}-1)$, a contradiction.

The condition that e be a prime power in Theorem 2 cannot be dropped. In Corollaries 4 and 5, we exhibit pairs e, p for which -1 is not a power of $p \pmod e$ and $G(\chi)$ is pure.

The following notation will be used. If $m > 0$, $p \nmid m$, let $o_m(p)$ denote the order of $p \pmod m$ and let $\langle p\rangle \pmod m$ denote the group of $o_m(p)$ powers of $p \pmod m$. Thus p is a primitive root $\pmod m$, if, and only if, $o_m(p) = \phi(m)$.

THEOREM 3. *Suppose that $e = DE$ with $(D, E) = 1$ and $\big(o_D(p), o_E(p)\big) = 1$. Then $G(\chi)$ is pure, if any of the following three conditions is satisfied.*

$$o_D(p) = \phi(D) \quad \text{and} \quad \delta \in \langle p\rangle \pmod E \text{ for some prime } \delta \mid D. \tag{22}$$

$$-1 \notin \langle p\rangle \pmod D,\ 2o_D(p) = \phi(D),\ \delta \in \langle p\rangle \pmod E \text{ for some prime } \delta \mid D, \text{ and all of this holds with } D \text{ and } E \text{ interchanged}. \tag{23}$$

$$2 \parallel e,\ 2+e/2 \notin \langle p\rangle \pmod D,\ 2o_D(p) = \phi(D),\ -1 \text{ or } \delta \text{ is in } \langle p\rangle \pmod E \text{ for some prime } \delta \mid D, \text{ and all of this holds with } D \text{ and } E \text{ interchanged.} \tag{24}$$

Proof. By the Hasse–Davenport theorem, we may assume that $r = o_e(p)$. By (7), it is to be shown that $\sum_{v=1}^{r} \big((bp^v/e)\big) = 0$, for each b prime to e. Write $\sum_{n*e}$ to denote summation over n with $0 < n < e$, $(n, e) = 1$. We have

$$\sum_{v=1}^{r} \big((bp^v/e)\big) = -\frac{r}{2} + \sum_{\substack{n*e \\ n/b \in \langle p\rangle \pmod e}} n/e,$$

so it suffices to show that

$$S = \sum_{\substack{n*e \\ n/b \in \langle p\rangle \pmod e}} n = er/2.$$

If $m > 0$, $p \nmid m$, define G_m to be the group of Dirichlet characters $\pmod m$ which map p to 1. One can regard G_m as the character group on $R_m/\langle p\rangle$, where R_m is the group of $\phi(m)$ reduced residues $\pmod m$. Thus $|G_m| = \phi(m)/o_m(p)$. Since $(D, E) = \big(o_D(p), o_E(p)\big) = 1$, we can regard G_e as the internal direct product of G_D and G_E. Thus each $\Lambda \in G_e$ can be uniquely written in the form $\Lambda = \psi\lambda$, where $\psi \in G_D$, $\lambda \in G_E$.

By definition of S,

$$S = |G_e|^{-1} \sum_{n*e} n \sum_{\Lambda \in G_e} \Lambda(n/b) = S_1 + S_2,$$

where

$$S_1 = |G_e|^{-1} \sum_{n*e} n, \quad S_2 = |G_e|^{-1} \sum_{1 \neq \Lambda \in G_e} \sum_{n*e} \Lambda(n/b)n.$$

It remains to show that $S_1 = er/2$ and $S_2 = 0$.

First, letting μ denote the Moebius function, we have

$$|G_e|S_1 = \sum_{0<n<e} n \sum_{d\mid n, d\mid e} \mu(d) = \sum_{d\mid e} d\mu(d) \sum_{0<k<e/d} k$$

$$= \sum_{d\mid e} d\mu(d) \frac{e}{2d}\left(\frac{e}{d} - 1\right) = \frac{e^2}{2}\sum_{d\mid e}\frac{\mu(d)}{d} = \frac{e\phi(e)}{2}.$$

Since $|G_e| = \phi(e)/r$, it follows that $S_1 = er/2$.

Next, if $|G_e| = 1$, then $S_2 = 0$ and the proof is complete. Therefore suppose that $|G_e| > 1$, and choose $\Lambda \neq 1$ in G_e. We must show that $\sum_{n*e}\Lambda(n)n = 0$, or, equivalently, that

$$\sum_{n*e} \psi\lambda(n)n = 0, \tag{25}$$

where ψ is a character (mod D), λ is a character (mod E), $\psi(p) = \lambda(p) = 1$, and not both λ and ψ are trivial.

