ACTA ARITHMETICA
XXXIX (1981)

Period polynomials and Gauss sums for finite fields

by

GERALD MYERSON (Buffalo, N. Y.)

1. Introduction. For each prime p and each divisor e of $p-1$ Gauss [7] introduced two families of exponential sums, the cyclotomic periods and the Gauss sums. His definitions have long since been extended to give families of sums for each prime power $q = p^a$ and each divisor e of $q-1$. The definitions are given below.

We first study the period polynomials, whose roots are the cyclotomic periods, and the modified period polynomials, whose roots are the Gauss sums. In the case $q = p$, these polynomials were shown by Gauss to be irreducible over the rationals. In the more general case, we prove a theorem on the number of factors of the polynomials, and we give necessary and sufficient conditions for irreducibility.

In the cases $e = 2$, 3, and 4, we derive explicit formulas for the period polynomials, and produce a detailed account of their factorizations over the rationals.

We then turn to the problem of the location of the Gauss sums. In the case $q = p$, there is a celebrated result of Gauss when $e = 2$, and a notoriously difficult problem when $e = 3$ or 4. The case $q = p^a$, $a > 1$, is often less difficult, and a number of explicit determinations of Gauss sums are given.

2. Notations, conventions, definitions. The following notations, conventions, and definitions will be maintained throughout.

e and f are positive integers such that $ef+1 = p^a = q$ is a prime power. $\boldsymbol{F}_q$ is the field of q elements, $\boldsymbol{F}_q^*$ its multiplicative group, g a generator of $\boldsymbol{F}_q^*$. C_0 is the group of eth powers in $\boldsymbol{F}_q^*$, and its cosets are $C_k = g^k C_0$, $k = 0, 1, \ldots, e-1$.

$\theta = \exp(2\pi i/p)$ is a primitive complex pth root of unity.

Tr is the trace map, $\mathrm{Tr}: \boldsymbol{F}_q \to \boldsymbol{F}_p$.

The cyclotomic periods η_k are given by

$$\eta_k = \sum_{x \in C_k} \theta^{\mathrm{Tr}x}, \qquad k = 0, 1, \ldots, e-1.$$

The Gauss sums G_k are given by

$$G_k = \sum_{x \in F_q} \theta^{\mathrm{Tr}\vartheta^k x^e}, \qquad k = 0, 1, \ldots, e-1.$$

If χ is a character on F_q^* of order d then the Lagrange resolvent $\tau(\chi)$ is given by

$$\tau(\chi) = \sum_{x \in F_q^*} \chi(x)\theta^{\mathrm{Tr}x}.$$

In the literature the term "Gauss sum" is used by some authors to mean G_k and by others to mean $\tau(\chi)$. The terminology used in this paper is for convenience only; the author makes no claim of historical accuracy. In this paper we are primarily concerned with the η_k and G_k, and only peripherally with the $\tau(\chi)$.

If $k \geqslant e$ then the subscripts in C_k, η_k, and G_k are to be interpreted (modulo e).

The period polynomials $\varphi_e(X)$ are given by

$$\varphi_e(X) = \prod_{k=0}^{e-1} (X - \eta_k),$$

and the modified period polynomials $F_e(X)$ by

$$F_e(X) = \prod_{k=0}^{e-1} (X - G_k).$$

$\delta = \gcd\bigl(e, (q-1)/(p-1)\bigr)$.

The elements of the Galois group of $\boldsymbol{Q}(\theta)/\boldsymbol{Q}$ are denoted by σ_a, $a = 1, 2, \ldots, p-1$, where $\sigma_a(\theta) = \theta^a$.

3. Well known facts. We gather in Proposition 1 a host of facts about our exponential sums which are well known or which follow directly from the definitions.

PROPOSITION 1. (a) $G_k = e\eta_k + 1$.

(b) $\sum_{k=0}^{e-1} \eta_k = -1$, $\sum_{k=0}^{e-1} G_k = 0$.

(c) $F_e(X) = e^e \varphi_e\bigl((X-1)/e\bigr)$, $\varphi_e(X) = e^{-e} F_e(eX+1)$.

(d) $\tau(\overline{\chi}) = \chi(-1)\overline{\tau(\chi)}$.

(e) $|\tau(\chi)| = \sqrt{q}$.

(f) *If ω is a primitive complex e-th root of unity, and we define the character χ_j by $\chi_j(g) = \omega^j$, then*

$$\tau(\chi_j) = \sum_{k=0}^{e-1} \omega^{jk}\eta_k \quad \textit{and} \quad \eta_k = \frac{1}{e}\sum_{j=0}^{e-1} \omega^{-jk}\tau(\chi_j).$$

(g)

$$G_k = \sum_{j=1}^{e-1} \omega^{-jk}\tau(\chi_j), \qquad \tau(\chi_j) = \begin{cases} \dfrac{1}{e}\displaystyle\sum_{k=0}^{e-1} \omega^{jk} G_k & \text{if} \quad j \neq 0, \\ -1 & \text{if} \quad j = 0. \end{cases}$$

(h) *If $e = 2$ and χ is the quadratic character then $G_0 = \tau(\chi)$.*

4. Factorization of the period polynomials. In this section we prove two theorems on the factorization of the polynomials $\varphi_e(X)$ and $F_e(X)$. Proofs will be given only for $\varphi_e(x)$; the results for $F_e(X)$ follow by Proposition 1 (c).

The effect of $\mathrm{Gal}\bigl(\boldsymbol{Q}(\theta)/\boldsymbol{Q}\bigr)$ on η_k is given by the following lemma.

LEMMA 2. *If $a \in \boldsymbol{F}_p \cap C_k$, then $\sigma_a(\eta_m) = \eta_{m+k}$.*

Proof. From $\eta_m = \sum_{x \in C_m} \theta^{\mathrm{Tr}x}$ we get

$$\sigma_a(\eta_m) = \sum_{x \in C_m} \theta^{a\,\mathrm{Tr}x} = \sum_{x \in C_m} \theta^{\mathrm{Tr}ax} = \sum_{x \in C_{m+k}} \theta^{\mathrm{Tr}x} = \eta_{m+k}.$$

From this it follows that the period polynomials have integer coefficients.

