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 $q = p^s$ 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 $q = p^s$, $s > 1$, 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 $ef+1 = p^s = q$ is a prime power. $F_q$ is the field of $q$ elements, $F_q^*$ its multiplicative group, $g$ a generator of $F_q^*$. $C_q$ is the group of $e$th powers in $F_q^*$, and its cosets are $C_k = g^k C_q$, $k = 0, 1, \ldots, e-1$.

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

$Tr$ is the trace map, $Tr : F_q \to F_q$.
The cyclotomic periods $\eta_k$ are given by
$$\eta_k = \sum_{\omega \in \mathbb{Z}^*} \omega^k, \quad k = 0, 1, \ldots, \phi-1.$$ 

The Gauss sums $G_k$ are given by
$$G_k = \sum_{\omega \in \mathbb{Z}^*} \omega^k \omega^s, \quad k, s = 0, 1, \ldots, \phi-1.$$ 

If $\chi$ is a character on $\mathbb{F}_q^*$ of order $d$ then the Lagrange resolvent $\tau(\chi)$ is given by
$$\tau(\chi) = \sum_{\omega \in \mathbb{Z}^*} \chi(\omega) \omega^{\phi d}.$$ 

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 $\eta_k$ and $G_k$, and only peripherally with the $\tau(\chi)$.

If $k \geq \phi$ then the subscripts in $G_k$, $\eta_k$, and $G_k$ are to be interpreted (modulo $\phi$).

The period polynomials $\varphi_k(X)$ are given by
$$\varphi_k(X) = \prod_{h=0}^{\phi-1} (X - \eta_h),$$
and the modified period polynomials $F_k(X)$ by
$$F_k(X) = \prod_{h=0}^{\phi-1} (X - G_h).$$

$\delta = \gcd\{\phi, (q-1)/(p-1)\}$.

The elements of the Galois group of $Q(\theta)/Q$ are denoted by $\sigma_\alpha$, $\alpha = 1, 2, \ldots, p-1$, where $\sigma_\alpha(\theta) = \theta^\alpha$.

### 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) $G_k = \phi \eta_k + 1$.

(b) $\sum_{h=0}^{\phi-1} \eta_h = -1$, $\sum_{k=0}^{\phi-1} G_k = 0$.

(c) $F_k(X) = \phi \varphi_k((X-1)/\phi)$, $\varphi_k(X) = \phi^{-1} F_k(\phi X + 1)$.

(d) $\chi(-1) = \tau(\chi)$.

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

(f) If $\omega$ is a primitive complex $d$-th root of unity, and we define the character $\chi$ by $\chi(\omega) = \omega^j$, then
$$\tau(\chi) = \sum_{h=0}^{\phi-1} \omega^h \eta_h \quad \text{and} \quad \eta_h = \frac{1}{\phi} \sum_{j=0}^{\phi-1} \omega^{-h} \tau(\chi).$$

(g) $G_k = \sum_{j=0}^{\phi-1} \omega^{-j} \tau(\chi)$, $\tau(\chi_j) = \begin{cases} \phi^{-1} \sum_{j=0}^{\phi-1} \omega^{-j} G_k & \text{if } j \neq 0, \\ -1 & \text{if } j = 0. \end{cases}$

(h) If $\phi = 2$ and $\chi$ 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 $\varphi_k(X)$ and $F_k(X)$. Proofs will be given only for $\varphi_k(X)$; the results for $F_k(X)$ follow by Proposition 1 (c).

The effect of $\text{Gal}(Q(\theta)/Q)$ on $\eta_k$ is given by the following lemma.