We first dispense with the case $\psi = 1$, *i.e.*, we show that

$$\sum_{n*e} \lambda(n)n = 0. \tag{26}$$

In view of (22)–(24), -1 or δ is in $\langle p\rangle$ (mod E) for some prime δ dividing D. Thus $\lambda(-1) = 1$ or $\lambda(\delta) = 1$. If $\lambda(-1) = 1$, then

$$\sum_{n*e}\lambda(n)n = \sum_{n*e}\lambda(e-n)(e-n) = -\sum_{n*e}\lambda(n)n,$$

and (26) follows. If $\lambda(\delta) = 1$, then letting D_0 denote the largest factor of D prime to δ, we have

$$\sum_{\substack{0<n<e\\ \delta\mid n, (n,D_0)=1}} \lambda(n)n = \delta \sum_{\substack{0<k<e/\delta\\ (k,D_0)=1}} \lambda(k)k = \sum_{\substack{0<k<e/\delta\\ (k,D_0)=1}} \lambda(k)\sum_{j=1}^{\delta}\left(k + \frac{je}{\delta}\right)$$

$$= \sum_{j=1}^{\delta}\sum_{\substack{0<k<e/\delta\\ (k,D_0)=1}} \lambda\left(k+\frac{je}{\delta}\right)\left(k+\frac{je}{\delta}\right) = \sum_{\substack{0<n<e\\ (n,D_0)=1}} \lambda(n)n, \tag{27}$$

where the second equality holds because

$$\sum_{\substack{0<k<e/\delta\\ (k,D_0)=1}} \lambda(k) = 0.$$

Subtraction of the left sum from the right in (27) yields (26). Thus (26) is proved.

If (22) holds, then $|G_D| = 1$, so ψ is trivial, and (25) follows from (26). Therefore assume that (23) or (24) holds. If either ψ or λ is trivial, then, by symmetry in D and E, (25) follows from (26). Thus assume that both λ and ψ are non-trivial. In view of (23), (24) and symmetry, $|G_E| = |G_D| = \phi(D)/o_D(p) = 2$, so λ and ψ are quadratic.

Assume that (23) holds. Then $\lambda(-1) = \psi(-1) = -1$, so $\lambda\psi(-1) = 1$. Thus $\sum_{n*e}\lambda\psi(n)n$ equals its negative, and (25) follows.

Finally, assume that (24) holds. Since $2 \parallel e$, we can define a non-trivial character Λ' (mod $e/2$) by

$$\Lambda'(n) = \begin{cases} \psi\lambda(n), & \text{if } 2 \nmid n\,, \\ \psi\lambda(n+e/2), & \text{if } 2 \mid n\,. \end{cases}$$

By (24), $\Lambda'(2) = (-1)(-1) = 1$. Thus (*cf.* (27)),

$$\sum_{\substack{0<n<e \\ 2\mid n}} \Lambda'(n)n = 2 \sum_{0<k<e/2} \Lambda'(k)k = \sum_{0<n<e} \Lambda'(n)n\,.$$

Subtraction of the left sum from the right yields $\sum_{n*e} \Lambda'(n)n = 0$, and (25) follows.

The corollaries below illustrate Theorem 3.

COROLLARY 4. *For a fixed pair e, p, $G(\chi)$ is pure and $-1 \notin \langle p\rangle$ (mod e), if either of the following conditions holds.*

$e = 2E$, where E is odd and divisible by a prime $c \equiv 7$ (mod 8), p is a square (mod c), and $2 \in \langle p\rangle$ (mod E) (for example, take $p \equiv 2$ (mod E)). (28)

$e = \delta^m E$, where δ is an odd prime, $m \geqslant 1$, $E > 2$, $\delta \nmid E$, p is a primitive root (mod δ^m), and $p \equiv \delta \equiv 1$ (mod E). (29)

Proof. If (29) holds, $-1 \notin \langle p\rangle$ (mod e) since $p \equiv 1$ (mod E) and $E > 2$. If (28) holds, then $-1 \notin \langle p\rangle$ (mod e) because p is a square (mod c) while -1 is not.

If (28) holds, then (22) is satisfied with $D = \delta = 2$, so $G(\chi)$ is pure by Theorem 3. If (29) holds, then (22) is satisfied with $D = \delta^m$, so $G(\chi)$ is pure.