THEOREM 3. $\varphi_e(X) \in Z[X]$, $F_e(X) \in Z[X]$.

Proof. Given any cyclotomic period, Lemma 2 shows that its conjugates are all periods, and that each conjugate occurs equally often among the periods. Thus $\varphi_e(X)$ is a product of powers of the minimal irreducible polynomials for the η_k. The η_k are algebraic integers, so $\varphi_e(X) \in Z[X]$.

In the case $q = p$, Gauss showed that the period polynomials are irreducible over the rationals. This is not always true in our more general setting. More precisely, we have

THEOREM 4. *$\varphi_e(X)$ and $F_e(X)$ split over the rationals into δ factors of degree e/δ. Each of these factors is irreducible or a power of an irreducible polynomial.*

We must first establish a lemma.

LEMMA 5. *$\boldsymbol{F}_p \cap C_k$ is non-empty if, and only if, $\delta | k$.*

Proof. Since $\delta = \gcd\bigl(e, (q-1)/(p-1)\bigr)$, there exist integers m and s such that $m(q-1)/(p-1) - es = k$ if, and only if, $\delta | k$. Now observe that

$$g^{m(q-1)/(p-1)} = g^k g^{es} \in \boldsymbol{F}_p \cap C_k.$$

Proof of Theorem 4. Let $\varphi^{(k)}(X) = (X-\eta_k)(X-\eta_{k+\delta})\dots(X-\eta_{k+e-\delta})$. By Lemmas 2 and 5, the roots of $\varphi^{(k)}(X)$ are the conjugates of η_k, each distinct conjugate occurring equally often. Thus $\varphi^{(k)}(X)$ is in $Z[X]$ and is irreducible or a power of an irreducible polynomial. Now $\varphi_e(X) = \prod_{k=0}^{\delta-1} \varphi^{(k)}(X)$, proving the theorem.

By way of an example, we take $e = 8$, $f = 3$, so $q = 25 = 5^2$. We can realize $\boldsymbol{F}_{25}$ as $\boldsymbol{F}_5(x) = \{ax+b\colon |a| \leqslant 2,\ |b| \leqslant 2\}$, where $x^2 = 2$, and we can take $g = x+2$. Then

$$C_0 = \{1, -2x+2, 2x+2\}, \qquad C_1 = \{x+2, -2x, x-2\},$$
$$C_2 = \{-x+1, x+1, -2\}, \qquad C_3 = \{-x, -2x-1, -2x+1\},$$
$$C_4 = \{-2x-2, -1, 2x-2\}, \qquad C_5 = \{-x+2, -x-2, 2x\},$$
$$C_6 = \{2, x-1, -x-1\}, \qquad C_7 = \{2x-1, x, 2x+1\}.$$

The conjugate of $ax+b$ over $\boldsymbol{F}_5$ is $-ax+b$, thus $\mathrm{Tr}(ax+b) = 2b$. Let $\beta = \exp(2\pi i/5)$. Then

$$\eta_0 = \beta^2+2\beta^4, \quad \eta_1 = 1+\beta+\beta^4, \quad \eta_2 = \beta+2\beta^2, \quad \eta_3 = 1+\beta^2+\beta^3,$$
$$\eta_4 = 2\beta+\beta^3, \quad \eta_5 = 1+\beta+\beta^4, \quad \eta_6 = 2\beta^3+\beta^4, \quad \eta_7 = 1+\beta^2+\beta^3,$$

and

$$\varphi_8(X) = [(X-\eta_0)(X-\eta_2)(X-\eta_4)(X-\eta_6)][(X-\eta_1)(X-\eta_3)][(X-\eta_5)\times$$
$$\times(X-\eta_7)] = (X^4+3X^3+9X^2+7X+11)(X^2-X-1)^2.$$

Also,

$$F_8(X) = 8^3\varphi_8((X-1)/8)$$
$$= (X^4+20X^3+510X^2+2500X+42025)(X^2-10X-55)^2.$$

When $\delta = 1$, Theorem 4 shows that $\varphi_e(X)$ and $F_e(X)$ are irreducible or a power of an irreducible polynomial. In fact, in this case these polynomials are always irreducible, as we now prove.

THEOREM 6. *$\varphi_e(X)$ and $F_e(X)$ are irreducible over the rationals if, and only if, $\delta = 1$.*

Proof. The necessity of the condition $\delta = 1$ is evident from Theorem 4. To prove sufficiency, we note that the coefficient of X^{e-1} in $\varphi_e(X)$ is $-\sum_{k=0}^{e-1} \eta_k = 1$. Therefore $\varphi_e(X)$ can not be a power higher than the first of another polynomial. Hence, if $\delta = 1$, then $\varphi_e(X)$ and $F_e(X)$ are irreducible.

COROLLARY 7. *The following are equivalent.*

(a) *$\varphi_e(X)$ is irreducible.*

(b) *$F_e(X)$ is irreducible.*

(c) *$\delta = 1$.*

(d) *$p \equiv 1 \pmod e$ and $(a, e) = 1$.*

Proof. The only part not already proved is the equivalence fo (c) and (d), which is an elementary calculation.

5. Cyclotomy and the cases $e = 2, 3, 4$. The first explicit formulas for the polynomials $\varphi(X)$ and $F(X)$ date back to Gauss and his contemporaries. These formulas cover the cases with $q = p$ and $e = 2$, 3, or 4. They were derived via Gauss' theory of cyclotomy for $\boldsymbol{F}_p$.