**Lemma 2.** If $\alpha \in \mathbb{F}_q \cap \mathbb{Z}$, then $\sigma_\alpha(\eta_m) = \eta_{m+\alpha}$.

**Proof.** From $\eta_m = \sum_{\omega \in \mathbb{Z}^*} \omega^{\phi m}$ we get
$$\sigma_\alpha(\eta_m) = \sum_{\omega \in \mathbb{Z}^*} \omega^{\phi m + \alpha} = \sum_{\omega \in \mathbb{Z}^*} \omega^{\phi \alpha m} = \eta_{m+\alpha}.$$ 

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

**Theorem 3.** $\varphi_k(X) \in \mathbb{Z}[X]$, $F_k(X) \in \mathbb{Z}[X]$.

**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 $\varphi_k(X)$ is a product of powers of the minimal irreducible polynomials for the $\eta_k$. The $\eta_k$ are algebraic integers, so $\varphi_k(X) \in \mathbb{Z}[X]$.

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.** $\varphi_k(X)$ and $F_k(X)$ split over the rationals into $d$ factors of degree $d/\delta$. Each of these factors is irreducible or a power of an irreducible polynomial.

We must first establish a lemma.

**Lemma 5.** $F_k \cap \mathbb{Z}$ is non-empty if $\delta$ and only if $\delta | k$.

**Proof.** Since $\delta = \gcd\{\phi, (q-1)/(p-1)\}$, there exist integers $m$ and $\alpha$ such that $m(q-1)/(p-1) - \alpha \theta = k$ if, and only if, $\delta | \theta$. Now observe that $\varphi_{m(q-1)/(p-1) - \alpha \theta} = \varphi_\alpha \varphi_\delta \in F_k \cap \mathbb{Z}$. 

Proof of Theorem 4. Let \( \varphi_{\delta}(X) = (X - \eta_0)(X - \eta_1)\cdots(X - \eta_{d-1}) \). By Lemmas 2 and 5, the roots of \( \varphi_{\delta}(X) \) are the conjugates of \( \eta_k \) in each distinct conjugate occurring equally often. Thus \( \varphi_{\delta}(X) \) is in \( \mathbb{Z}[X] \) and is irreducible or a power of an irreducible polynomial. Now \( \varphi_0(X) = 1 \) = \( \prod_{k=0}^{d-1} \varphi_{0}(X) \), proving the theorem.

By way of an example, we take \( e = 8, f = 3 \), so \( q = 25, \mathbb{F} \). We can realize \( P_{12} \) as \( P_{12}(x) = \{ ax + b : |a| \leq 2, |b| \leq 2 \} \), where \( a^2 = 2 \), and we can take \( g = a + b \). Then

\[
\begin{align*}
C_0 &= \{1, -2x + 2, 2x + 2\}, & C_1 &= \{x + 2, -2x, -2\}, \\[5pt]
C_2 &= \{-x + 1, x + 1, -2\}, & C_3 &= \{-x, -2x - 1, -2x + 1\}, \\[5pt]
C_4 &= \{-2x - 2, -x - 2, 2x - 2\}, & C_5 &= \{-2x, -2x + 2, 2x\}, \\[5pt]
C_6 &= \{2, x - 1, -x - 1\}, & C_7 &= \{2x - 1, x, 2x + 1\}.
\end{align*}
\]

The conjugate of \( ax + b \) over \( F_p \) is \( -ax + b \), thus \( \text{Tr}(ax + b) = 2b \). Let \( \beta = \exp(2\pi i / 8) \). Then

\[
\begin{align*}
\eta_0 &= \beta^2 + 2\beta^4, & \eta_1 &= 1 + \beta + \beta^4, & \eta_2 &= \beta + 2\beta^4, & \eta_3 &= 1 + \beta^2 + \beta^4, \\[5pt]
\eta_4 &= 2\beta + \beta^3, & \eta_5 &= 1 + \beta + \beta^4, & \eta_6 &= 2\beta^2 + \beta^4, & \eta_7 &= 1 + \beta^2 + \beta^3,
\end{align*}
\]

and

\[
\varphi_0(X) = (X - \eta_0)(X - \eta_1)(X - \eta_2)(X - \eta_3)(X - \eta_4)(X - \eta_5)(X - \eta_6)(X - \eta_7) = (X^8 + 33X^7 + 210X^6 + 96X^5 + 7X^4 + 11)(X^3 - X - 1)^2.
\]