The next corollary provides specific examples in which $e = BF$ is a small multiple of $F = c^m$, where c is an odd prime, $c \nmid B$, $m \geqslant 1$, and p is either a primitive root (mod F), in which case we write $p \equiv G$ (mod F), or the square of a primitive root (mod F), in which case we write $p \equiv G^2$ (mod F).

COROLLARY 5. *For a fixed pair e, p as above, $G(\chi)$ is pure and $-1 \notin \langle p\rangle$ (mod e), if any of the following conditions holds.*

$$e = 2F, \quad c \equiv 7 \pmod 8, \quad p \equiv G^2 \pmod F\,. \tag{30}$$

$$e = 3F, \quad c \equiv 11 \pmod{12}, \quad p \equiv G^2 \pmod F, \quad p \equiv 2 \pmod 3\,. \tag{31}$$

$$e = 4F, \quad c \equiv 7 \pmod 8, \quad p \equiv G^2 \pmod F, \quad p \equiv 3 \pmod 4\,. \tag{32}$$

$$e = 5F, \quad c \equiv 11 \text{ or } 19 \pmod{20}, \quad p \equiv G^2 \pmod F, \quad p \equiv \pm 2 \pmod 5\,. \tag{33}$$

$$e = 6F, \quad c \equiv 7, 11 \text{ or } 23 \pmod{24}, \quad p \equiv G^2 \pmod F, \quad p \equiv 5 \pmod 6\,. \tag{34}$$

$$e = 6F, \quad c \equiv 7 \text{ or } 13 \pmod{24}, \quad p \equiv G^2 \pmod F, \quad p \equiv 1 \pmod 6\,. \tag{35}$$

$$e = 6F, \quad c \equiv 5 \text{ or } 13 \pmod{24}, \quad p \equiv G \pmod F, \quad p \equiv 5 \pmod 6\,. \tag{36}$$

Proof. If one of (30)–(34) holds, then $-1 \notin \langle p \rangle \pmod{e}$ since p is a square $\pmod{c}$ while -1 is not. If (35) holds, $-1 \notin \langle p \rangle \pmod{e}$ since $p \equiv 1 \pmod{6}$. If (36) holds and $-1 \equiv p^a \pmod{e}$, then a is odd because $p \equiv 5 \pmod{6}$, but a is even because -1 is a square $\pmod{c}$ while p is not; thus $-1 \notin \langle p \rangle \pmod{e}$.

If (36) holds, then (22) is satisfied with $D = \delta = 2$, $E = 3F$, so $G(\chi)$ is pure by Theorem 3. If (35) holds with $c \equiv 7 \pmod{24}$, then (23) is satisfied with $D = 6$, $E = F$, where $\delta = 2$ is the relevant divisor of D. If (35) holds with $c \equiv 13 \pmod{24}$, then (24) is satisfied with $D = 6$, $E = F$, where $\delta = 3$ is the relevant divisor of D. Thus $G(\chi)$ is pure if (35) holds. If one of (30)–(34) holds, then (22) is satisfied with $D = B$, $E = F$, so $G(\chi)$ is pure.

Numerical examples. Let V denote the set of pairs e, p for which $G(\chi)$ is pure and $-1 \notin \langle p \rangle \pmod{e}$. If the pair e, p is in V, so is e, p' for any prime $p' \equiv p \pmod{e}$, and we will not distinguish between e, p and e, p'. There are 58 pairs e, p in V with $e < 60$. They correspond to twelve values of e, namely $e = 14, 20, 21, 28, 30, 33, 39, 42, 46, 52, 55$ and 57. All 58 pairs can be found through Theorem 3, most often *via* (22), but a few times *via* (23) and (24). The first 14 pairs in V are given in the following table.

e	14	20	21	28	30	33
$p \pmod{e}$	9, 11	13, 17	10, 19	11, 23	17, 23	5, 14, 20, 26

For a pair e, p in V, $o_e(p) \geqslant 3$ (see [**3**, p. 346]). One might ask: for which fixed values of $r = o_e(p)$ do there correspond infinitely many pairs e, p in V?