The theory of cyclotomy has been extended to the fields $\boldsymbol{F}_q$. We present the relevant details, referring the reader to [15] for proofs, and we apply the extended theory to finding formulas for $\varphi(X)$ and $F(X)$ in the cases with $q = p^a$ and $e = 2$, 3, or 4.

DEFINITION. The *cyclotomic constant* (k, h) is the number of elements s in C_k such that $1+s$ is in C_h. The *cyclotomic matrix* $M^{(e)}$ is the matrix whose entry in position (k, h) is the constant (k, h).

The constants (k, h) depend on our parameters e and f; also, a different choice of generator g, by permuting the cosets C_k, will permute the constants (k, h). Their relevance to our discussion of period polynomials stems from the following proposition:

PROPOSITION 8. *We have*

$$\eta_m\eta_{m+k} = \sum_{h=0}^{e-1} (k, h)\eta_{m+h} + fn_k,$$

where n_k is defined by

$$n_0 = 1 \quad \text{if} \quad pf \text{ is even},$$
$$n_{e/2} = 1 \quad \text{if} \quad pf \text{ is odd},$$
$$n_k = 0 \quad \text{in all other cases}.$$

This is the corollary to Lemma 8 of [15].

Since the coefficients of $\varphi(x) = \prod(X-\eta_k)$ are all sums of products of periods, repeated application of Proposition 8 will enable us to find these coefficients, provided we know the constants (k, h). The constants are given, in the cases $e = 2$, 3, and 4, by the following propositions.

PROPOSITION 9. *Let $e = 2$.*

If f is even, then

$$M^{(2)} = \begin{pmatrix} A & B \\ B & B \end{pmatrix}, \quad \text{where} \quad 4A = q-5,\ 4B = q-1.$$

If f is odd, then

$$M^{(2)} = \begin{pmatrix} A & B \\ A & A \end{pmatrix}, \quad \text{where} \quad 4A = q-3,\ 4B = q+1.$$

PROPOSITION 10. *Let $e = 3$. Let c and d be defined by $4q = c^2+27d^2$, $c \equiv 1 \pmod 3$, and, if $p \equiv 1 \pmod 3$, then $(c, p) = 1$; these restrictions determine c uniquely, and d up to sign. Then*

$$M^{(3)} = \begin{pmatrix} A & B & C \\ B & C & D \\ C & D & B \end{pmatrix}, \quad \text{where} \quad \begin{aligned} 9A &= q-8+c, \\ 18B &= 2q-4-c-9d, \\ 18C &= 2q-4-c+9d, \\ 9D &= q+1+c. \end{aligned}$$

PROPOSITION 11. *Let $e = 4$. Let s and t be defined by $q = s^2+4t^2$, $s \equiv 1 \pmod 4$, and, if $p \equiv 1 \pmod 4$, then $(s, p) = 1$; these conditions determine s uniquely, and t up to sign.*

If f is even, then

$$M^{(4)} = \begin{pmatrix} A & B & C & D \\ B & D & E & E \\ C & E & C & E \\ D & E & E & B \end{pmatrix}, \quad \text{where} \quad \begin{aligned} 16A &= q-11-6s, \\ 16B &= q-3+2s+8t, \\ 16C &= q-3+2s, \\ 16D &= q-3+2s-8t, \\ 16E &= q+1+2s. \end{aligned}$$

If f is odd, then

$$M^{(4)} = \begin{pmatrix} A & B & C & D \\ E & E & D & B \\ A & E & A & E \\ E & D & B & E \end{pmatrix}, \quad \text{where} \quad \begin{aligned} 16A &= q-7+2s, \\ 16B &= q+1+2s+8t, \\ 16C &= q+1-6s, \\ 16D &= q+1+2s-8t, \\ 16E &= q-3-2s. \end{aligned}$$

These propositions are Lemmas 6, 7, 19, and 19′ of [15]. The case $e = 2$ dates back to Dickson ([6], p. 48).

We now present formulas for $\varphi_e(X)$ and $F_e(X)$.

THEOREM 12. *If f is even, then*

$$\varphi_2(X) = X^2+X-(q-1)/4 \quad \text{and} \quad F_2(X) = X^2-q.$$

If f is odd, then

$$\varphi_2(X) = X^2+X+(q+1)/4 \quad \text{and} \quad F_2(X) = X^2+q.$$

THEOREM 13. *Let c be as defined in Proposition 10. Then*

$$\varphi_3(X) = X^3+X^2-\big((q-1)/3\big)X-\big((c+3)q-1\big)/27,$$
$$F_3(X) = X^3-3qX-cq.$$

THEOREM 14. *Let s be as defined in Proposition 11.*

If f is even, then

$$\varphi_4(X) = X^4+X^3-\frac{1}{8}(3q-3)X^2+\frac{1}{16}\big((2s-3)q+1\big)X+\frac{1}{256}\big(q^2-$$
$$-(4s^2-8s+6)q+1\big),$$
$$F_4(X) = (X^2-q)^2-4q(X-s)^2.$$

If f is odd, then

$$\varphi_4(X) = X^4+X^3+\frac{1}{8}(q+3)X^2+\frac{1}{16}\big((2s+1)q+1\big)X+\frac{1}{256}\big(9q^2-$$
$$-(4s^2-8s-2)q+1\big),$$
$$F_4(X) = (X^2+3q)^2-4q(X-s)^2.$$

The proofs are all straightforward calculations. We illustrate with the case $e = 3$.

Proof of Theorem 13. We have $\varphi_3(X) = (X-\eta_0)(X-\eta_1)(X-\eta_2)$ $= X^3-LX^2+MX-N$, where $L = \eta_0+\eta_1+\eta_2$, $M = \eta_0\eta_1+\eta_1\eta_2+\eta_0\eta_2$, $N = \eta_0\eta_1\eta_2$. By Proposition 1(b), $L = -1$.