Also,

\[
P_0(X) = 8\varphi_0((X - 1)/8) = (X^8 + 20X^7 + 51X^6 + 250X^5 + 4920X^4)(X^3 - 10X - 55)^4.
\]

When \( \delta = 1 \), Theorem 4 shows that \( \varphi_0(X) \) and \( P_0(X) \) 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. \( \varphi_0(X) \) and \( P_0(X) \) 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 \( X^{d-1} \) in \( \varphi_0(X) \) is \( - \sum_{k=0}^{d-1} \eta_k \). Therefore \( \varphi_0(X) \) cannot be a power higher than the first of another polynomial. Hence, if \( \delta = 1 \), then \( \varphi_0(X) \) and \( P_0(X) \) are irreducible.

Corollary 7. The following are equivalent.

(a) \( \varphi_0(X) \) is irreducible.
(b) \( P_0(X) \) 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 to (e) and (f), 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 \( q = p^e \) and \( e = 2, 3, \) or 4. They were derived via Gauss’ theory of cyclotomy for \( F_p \).

The theory of cyclotomy has been extended to the fields \( F_{q} \). 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 \( q = p^e \) and \( e = 2, 3, \) or 4.

Definition. The cyclotomic constant \( (k, h) \) is the number of elements \( a \) in \( C_h \), such that \( 1 + a \in C_h \). 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 \( C_h \), will permute the constants \( (k, h) \). Their relevance to our discussion of period polynomials stems from the following proposition:

Proposition 8. We have

\[
\eta_{m+n} = \sum_{k=0}^{m-1} (k, h) \eta_{m+n+k} + f n_k,
\]

where \( n_k \) is defined by

\[
\begin{align*}
n_0 &= 1 \quad \text{if} \ \eta_{m} \ \text{is even}, \\[5pt]
n_{2k} &= 1 \quad \text{if} \ \eta_{m} \ \text{is odd}, \\[5pt]
n_{2k+1} &= 0 \quad \text{in all other cases}.
\end{align*}
\]

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

Since the coefficients of \( \varphi(X) = \sum (X - \eta)_k \) are all sums of products of periods, repeated application of Proposition 8 will enable us to find those 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

\[
M^{(e)} = \begin{pmatrix} A & B \\ B & A \end{pmatrix}, \quad \text{where} \quad 4A = g - 5, \ 4B = g - 1.
\]

4. --- Acta Arithmetica XXXIX. 3
If \( f \) is odd, then
\[
M^{(a)} = \begin{bmatrix} A & B \\ A & A \end{bmatrix}, \quad \text{where} \quad 4A = q - 3, \ 4B = q + 1.
\]

**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
\[
9A = q - 8 + c, \\
18 B = 2q - 4 - c - 9d, \\
18C = 2q - 4 - c + 9d, \\
9D = q + 1 + c.
\]

**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
\[
M^{(a)} = \begin{bmatrix} A & B & C & D \\ B & D & E & E \\ C & E & C & E \\ D & E & B & B \end{bmatrix}, \quad \text{where} \quad 16A = q - 11 - 6s, \\
16B = q - 3 + 2s + 8t, \\
16C = q - 3 + 2s, \\
16D = q - 3 + 2s - 8t, \\
16E = q + 1 + 2s.
\]

If \( f \) is odd, then
\[
M^{(a)} = \begin{bmatrix} A & B & C & D \\ B & D & E & E \\ A & E & A & E \\ D & E & B & B \end{bmatrix}, \quad \text{where} \quad 16A = q - 7 + 2s, \\
16B = q + 1 + 2s + 8t, \\
16C = q + 1 - 6s, \\
16D = q + 1 + 2s - 8t, \\
16E = q - 3 - 2s.
\]

These propositions are Lemmas 6, 7, 19, and 19' of [15]. The case \( e = 2 \) dates back to Dickson ([8], p. 48).

We now present formulas for \( q_4(X) \) and \( F_4(X) \).

