On the factors $\Phi^{j\delta/m}$ of the period polynomial for finite fields

by

S. Gurak (San Diego, CA)

1. Introduction. Let $q = p^a$ be a power of a prime, and $e$ and $f$ positive integers such that $ef + 1 = q$. Let $F_q$ denote the field of $q$ elements, $F_q^*$ its multiplicative group and $g$ a fixed generator of $F_q^*$. Let $\text{Tr} : F_q \rightarrow F_p$ be the usual trace map and set $\zeta_m = \exp(2\pi i/m)$ for any positive integer $m$. Put

$$\delta = \gcd\left(\frac{q-1}{p-1}, e\right) \quad \text{and} \quad R = \frac{q-1}{\delta(p-1)} = \frac{f}{\gcd(p-1, f)},$$

and let $C_e$ denote the group of $e$th powers in $F_q^*$. The Gauss periods are

$$\eta_j = \sum_{x \in C_e} \zeta_{\text{Tr}g^jx} (1 \leq j \leq e)$$

and satisfy the period polynomial

$$\Phi(x) = \prod_{j=1}^{e} (x - \eta_j).$$

G. Myerson [8] showed that $\Phi(x)$ splits over $\mathbb{Q}$ into $\delta$ factors

$$\Phi(x) = \prod_{w=1}^{\delta} \Phi^{(w)}(x),$$

where

$$\Phi^{(w)}(x) = \prod_{k=0}^{e/\delta - 1} (x - \eta_{w+k\delta}) \quad (1 \leq w \leq \delta).$$

The coefficients $a_r = a_r(w)$ of the factor

$$\Phi^{(w)}(x) = x^{e/\delta} + a_1 x^{e/\delta - 1} + \ldots + a_{e/\delta},$$

If $S_e$ are expressed in terms of the symmetric power sums

$$(6) \quad F^{(w)}(X) = X^{e/\delta} \Phi^{(w)}(X^{-1}) = 1 + a_1 X + \ldots + a_{e/\delta} X^{e/\delta},$$

are expressed in terms of the symmetric power sums

$$(7) \quad S_n = S_n(w) = \sum_{k=0}^{e/\delta - 1} (\eta_w + k\delta)^n \quad (n \geq 0)$$

through Newton's identities

$$(8) \quad S_r + a_1 S_{r-1} + \ldots + a_{r-1} S_1 + ra_r = 0 \quad (1 \leq r \leq e/\delta).$$

If $t_w(n)$ counts the number of $n$-tuples $(x_1, \ldots, x_n)$ with $x_i \in C_e \ (1 \leq i \leq n)$ for which $\text{Tr}(g^w(x_1 + \ldots + x_n)) = 0$, then $S_n(w)$ can be computed using

$$(9) \quad S_n(w) = (p t_w(n) - f^n)/\gcd(p - 1, f).$$

In the classical case $q = p$ (so $\delta = 1$), Gauss showed that $\Phi(x)$ is irreducible over $\mathbb{Q}$ and determined the polynomial for small values of $e$ and $f$. For $f = 2$, he showed (see [3]) that the coefficients of $\Phi(x) = \Phi^{(2)}(x)$ in (5) are given by

$$(10) \quad a_v = (-1)^{[v/2]} \left[ (p - 1 - v)/2 \right] \quad (1 \leq v \leq e = (p - 1)/2).$$

In 1982 I determined [3] how to compute the beginning coefficients for the classical case when $f > 2$ is fixed. (See also [2].) In later work [5] I studied the last factor $\Phi^{(2)}(x)$ when $f$ is fixed, and showed that the beginning coefficients of the factor $\Phi^{(2)}(x)$ can be computed in a fashion similar to those of the period polynomial in the classical case $q = p$. Recently [7] I found similar results for the middle factor $\Phi^{(2/\delta)}(x)$ when $\delta$ is even. The goal of this current paper is to describe analogous results concerning the factors $\Phi^{(w)}(x)$, where $w = j\delta/m$ for $m | \delta, 1 \leq j \leq m$ and $\gcd(j, m) = 1$. This is done in the next section. Later in Sections 3 and 4, I give some explicit formulas for the factors $\Phi^{(j\delta/m)}(x)$ and certain related counting functions.

2. The factors $\Phi^{(j\delta/m)}(x)$. Throughout the paper $f > 1$ is fixed with specified odd reduced residue $r$ modulo $f$, say with $\text{ord}_f r = b$. Also fix an integer $m > 0$, together with a specified reduced residue $s$ modulo $m$ satisfying $s \equiv r \pmod{\gcd(f, m)}$, say with $\text{ord}_m s = c$. In addition to considering primes $p \equiv r \pmod{f}$ and finite fields $\mathbb{F}_q$ with $q = p^e$, I shall also require that $p \equiv s \pmod{m}$ and $m \mid \delta$. All such primes $p$ have common decomposition fields $K$ in $\mathbb{Q}(\zeta_f)$ and $k$ in $\mathbb{Q}(\zeta_m)$. (The field $K$ is that subfield of $\mathbb{Q}(\zeta_f)$ fixed by the action $\zeta_f \to \zeta_f^j$; similarly the field $k$ is that subfield of $\mathbb{Q}(\zeta_m)$ fixed by the action $\zeta_m \to \zeta_m^s$.) My goal here is to study the factors $\Phi^{(j\delta/m)}(x)$ of the period polynomial $\Phi(x)$ in (3) with $1 \leq j \leq m$ and $\gcd(j, m) = 1$. While the relative order of the factors $\Phi^{(u)}(x)$ in (3)
depends on the choice of a generator $g$ for $\mathbb{F}_q^*$; a different choice always permutes the factors $\Phi^{(j\delta/m)}(x)$ among themselves. In addition, certain duplication among the factors is predicted by Proposition 5 of [4]; namely, $\Phi^{(sj\delta/m)}(x) = \Phi^{(j\delta/m)}(x)$ since $pj\delta/m \equiv sj\delta/m \pmod{\delta}$. (Here I identify $\Phi^{(w)}(x)$ with $\Phi^{(w)}(x)$ where $w \equiv m \pmod{\delta}$ for $1 \leq \delta \leq \mu$.)