§5. *Evaluations of certain pure Gauss sums.*

LEMMA 6. *If $G(\chi)$ is pure, then $\theta = q^{-1/2}G(\chi)$ satisfies $\theta^{2d} = 1$, where $d = (e, p-1)$.*

Proof. Let v be 1 or 2 according as $2 \nmid e$ or $2 \mid e$. By (8), $2 \mid r$ when $2 \nmid e$. Thus, by the definition of θ, $\theta^v \in \mathbb{Q}(\zeta_{pe})$. Therefore, $\theta^{2pe} = 1$. By (4), $\theta^{ve} \in \mathbb{Q}(\zeta_e)$, so $\theta^{2e^2} = 1$. Since $(2pe, 2e^2) = 2e$,

$$\theta^{2e} = 1\,. \tag{37}$$

Let a satisfy $a \equiv p \pmod{e}$, $a \equiv 1 \pmod{p}$. Define $\sigma_a \in \mathrm{Gal}\left(\mathbb{Q}(\zeta_{pe})/\mathbb{Q}\right)$ by $\sigma_a(\zeta_{pe}) = \zeta_{pe}^a$. Then

$$\sigma_a G(\chi) = \bar{\chi}^a(a) G(\chi^a) = G(\chi^a) = G(\chi^p) = G(\chi)\,.$$

Therefore $\sigma_a(\theta^2) = \theta^2$. On the other hand, by (37), $\sigma_a(\theta^2) = \theta^{2a} = \theta^{2p}$, so $\theta^{2(p-1)} = 1$. Together with (37), this implies that $\theta^{2d} = 1$.

THEOREM 7. *Suppose that $e = BF$, $(B, F) = 1$, $B > 1$, $F = c^m$, $m \geqslant 1$, c is an odd prime, $p \not\equiv 1 \pmod{c}$, and $G(\chi)$, $G(\chi^F)$ are pure. Then $G(\chi) = G(\chi^{FH})$, where $H \equiv F^{-1} \pmod{B}$.*

Proof. Write $\lambda_F = 1-\zeta_F$. For each $n \in GF(q)$, $\chi(n) \equiv \chi(n)^{FH} \pmod{\lambda_F}$, so

$$G(\chi) \equiv G(\chi^{FH}) \pmod{\lambda_F}. \tag{38}$$

Since $G(\chi^{FH})$ is an algebraic conjugate of the pure Gauss sum $G(\chi^F)$, we can write

$$G(\chi) = \theta q^{1/2}, \quad G(\chi^{FH}) = \varepsilon q^{1/2}, \tag{39}$$

where θ and ε are roots of unity. By (38) and (39), $\theta \equiv \varepsilon \pmod{\lambda_F}$, so since $F = c^m$,

$$\theta/\varepsilon = \zeta_F^n \quad \text{for some integer } n. \tag{40}$$

By Lemma 6 with B in place of e, $\varepsilon^{2B} = 1$. Since $2(e, p-1)$ divides $2B$, Lemma 6 gives $\theta^{2B} = 1$, so $(\theta/\varepsilon)^{2B} = 1$. By (40), $\zeta_F^{2nB} = 1$, so $F \mid n$; (40) and (39) now yield the desired result.

We now apply Theorem 7 to evaluate, for example, some pure Gauss sums that arose in the last section.

Corollary 8. *Suppose that $e = 2E = 2\prod_{i=1}^{k} c_i^{m_i}$, where $m_i \geqslant 1$, the c_i are distinct odd primes, $(E, p-1) = 1$, and $2 \in \langle p \rangle \pmod{E}$, e.g., take $p \equiv 2 \pmod{E}$. Then $G(\chi) = -(-i_p)^r q^{1/2}$.*

Proof. Write $e = BF$ with $F = c_k^{m_k}$. Since (22) holds with $D = 2$, $G(\chi)$ is pure by Theorem 3. Similarly, $G(\chi^F)$ is pure. By Theorem 7, $G(\chi) = G(\chi^{FH})$, where $H \equiv F^{-1} \pmod{B}$. Iterating this process k times, we ultimately find that $G(\chi) = G(\chi^E)$, so by (6), $G(\chi) = -(-i_p)^r q^{1/2}$.

Note that Corollary 8 provides an evaluation of $G(\chi)$ when (30) holds. Corollary 9 below evaluates $G(\chi)$ when (31), (32), (33), (34) or (36) holds. Finally, (35) is considered in Theorem 10.