**Theorem 12.** If \( f \) is even, then
\[
q_4(X) = X^4 + X^3 - \frac{1}{8}(3q - 3)X^2 + \frac{1}{16}(2s - 3)q + 1)X + \frac{1}{256}(q^4 - \frac{1}{4}(3q - 3)X^2 - \frac{1}{4}(2s - 3)q + 1)X + \frac{1}{256}(q^4 - \frac{1}{4}(3q - 3)X^2 - \frac{1}{4}(2s - 3)q + 1),
\]
\[
F_4(X) = (X^2 - q)^3 - 4q(X - s)^2.
\]

If \( f \) is odd, then
\[
q_4(X) = X^4 + X^3 + \frac{1}{8}(3q + 3)X^2 + \frac{1}{16}(2s + 1)q + 1)X + \frac{1}{256}(q^4 - \frac{1}{4}(3q + 3)X^2 - \frac{1}{4}(2s + 1)q + 1)X + \frac{1}{256}(q^4 - \frac{1}{4}(3q + 3)X^2 - \frac{1}{4}(2s + 1)q + 1),
\]
\[
F_4(X) = (X^2 + q)^3 - 4q(X - s)^2.
\]

The proofs are all straightforward calculations. We illustrate with the case \( e = 3 \).

Proof of Theorem 13. We have \( q_4(X) = (X - \eta_0)(X - \eta_1)(X - \eta_2) = X^3 - M X - N \), where \( L = \eta_0 + \eta_1 + \eta_2 \), \( M = \eta_0 \eta_1 + \eta_1 \eta_2 + \eta_2 \eta_0 \), \( N = \eta_0 \eta_1 \eta_2 \). By Proposition 1(b), \( L = 1 \).

By Propositions 8 and 10 we have
\[
M = (\beta \eta_0 + C \eta_1 + D \eta_2) + (D \eta_0 + \beta \eta_1 + C \eta_2) + (C \eta_0 + D \eta_1 + \beta \eta_2) = (B + C + D) \eta_0 + (B + C + D) \eta_1 + (B + C + D) \eta_2 = -(B + C + D) + \eta_0.
\]

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

Finally, \( N = \eta_0 \eta_1 \eta_2 = (B \eta_0 + C \eta_1 + D \eta_2) \eta_0 = K \eta_0 + K \eta_2 + K \eta_0 + K \eta_2 + K \eta_0 + K \eta_2 = B^2 + C^2 + AD \). Substituting the values of \( A \), \( B \), \( C \), \( D \) from Proposition 10 yields \( 27K_a = 27K_b = 27K_c = q^3 - 3q - c + (q - 1)q + 1 + (q - 1)q + 1 = (q - 3)q - c - 1 \), as asserted.

We find \( F_4(X) \) from \( F_4(X) = 27q_4(X - 1)/3 \).

**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 \( F_4(X) \), and these are more convenient to study than the \( q_4(X) \), since they have simpler formulas.

**Theorem 15.** (a) If \( a = 2 \gamma \) then \( F_4(X) = (X - \gamma^\gamma)(X + \gamma^\gamma) \).

(b) If \( a \) is odd then \( F_4(X) \) is irreducible.

Proof. If \( a = 2 \gamma \) then \( q = \gamma^\gamma + 1 \pmod{4} \); 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 \( p = 2 \pmod{3} \) and \( q = \varphi^p \) then
\[
F_q(X) = \begin{cases} 
(X + 2p^r)(X - p^r) & \text{if } \gamma \text{ is even,} \\
(X - 2p^r)(X + p^r) & \text{if } \gamma \text{ is odd.}
\end{cases}
\]

(b) If \( p = 1 \pmod{3} \), and \( 3 \nmid a \), then \( F_q(X) \) is irreducible.

(c) If \( p = 1 \pmod{3} \), and \( q = \varphi^p \), then
\[
F_q(X) = (X - a \varphi^p)(X + \frac{1}{2}(a + 9d_1)\varphi^p)(X + \frac{1}{2}(a - 9d_1)\varphi^p),
\]
where \( a, 1, d_1 \) are given by \( 4p^2 = a^2 - 27d_1^2, a = 1 \pmod{3} \), \( (a, p) = 1 \).