Now write $R = R_1m_1$ where $\gcd(R_1, m) = 1$ and $m_1 | m^n$ for sufficiently large $n$. The factor $R_1$ is the largest factor of $R$ which is prime to $m$. There are $m_1$ distinct reduced residues $s_1$ modulo $M$, where $M = mm_1$, satisfying $s_1 \equiv s \pmod{m}$. Select one such $s_1$, say with $\text{ord}_M s_1 = c_1$, and let $k'$ be the subfield of $\mathbb{Q}(\zeta_M)$ fixed by the action $\zeta_M \rightarrow \zeta_M^j$. Fixing $j$, with $1 \leq j \leq m$ and $\gcd(j, m) = 1$, I now consider the factor $\Phi^{(j\delta/m)}(x)$ (relative to the ordering determined by the chosen generator $g$ for $\mathbb{F}_q^*$) for the finite fields $\mathbb{F}_q$ with $q = p^n, p \equiv r \pmod{f}$, $p \equiv s_1 \pmod{M}$ and $m | \delta$. First note that $\delta R = 1 + p + \ldots + p^{a-1} \equiv 0 \pmod{M}$, so $l = \text{lcm}(b, c)$ must divide $a$. (In fact, $\text{lcm}(b, c_1) | a$.) Since $1 + p + \ldots + p^{b-1} \equiv 0 \pmod{R}$, one may write

$$1 + s_1 + \ldots + s_1^{l-1} = \mu mm_1/d,$$

where $\gcd(\mu, d) = 1$ and $d | m$ with $d > 0$. Then set

$$x_i = s_1^{l-1} - 1 \over s_1 - 1 = s_1^{l-1} - 1 \over 1 + s_1 + \ldots + s_1^{(l-1)} \quad (i > 0).$$

The expression (11) uniquely determines $d$. Since $s_1^l \equiv 1 \pmod{m}$, from (11) one sees that $x_i \equiv ix_1 \equiv i\mu m_1m/d \equiv 0 \pmod{M}$ if and only if $d | i$. In particular, as $M | \delta R$ one finds that $l d | a$.

Next note that since $R_1$ is relatively prime to both $e/\delta$ and $M$, one can express $R_1v + (e/\delta)Mu = 1$ for integers $v$ and $u$. Thus $g^{j\delta/m} = g^{j\delta Rv/M + ejum}$, so the values $\text{Tr} g^{j\delta Rv/M + \epsilon a}$ have the form

$$y_\alpha = \text{Tr} g^{j\delta Rv/M + \epsilon a}$$

$$= g^{j\delta Rv/M + \epsilon a} + g^{j\delta Rv/M + pe \epsilon a} + \ldots + g^{j\delta Rv/M + p^{a-1} \epsilon a}$$

$$= h^{\delta R/M} (g^{\epsilon a} + h^{\delta R(p-1)/M} g^{pe \epsilon a} + \ldots + h^{\delta R(p^{a-1}-1)/M} g^{p^{a-1} \epsilon a})$$

$$= h^{\delta R/M} (g^{\epsilon a} + h^{(q-1)/M} g^{pe \epsilon a} + h^{(q-1)(1+p)/M} g^{p^{2} \epsilon a}$$

$$+ \ldots + h^{(q-1)(1+p+\ldots+p^{a-2})/M} g^{p^{a-1} \epsilon a})$$

for $0 \leq \alpha < f$, where $h = g^{jv}$. Since $h^{\delta R/M} \neq 0$, the function $t_{j\delta/m}(n)$ in (9) also counts the number of times a sum $z_\alpha + \ldots + z_{\alpha n}$ equals zero for $0 \leq \alpha < f$, where

$$z_\alpha = g^{e \epsilon a} + g^{i(v(q-1)/M) g^{pe \epsilon a} + \ldots + g^{i(v(q-1)(1+p+\ldots+p^{a-2})/M) g^{p^{a-1} \epsilon a}}.$$

The following proposition completely determines $\Phi^{(j\delta/m)}(x)$ when $d > 1$, and generalizes the result of Proposition 1 of [7].

**Proposition 1.** If $d > 1$ then $\Phi^{(j\delta/m)}(x) = (x - f)^{e/\delta}$. 
Proof. I assert that each \( z_\alpha \) is 0 in (13) so that \( t_{j\delta/m}(n) = f^n \) for any \( n > 0 \), and hence \( \Phi^{j\delta/m}(x) = (x - f)^{\delta} \) from relations (8) and (9). Since \( g^{j\delta M}/M \) has order \( M(p - 1)|p^d - 1 \) and \( g^e \) has order \( f | p^d - 1 \), each trace

\[
y_\alpha = \text{Tr} g^{j\delta M/M + e\alpha} = \frac{a}{d!} \text{Tr}_{\mathbb{F}_p/\mathbb{F}_p} g^{j\delta M/M + e\alpha} \quad (0 \leq \alpha < f).
\]

Thus to show each \( z_\alpha \) in (13) is zero, one may assume without loss of generality that \( a = dl \). Now choose any \( 0 \leq \alpha < f \). Note that in terms of \( r, s_1 \) and \( x_t \),

\[
z_\alpha = g^{e\alpha} + t g^{r\alpha} + \ldots + t^{s_1} g^{r\alpha} + t s_1 x_t g^{r\alpha} + t s_1 x_t^{s_1} g^{r\alpha} + \ldots + t x_t^{s_1} g^{r\alpha} + t x_t^{s_1} x_t g^{r\alpha} + \ldots + t x_t^{s_1} x_t^{s_1} g^{r\alpha} + \ldots + t x_t^{s_1} x_t^{s_1} g^{r\alpha}
\]

in (13), where \( t = g^{j\delta/(q-1)/M} \). Now each of the bracketed sums in the last expression has the form \( 1 + g g^{r\alpha} + \ldots + g^{s_1 \alpha} \) with \( y = t \xi \) of order \( d \). Since \( d > 1 \) and \( \text{gcd}(s_1, M) = 1 \) each of those sums is zero, so \( z_\alpha = 0 \) as claimed.

In view of the above proposition, I shall assume \( d = 1 \) in (11) throughout the remainder of the paper (so \( l = \text{lcm}(b, c) = \text{lcm}(b, c_1) \)). To generalize the results known for the middle and last factor [5, 7], here it is necessary to find a suitable counting function \( b_{j, n}(n) \) which coincides with \( t_{j\delta/m}(n) \) for almost all primes \( p \equiv r \pmod{f} \) and \( p \equiv s_1 \pmod{M} \) with \( m | \delta \). To this end, define algebraic integers \( \omega_{j, \alpha} \) in \( \mathbb{Q}(\zeta_M, \zeta_f) \) by

\[
(14) \quad \omega_{j, \alpha} = \zeta_M^\alpha + \zeta_M^{j(1+s_1)} \zeta_f^{\alpha} + \ldots + \zeta_M^{j(s_1+\ldots+s_1)} \zeta_f^{\alpha-1}
\]

for \( 0 \leq \alpha < f \), and let \( b_{j, n}(n) \) count the number of times one has

\[
(15) \quad \omega_{j, \alpha_1} + \ldots + \omega_{j, \alpha_n} = 0
\]

for \( 0 \leq \alpha_i < f, \ 1 \leq i \leq n \). I find that \( b_{j, n}(n) \) is the desired counting function.

**Proposition 2.** For all primes \( p \equiv r \pmod{f} \) and \( p \equiv s_1 \pmod{M} \) with \( m | \delta \)

\[
b_{m, j}(n) \leq t_{j\delta/m}(n) \quad \text{for } n > 0.
\]

Equality holds for any such prime \( p \mid a \), except those lying in a computable finite set \( \xi_{j,n} \).

