ACTA ARITHMETICA
XCII.2 (2000)

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 $\mathbb{F}_q$ denote the field of q elements, $\mathbb{F}_q^*$ its multiplicative group and g a fixed generator of $\mathbb{F}_q^*$. Let $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ 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 eth powers in $\mathbb{F}_q^*$. The Gauss periods are

$$\eta_j = \sum_{x \in C_e} \zeta_p^{\mathrm{Tr}\, g^j x} \qquad (1 \le j \le e) \tag{1}$$

and satisfy the period polynomial

$$\Phi(x) = \prod_{j=1}^{e} (x - \eta_j). \tag{2}$$

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

$$\Phi(x) = \prod_{w=1}^{\delta} \Phi^{(w)}(x), \tag{3}$$

where

$$\Phi^{(w)}(x) = \prod_{k=0}^{e/\delta - 1} (x - \eta_{w+k\delta}) \qquad (1 \le w \le \delta). \tag{4}$$

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

$$\Phi^{(w)}(x) = x^{e/\delta} + a_1 x^{e/\delta - 1} + \ldots + a_{e/\delta}, \tag{5}$$

2000 *Mathematics Subject Classification*: Primary 11T22, 11T24.

or equivalently of

$$(6)\qquad F^{(w)}(X) = X^{e/\delta}\Phi^{(w)}(X^{-1}) = 1 + a_1X + \ldots + a_{e/\delta}X^{e/\delta},$$

are expressed in terms of the symmetric power sums

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

through Newton's identities

$$(8)\qquad S_r + a_1S_{r-1} + \ldots + a_{r-1}S_1 + ra_r = 0 \quad (1 \leq r \leq e/\delta).$$

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 $\mathrm{Tr}(g^w(x_1 + \ldots + x_n)) = 0$, then $S_n(w)$ can be computed using

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

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 $\Phi(x) = \Phi^{(\delta)}(x)$ in (5) are given by

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

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 $\Phi^{(\delta)}(x)$ when f is fixed, and showed that the beginning coefficients of the factor $\Phi^{(\delta)}(x)$ 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 $\Phi^{(\delta/2)}(x)$ when δ 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 $m \mid \delta$, $1 \leq j \leq m$ 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 $\mathrm{ord}_f\, r = b$. 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 $\mathrm{ord}_m\, s = c$. In addition to considering primes $p \equiv r \pmod f$ and finite fields $\mathbb{F}_q$ with $q = p^a$, 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 $\zeta_f \to \zeta_f^r$; 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 $\Phi^{(w)}(x)$ 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 $\Phi^{(\overline{w})}(x)$ where $w \equiv \overline{w} \pmod{\delta}$ for $1 \le \overline{w} \le \delta$.)

Now write $R = R_1 m_1$ where $\gcd(R_1, m) = 1$ and $m_1 \mid m^n$ 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 $\mathrm{ord}_M s_1 = c_1$, and let k' be the subfield of $\mathbb{Q}(\zeta_M)$ fixed by the action $\zeta_M \to \zeta_M^{s_1}$. Fixing j, with $1 \le j \le m$ 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 $q = p^a$, $p \equiv r \pmod{f}$, $p \equiv s_1 \pmod{M}$ and $m \mid \delta$. First note that $\delta R = 1 + p + \ldots + p^{a-1} \equiv 0 \pmod{M}$, so $l = \mathrm{lcm}(b, c)$ must divide a. (In fact, $\mathrm{lcm}(b, c_1) \mid a$.) Since $1 + p + \ldots + p^{b-1} \equiv 0 \pmod{R}$, one may write

$$1 + s_1 + \ldots + s_1^{l-1} = \mu m m_1/d, \tag{11}$$

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

$$x_i = \frac{s_1^{li} - 1}{s_1 - 1} = \frac{s_1^l - 1}{s_1 - 1}(1 + s_1^l + \ldots + s_1^{l(i-1)}) \qquad (i > 0). \tag{12}$$

The expression (11) uniquely determines d. Since $s_1^l \equiv 1 \pmod{m}$, from (11) one sees that $x_i \equiv ix_1 \equiv i\mu m_1 m/d \equiv 0 \pmod{M}$ if and only if $d \mid i$. In particular, as $M \mid \delta R$ one finds that $ld \mid a$.