By Propositions 8 and 10 we have

$$\begin{aligned} M &= (\beta\eta_0+C\eta_1+D\eta_2)+(D\eta_0+\beta\eta_1+C\eta_2)+(C\eta_0+D\eta_1+\beta\eta_2) \\ &= (B+C+D)\eta_0+(B+C+D)\eta_1+(B+C+D)\eta_2 = -(B+C+D). \end{aligned}$$

Then $18M = -(18A+18B+18C) = -(6q-6)$, and $M = -\big((q-1)/3\big)$.

Finally, $N = (\eta_0\eta_1)\eta_2 = (B\eta_0+C\eta_1+D\eta_2)\eta_2 = K_0\eta_0+K_1\eta_1+K_2\eta_2+$ $+fD$, where $K_0 = K_1 = BC+CD+BD$, $K_2 = B^2+C^2+AD$. Substituting the values of A, B, C, D from Proposition 10 yields $27K_0 = 27K_1 = 27K_2$ $= q^2-3q-c$, $27fD = (q-1)(q+1+c)$. Then $27N = -(q^2-3q-c)+$ $+(q-1)(q+1+c) = (c+3)q-1$, as asserted.

We find $F_3(X)$ from $F_3(X) = 27\varphi_3\big((X-1)/3\big)$.

6. Factorizations; $e = 2, 3, 4$. We now give a complete description of the factorizations of the period polynomials over the rationals in the cases $e = 2$, 3, and 4. By Proposition 1(c) it suffices to study the polynomials $F_e(X)$, and these are more convenient to study than the $\varphi_e(X)$, since they have simpler formulas.

THEOREM 15. (a) *If $a = 2\gamma$ then $F_2(X) = (X-p^\gamma)(X+p^\gamma)$.*

(b) *If a is odd then $F_2(X)$ is irreducible.*

Proof. If $a = 2\gamma$ then $q = p^{2\gamma} \equiv 1 \pmod 4$; thus f is even, and the factorization is immediate from Theorem 12. If a is odd the irreducibility is immediate from Corollary 7.

THEOREM 16. (a) *If* $p \equiv 2 \pmod 3$ *and* $q = p^{2\gamma}$ *then*

$$F_3(X) = \begin{cases} (X+2p^\gamma)(X-p^\gamma)^2 & \text{if } \gamma \text{ is even,} \\ (X-2p^\gamma)(X+p^\gamma)^2 & \text{if } \gamma \text{ is odd.} \end{cases}$$

(b) *If* $p \equiv 1 \pmod 3$, *and* $3 \nmid a$, *then* $F_3(X)$ *is irreducible.*

(c) *If* $p \equiv 1 \pmod 3$, *and* $q = p^{3\gamma}$, *then*

$$F_3(X) = (X - c_1 p^\gamma)\left(X + \tfrac{1}{2}(c_1 + 9d_1)p^\gamma\right)\left(X + \tfrac{1}{2}(c_1 - 9d_1)p^\gamma\right),$$

where c_1 *and* d_1 *are given by* $4p^\gamma = c_1^2 + 27d_1^2$, $c_1 \equiv 1 \pmod 3$, $(c_1, p) = 1$.

Proof. (a) If $p \equiv 2 \pmod 3$, and $q = p^a \equiv 1 \pmod 3$ then a is even; let $a = 2\gamma$. Under these hypotheses, if $4q = c^2 + 27d^2$ then $c = \pm 2p^\gamma$. To insure $c \equiv 1 \pmod 3$ we take $c = -2p^\gamma$ if γ is even, $c = 2p^\gamma$ if γ is odd. Then $F_3(X) = X^3 - 3p^{2\gamma}X + 2p^{3\gamma}$ if γ is even, $F_3(X) = X^3 - 3p^{2\gamma}X - 2p^{3\gamma}$ if γ is odd, and the factorizations are immediate.

(b) The irreducibility is immediate from Corollary 7.

(c) With c_1 and d_1 as given, define

$$c = (c_1^3 - 81c_1d_1^2)/4, \qquad d = (3c_1^2d_1 - 27d_1^3)/4.$$

Direct calculation shows $c^2 + 27d^2 = 4q$. We have $c \equiv 1 \pmod 3$, since $c_1 \equiv 1 \pmod 3$. From $c = (c_1^3 - 81c_1d_1^2)/4 = c_1(p^\gamma - 108d_1^2)/4$ and $(c_1, p) = (d_1, p) = 1$ we infer $(c, p) = 1$. Thus the c we have defined is the c in the formula for $F_3(X)$. Verification of

$$(X - c_1p^\gamma)\left(X + \tfrac{1}{2}(c_1 + 9d_1)p^\gamma\right)\left(X + \tfrac{1}{2}(c_1 - 9d_1)p^\gamma\right) = X^3 - 3p^{3\gamma}X - p^{3\gamma}c$$

is now a straightforward calculation.

THEOREM 17. (a) *If* $p \equiv 3 \pmod 4$, *and* $q = p^{2\gamma}$, *then*

$$F_4(X) = \begin{cases} (X+3p^\gamma)(X-p^\gamma)^3 & \text{if } \gamma \text{ is even,} \\ (X-3p^\gamma)(X+p^\gamma)^3 & \text{if } \gamma \text{ is odd.} \end{cases}$$

(b) *If* $p \equiv 1 \pmod 4$, *and* a *is odd, then* $F_4(X)$ *is irreducible.*

(c) *If* $p \equiv 1 \pmod 4$, $q = p^{2\gamma}$, *and* γ *is odd, then*

$$F_4(X) = (X^2 + 2p^\gamma X - p^{2\gamma} - 2p^\gamma s)(X^2 - 2p^\gamma X - p^{2\gamma} + 2p^\gamma s),$$

the quadratics being irreducible.