**Proof.** Since \( l = \text{lcm}(b, c) \), one finds that \( \text{lcm}(f, M) \) divides \( p^d - 1 \), so the elements \( g^e \) and \( g^{(q-1)/M} \) lie in \( \mathbb{F}_p \). In particular, one may identify...
Factors of the period polynomial

\[ \mathbb{F}_{p'} / \mathbb{F}_p \] as the residue field extension at \( p \) for the extension \( L = \mathbb{Q}(\zeta_f, \zeta_M) \).

By appropriately choosing the generator \( g \), the identification can be made such that \( g^{(q-1)/M} \) corresponds to \( \zeta_M^{R_i} \) modulo \( P \) for some \( L \)-prime \( P \) lying above \( p \). With respect to this identification \( g^e \) corresponds to a primitive \( f \)-root of unity, say \( \zeta_p^e \), for some integer \( \mu \) prime to \( f \). So \( z_{n_A} \) in (13) corresponds to \( (a/l) \omega_{j,\alpha}^{R_i} \) modulo \( P \) for some \( L \)-prime \( P \) lying above \( p \).

With respect to this identification \( g \) corresponds to a primitive \( f \)-root of unity, say \( \zeta_p^e \), for some integer \( \mu \) prime to \( f \). So \( z_{n_A} \) in (13) corresponds to \( (a/l) \omega_{j,\alpha}^{R_i} \) modulo \( P \) for some \( L \)-prime \( P \) lying above \( p \).

It follows that \( t_{j^e/m}(n) \) counts precisely the number of times one has

\[ \sum_{\alpha_1, \ldots, \alpha_n} \equiv 0 \pmod{P} \]

for a choice of \( \omega_{j,\alpha} \) in (14) where \( 0 \leq \alpha_1, \ldots, \alpha_n < f \). In particular, \( b_{m,j}(n) \leq t_{j^e/m}(n) \) for \( n > 0 \). Equality holds for any prime \( p \) not dividing \( a \) and for which \( P \) does not divide any of the non-zero right-hand sums in (16). If \( \tilde{p} \) is the \( k \)-prime lying between \( P \) and \( p \), then the latter exception is equivalently expressed by requiring that \( p \notin \xi_{j,n} \), where \( \xi_{j,n} \) consists of all rational primes \( p \equiv r \pmod{f} \) and \( p \equiv s \pmod{m} \) for which \( \tilde{p} \) divides some non-zero norm \( N_{L/k}(\omega_{j,\alpha_1} + \ldots + \omega_{j,\alpha_n}) \) for a choice of \( \omega_{j,\alpha} \) in (14).

This completes the proof of the proposition.

Now let \( h \) be the smallest positive integer for which \( b_{m,j}(h) \neq 0 \). Using (8), (9) and the above proposition, one may obtain the following generalization of Theorem 1 of [5]. Since the argument is identical to that used in obtaining Theorem 1 of [5], I shall omit it here.

**Theorem 1.** For all primes \( p \nmid a \) such that \( p \equiv r \pmod{f} \), \( p \equiv s_1 \pmod{M} \) but \( p \notin \xi_{j,n} \) (\( n \leq v \)), and \( d = 1 \) in (11), the coefficient \( a_v \) for \( \Phi^{j^e/m}(x) \) in (5) (or \( F^{j^e/m}(X) \) in (6)) satisfies \( a_v = \theta_v(p) \), where \( \theta_v \) is a polynomial of degree \( [v/h] \).

Now consider the rational power series

\[ C_{m,j}(X) = \exp \left( -\frac{R}{f} \sum_{n=1}^{\infty} b_{m,j}(n)X^n/n \right) \]

defined in terms of the counting function \( b_{m,j}(n) \). The argument in the proof of Theorem 1 of [2] extends in a straightforward manner to yield

**Theorem 2.** For any \( v > 0 \) and prime \( p \nmid a \) such that \( p \equiv r \pmod{f} \), \( p \equiv s_1 \pmod{M} \) but \( p \notin \xi_{j,n} \) (\( n \leq v \)), and \( d = 1 \) in (11), we have

\[ F^{j^e/m}(X) \equiv \frac{C_{m,j}(X)^p}{(1-fX)^{R/f}} \pmod{X^{v+1}} \]

in \( \mathbb{Z}[[X]] \).

To illustrate Proposition 1 and Theorems 1 and 2 above, consider the following examples.
Example 1. Consider the case $f = m = 4$ with $r = s = 3$ so $K = k = \mathbb{Q}$. Here $l = b = c = 2$ with $R = 2, R_1 = 1$ and $m_1 = 2$. The possible choices for $s_1 \pmod{M}$ with $s_1 \equiv s \pmod{m}$ are 3 and 7 (mod 8), each with $c_1 = 2$, but with $d = 2$ and 1, respectively, in (11). By Proposition 1, 

$$
\Phi^{(\delta/4)}(x) = \Phi^{(3\delta/4)}(x) = (x - 4)^{(p-1)/2} \quad \text{for } p \equiv 3 \pmod{8}.
$$

For the other case $p \equiv 7 \pmod{8}$, I illustrate Theorems 1 and 2 in (11) and The possible choices with $q = p^2$. One finds

$$\omega_{1,3} = -\omega_{j,3} = i(1 - \zeta_8^j) \quad \text{and} \quad \omega_{j,0} = -\omega_{j,2} = 1 + \zeta_8^j \quad \text{in (14)}$$

for this case, where $L = \mathbb{Q}(\zeta_8)$ in the proof of Proposition 2 and $k' = \mathbb{Q}(\sqrt{2})$. The corresponding counting functions $b_{4,i}(n)$ satisfy

$$
b_{4,1}(n) = b_{4,3}(n) = \begin{cases} 
\left( \frac{n}{2} \right)^2 & \text{if } n \text{ is even}, \\
0 & \text{otherwise},
\end{cases}
$$

so $C_{4,1}(X) = C_{4,3}(X) = 1 - X^2 - 4X^4 - 29X^6 - 265X^8 - \ldots$ in (17). The first few polynomial expressions for the beginning coefficients of $\Phi^{(\delta/4)}(x)$ from Theorem 1 are found to be

$$
\vartheta_1(p) = 2, \quad \vartheta_2(p) = -p + 6, \quad \vartheta_3(p) = -2p + 20,
\vartheta_4(p) = \frac{1}{3}(p^2 - 21p + 140), \quad \vartheta_5(p) = p^2 - 29p + 252, \quad \ldots
$$

The prime $p = 7$ first appears in the exceptional sets $\xi_{1,n} = \zeta_{3,n}$ ($n > 0$), when $n = 3$. Incidentally, one finds that $3 + \sqrt{2}$ divides $2\omega_{1,1} + \omega_{1,0}$ and $2\omega_{1,3} + \omega_{1,2}$ in $L$, while $3 - \sqrt{2}$ divides $\omega_{1,3} + 2\omega_{1,0}$ and $\omega_{1,1} + 2\omega_{1,2}$. Specifically, for $p = 7$ (where $\delta = 4$) one may take $q = 2 + i$ to generate $\mathbb{F}_{10}$ with $g^{(q-1)/M} = g^6 \equiv 2i + 2 \equiv \zeta_8$ (mod $3 + \sqrt{2}$) and $g^e = g^{12} \equiv i$ (mod $3 + \sqrt{2}$), so $\omega_{j,\alpha} \equiv \omega_{j,\alpha}$ (mod $3 + \sqrt{2}$) in (13). One computes $t_1(1) = t_3(1) = 0, t_1(2) = t_3(2) = 4$ and $t_1(3) = t_5(3) = 6$ so $\Phi^{(1)}(x) = \Phi^{(3)}(x) = x^3 + 2x^2 - x - 1$ from (8) and (9). As expected, the underscored coefficient $\vartheta_3(7) = 6$.