Next note that since R_1 is relatively prime to both e/δ and M, one can express $R_1 v + (e/\delta)Mu = 1$ for integers v and u. Thus $g^{j\delta/m} = g^{j\delta Rv/M + ejum_1}$, so the values $\mathrm{Tr}\, g^{j\delta/m}x$ ($x \in C_e$) have the form

$$\begin{aligned} y_\alpha &= \mathrm{Tr}\, g^{j\delta Rv/M + e\alpha} \\ &= g^{j\delta Rv/M + e\alpha} + g^{j\delta Rvp/M + pe\alpha} + \ldots + g^{j\delta Rvp^{a-1}/M + p^{a-1}e\alpha} \\ &= h^{\delta R/M}(g^{e\alpha} + h^{\delta R(p-1)/M} g^{pe\alpha} + \ldots + h^{\delta R(p^{a-1}-1)/M} g^{p^{a-1}e\alpha}) \\ &= h^{\delta R/M}(g^{e\alpha} + h^{(q-1)/M} g^{pe\alpha} + h^{(q-1)(1+p)/M} g^{p^2 e\alpha} \\ &\quad + \ldots + h^{(q-1)(1+p+\ldots+p^{a-2})/M} g^{p^{a-1}e\alpha}) \end{aligned}$$

for $0 \le \alpha < f$, where $h = g^{jv}$. Since $h^{\delta R/M} \ne 0$, the function $t_{j\delta/m}(n)$ in (9) also counts the number of times a sum $z_{\alpha_1} + \ldots + z_{\alpha_n}$ equals zero for $0 \le \alpha_i < f$, where

$$z_\alpha = g^{e\alpha} + g^{jv(q-1)/M} g^{pe\alpha} + \ldots + g^{jv(q-1)(1+p+\ldots+p^{a-2})/M} g^{p^{a-1}e\alpha}. \tag{13}$$

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_α is 0 in (13) so that $t_{j\delta/m}(n) = f^n$ for any $n > 0$, and hence $\Phi^{(j\delta/m)}(x) = (x-f)^{e/\delta}$ from relations (8) and (9). Since $g^{j\delta Rv/M}$ has order $M(p-1) \mid p^{dl}-1$ and g^e has order $f \mid p^l - 1$, each trace

$$y_\alpha = \operatorname{Tr} g^{j\delta Rv/M+e\alpha} = \frac{a}{dl} \operatorname{Tr}_{\mathbb{F}_{p^{dl}}/\mathbb{F}_p} g^{j\delta Rv/M+e\alpha} \qquad (0 \le \alpha < f).$$

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

$$\begin{aligned} z_\alpha = {} & g^{e\alpha} + tg^{re\alpha} + \ldots + t^{1+s_1+\ldots+s_1^{l-2}} g^{r^{l-1}e\alpha} + t^{x_1} g^{r^l e\alpha} + t^{s_1x_1+1} g^{r^{l+1}e\alpha} \\ & + \ldots + t^{s_1^{l-1}x_1+1+s_1+\ldots+s_1^{l-2}} g^{r^{2l-1}e\alpha} + \ldots + t^{x_{d-1}} g^{r^{l(d-1)}e\alpha} \\ & + t^{s_1x_{d-1}+1} g^{r^{l(d-1)+1}e\alpha} + \ldots + t^{s_1^{l-1}x_{d-1}+1+s_1+\ldots+s_1^{l-2}} g^{r^{l(d-1)+l-1}e\alpha} \\ = {} & g^{e\alpha}[1 + t^{x_1} + \ldots + t^{x_{d-1}}] \\ & + g^{re\alpha} t[1+t^{s_1x_1} + \ldots + t^{s_1x_{d-1}}] + g^{r^2e\alpha} t^{1+s_1}[1 + t^{s_1^2x_1} + \ldots + t^{s_1^2x_{d-1}}] \\ & + \ldots + g^{r^{l-1}e\alpha} t^{1+s_1+\ldots+s_1^{l-2}}[1 + t^{s_1^{l-1}x_1} + \ldots + t^{s_1^{l-1}x_{d-1}}] \end{aligned}$$