Proof. (a) If \( p = 2 \pmod{3} \), and \( q = \varphi^p = 1 \pmod{3} \) then \( a \) is even; let \( a = 2\gamma \). Under these hypotheses, if \( 4\gamma \) is \( 2 \pmod{3} \), \( \gamma = \pm 2p^r \). To ensure \( \gamma = \pm 2p^r \), we choose \( \gamma = 2p^r \). \( \gamma \) is odd. Then \( F_q(X) = (X - 3p^r X + 2p^r) \) if \( \gamma \) is even, \( F_q(X) = (X^3 - 3p^r X - 2p^r) \) if \( \gamma \) is odd, and the factorizations are immediate.

(b) The irreducibility is immediate from Corollary 7.

(c) With \( c_1 \) and \( c_2 \) as given, define
\[
\sigma = (c_1^2 - 81c_2^2)/4, \quad d = (3c_1d_1 - 27d_1^2)/4.
\]

Direct calculation shows \( c^2 - 27d^2 = 4q \). We have \( \sigma = 1 \pmod{3} \), \( \sigma = 1 \pmod{3} \). From \( \sigma = (c_1^2 - 81c_2^2)/4 = a_1(p^2 - 108d_1^2)/4 \) and \( (c_1, p) = (d_1, p) = 1 \) we infer \( c, (c_1, p) = 1 \). Thus the \( c \) in the formula for \( F_q(X) \). Verification of \( (X - a \varphi^p)(X + \frac{1}{2}(a + 9d_1)\varphi^p)(X + \frac{1}{2}(a - 9d_1)\varphi^p) \) is now a straightforward calculation.

Theorem 17. (a) If \( p = 3 \pmod{4} \), and \( q = \varphi^p \), then
\[
F_q(X) = \begin{cases} 
(X + 3p^r)(X - p^r) & \text{if } \gamma \text{ is even,} \\
(X - 3p^r)(X + p^r) & \text{if } \gamma \text{ is odd.}
\end{cases}
\]

(b) If \( p = 1 \pmod{4} \), and \( a \) is odd, then \( F_q(X) \) is irreducible.

(c) If \( p = 1 \pmod{4} \), \( q = \varphi^p \), and \( \gamma \) is odd, then
\[
F_q(X) = (X^3 - 3p^r X - 2p^r)\varphi^p + X^3 - 3p^r X - 2p^r + 2p^r s, \]
the quadratics being irreducible.

(d) If \( p = 1 \pmod{4} \) and \( q = \varphi^p \), then
\[
F_q(X) = (X + p^r + 2p^r s_1)(X + p^r - 2p^r s_1)(X - p^r + 4p^r t_1)(X - p^r + 4p^r t_1),
\]
where \( s_1 \) and \( t_1 \) are given by \( p^r = s_1^2 + 4t_1^2, s_1 = 1 \pmod{4}, (s_1, p) = 1 \).

Proof. (a) If \( p = 3 \pmod{4} \) and \( q = \varphi^p = 1 \pmod{4} \) then \( a \) is even; let \( a = 2\gamma \). Since \( q = \varphi^p = 1 \pmod{8} \), \( f \) is even. Under these hy-

potless, if \( q = s^2 + 4t^2 \) then \( s = \pm p^r \). To ensure \( s = 1 \pmod{4} \) we take \( s = p^r \) if \( \gamma \) is even, \( s = -p^r \) if \( \gamma \) is odd. We have \( F_q(X) = (X^2 - p^r)^2 \) for \( \gamma \) odd. We have \( F_q(X) = (X^3 - 3p^r X - 2p^r) \) for \( \gamma \) odd.

(b) The irreducibility is immediate from Corollary 7.