Example 2. Now consider the case $f = 3$ and $m = 5$ with $r = 2$ and $s = 4$ with $q = p^2$. Here $R = R_1 = 3, m_1 = 1$, $l = b = c = c_1 = 2$ and $\delta = (p + 1)/3$ with $p \equiv 14 \pmod{15}$. In addition, $L = \mathbb{Q}(\zeta_5)$, $K = \mathbb{Q}$ and $k = k' = \mathbb{Q}(\sqrt{5})$, with $d = 1$ in (11) and $\omega_{j,\alpha} = \zeta_5^j + \zeta_5^j\zeta_5^{2\alpha}$ ($1 \leq j \leq 4, 0 \leq \alpha \leq 2$) in (14). One finds $\Phi^{(3/5)}(x) = \Phi^{(3\delta/5)}(x)$ and $\Phi^{(2\delta/5)}(x) = \Phi^{(3\delta/5)}(x)$ here. The function $b_{m,j}(n)$ is seen to satisfy

$$
b_{m,j}(n) = \begin{cases} 
\{n/((n/3)!)]^3 & \text{if } 3 \mid n, \\
0 & \text{otherwise},
\end{cases}
$$

for $1 \leq j \leq 4$, so each $C_{m,j}(X) = 1 - 2X^3 - 9X^6 - 158X^9 - \ldots$ in (17). The first few polynomial expressions for the beginning coefficients of $\Phi^{(3\delta/m)}(x)$ from Theorem 1 are found to be

$$
\vartheta_1(p) = 3, \quad \vartheta_2(p) = 9, \quad \vartheta_3(p) = -2p + 27, \quad \vartheta_4(p) = -6p + 81, \\
\vartheta_5(p) = -18p + 243, \quad \vartheta_6(p) = 2p^2 + 69p + 729, \quad \vartheta_7(p) = 6p^2 - 207p + 2187, \ldots
$$
For \( p = 59 \) one may choose \( g = 2 + \zeta_5 \) to generate \( \mathbb{F}_{59^2}^* \), so \( g^{(q - 1)/m} = g^{696} = \zeta_5^3 \) modulo \( (8 + \sqrt{5}) \) in \( \mathbb{Q}(\zeta_5) \). For an appropriate choice of an \( L \)-prime \( P \) lying above \( (8 + \sqrt{5}) \) one has \( g^6 = g^{1160} \equiv \zeta_3 \pmod{P} \), so \( z_n \equiv \omega_{j,n} \pmod{P} \) in (13). The prime 59 first appears in the exceptional sets \( \xi_{1,n} = \xi_{4,n} \) \((n > 0)\) when \( n = 4 \), but not in \( \xi_{2,n} = \xi_{3,n} \) \((n > 0)\) until \( n = 7 \). In verifying this, one finds

\[
N_{L/k}(3\omega_{1,1} + \omega_{1,2}) = N_{L/k}(3\omega_{4,1} + \omega_{4,2}) = (8 + \sqrt{5})^2((1 - \sqrt{5})/2)^2
\]
and

\[
N_{L/k}(2\omega_{2,0} + 5\omega_{2,2}) = N_{L/k}(2\omega_{3,0} + 5\omega_{3,2}) = (8 + \sqrt{5})^2((11 + \sqrt{5})/2)^2.
\]
The relevant \( t_{j\delta/m}(n) = t_{4j}(n) \) are tabulated below:

\[
\begin{array}{cccccccc}
  j \backslash n & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\
  1 & 0 & 0 & 6 & 4 & 10 & 90 & 105 \\
  2 & 0 & 0 & 6 & 0 & 0 & 90 & 21 \\
  3 & 0 & 0 & 6 & 0 & 0 & 90 & 21 \\
  4 & 0 & 0 & 6 & 4 & 10 & 90 & 105 \\
\end{array}
\]

From (8) and (9) one now finds that \( \Phi^{(4)}(x) = \Phi^{(16)}(x) \) equals

\[
x^{58} + 3x^{57} + 9x^{56} - 91x^{55} - 332x^{54} - 1114x^{53} + 2735x^{52} + 14282x^{51} + \ldots
\]
and \( \Phi^{(8)}(x) = \Phi^{(12)}(x) \) equals

\[
x^{58} + 3x^{57} + 9x^{56} - 91x^{55} - 273x^{54} - 819x^{53} + 3620x^{52} + 10683x^{51} + \ldots
\]
The underscored coefficients deviate as expected from the pattern of the beginning coefficients given by \( a_v = \vartheta_v(p) \). Incidentally, it is convenient to use the formula from Proposition 4 of [4] here. Further computation shows that \( \eta_4 \) and \( \eta_{16} \) are both conjugates of \( \zeta_5^2 + \zeta_5^4 + \zeta_5^{-3} \), while \( \eta_8 \) and \( \eta_{12} \) are conjugates of \( \zeta_5^2 + \zeta_5^4 + \zeta_5^{-5} \).