in (13), where $t = g^{jv(q-1)/M}$. Now each of the bracketed sums in the last expression has the form $1 + \overline{g}^{s_1^\lambda} + \overline{g}^{2s_1^\lambda} + \ldots + \overline{g}^{(d-1)s_1^\lambda}$ with $\overline{g} = t^{x_1}$ of order d. Since $d > 1$ and $\gcd(s_1, M) = 1$ 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 $l = \operatorname{lcm}(b,c) = \operatorname{lcm}(b,c_1)$ as $c \mid c_1 \mid l$). To generalize the results known for the middle and last factor [5, 7] here, it is necessary to find a suitable counting function $b_{j,m}(n)$ 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 $m \mid \delta$. To this end, define algebraic integers $\omega_{j,\alpha}$ in $\mathbb{Q}(\zeta_M, \zeta_f)$ by

$$\omega_{j,\alpha} = \zeta_f^\alpha + \zeta_M^j \zeta_f^{r\alpha} + \zeta_M^{j(1+s_1)} \zeta_f^{r^2\alpha} + \ldots + \zeta_M^{j(1+s_1+\ldots+s_1^{l-2})} \zeta_f^{r^{l-1}\alpha} \tag{14}$$

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

$$\omega_{j,\alpha_1} + \ldots + \omega_{j,\alpha_n} = 0 \tag{15}$$

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

PROPOSITION 2. *For all primes $p \equiv r \pmod f$ and $p \equiv s_1 \pmod M$ with $m \mid \delta$*

$$b_{m,j}(n) \le t_{j\delta/m}(n) \qquad \text{for } n > 0.$$

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

Proof. Since $l = \operatorname{lcm}(b, c_1)$, one finds that $\operatorname{lcm}(f, M)$ divides $p^l - 1$, so the elements g^e and $g^{(q-1)/M}$ lie in $\mathbb{F}_{p^l} \subseteq \mathbb{F}_q$. In particular, one may identify

$\mathbb{F}_{p^l}/\mathbb{F}_p$ 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 $\zeta_M^{R_1}$ 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 ζ_f^μ, for some integer μ prime to f. So z_α in (13) corresponds to $(a/l)\omega_{j,\alpha\mu}$ modulo P, since $R_1 v \equiv 1 \pmod{M}$. It follows that $t_{j\delta/m}(n)$ counts precisely the number of times one has

$$\frac{a}{l}(\omega_{j,\alpha_1} + \ldots + \omega_{j,\alpha_n}) \equiv 0 \pmod{P} \tag{16}$$

for a choice of $\omega_{j,\alpha}$ in (14) where $0 \le \alpha_1, \ldots, \alpha_n < f$. In particular, $b_{m,j}(n) \le t_{j\delta/m}(n)$ 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 $\widehat{p}$ 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 $\widehat{p}$ 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 $b_{m,j}(h) \ne 0$. 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 $p \notin \xi_{j,n}$ $(n \le v)$, and $d = 1$ in* (11), *the coefficient a_v for $\Phi^{(j\delta/m)}(x)$ in* (5) (*or $F^{(j\delta/m)}(X)$ in* (6)) *satisfies $a_v = \vartheta_v(p)$, where ϑ_v is a polynomial of degree $[v/h]$.*