(c) Here \( f \) is even, and \( F_q(X) \) factors as a difference of two squares,
\[
F_q(X) = (X^3 + 2p^r X - 2p^r)\varphi^p + X^3 - 3p^r X - 2p^r + 2p^r s.
\]

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

(d) Again, \( f \) is even. The roots of \( F_q(X) \) are
\[
\pm p^r \pm p^r \sqrt{2} \left( \frac{p^r + s}{p^r + s} \right), \quad p^r \pm p^r \sqrt{2} \left( \frac{p^r + s}{p^r + s} \right).
\]
We claim \( s = s_1^2 - 4t_1^2 \). Indeed, by direct calculation, \( q = (s_1^2 - 4t_1^2)^2 \). Clearly, \( s_1^2 - 4t_1^2 = 1 \pmod{4} \). And \( s_1^2 - 4t_1^2 = p^r + 8t_1^2 \) is prime to \( p \) since \( t_1 \) is, establishing the claim. It follows that \( p^r + s = (s_1^2 + 4t_1^2) + (s_1^2 - 4t_1^2) = 2s_1^2 \), \( p^r - s = 8t_1^2 \), and the roots of \( F_q(X) \) are as given in the theorem.

7. Location of the Gauss sums. Having the Gauss sums \( G_0 \), the polynomials \( F_q(X) \) 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 \( G_0 = \sum \exp(2\pi i p^r \zeta^p) \), which of the roots of \( F_q(X) \) will this be? This is the notorious problem of the location of the Gauss sums.

When \( F_q(X) \) 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 \( q = p^e \) via the theory 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 Caesal [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 \( F_q(X) \) is not irreducible over the rationals, it is often possible to identify among its irreducible factors the one containing \( G_0 \). In particular, when \( F_q(X) \) 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 \( \chi \) be a multiplicative character on \( F_p \). Define a multiplicative character \( \chi^{(q)} \) on \( F_q \) by \( \chi^{(q)}(x) = \chi(Nx) \), where \( N \) denotes the norm, \( N : F_q \to F_p \). Then

\[
\tau(\chi^{(q)}) = (-1)^{q-1}(\tau(\chi))^{q}. 
\]

We now consider the quadratic case.

**Proposition 19.** Let \( q = 2 \). Then \( G_2 = i^* \sqrt{q} \), where \( i^* \) is given by

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

Proof. If \( q = p \) and \( \chi \) 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. 193–199, [8], pp. 469–478, [10], pp. 88–90, and elsewhere. The proposition follows from Davenport–Hasse and the observation (Proposition 1(h)) that \( G_1 = \tau(\chi) \).

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 \( p^{j} = -1 \pmod{c} \), and assume \( j \) is the least such. Let \( q = p^j \) with \( e = 2jy \). Then the Gauss sum are given by

(a) If \( p, \chi \), and \( (p^j+1)/e \) are all odd, then \( G_{en} = (e-1)p^{jy} \), \( G_{ek} = -p^{jy} \) for \( k \neq e;2 \);

(b) In all other cases, \( G_{ek} = -(1-p^{jy})p^{jy} \), \( G_{ek} = -(1-p^{jy})p^{jy} \) for \( k \neq 0 \).

Proof. In essence the result goes back to Stickelberger ([14], 3.6 and 3.10); see also [2], p. 185. In these sources the results are stated for the sums \( \tau(\chi) \) rather than \( \theta_2 \), but the translation, via Proposition 1(f) and (g), is simple.

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

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

Define the integers \( A_{\gamma} \) and \( B_{\gamma} \) by

\[
4p^{\gamma+3m} = A_{\gamma} + \varepsilon B_{\gamma}, \quad (A_{\gamma}, p) = 1, \quad p^{\gamma}A_{\gamma} = -2 \pmod{e}, \quad \text{and } A_{\gamma}B_{\gamma} > 0;
\]

this determines \( A_{\gamma} \) and \( B_{\gamma} \) uniquely. Then the Gauss sums are given by

\[
G_{\gamma} = (\varepsilon - 1)A_{\gamma} p^{\gamma}, \\
G_{\gamma} = -(B_{\gamma} - A_{\gamma}) p^{\gamma} \quad \text{if } \left( \frac{k}{e} \right) = 1, \\
G_{\gamma} = -(B_{\gamma} - A_{\gamma}) p^{\gamma} \quad \text{if } \left( \frac{k}{e} \right) = -1.
\]