While Theorems 1 and 2 yield an elegant, formal way to obtain the beginning coefficients of a factor \( \Phi^{(j\delta/m)}(x) \), the approach is impractical since the counting function \( b_{m,j}(n) \) is difficult to compute in general. However, there are several special situations where \( b_{m,j}(n) \) can be readily determined, which often lead to explicit formulas for \( C_{m,j}(X) \) and expressions for the beginning coefficients of \( \Phi^{(j\delta/m)}(x) \). In describing these situations, it is convenient to express

\[
1 + s_1 + \ldots + s_{c_1-1} = \frac{uM}{t}
\]
where \( \gcd(u, t) = 1 \) and \( t \mid M \) with \( t > 0 \). The expression (18) uniquely determines \( t \). For the sake of brevity, the specific cases I investigate in the next sections are for \( t = 1 \) and \( t = M \). The intermediate cases when \( t \) is a proper divisor of \( M \) are less manageable, though they may be handled in a similar, albeit more tedious, fashion.
3. The case \( t = 1 \). I retain the notation of the previous section, requiring again that \( d = 1 \) in (11), but assume now that \( t = 1 \) in (18). I shall assume here that \( \text{ord}_M s_1 = c_1 > 1 \) since \( t = M \) in (18) if \( c_1 = 1 \). The results I describe primarily rely on some knowledge about the set 
\[ \{1, \zeta_M^{1+s_1}, \ldots, \zeta_M^{1+s_1+s_1^{-1}}\} \] 
in \( \mathbb{Q}(\zeta_M) \). The first is

**Theorem 3.** Let \( W \) be the subfield of \( \mathbb{Q}(\zeta_f) \) fixed by the action \( \zeta_f \mapsto \zeta_f^{\gcd(b, c_1)} \). Suppose \( \{1, \zeta_M^{1+s_1}, \ldots, \zeta_M^{1+s_1+s_1^{-1}}\} \) is linearly independent over \( W \) with \( t = 1 \) in (18). Then \( b_{m,j}(n) \) counts the number of times 
\[ \text{Tr}_{\mathbb{Q}(\zeta_f)/W}(x_1 + \ldots + x_n) \] 
is zero for a choice of \( f \)-roots of unity \( x_1, \ldots, x_n \) lying in \( \mathbb{Q}(\zeta_f) \). (In particular, if \( \gcd(b, c_1) = 1 \) then \( b_{m,j}(n) = \beta_{K}(n) \), the counting function given for the last factor \( \Phi^{(3)}(x) \) in [5].)

**Proof.** Put \( d_1 = \gcd(b, c_1) \). Without loss of generality, one may assume \( a = l \). Then, in (14),
\[ \omega_{j, \alpha} = (\zeta_f^\alpha + \zeta_f^{r^1\alpha} + \ldots + \zeta_f^{r^{c_1-1}\alpha}) + \zeta_M^{j}(\zeta_f^\alpha + \zeta_f^{r^1\alpha} + \ldots + \zeta_f^{r^{c_1-1}\alpha}) \]
\[ + \ldots + \zeta_M^{j(1+s_1+\ldots+s_1^{-1})}(\zeta_f^\alpha + \zeta_f^{r^1\alpha} + \ldots + \zeta_f^{r^{c_1-1}\alpha}) \]
\[ + \ldots + \zeta_M^{j(1+s_1+\ldots+s_1^{-1})}(\zeta_f^{r^{s_1-1}\alpha} + \zeta_f^{2c_1-1\alpha} + \ldots + \zeta_f^{l-1\alpha}) \]
since \( t = 1 \). Further, any sum \( \zeta_f^{r^1\alpha} + \zeta_f^{r^{c_1-1}\alpha} + \ldots + \zeta_f^{r^{c_1-1}\alpha} \) which appears is the trace \( \text{Tr}_{\mathbb{Q}(\zeta_f)/W}(\zeta_f^{r^\alpha}) \) since \( \text{ord}_f r^{c_1} = b/d_1 = l/c_1 \). By hypothesis \( \{1, \zeta_M^{j}, \ldots, \zeta_M^{j(1+s_1+\ldots+s_1^{-1})}\} \) is linearly independent over \( W \), so a sum \( \omega_{j, \alpha_1} + \ldots + \omega_{j, \alpha_n} \) is zero if and only if the corresponding sum
\[ \text{Tr}_{\mathbb{Q}(\zeta_f)/W}(\zeta_f^{r^{\alpha_1} + \ldots + \zeta_f^{r^{\alpha_n}}}) \] 
is zero. This yields the theorem’s assertion about the count \( b_{m,j}(n) \). When \( d_1 = 1, W = K \) so the last statement of the theorem readily follows.

The following corollary is immediate in view of Propositions 4 and 5 of [5].

**Corollary 1.** Suppose \( \{1, \zeta_M^{1+s_1}, \ldots, \zeta_M^{1+s_1+s_1^{-1}}\} \) is linearly independent over \( \mathbb{Q}(\zeta_f) \) with \( t = 1 \) in (18). Put \( \lambda = b/\gcd(b, c_1) \). Then for \( f = \ell \) a prime,
\[ b_{m,j}(n) = \begin{cases} \lambda^{n(\ell-1)/\ell} \frac{n!}{((\lambda n/\ell)!)^{(\ell-1)/\ell}} & \text{if } \ell \mid n, \\ 0 & \text{otherwise}. \end{cases} \]

For \( f = 4, b_{m,j}(n) = \binom{2n}{n} \) if \( \lambda = 2 \); otherwise if \( \lambda = 1, \)
\[ b_{m,j}(n) = \begin{cases} \binom{n}{n/2}^2 & \text{if } 2 \mid n, \\ 0 & \text{otherwise}. \end{cases} \]
I note that Example 1 of the previous section illustrates the above corollary when \( f = 4 \) and \( \lambda = 1 \).

Consider again the prime \( P \) that appeared in the proof of Proposition 2 through which the finite field extension \( \mathbb{F}_p/\mathbb{F}_q \) is identified as the residue field extension at \( p \) for the extension \( L = \mathbb{Q}(\zeta_f, \zeta_M) \). Recall the identification was made in such a way that \( g^{(q-1)/M} \) corresponds to \( \zeta_M^{R_1} \) modulo \( P \), with \( k \)-prime \( p \) lying between \( P \) and \( p \).

The next result concerns the special case when \( K = \mathbb{Q} \) or \( K = \mathbb{Q}(\zeta_f) \).

**Corollary 2.** Suppose \( \text{ord}_f r = 1 \) or \( \phi(f) \) with \( \gcd(b, c_1) = 1 \) and \( t = 1 \) in (18). Then
\[
\Phi^{(j\delta/m)}(x) = \begin{cases} 
\Phi^{(\delta)}(x) & \text{if } p \text{ is prime to } 1 + \zeta_f^j + \ldots + \zeta_f^{j(s_1 + \ldots + s_i - 2)} \\
(x - f)^{c/\delta} & \text{otherwise.}
\end{cases}
\]  

The proof of the above corollary follows from that of Theorem 3, once one observes that the counting functions \( t_{j\delta/m}(n) \) and \( t_\delta(n) \) are identical here when \( p \) is prime to \( 1 + \zeta_f^j + \ldots + \zeta_f^{j(s_1 + \ldots + s_i - 2)} \). Formula (19) exactly determines the factor \( \Phi^{(j\delta/m)}(x) \) when \( f = 2 \) or \( f = 4 \) with \( r = 3 \), since in these cases closed form expressions are known [6] for the last factor \( \Phi^{(\delta)}(x) \).

I also note that if \( \gcd(s - 1, m) = 1 \) then the condition in (19) can be checked working solely in \( k \). One need only check if \( p \) divides the trace \( Tr_Q(\zeta_M)\zeta^{s_1}(\zeta_M) \), where \( u \) satisfies \( u(s_1 - 1) \equiv 1 \) (mod \( M \)). This is a consequence of the following observation.