(d) *If* $p \equiv 1 \pmod 4$ *and* $q = p^{4\gamma}$, *then*

$$F_4(X) = (X + p^{2\gamma} + 2p^\gamma s_1)(X + p^{2\gamma} - 2p^\gamma s_1)(X - p^{2\gamma} + 4p^\gamma t_1)(X - p^{2\gamma} - 4p^\gamma t_1),$$

where s_1 *and* t_1 *are given by* $p^{2\gamma} = s_1^2 + 4t_1^2$, $s_1 \equiv 1 \pmod 4$, $(s_1, p) = 1$.

Proof. (a) If $p \equiv 3 \pmod 4$ and $q = p^a \equiv 1 \pmod 4$ then a is even; let $a = 2\gamma$. Since $q = p^{2\gamma} \equiv 1 \pmod 8$, f is even. Under these hypotheses, if $q = s^2 + 4t^2$ then $s = \pm p^\gamma$. To insure $s \equiv 1 \pmod 4$ we take $s = p^\gamma$ if γ is even $s = -p^\gamma$ if γ is odd. We have $F_4(X) = (X^2 - p^{2\gamma})^2 - 4p^{2\gamma}(X - p^\gamma)^2$ if γ is even, $F_4(X) = (X^2 - p^{2\gamma})^2 - 4p^{2\gamma}(X + p^\gamma)^2$ if γ is odd, and the factorizations are immediate.

(b) The irreducibility is immediate from Corollary 7.

(c) Here f is even, and $F_4(X)$ factors as a difference of two squares,

$$F_4(X) = (X^2 + 2p^\gamma X - p^{2\gamma} - 2p^\gamma s)(X^2 - 2p^\gamma X - p^{2\gamma} + 2p^\gamma s).$$

Let $A(X)$ stand for either quadratic factor. Then $p^{1-\gamma}A(p^{(\gamma-1)/2}X)$ is Eisenstein, hence irreducible. Thus, the original quadratics are irreducible.

(d) Again, f is even. The roots of $F_4(X)$ are

$$-p^{2\gamma} \pm p^\gamma\sqrt{2(p^{2\gamma} + s)}, \qquad p^{2\gamma} \pm p^\gamma\sqrt{2(p^{2\gamma} - s)}.$$

We claim $s = s_1^2 - 4t_1^2$. Indeed, by direct caclulation, $q = (s_1^2 - 4t_1^2)^2 + 4(2s_1t_1)^2$. Clearly, $s_1^2 - 4t_1^2 \equiv 1 \pmod 4$. And $s_1^2 - 4t_1^2 = p^{2\gamma} - 8t_1^2$ is prime to p since t_1 is, establishing the claim. It follows that $p^{2\gamma} + s = (s_1^2 + 4t_1^2) + (s_1^2 - 4t_1^2) = 2s_1^2$, $p^{2\gamma} - s = 8t_1^2$, and the roots of $F_4(X)$ are as given in the theorem.

7. Location of the Gauss sums. Having the Gauss sums G_k, and the polynomials $F_e(X)$ of which they are the roots, it is natural to ask, which sum corresponds to which root? In particular, if we single out the sum $G_0 = \sum \exp\left((2\pi i \operatorname{Tr} x^e)/p\right)$, which of the roots of $F_e(X)$ will this be? This is the notorious problem of the location of the Gauss sums.

When $F_e(X)$ is irreducible over the rationals (and this includes the classical case, where $q = p$), the answer is known only in the quadratic ($e = 2$) case. The location of the quadratic Gauss sum, in the case $q = p$, is a celebrated result of Gauss', which generalizes easily to $q = p^a$ via the theorem of Davenport–Hasse. We quote the result below. The cubic ($e = 3$) and biquadratic ($e = 4$) cases are unsolved; there are interesting conjectures due to Cassels [4], McGettrick [13], and Loxton [11]. The author understands that recent work, as yet unpublished, of Patterson and Heath-Brown, has settled a number of the outstanding conjectures in the cubic case. Their results concern the average behavior of the sums over a range of values of p, while in this paper we are concerned with sums for individual values of p.

When $F_e(X)$ is not irreducible over the rationals, it is often possible to identify among its irreducible factors the one containing G_0. In particular, when $F_e(X)$ splits completely over the rationals, it is often possible to identify G_0 among its roots. In this section we bring together the many such results we have found the literature, and some results which we believe to be new.

A useful tool in this research is a theorem of Davenport and Hasse [5], which we quote. Proofs have appeared in [5], [9], [12], and elsewhere.

PROPOSITION 18. *Let χ be a multiplicative character on F_p. Define a multiplicative character $\chi^{(a)}$ on F_q by $\chi^{(a)}(x) = \chi(Nx)$, where N denotes the norm, $N: F_q \to F_p$. Then*

$$\tau(\chi^{(a)}) = (-1)^{a+1}(\tau(\chi))^a.$$

We now consider the quadratic case.

PROPOSITION 19. *Let $e = 2$. Then $G_0 = i^*\sqrt{q}$, where i^* is given by*

$$i^* = \begin{cases} -i & \text{if } p \equiv 3 \pmod 4 \text{ and } a \equiv 3 \pmod 4, \\ 1 & \text{if } p \equiv 3 \pmod 4 \text{ and } a \equiv 2 \pmod 4, \\ & \text{or if } p \equiv 1 \pmod 4 \text{ and } a \text{ is odd}, \\ i & \text{if } p \equiv 3 \pmod 4 \text{ and } a \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv 3 \pmod 4 \text{ and } a \equiv 0 \pmod 4, \\ & \text{or if } p \equiv 1 \pmod 4 \text{ and } a \text{ is even}. \end{cases}$$

Proof. If $q = p$ and χ is the quadratic character Gauss showed $\tau(\chi) = \sqrt{p}$ if $p \equiv 1 \pmod 4$ and $\tau(\chi) = i\sqrt{p}$ if $p \equiv 3 \pmod 4$. Proofs can be found in [1], pp. 195–199, [8], pp. 469–478, [10], pp. 88–90, and elsewhere. The proposition follows from Davenport–Hasse and the observation (Proposition 1(h)) that $G_0 = \tau(\chi)$.