Now consider the rational power series

$$C_{m,j}(X) = \exp\left(-\frac{R}{f}\sum_{n=1}^{\infty} b_{m,j}(n)X^n/n\right) \tag{17}$$

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 $p \notin \xi_{j,n}$ $(n \le v)$, and $d = 1$ in* (11), *we have*

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

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, $\Phi^{(\delta/4)}(x) = \Phi^{(3\delta/4)}(x) = (x-4)^{(p-1)/2}$ for the case $p \equiv 3 \pmod{8}$. For the other case $p \equiv 7 \pmod{8}$, I illustrate Theorems 1 and 2 with $q = p^2$. One finds $\omega_{j,1} = -\omega_{j,3} = i(1-\zeta_8^j)$ and $\omega_{j,0} = -\omega_{j,2} = 1 + \zeta_8^j$ 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 $b_{4,j}(n)$ satisfy

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

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 $\Phi^{(\delta/4)}(x) = \Phi^{(3\delta/4)}(x)$ from Theorem 1 are found to be

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

The prime $p = 7$ first appears in thei exceptional sets $\xi_{1,n} = \xi_{3,n}$ $(n > 0)$, 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 $g = 2 + i$ to generate $\mathbb{F}_{49}^*$ with $g^{(q-1)/M} = g^6 \equiv 2i + 2 \equiv \zeta_8 \pmod{(3+\sqrt{2})}$ and $g^e = g^{12} \equiv i \pmod{(3+\sqrt{2})}$, so $z_\alpha \equiv \omega_{j,\alpha} \pmod{(3+\sqrt{2})}$ in (13). One computes $t_1(1) = t_3(1) = 0$, $t_1(2) = t_3(2) = 4$ and $t_1(3) = t_3(3) = 6$ so $\Phi^{(1)}(x) = \Phi^{(3)}(x) = x^3 + 2x^2 - x - \underline{1}$ from (8) and (9). As expected, the underscored coefficient $a_3 \neq \vartheta_3(7) = 6$.

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, $L = \mathbb{Q}(\zeta_{15})$, $K = \mathbb{Q}$ and $k = k' = \mathbb{Q}(\sqrt{5})$, with $d = 1$ in (11) and $\omega_{j,\alpha} = \zeta_3^\alpha + \zeta_5^j \zeta_3^{2\alpha}$ $(1 \le j \le 4,\ 0 \le \alpha \le 2)$ in (14). One finds $\Phi^{(\delta/5)}(x) = \Phi^{(4\delta/5)}(x)$ 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 $1 \le j \le 4$, 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 $\Phi^{(j\delta/m)}(x)$ from Theorem 1 are found to be

$$\vartheta_1(p) = 3, \quad \vartheta_2(p) = 9, \quad \vartheta_3(p) = -2p + 27, \quad \vartheta_4(p) = -6p + 81,$$
$$\vartheta_5(p) = -18p + 243, \ \vartheta_6(p) = 2p^2 + 69p + 729, \ \vartheta_7(p) = 6p^2 - 207p + 2187, \ldots$$

For $p = 59$ one may choose $g = 2+\zeta_5$ to generate $\mathbb{F}_{59^2}^*$, so $g^{(q-1)/m} = g^{696} \equiv \zeta_5^3$ 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 $g^e = g^{1160} \equiv \zeta_3 \pmod{P}$, so $z_\alpha \equiv \omega_{j,\alpha} \pmod{P}$ 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:

$j\backslash n$	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

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

$$x^{58} + 3x^{57} + 9x^{56} - 91x^{55} - \underline{332}x^{54} - \underline{1114}x^{53} + \underline{2735}x^{52} + \underline{14282}x^{51} + \ldots$$

and $\Phi^{(8)}(x) = \Phi^{(12)}(x)$ equals

$$x^{58} + 3x^{57} + 9x^{56} - 91x^{55} - 273x^{54} - 819x^{53} + 3620x^{52} + \underline{10683}x^{51} + \ldots$$

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 η_4 and η_{16} are both conjugates of $\zeta_{59}^1 + \zeta_{59}^2 + \zeta_{59}^{-3}$, while η_8 and η_{12} are conjugates of $\zeta_{59}^2 + \zeta_{59}^3 + \zeta_{59}^{-5}$.