Proof. This result, stated in terms of the \( \tau(\chi) \) and \( \eta_2 \), 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 \( p = 2 \pmod{3} \), is covered by the semiprimitive case, Proposition 20. Case (b), in which \( p = 1 \pmod{3} \), \( q = p^s \), \( 3|\gamma \), 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 \( p = 1 \pmod{3} \), let \( q = p^s \). Let \( c_1 \) and \( d_1 \) be as in Theorem 16 (c). Then

\[
G_{\gamma} = c_1 p^r \quad \text{and} \quad \{G_{1}, G_{2}\} = \{-(c_1 + 9d_1)p^r/2, -(c_1 - 9d_1)p^r/2\}.
\]

First Proof. Let \( e = 3 \). Since \( q \) is not a cube in \( F_3 \), \( F_3 \), \( F_p \), is not divisible by three. Thus \( \{F_3(q) \in F_p \} \), which equals the number of distinct conjugates of \( c_1 \), is divisible by 3. These conjugates are all in \( F_3 \), since, for every \( k, X^3 \) is in \( F_p \), and \( p^3 = 1 \pmod{3} \). Then \( \eta_3 = \frac{1}{3} \) is divisible by 3. By the same argument, \( \eta_2 \). Thus, \( \eta_1 = \eta_2 \pmod{3} \), and \( G_{\gamma} = G_{\gamma} \pmod{3} \). From Theorem 16(c) we see the roots of \( F_3(X) \) are congruent to \( c_1 p^r \), \( -c_1 p^r/2 \), and \( -c_1 p^r/2 \pmod{9} \), and the theorem follows.

Second Proof. Let \( \chi \) be a cubic character \( \pmod{p} \), and define the cubic character \( \chi^{(3)} \) on \( F_q \) by \( \chi^{(3)}(x) = \chi(Nx) \), where \( N \) denotes the norm from \( F_q \) to \( F_p \). Then \( \tau(\chi) = \tau(\chi) \), where \( \tau = (\varepsilon + d^2 - 27)/2 \), \( \tau = (\varepsilon + d^2 - 27)/2 \) (see [8] or [9]). We have \( G_{\gamma} = \tau(\chi^{(3)}) \) \( \tau(\chi^{(3)}) \) by Proposition 1(g), thus \( G_{\gamma} = \tau(\chi^{(3)}) + \tau(\chi^{(3)}) \) by Proposition 1(d). We have \( G_{\gamma} = (\tau^{(3)}) \) \( \tau(\chi) + \tau(\chi) \) by Davenport–Hasse, and, finally, \( G_{\gamma} = (\tau^{(3)} + \tau(\chi^{(3)})) \) \( \tau(\chi^{(3)}) \) by Proposition 1(d). To show \( G_{\gamma} = \tau(\chi^{(3)}) \) we must show \( (-1)^{\gamma} p^{\gamma} = (c_1 + d^2 - 27)/2 \). Let \( (1)^{\gamma} p^{\gamma} = (d + d^2 - 27)/2 \), then \( c_1 + 9d_1 p^r = 4p^r \), and it is easily checked that \( (c_1, p) = 1 \), and \( c_1 = 1 \pmod{3} \). Thus \( c_1 = c_1 \) and we have evaluated.
$G_2$ and $G_3$ can be obtained from Theorem 16(α), or we can keep the proof independent of that theorem, finding $G_1$ from $G_1 = \tau(x^{(2p)}) \sigma + \tau(x^{(2p)}) \sigma^2$, where $\sigma^2 = 1$, 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 $p = 3 \pmod{4}$, 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 $G_{23}$ can be determined up to a single ambiguity of sign.