Before proceeding to the cubic and biquadratic cases we present two results concerning what have come to be known in the literature of coding theory as the semiprimitive case and the quadratic residue case.

PROPOSITION 20. *Assume there exists a positive integer j such that $p^j \equiv -1 \pmod e$, and assume j is the least such. Let $q = p^a$ with $a = 2j\gamma$. Then the Gauss sums are given by*

(a) *If γ, p, and $(p^j+1)/e$ are all odd, then $G_{e/2} = (e-1)p^{j\gamma}$, $G_k = -p^{j\gamma}$ for $k \neq e/2$;*

(b) *In all other cases, $G_0 = -(-1)^\gamma(e-1)p^{j\gamma}$, $G_k = (-1)^\gamma p^{j\gamma}$ for $k \neq 0$.*

Proof. In essence the result goes back to Stickelberger ([14], 3.6 and 3.10); see also [2], p. 168. In these sources the results are stated for the sums $\tau(\chi)$ rather than G_k, but the translation, via Proposition 1(f) and (g), is simple.

PROPOSITION 21. *Assume $e > 3$ is prime, $e \equiv 3 \pmod 4$, and assume p generates the quadratic residues $\pmod e$. Let $h = (e-1)/2$, and let $q = p^a = p^{h\gamma}$. Define the integer m by*

$$2em = \sum_{a=1}^{e-1}\left(1 + \left(\frac{a}{e}\right)\right)a.$$

Define the integers A_γ and B_γ by

$$4p^{\gamma(h-2m)} = A_\gamma^2 + eB_\gamma^2, \quad (A_\gamma, p) = 1, \quad p^{m\gamma}A_\gamma \equiv -2 \pmod e, \quad \text{and } A_\gamma B_\gamma > 0;$$

this determines A_γ and B_γ uniquely. Then the Gauss sums are given by

$$2G_0 = (e-1)A_\gamma p^{m\gamma},$$

$$2G_k = (B_\gamma e - A_\gamma)p^{m\gamma} \quad \text{if} \quad \left(\frac{k}{e}\right) = 1,$$

$$2G_k = (-B_\gamma e - A_\gamma)p^{m\gamma} \quad \text{if} \quad \left(\frac{k}{e}\right) = -1.$$

Proof. This result, stated in terms of the $\tau(\chi)$ and η_k, is proved in [3].

We now return to the problem of the location of the cubic Gauss sums. In Theorem 16 we made a subdivision into three cases. Case (a), in which $p \equiv 2 \pmod 3$, is covered by the semiprimitive case, Proposition 20. Case (b), in which $p \equiv 1 \pmod 3$, $q = p^a$, $3 \nmid a$, is the irreducible case; it includes the classical case, and there is no progress. Case (c) is settled by the following theorem.

THEOREM 22. *Let $e = 3$, let $p \equiv 1 \pmod 3$, let $q = p^{3\gamma}$. Let c_1 and d_1 be as in Theorem 16 (c). Then*

$$G_0 = c_1 p^\gamma \quad \text{and} \quad \{G_1, G_2\} = \{-(c_1 + 9d_1)p^\gamma/2,\ -(c_1 - 9d_1)p^\gamma/2\}.$$

First proof. Let $x \in C_1$. Since x is not a cube in F_q, $[F_q: F_p(x)]$ is not divisible by three. Thus $[F_p(x): F_p]$, which equals the number of distinct conjugates of x, is divisible by 3. These conjugates are all in C_1, since, for every k, X^{p^k} is in C_{p^k} and $p^k \equiv 1 \pmod 3$. Then $\eta_1 = \sum_{x \in C_1} \theta^{\mathrm{Tr}x}$ is divisible by 3. By the same argument, $3 | \eta_2$. Thus, $\eta_1 \equiv \eta_2 \pmod 3$, and $G_1 \equiv G_2 \pmod 9$. Now from Theorem 16(c) we see the roots of $F_3(X)$ are congruent to $c_1 p^\gamma$, $-c_1 p^\gamma/2$, and $-c_1 p^\gamma/2 \pmod 9$, and the theorem follows.

Second proof. Let χ be a cubic character $(\mathrm{mod}\, p)$, and define the cubic character $\chi^{(3\gamma)}$ on F_q by $\chi^{(3\gamma)}(x) = \chi(Nx)$, where N denotes the norm from F_q to F_p. Then $\tau^3(\chi) = p\pi$, where $\pi = (c + d\sqrt{-27})/2$, $4p = c^2 + 27d^2$, $c \equiv 1 \pmod 3$ (see [8] or [9]). We have $G_0 = \tau(\chi^{(3\gamma)}) + \tau(\overline{\chi^{(3\gamma)}})$ by Proposition 1(g), thus $G_0 = \tau(\chi^{(3\gamma)}) + \overline{\tau(\chi^{(3\gamma)})}$ by Proposition 1(d), thus $G_0 = (-1)^{3\gamma+1}(\tau^{3\gamma}(\chi) + \overline{\tau^{(3\gamma)}(\chi)})$ by Davenport–Hasse, and, finally, $G_0 = (-1)^{3\gamma+1}p^\gamma(\pi^\gamma + \bar{\pi}^\gamma)$. To show $G_0 = c_1 p^\gamma$ it suffices to show $(-1)^{\gamma+1}\pi^\gamma = (c_1 + d_1\sqrt{-27})/2$. Let $(-1)^{\gamma+1}\pi^\gamma = (-1)^{\gamma+1}((c + d\sqrt{-27}/2)^\gamma) = (C + D\sqrt{-27})/2$. Then $C^2 + 27D^2 = 4\pi^\gamma\bar{\pi}^\gamma = 4p^\gamma$, and it is easily checked that $(C, p) = 1$, and $C \equiv 1 \pmod 3$. Thus $C = c_1$ and we have evaluated

G_0. Now G_1 and G_2 can be obtained from Theorem 16(c), or we can keep the proof independent of that theorem, finding G_1 from $G_1 = \tau(\chi^{(3\gamma)})\omega + \tau(\chi^{(3\overline{\gamma})})\omega^2$, where $\omega^3 = 1$, etc.