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

$$1 + s_1 + \ldots + s_1^{c_1-1} = \frac{uM}{t} \tag{18}$$

where $\gcd(u,t) = 1$ and $t \,|\, M$ 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 $\operatorname{ord}_M s_1 = c_1 > 1$ since $t = M$ in (18) if $c_1 = 1$. The results I describe primarily rely on some knowledge about the set $\{1, \zeta_M, \zeta_M^{1+s_1}, \ldots, \zeta_M^{1+s_1+\ldots+s_1^{c_1-2}}\}$ in $\mathbb{Q}(\zeta_M)$. The first is

THEOREM 3. *Let W be the subfield of $\mathbb{Q}(\zeta_f)$ fixed by the action $\zeta_f \to \zeta_f^{r^{\gcd(b,c_1)}}$. Suppose $\{1, \zeta_M, \zeta_M^{1+s_1}, \ldots, \zeta_M^{1+s_1+\ldots+s_1^{c_1-2}}\}$ is linearly independent over W with $t = 1$ in* (18). *Then $b_{m,j}(n)$ counts the number of times $\operatorname{Tr}_{\mathbb{Q}(\zeta_f)/W}(x_1 + \ldots + x_n)$ 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 $\Phi^{(\delta)}(x)$ in* [5].)

P r o o f. Put $d_1 = \gcd(b, c_1)$. Without loss of generality, one may assume $a = l$. Then, in (14),

$$\begin{aligned}\omega_{j,\alpha} = (\zeta_f^{\alpha} + \zeta_f^{r^{c_1}\alpha} + \ldots + \zeta_f^{r^{l-c_1}\alpha}) + \zeta_M^{j}(\zeta_f^{r\alpha} + \zeta_f^{r^{c_1+1}\alpha} + \ldots + \zeta_f^{r^{l-c_1+1}\alpha}) \\ + \ldots + \zeta_M^{j(1+s_1+\ldots+s_1^{i-1})}(\zeta_f^{r^{i}\alpha} + \zeta_f^{r^{c_1+i}\alpha} + \ldots + \zeta_f^{r^{l-c_1+i}\alpha}) \\ + \ldots + \zeta_M^{j(1+s_1+\ldots+s_1^{c_1-1})}(\zeta_f^{r^{c_1-1}\alpha} + \zeta_f^{r^{2c_1-1}\alpha} + \ldots + \zeta_f^{r^{l-1}\alpha})\end{aligned}$$

since $t = 1$. Further, any sum $\zeta_f^{r^{i}\alpha} + \zeta_f^{r^{c_1+i}\alpha} + \ldots + \zeta_f^{r^{l-c_1+i}\alpha}$ which appears is the trace $\operatorname{Tr}_{\mathbb{Q}(\zeta_f)/W}(\zeta_f^{r^{i}\alpha})$ since $\operatorname{ord}_f r^{c_1} = b/d_1 = l/c_1$. By hypothesis $\{1, \zeta_M^{j}, \ldots, \zeta_M^{j(1+s_1+\ldots+s_1^{c_1-2})}\}$ 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 $\operatorname{Tr}_{\mathbb{Q}(\zeta_f)/W}(\zeta_f^{\alpha_1} + \ldots + \zeta_f^{\alpha_n})$ 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 $\{1, \zeta_M, \zeta_M^{1+s_1}, \ldots, \zeta_M^{1+s_1+\ldots+s_1^{c_1-2}}\}$ 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,*

$$b_{m,j}(n) = \begin{cases} \lambda^{n(\ell-1)/\ell} \dfrac{n!}{(n/\ell)!((\lambda n/\ell)!)^{(\ell-1)/\lambda}} & \text{if } \ell \mid n, \\ 0 & \text{otherwise.} \end{cases}$$