**Lemma 1.** Suppose \( u \) is an integer satisfying \( u(s_1 - 1) \equiv 1 \) (mod \( M \)). Then
\[
\zeta_M^{1+s_1+\ldots+s_i+u} = \zeta_M^{u(s_i+1)} \text{ for } i \geq 0.
\]

The proof of Lemma 1 involves a straightforward induction argument which I shall omit here. To illustrate Corollary 2 and the above remark consider the following example.

**Example 3.** Let \( f = 4 \) and \( m = 11 \) with \( r = s = 3 \) and \( q = p^{10} \). Here \( R = 2 \) so \( m_1 = R_1 = 1 \) and \( s_1 = s \). Also, \( b = c_1 = c = 2 \), \( e/\delta = (p - 1)/2 \), \( K = \mathbb{Q} \) and \( k' = k = \mathbb{Q}(\sqrt{-\Pi}) \), and \( t = 1 \) in (18). Then
\[
\omega_{j,\alpha} = (c_4^\alpha + \zeta_4^{-\alpha})(1 + \zeta_4^j + \bar{\zeta}_4^j + \zeta_4^j) = (c_4^\alpha + \zeta_4^{-\alpha})\zeta_4^{-5j} \frac{Tr_Q(\zeta_{11}^{j})}{\zeta_{11}^{j}}\zeta_{11}^{6j} = (c_4^\alpha + \zeta_4^{-\alpha})\zeta_{11}^{5j}\left(-1 \mp \frac{\sqrt{-\Pi}}{2}\right)
\]
according as \( j \) is a quadratic non-residue or residue modulo 11. By Corollary 2 and Proposition 6 of [7], each finite field \( \mathbb{F}_{p^{10}} \), where the prime \( p \neq 3 \) satisfies \( p \equiv 3 \pmod{44} \), has a period polynomial \( \Phi(x) \) in (3) with factors

\[
\Phi^{(j\delta/11)}(x) = \sum_{v=0}^{(p-1)/2} (-1)^v \binom{p-v-1}{v} x^{(p-1)/2-v} \quad \text{for } 1 \leq j \leq 10.
\]

For the exceptional prime \( p = 3 \), the corresponding period polynomial has half of its factors \( \Phi^{(j\delta/11)}(x) \) (\( 1 \leq j \leq 10 \)) equal to \( x − 1 \) and half equal to \( x − 4 \).

4. The case \( t = M \). Keeping the notation of the previous sections and requiring that \( d = 1 \) in (11), I now assume \( t = M \) in (18), or equivalently that \( s_1 = 1 \). Then \( M \mid b \) from (11) since \( l = b \).

I begin with a preliminary observation concerning the factorization of \( \Phi^{(j\delta/m)}(x) \).

**Proposition 3.** \( \Phi^{(j\delta/m)}(x) \) has at least \( m/\gcd(r-1, f) \) identical factors when \( s = 1 \).

**Proof.** I shall apply Proposition 5 of [4] to the situation here, where \( e = \frac{p-1}{\gcd(p-1, f)} \delta \). Since \( m \mid p-1 \) and \( \gcd(j, m) = 1 \), one finds that \( \Phi^{(j\delta/m)}(x) \) has at least

\[
\frac{e}{\gcd(e, (p-1)j\delta/m)} = \frac{(p-1)\delta/\gcd(p-1, f)}{m} \frac{\gcd(p-1, f)}{\gcd(r-1, f)}
\]

factors.

For the most part, the results described in this section are seen to depend on facts concerning ordinary Gauss sums of order \( m \) defined modulo an odd prime \( \ell \equiv 1 \pmod{m} \). Such sums have the form

\[
\tau_\alpha(\chi) = \sum_{x=1}^{\ell-1} \chi(x) \zeta_\ell^{\alpha x}
\]

for some integer \( \alpha \), where \( \chi \) is a numerical character of order \( m \) modulo \( \ell \). Of particular interest here is the situation when \( r \) is a primitive root of \( f \) (so \( b = \phi(f) \)), or equivalently \( K = \mathbb{Q} \), where the \( \omega_{j,\alpha} \) in (14) are just integer multiples of the Gauss sums in (20) for some fixed character \( \chi \). Here and throughout the remainder of this section I assume \( m > 1 \). The following lemma explicitly gives \( \omega_{j,\alpha} \) for the cases \( f = \ell^r \) and \( 2\ell^r \), where \( \ell \) is an odd prime. I note that since \( p \equiv 1 \pmod{M} \) and \( l = \ell^{r-1}(\ell - 1) \), \( M \) must actually divide \( \ell - 1 \) from (11). (Otherwise if \( \ell \mid M \) then \( r \equiv p \equiv 1 \pmod{\ell} \) is not a primitive root of \( f \).) But then \( \gcd(m, R) = 1 \) so \( m_1 = 1 \) and \( R_1 = R \).
Lemma 2. Suppose $K = \mathbb{Q}$ and $s = 1$ with $m \mid \ell - 1$. For $f = \ell^v$,

$$\omega_{j,\alpha} = \begin{cases} 
\ell^v \tau_\alpha(\chi) & \text{if } \ell^v \parallel \alpha, \\
0 & \text{otherwise.}
\end{cases}$$

For $f = 2\ell^v$,

$$\omega_{j,\alpha} = \begin{cases} 
\ell^v \tau_\alpha(\chi) & \text{if } \ell^v \parallel \alpha \text{ with } \alpha \text{ even}, \\
-\ell^v \tau(\ell^v + 1)\alpha/2(\chi) & \text{if } \ell^v \parallel \alpha \text{ with } \alpha \text{ odd}, \\
0 & \text{otherwise.}
\end{cases}$$

Here $\chi$ is the character induced by setting $\chi(r) = \zeta_m^j$.

The proof of the lemma involves routine manipulations with Gauss sums so I omit it here. Since $\tau_1(\chi) = \zeta_m^{-ij}\tau(\chi)$, the non-zero $\omega_{j,\alpha}$ in the lemma are equal up to multiplication by a root of unity. In fact, one readily sees that there are $(\ell - 1)/m$ occurrences of each possible value $\ell^v\zeta_m^w\tau_1(\chi)$ ($0 \leq w < m$), and also of $-\ell^v\zeta_m^w\tau(\chi)$ ($0 \leq w < m$) if $f = 2\ell^v$.

Now define a counting function $b_m(i)$ by setting $b_m(0) = 1$, and for $i > 0$, let $b_m(i)$ count the number of times a sum of $i$ $m$th roots of unity equals zero. One finds the following formulas for the counting function $b_{m,j}(n)$ in terms of the values $b_m(i)$.