Finally, we consider the location of the biquadratic Gauss sums. In Theorem 17 we introduced a subdivision into four cases. Case (a), in which $p \equiv 3 \pmod 4$, is covered by the semiprimitive case, Proposition 20. Case (b) is the irreducible case, which includes the classical case. Here it is well-known that G_0 can be determined up to a single ambiguity of sign.

PROPOSITION 23. *Let* $e = 4$, $p \equiv 1 \pmod 4$, $q = p^a$, a *odd. If* $p \equiv 1 \pmod 8$ *then* G_0 *is a root of* $X^2 - 2\sqrt{q}X - q + 2\sqrt{q}s$. *If* $p \equiv 5 \pmod 8$ *then* G_0 *is a root of* $X^2 - 2\sqrt{q}X + 3q + 2\sqrt{q}s$. *Here* s *is as in Proposition* 11.

Proof. We give the proof in the case $p \equiv 1 \pmod 8$; the adjustments needed when $p \equiv 5 \pmod 8$ are minor and obvious. By Theorem 14, G_0 is a root of $(X^2 - q)^2 - 4q(X - s)^2$, hence either of $X^2 - 2\sqrt{q}X - q + 2\sqrt{q}s$ or of $X^2 + 2\sqrt{q}X - q - 2\sqrt{q}s$. Using superscripts to denote the values of e, we have $G_0^{(4)} + G_2^{(4)} = 2G_0^{(2)}$; by Proposition 19, $G_0^{(2)} = \sqrt{q}$. Thus, $G_0^{(4)} + G_2^{(4)} = 2\sqrt{q}$, $G_1^{(4)} + G_3^{(4)} = -2\sqrt{q}$, and the result follows.

In cases (c) and (d) the Gauss sums can be located without any ambiguity.

THEOREM 24. *Let* $e = 4$, $p \equiv 1 \pmod 4$, $q = p^{2\gamma}$, γ *odd. Then* $G_0 = 2s\sqrt{p^\gamma} - p^\gamma$, *where* s *is given by* $p^\gamma = s^2 + 4t^2$, $s \equiv 1 \pmod 4$, $(s, p) = 1$.

Proof. In this proof χ will denote a biquadratic character, χ_{quad} will denote the quadratic character, and superscripts on χ, χ_{quad}, and G_0 will indicate the degree of the field. Thus, $G_0^{(a)}$ is the biquadratic Gauss sum in the field of p^a elements.

By Proposition 1(g), $G_0^{(2\gamma)} = \tau(\chi^{(2\gamma)}) + \tau(\overline{\chi^{(2\gamma)}}) + \tau(\chi_{\text{quad}}^{(2\gamma)})$. Since $q \equiv 1 \pmod 8$, we have $\chi^{(2\gamma)}(-1) = 1$, and $\tau(\overline{\chi^{(2\gamma)}}) = \overline{\tau(\chi^{(2\gamma)})}$. With $\tau(\chi_{\text{quad}}^{(2\gamma)}) = -\sqrt{q}$ given by Proposition 19, we have

$$G_0^{(2\gamma)} = \tau(\chi^{(2\gamma)}) + \overline{\tau(\chi^{(2\gamma)})} - \sqrt{q}.$$

By Davenport–Hasse, $\tau(\chi^{(2\gamma)}) = -\tau^2(\chi^{(\gamma)})$, so

$$(*) \qquad G_0^{(2\gamma)} = -\tau^2(\chi^{(\gamma)}) - \overline{\tau^2(\chi^{(\gamma)})} - \sqrt{q}.$$

We now continue the proof on the hypothesis $p \equiv 1 \pmod 8$, and again leave to the reader the adjustments necessary when $p \equiv 5 \pmod 8$. We have

$$G_0^{(\gamma)} = \tau(\chi^{(\gamma)}) + \overline{\tau(\chi^{(\gamma)})} + \tau(\chi_{\text{quad}}^{(\gamma)})$$

from Proposition 1(g), and

$$G_0^{(\gamma)} = \sqrt{p^\gamma} \pm \sqrt{2p^\gamma - 2s\sqrt{p^\gamma}}$$

from Proposition 23; also, $\tau(\chi_{\text{quad}}^{(\gamma)}) = \sqrt{p^\gamma}$ from Proposition 19. Combining, and noting $\tau(\overline{\chi^{(\gamma)}}) = \chi(-1)\overline{\tau(\chi^{(\gamma)})} = \overline{\tau(\chi^{(\gamma)})}$, we have

$$\pm\sqrt{2p^\gamma - 2s\sqrt{p^\gamma}} = \tau(\chi^{(\gamma)}) + \overline{\tau(\chi^{(\gamma)})}.$$

Squaring both sides, applying Proposition 1(e), and cancelling, yields

$$-2s\sqrt{p^\gamma} = \tau^2(\chi^{(\gamma)}) + \overline{\tau^2(\chi^{(\gamma)})}.$$

Now comparison with (*) yields the theorem.

THEOREM 25. *Let* $e = 4$, $p \equiv 1 \pmod 4$, $q = p^{4\gamma}$. *Let* s_1 *and* t_1 *be as given in Theorem* 17(d). *Then* $G_0 = -p^{2\gamma} - 2s_1p^\gamma$, $G_2 = -p^{2\gamma} + s_1p^\gamma$, *and* $\{G_1, G_3\} = \{p^{2\gamma} \pm 4t_1p^\gamma\}$.