Corollary 9. *According as (31), (32), (33), (34) or (36) holds, $-q^{-1/2}G(\chi) = (-1)^{r/2}, (-1)^{r(p-3)/8}, (-1)^{r/4}, (-1)^{r(p-5)/8}$ or 1.*

Proof. In all five cases, $-1 \in \langle p \rangle \pmod{B}$, where $e = BF$, so $G(\chi^F)$ is pure by Theorem 1. Thus Theorem 7 may be applied to yield $G(\chi) = G(\chi^{FH})$. Applying (13) with, say, B, x, y in place of e, t, s, we therefore obtain

$$-q^{-1/2}G(\chi) = \begin{cases} 1, & \text{if } 2 \mid B,\ 2 \nmid (p^x+1)/B, \\ (-1)^y, & \text{otherwise}. \end{cases}$$

The result now easily follows; for example, if (36) holds, then $B = 6$, $x = 1$, $y = r/2$ and $4 \mid r$, since $4 \mid o_E(p)$, so $-q^{-1/2}G(\chi) = 1$.

Theorem 10. *Let $\lambda_F = 1-\zeta_F$. If (35) holds, then $G(\chi) = \theta q^{1/2}$ for the twelfth root of unity θ satisfying*

$$\theta \equiv (-1)^{r-1}(p^2 J^2(\psi)/i_p)^{r/3} \pmod{\lambda_F}, \tag{41}$$

where ψ *is the cubic character* (mod p) *defined by* $\psi(g_r^{(p^r-1)/(p-1)}) = \zeta_3$, *and* $J(\psi)$ *is the Jacobi sum*

$$\sum_{a \pmod p} \psi(a(1-a)).$$

Proof. By Lemma 6, $\theta = q^{-1/2}G(\chi)$ is a twelfth root of unity. Since $F \equiv 1 \pmod 6$, $\chi(n) \equiv \chi(n)^F \pmod{\lambda_F}$ for each $n \in GF(q)$, so

$$\theta q^{1/2} = G(\chi) \equiv G(\chi^F) \pmod{\lambda_F}. \tag{42}$$

By (5) with $n = 1$,

$$G(\chi^F) = (-1)^{r-1} G_1(\Omega)^r, \tag{43}$$

where Ω is a character (mod p) of order 6 defined by $\Omega(g_r^{(p^r-1)/(p-1)}) = \zeta_6$. By (42) and (43),

$$\theta q^{1/2} \equiv (-1)^{r-1}(G_1^3(\Omega))^{r/3} \pmod{\lambda_F}. \tag{44}$$

Note that $3 \mid r$ since $3 \mid o_F(p)$. From [2, Theorem 3.1], $G_1^3(\Omega) = p^{1/2}J^2(\psi)/i_p$, where $\psi = \Omega^2$ and i_p is defined in (6). Thus (41) follows from (44).

Numerical example. Suppose that $e = 42$, $p = 67$, $r = 3$. By (41), $\theta = q^{-1/2}G(\chi)$ satisfies

$$\theta \equiv -2iJ^2(\psi) \pmod{\lambda_7}.$$

Using [2, Theorem 3.4], we see that $J(\psi) = (-5+9\varepsilon i\sqrt{3})/2$, where $\varepsilon = \pm 1$. Thus $J(\psi) \equiv 1+\varepsilon i\sqrt{3} = 2\zeta_6^{\varepsilon} \pmod{\lambda_7}$, so $\theta = -i\zeta_3^{\varepsilon}$.

The author is grateful to Neal Olander for his valuable assistance in efficient Fortran programming.

References

1. L. D. Baumert, W. H. Mills and R. L. Ward. "Uniform cyclotomy", *J. Number Theory* (to appear).
2. B. C. Berndt and R. J. Evans. "Sums of Gauss, Jacobi, and Jacobsthal", *J. Number Theory*, 11 (1979), 349–398.
3. R. J. Evans. "Generalizations of a theorem of Chowla on Gaussian sums", *Houston J. Math.*, 3 (1977), 343–349.
4. R. E. Giudici, J. B. Muskat and S. F. Robinson. "On the evaluation of Brewer's character sums", *Trans. Amer. Math. Soc.*, 171 (1972), 317–347.
5. K. Ireland and M. I. Rosen. *Elements of number theory* (Bogden & Quigley, Tarrytown-on-Hudson, 1972).
6. D. S. Kubert and S. Lang. "Independence of modular units on Tate curves", *Math. Annalen*, 240 (1979), 191–201.
7. L. Stickelberger. "Über eine Verallgemeinerung der Kreistheilung", *Math. Annalen*, 37 (1890), 321–367.

Prof. R. J. Evans,
Department of Mathematics,
University of California, San Diego,
La Jolla, California 92093,
U.S.A.

10G05: *NUMBER THEORY; Trigonometric sums, exponential sums and character sums; exponential sums.*

Received on the 26th of March, 1981.