Proposition 4. Suppose $K = \mathbb{Q}$ and $s = 1$ with $m \mid \ell - 1$. For $f = \ell^v$,

$$b_{m,j}(n) = \sum_{i=0}^{n} \binom{n}{i} b_m(i) \left( \frac{\ell - 1}{m} \right)^i (\ell^v - \ell + 1)^{n-i}.$$ 

For $f = 2\ell^v$,

$$b_{m,j}(n) = \begin{cases} 
\sum_{i=0}^{n} \binom{n}{i} b_{2m}(i) \left( \frac{\ell - 1}{m} \right)^i (2(\ell^v - \ell + 1))^{n-i} & \text{if } m \text{ odd,} \\
2^n \sum_{i=0}^{n} \binom{n}{i} b_m(i) \left( \frac{\ell - 1}{m} \right)^i (\ell^v - \ell + 1)^{n-i} & \text{if } m \text{ even.}
\end{cases}$$

Proof. In view of the remark prior to stating this proposition and the fact that $\tau_1(\chi) \neq 0$ here, the number of times a sum $\omega_{j,\alpha_1} + \ldots + \omega_{j,\alpha_n}$ equals zero for which $i$ of the values $\omega_{j,\alpha}$ are non-zero and the remaining $n-i$ values are zero equals

$$\binom{n}{i} \left( \frac{\ell - 1}{m} \right)^i b_m(i)(\ell^v - \ell + 1)^{n-i} \quad \text{if } f = \ell^v.$$ 

If $f = 2\ell^v$, then this number is

$$\binom{n}{i} \left( \frac{\ell - 1}{m} \right)^i b_{2m}(i)(2(\ell^v - \ell + 1))^{n-i} \quad \text{when } m \text{ is odd,}$$
and
\[ \binom{n}{i} \left( \frac{2(\ell - 1)}{m} \right)^i b_m(i)(2(\ell' - \ell + 1))^{n-i} \] when \( m \) is even.

In each case, this yields the desired expressions for \( b_{m,j}(n) \).

Now let \( B_m(X) = \exp(-\sum_{n=1}^{\infty} b_m(n)X^n/n) \), which is the “integral” power series introduced by Gupta and Zagier in [2]. The formulas for the \( b_{m,j}(n) \) in the above proposition yield explicit expressions for the corresponding power series (17) in terms of the series \( B_m(X) \).

**Proposition 5.** Suppose \( K = \mathbb{Q} \) and \( s = 1 \) with \( m | \ell - 1 \). For \( f = \ell' \),
\[
C_{m,j}(X) = (1 - (\ell' - \ell + 1)X)B_m \left( \frac{(\ell - 1)X/m}{1 - (\ell' - \ell + 1)X} \right).
\]

For \( f = 2\ell' \),
\[
C_{m,j}(X) = \begin{cases} 
(1 - 2(\ell' - \ell + 1)X)B_{2m} \left( \frac{(\ell - 1)X/m}{1 - 2(\ell' - \ell + 1)X} \right)^{1/2} & \text{if } m \text{ odd}, \\
(1 - 2(\ell' - \ell + 1)X)B_m \left( \frac{2(\ell - 1)X/m}{1 - 2(\ell' - \ell + 1)X} \right)^{1/2} & \text{if } m \text{ even}.
\end{cases}
\]

**Proof.** I consider only the case \( f = \ell' \) here, since the argument when \( f = 2\ell' \) is similar. For \( f = \ell' \), one obtains
\[
\frac{b_{j,m}(n)}{((\ell - 1)/m)^n} = \sum_{i=0}^{n} \binom{n}{i} b_m(i) \left( \frac{\ell' - \ell + 1}{(\ell - 1)/m} \right)^{n-i}
\]
from Proposition 4. Thus, from (17), \(-\ln C_{m,j}(\frac{mX}{\ell - 1})\) equals
\[
\sum_{n=1}^{\infty} \frac{b_{m,j}(n)}{((\ell - 1)/m)^n} X^n/n
\]
\[
= -\sum_{n=1}^{\infty} \sum_{i=0}^{n} \binom{\ell' - \ell + 1}{(\ell - 1)/m}^{n-i} \binom{n}{i} b_m(i) X^n/n
\]
\[
= -\sum_{n=1}^{\infty} \frac{(\ell' - \ell + 1)X^n}{(\ell - 1)/m} - \sum_{i=1}^{\infty} b_m(i) X^i (1 - \frac{\ell' - \ell + 1}{(\ell - 1)/m})^{-i}/i
\]
\[
= \ln \left( 1 - \frac{\ell' - \ell + 1}{(\ell - 1)/m} \right) + B_m(X/(1 - mX(\ell' - \ell + 1)/(\ell - 1)))
\]
since \( R/f = 1 \) here. Replacing \( X \) by \( \frac{\ell - 1}{m}X \) yields the desired formula.
For $d \mid p - 1$, let $f_d(x)$ denote the minimal polynomial for the ordinary cyclotomic period $\zeta_p^e + \ldots + \zeta_p^{ed}$, where $z$ generates $(\mathbb{F}_p^*)^{(p-1)/d}$. Propositions 4 and 5 suggest that the factor $\Phi^{j\delta/m}(x)$ is related to the ordinary period polynomial $f_m(x)$ or $f_{2m}(x)$ when $f = 2\ell^\nu$ with $m$ odd. Indeed this is seen to be the case.

**Theorem 4.** Suppose $K = \mathbb{Q}$ and $s = 1$ with $m \mid \ell - 1$ and $f = \ell^\nu$ or $2\ell^\nu$. If $p \mid b$ then $\Phi^{j\delta/m}(x) = (x - f)^{e/\delta}$ else

$$
\Phi^{j\delta/m} = \begin{cases} 
\left(\frac{\ell - 1}{m}\right)^{p-1} f_m \left(\frac{m}{\ell - 1}(X - (\ell^\nu - \ell + 1))\right)^m & \text{if } f = \ell^\nu, \\
\left(\frac{\ell - 1}{m}\right)^{\frac{(p-1)/2}{}} f_{2m} \left(\frac{m}{\ell - 1}(X - 2(\ell^\nu - \ell + 1))\right)^m & \text{if } f = 2\ell^\nu, m \text{ odd,} \\
\left(\frac{2(\ell - 1)}{m}\right)^{\frac{(p-1)/2}{}} f_m \left(\frac{m}{2(\ell - 1)}(X - 2(\ell^\nu - \ell + 1))\right)^{m/2} & \text{if } f = 2\ell^\nu, m \text{ even.}
\end{cases}
$$

**Proof.** First note that the element $q^{\delta/m}$ has order $mR(p - 1)$ dividing $p^b - 1$ since $p \equiv 1 \pmod{m}$, $m \mid \ell - 1 \mid b$ and $R = \ell^\nu$ here. Thus each of the traces $\text{Tr} g^{j\delta/m} x = 0$ for $x \in C_\ell$ if $p \mid a$, so $t_{j\delta/m}(n) = f^n (n > 0)$ and hence $\Phi^{j\delta/m}(x) = (x - f)^{e/\delta}$ in that case. So suppose $p \nmid a$. In view of Proposition 3, it is enough to show in this case that $\eta_{j\delta/m}$ is a conjugate of $(\ell^\nu - \ell + 1) + \frac{t}{m}(\zeta_p^z + \ldots + \zeta_p^{zm})$ if $f = \ell^\nu$ or a conjugate of $2(\ell^\nu - \ell + 1) + \frac{t}{m}(\zeta_p^z + \ldots + \zeta_p^{zm} + \zeta_p^{-z} + \ldots + \zeta_p^{-zm})$ if $f = 2\ell^\nu$, where $z$ has order $m$ modulo $p - 1$.