Proof. (Compare with the first proof of Theorem 22.) Let x be in C_k, $k \neq 0$. Since x is not a fourth power in F_q, $[F_p(x): F_p]$ is even. The conjugates of x are thus even in number. Moreover, they are all in C_k. Thus η_k is even for $k = 1, 2, 3$. By Proposition 1(b), η_0 is odd. By Proposition 1(a), we have $G_0 \equiv 5 \pmod 8$, $G_1 \equiv G_2 \equiv G_3 \equiv 1 \pmod 8$.

Inspection of the roots of $F_4(X)$, given in Theorem 17(d), shows that only $-p^{2\gamma} - 2s_1p^\gamma$ is congruent to 5 (mod 8). Thus, $G_0 = -p^{2\gamma} - 2s_1p^\gamma$. Now $G_0 + G_2$ is twice a quadratic Gauss sum, equal by Proposition 19 to $-2p^{2\gamma}$, so $G_2 = -p^{2\gamma} + 2s_1p^\gamma$, proving the theorem.

A second proof can be constructed along the lines of the second proof of Theorem 22. One needs to know that if χ is a biquadratic character on F_p then $\tau^4(\chi) = p\pi^2$, where $\pi = s + 2it$, $p = s^2 + 4t^2$, $s \equiv 1 \pmod 4$ (see [8]).

Added in Proof, June 1981. Considerable progress has recently been made on the problem of the location of the Gauss sum in the classical case. See D. R. Heath-Brown and S. J. Patterson, *The distribution of Kummer sums at prime arguments*, J. Reine Angew. Math. 310 (1979), pp. 111–130; C. R. Matthews, *Gauss sums and elliptic functions I. The Kummer sum*, Inv. Math. 52 (1979), pp. 163–185; and C. R. Matthews, *Gauss sums and elliptic functions II. The quartic sum*, Inv. Math. 54 (1979), pp. 23–52.

References

[1] T. M. Apostol, *Introduction to analytic number theory*, Springer-Verlag 1976.

[2] L. D. Baumert and R. J. McEliece, *Weights of irreducible cyclic codes*, Information and Control 20 (1972), pp. 158–175.

[3] L. D. Baumert and J. Mykkeltveit, *Weight distributions of some irreducible cyclic codes*, DSN Progress Report 16 (1973), pp. 128–131. (Published by Jet Propulsion Laboratory, Pasadena, California.)

[4] J. W. S. Cassels, *On Kummer sums*, Proc. London Math. Soc. (3) 21 (1970), pp. 19–27.
[5] H. Davenport und H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. 172 (1934/5), pp. 151–182.
[6] L. E. Dickson, *Linear groups*, Dover 1958.
[7] C. F. Gauss, *Disquisitiones arithmeticae*, Yale 1966.
[8] H. Hasse, *Vorlesungen über Zahlentheorie*, 2nd ed., Springer-Verlag, 1964.
[9] K. Ireland and M. I. Rosen, *Elements of number theory*, Bogden and Quigley, 1972.
[10] S. Lang, *Algebraic number theory*, Addison-Wesley, 1970.
[11] J. H. Loxton, *Some conjectures concerning Gauss sums*, J. Reine Angew. Math. 297 (1978), pp. 153–158.
[12] R. J. McEliece and J. Rumsey, Jr., *Euler products, cyclotomy, and coding*, J. Number Theory 4 (1972), pp. 302–311.
[13] A. D. McGettrick, *On the biquadratic Gauss sum*, Proc. Camb. Philos. Soc. 21 (1972), pp. 79–83.
[14] L. Stickelberger, *Über eine Verallgemeinerung der Kreistheilung*, Math. Ann. 37 (1890), pp. 321–367.
[15] T. Storer, *Cyclotomy and difference sets*, Markham, 1967.

Received on 19. 9. 1978 (1103)

ACTA ARITHMETICA
XXXIX (1981)

On the theorem of Jarník and Besicovitch

by

R. KAUFMAN (Urbana, Ill.)

1. Let $\alpha > 0$ be fixed in all that follows and $E(\alpha)$ be the set of real numbers x such that the inequality $\|nx\| \leqslant n^{-1-\alpha}$ has arbitrarily large integer solutions n. (As usual $\|t\|$ is the distance from t to the nearest integer.) We recall the classical theorem of Jarník [3] and Besicovitch [1].

I. $E(\alpha)$ has Hausdorff dimension $2(2+\alpha)^{-1}$.

We shall obtain for $E(\alpha)$ a stronger property:

II. There exists a positive measure μ whose support is a compact subset of $E(\alpha)$, whose Fourier–Stieltjes transform obeys the relation

$$\hat{\mu}(u) = o(\log|u|)\,|u|^{-1/2+\alpha}, \qquad |u| \to +\infty.$$

By a theorem of Beurling [3, III], the closed support of μ (or any Borel set of positive μ-measure) must have dimension at least $2(2+\alpha)^{-1}$; however the property of $E(\alpha)$ is not shared by certain sets of positive Lebesgue measure, so that II could not be deduced from I (see [4], p. 351).

2. In this paragraph we define some auxiliary functions, and obtain an inequality on Fourier coefficients, more or less equivalent to the main result II. First of all we construct the function $F_R(x)$, $0 < R < 1/4$,

$$F_R(x) = \begin{cases} 35(32)^{-1}R^{-7}(R^2-x^2)^3, & |x| \leqslant R, \\ 0, & R \leqslant |x| \leqslant 1/2. \end{cases}$$

Then we extend F_R to a periodic function and expand it in a Fourier series

$$F_R(x) = \sum a_m^{(R)} e^{2\pi i m x},$$

$$a_0^{(R)} = 1, \qquad |a_m^{(R)}| \leqslant 1, \qquad |a_m^{(R)}| \leqslant m^{-2}R^{-2}.$$

In the construction below M is a large positive integer and $R = (4M)^{-1-\alpha}$; we write $q_m(x) = \sum_p{}^{*} F_R(px)$, where $\sum_p{}^{*}$ means that the sum is extended over primes p in the interval $M \leqslant p \leqslant 2M$. We also