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

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

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

**Theorem 24.** Let $a = 4$, $p = 1 \pmod{4}$, $q = p^r$, $r$ odd. Then $G_a = 2\sqrt{p}p^{r-2} - p^{r-2}$, where $s$ is given by $p^r = s^2 + 4sp$, $s = 1 \pmod{4}$, $(s, p) = 1$.

**Proof.** In this proof $\chi$ will denote a biquadratic character, $\chi_{\text{quad}}$ and $\chi_{\text{quadr}}$, and $G_a$ will indicate the degree of the field. Thus, $G_{a}^{(2)}$ is the biquadratic Gauss sum in the field of $p^r$ elements.

By Proposition 1(α), $G_{a}^{(2)} = \tau(x^{(2p)}) + \tau(x^{(2p)}) + \tau(x^{(2p)})$. Since $q = 1 \pmod{8}$, we have $x^{(2p)} \equiv 1 \pmod{8}$, and $\tau(x^{(2p)}) = \tau(x^{(2p)})$. With $\tau(x^{(2p)}) = -\sqrt{q}$ given by Proposition 19, we have

$$G_{a}^{(2)} = \tau(x^{(2p)}) + \tau(x^{(2p)}) - \sqrt{q}.$$ 

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

$$G_{a}^{(2)} = -\tau(x^{(2p)}) - \tau(x^{(2p)}) - \sqrt{q}.$$ 

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

$$G_{a}^{(2)} = \tau(x^{(2p)}) + \tau(x^{(2p)}) + \tau(x^{(2p)})$$

from Proposition 1(α), and

$$G_{a}^{(2)} = \sqrt{2p} + \sqrt{2p} - 2\sqrt{p}$$

from Proposition 23; also, $\tau(x^{(2p)}) = \sqrt{2p}$ from Proposition 19. Combining, and noting $\tau(x^{(2p)}) = \chi^2(1) = \tau(x^{(2p)}) = \tau(x^{(2p)})$, we have

$$\pm \sqrt{2p} = 2\sqrt{p} = \tau(x^{(2p)}) + \tau(x^{(2p)})$$

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

$$-2\sqrt{2p} = \tau(x^{(2p)}) + \tau(x^{(2p)})$$

Now comparison with (*) yields the theorem.

**Theorem 25.** Let $a = 4$, $p = 1 \pmod{4}$, $q = p^r$. Let $s_1$ and $t_2$ be as given in Theorem 17(α). Then $G_{a} = -p^{2r} - 2p^{r}G_{a} = -p^{2r} - 8p^{r}$, and $\{G_{a}, 1\} = \{p^{2r} + 4hG^{2r}\}$

**Proof.** (Compare with the first proof of Theorem 22.) Let $x$ be in $G_1$, $k \neq 0$. Since $x$ is not a fourth power in $F_{2}$, $[F_2(x) : F_2]$ is even. The conjugates of $x$ are thus even in number. Moreover, they are all in $G_k$. Thus $\eta_k$ is even for $k = 1, 2, 3$. By Proposition 1(β), $\eta_0$ is odd. By Proposition 1(α), we have $G_{a} = 5 \pmod{8}$, $G_{a} = G_{a} = 1 \pmod{8}$.

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

A second proof can be constructed along the lines of the second proof of Theorem 23. One needs to know that if $\chi$ is a biquadratic character on $F_{2}$, then $\tau(\chi) = p^{2r}$, where $\pi = s + 4sp$, $s = 1 \pmod{4}$ (see [8]).


**References**

On the theorem of Jarnik and Besicovitch

by

R. Kauflman (Urbana, Ill.)

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

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

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

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

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

By a theorem of Beurling [3, III], the closed support of $\mu$ (or any Borel set of positive $\mu$-measure) must have dimension at least $2(2+a)^{-1}$; however the property of $E(a)$ 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 $F_R(x)$, $0 < R < 1/4$, 

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

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

$$F_R(x) = \sum_{n=-\infty}^{\infty} a_n e^{2\pi i nx},$$

$$a_n = 1, \quad |a_{mR}| \leq 1, \quad |a_{mR^{1/2}}| \leq m^{-2/4}.$$  

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