For this purpose, I employ the formula from Proposition 4 of [4] to compute $\eta_{j\delta/m}$ here, based on certain counts concerning the non-zero values among the traces $\text{Tr} g^{\nu + j\delta/m}$ ($1 \leq \nu \leq R$). In particular, let $N$ count the number of non-zero values among $\text{Tr} g^{\nu + j\delta/m}$ ($1 \leq \nu \leq R$) and $n_t$ count the number of times $\text{Tr} g^{\nu + j\delta/m}$ for $1 \leq \nu \leq R$ lies in the coset $G^t (\mathbb{F}_p^*)^{e/\delta}$ ($1 \leq t \leq e/\delta$), where $G = g^{(q-1)/(p-1)}$. Then

$$
(21) \quad \eta_{j\delta/m} = \delta(p - 1)(R - N)/e + \sum_{t=1}^{e/\delta} n_t \psi_t,
$$

where $\psi_t = \zeta_p^{G^t} + \zeta_p^{G^{t+e/\delta}} + \ldots + \zeta_p^{G^{t+p-1-e/\delta}}$ is an ordinary cyclotomic period of order $e/\delta$. To determine the counts $N$ and $n_t$ for the situation at hand, first write $Rv + (e/\delta)mu = 1$ for integers $u$ and $v$ as in the remark preceding (13), recalling that $m_1 = 1$ and $R_1 = R$ here. Then $\delta/m = eu + (\delta R/m)v$, so
that \(g^{y + jδ/m} = g^{y'} + jδRv/m\) where \(y' = y + ju\). Without loss of generality one may use the traces \(\text{Tr}_g g^δRv/m \cdot e^{y'}\) instead to find \(N\) and \(n_1\). Now \(\text{Tr}_g g^δRv/m \cdot e^{y'} = \frac{a}{b} G^{jv/m}\) \(\text{Tr}_g g^δRv/m \cdot e^{y'} = 0\) if \(ℓ^{(ν−1)} y'\), since \(g^δRv/m = G^{jv/m}\) lies in \(F^{p−1}\) and \(g^e\) is a primitive \(f\)-root of unity. In particular, the proof of the theorem when \(p \nmid q\) is reduced to the case \(ν = 1\) where \(a = b = ℓ − 1\). For this case one has traces

\[
\text{Tr}_g G^{jv/m} \cdot e^{y'} = G^{jv/m} \cdot e^{y'} + G^{jv/m} \cdot e^{py'} + \ldots + G^{jv/m} \cdot e^{(p−1)y'}
\]

or

\[
G^{jv/m}[e^{y'} + \frac{p−1}{m} \cdot e^{py'} + \ldots + \frac{p^{(ℓ−1)}−1}{m} \cdot e^{(p^{(ℓ−1)}−1)y'}]
\]

for \(1 ≤ y' ≤ ℓ\) since \(p ≡ 1\) (mod \(m\)). Taking \(g^e\) as \(ζ^p\) and \(G^{(p−1)/m} = g^{(q−1)/m}\) as \(ζ^R\) modulo \(P\) in the residue field of \(L = \mathbb{Q}(ζ_f,ζ_m)\) for some \(L\)-prime \(P\) lying above \(p\) as in the proof of Proposition 2, one identifies the bracketed expression in (22) as the Gauss sum

\[
ζ^p y' + ζ^{Ry'} \cdot e^{py'} + \ldots + ζ^{Ry^{(ℓ−1)}} \cdot e^{(p^{(ℓ−1)}−1)y'}.
\]

If \(f = ℓ\), the sum (23) is just \(τ_{μν}(χ^j)\) in (20), with \(χ\) determined by the condition \(χ(p) = ζ^R\). A routine calculation now shows that the trace values in (22) consist of one zero and \((ℓ − 1)/m\) repetitions of each of the non-zero values \(G^{jv/m} τ_μ(χ^j), G^{jv^{(p−1)/m}} τ_μ(χ^j), \ldots, G^{jv^{(m−1)(p−1)/m}} τ_μ(χ^j)\) in this case, so

\[
η_{jδ/m} = 1 + \frac{ℓ−1}{m}(ζ^p + ζ^p G^{−(p−1)/m} + \ldots + ζ^p G^{−(m−1)(p−1)/m})
\]

in (21) where \(λ = G^{jv/m} τ_μ(χ^j)\) in \(F_p\). The conclusion of the theorem now follows when \(f = ℓ\) (and more generally when \(f = ℓ^ν\)).

For \(f = 2ℓ\), the sum (23) equals \(τ_{μν}/2(χ^j)\) in (20) if \(y'\) is even, and \(-τ_{μν}/2(χ^j)\) if \(y'\) is odd. A routine calculation shows that the trace values in (22) consist of one zero and \((ℓ − 1)/m\) repetitions of each of the cosets \(±G^{jv/m} τ_μ(χ^j), ±G^{jv^{(p−1)/m}} τ_μ(χ^j), \ldots, ±G^{jv^{(m−1)(p−1)/m}} τ_μ(χ^j)\) of \(F_p^*/\{1\}\). (Note that when \(m\) is even, each coset listed actually appears twice since \(G^{(p−1)/2} = −1\.) Since \(e/δ = (p−1)/2\), \(ψ_t = ζ^G + ζ^G^-1\) in (21) in this case, so

\[
η_{jδ/m} = 2 + \frac{ℓ−1}{m}(ζ^λ + ζ^-λ + ζ^G^{−(p−1)/m} + ζ^-G^{−(p−1)/m} + \ldots + ζ^G^{−(m−1)(p−1)/m} + ζ^-G^{−(m−1)(p−1)/m})
\]

from (21) where \(λ = G^{jv/m} τ_μ(χ^j)\) in \(F_p\). The conclusion of the theorem now holds when \(f = 2ℓ\) (and more generally when \(f = 2ℓ^ν\)), regardless of the parity of \(m\).
The above result generalizes Corollary 1 of [7] where the case $m = 2$ is considered. There the middle factor $\Phi^{(0)/2}(x)$ is determined explicitly since $f_2(x)$ is given by (10).

References


Department of Mathematics and Computer Science
University of San Diego
San Diego, CA 92110-2492, U.S.A.
E-mail: gurak@pwa.acusd.edu

Received on 4.8.1998
and in revised form on 31.5.1999