For $f = 4$, $b_{m,j}(n) = \binom{2n}{n}$ if $\lambda = 2$; otherwise if $\lambda = 1$,

$$b_{m,j}(n) = \begin{cases} \dbinom{n}{n/2}^2 & \text{if } 2 \mid n, \\ 0 & \text{otherwise.} \end{cases}$$

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 $\mathbb{F}_{p^l}/\mathbb{F}_p$ 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 $\widehat{p}$ 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* $\operatorname{ord}_f r = 1$ *or* $\phi(f)$ *with* $\gcd(b, c_1) = 1$, $p \nmid a$ *and* $t = 1$ *in* (18). *Then*

(19)
$$\Phi^{(j\delta/m)}(x) = \begin{cases} \Phi^{(\delta)}(x) & \text{if } \widehat{p} \text{ is prime to } 1 + \zeta_M^j + \ldots + \zeta_M^{j(1+s_1+\ldots+s_1^{c_1-2})}, \\ (x-f)^{e/\delta} & \text{otherwise.} \end{cases}$$

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 $\widehat{p}$ is prime to $1 + \zeta_M^j + \ldots + \zeta_M^{j(1+s_1+\ldots+s_1^{c_1-2})}$. 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 $\widehat{p}$ divides the trace $\operatorname{Tr}_{\mathbb{Q}(\zeta_M)/k}(\zeta_M^{ju})$, where u satisfies $u(s_1 - 1) \equiv 1 \pmod{M}$. This is a consequence of the following observation.

LEMMA 1. *Suppose u is an integer satisfying* $u(s_1 - 1) \equiv 1 \pmod{M}$. *Then*

$$\zeta_M^{1+s_1+\ldots+s_1^i+u} = \zeta_M^{us_1^{i+1}} \quad \text{for } i \geq 0.$$

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 $k' = k = \mathbb{Q}(\sqrt{-11})$, and $t = 1$ in (18). Then

$$\begin{aligned} \omega_{j,\alpha} &= (\zeta_4^\alpha + \zeta_4^{-\alpha})(1 + \zeta_{11}^j + \zeta_{11}^{4j} + \zeta_{11}^{2j} + \zeta_{11}^{7j}) \\ &= (\zeta_4^\alpha + \zeta_4^{-\alpha})\zeta_{11}^{-5j} \operatorname{Tr}_{\mathbb{Q}(\zeta_{11})/\mathbb{Q}(\sqrt{-11})} \zeta_{11}^{6j} \\ &= (\zeta_4^\alpha + \zeta_4^{-\alpha})\zeta_{11}^{-5j} \left(\frac{-1 \pm \sqrt{-11}}{2} \right) \end{aligned}$$

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

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

For the exceptional prime $p = 3$, the corresponding period polynomial has half of its factors $\Phi^{(j\delta/11)}(x)$ $(1 \le j \le 10)$ 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

$$\frac{e}{\gcd(e, (p-1)j\delta/m)} = \frac{(p-1)\delta/\gcd(p-1, f)}{(p-1)\delta/m} = \frac{m}{\gcd(p-1, f)} \quad \text{or} \quad \frac{m}{\gcd(r-1, f)}$$

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

$$\tau_\alpha(\chi) = \sum_{x=1}^{\ell-1} \chi(x)\zeta_\ell^{\alpha x} \tag{20}$$

for some integer α, where χ is a numerical character of order m modulo ℓ. 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 χ. Here and throughout the remainder of this section I assume $m > 1$. The following lemma explicitly gives $\omega_{j,\alpha}$ for the cases $f = \ell^\nu$ and $2\ell^\nu$, where ℓ is an odd prime. I note that since $p \equiv 1 \pmod{M}$ and $l = \ell^{\nu-1}(\ell - 1)$, 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 $f = \ell^\nu$,*

$$\omega_{j,\alpha} = \begin{cases} \ell^{\nu-1}\tau_\alpha(\chi) & \text{if } \ell^{\nu-1} \parallel \alpha, \\ 0 & \text{otherwise.} \end{cases}$$

For $f = 2\ell^\nu$,

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

Here χ 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 $\tau_{r^i}(\chi) = \zeta_m^{-ij}\tau_1(\chi)$, 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 $\ell^{\nu-1}\zeta_m^w\tau_1(\chi)$ $(0 \le w < m)$, and also of $-\ell^{\nu-1}\zeta_m^w\tau_1(\chi)$ $(0 \le w < m)$ if $f = 2\ell^\nu$.

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 mth 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 $f = \ell^\nu$,*

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

For $f = 2\ell^\nu$,

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

Proof. In view of the remark prior to stating this proposition and the fact that $\tau_1(\chi) \ne 0$ 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

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

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

$$\binom{n}{i}\left(\frac{\ell-1}{m}\right)^i b_{2m}(i)(2(\ell^\nu - \ell + 1))^{n-i} \quad \text{when } m \text{ is odd},$$

and

$$\binom{n}{i}\left(\frac{2(\ell-1)}{m}\right)^{i} b_m(i)(2(\ell^\nu-\ell+1))^{n-i} \quad \text{when } m \text{ is even.}$$

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 $m \mid \ell-1$. For $f=\ell^\nu$,*

$$C_{m,j}(X) = (1-(\ell^\nu-\ell+1)X)B_m\left(\frac{(\ell-1)X/m}{1-(\ell^\nu-\ell+1)X}\right).$$

For $f=2\ell^\nu$,

$$C_{m,j}(X) = \begin{cases} \left((1-2(\ell^\nu-\ell+1)X)B_{2m}\left(\dfrac{(\ell-1)X/m}{1-2(\ell^\nu-\ell+1)X}\right)\right)^{1/2} & \text{if } m \text{ odd,} \\ \left((1-2(\ell^\nu-\ell+1)X)B_{m}\left(\dfrac{2(\ell-1)X/m}{1-2(\ell^\nu-\ell+1)X}\right)\right)^{1/2} & \text{if } m \text{ even.} \end{cases}$$

Proof. I consider only the case $f=\ell^\nu$ here, since the argument when $f=2\ell^\nu$ is similar. For $f=\ell^\nu$, one obtains

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

from Proposition 4. Thus, from (17), $-\ln C_{m,j}\left(\frac{mX}{\ell-1}\right)$ equals

$$\begin{aligned}
&\sum_{n=1}^{\infty}\frac{b_{m,j}(n)}{((\ell-1)/m)^n}X^n/n \\
&= -\sum_{n=1}^{\infty}\sum_{i=0}^{n}\left(\frac{\ell^\nu-\ell+1}{(\ell-1)/m}\right)^{n-i}\binom{n}{i} b_m(i)X^n/n \\
&= -\sum_{n=1}^{\infty}\left(\frac{\ell^\nu-\ell+1}{(\ell-1)/m}X\right)^{n}/n - \sum_{i=1}^{\infty} b_m(i)X^i\sum_{n=1}^{\infty}\left(\frac{\ell^\nu-\ell+1}{(\ell-1)/m}X\right)^{n-i}\binom{n}{i}/n \\
&= \ln\left(1-\frac{\ell^\nu-\ell+1}{(\ell-1)/m}X\right) - \sum_{i=1}^{\infty} b_m(i)X^i\left(1-\frac{\ell^\nu-\ell+1}{(\ell-1)/m}X\right)^{-i}/i \\
&= \ln\left(1-\frac{\ell^\nu-\ell+1}{(\ell-1)/m}X\right) + B_m(X/(1-mX(\ell^\nu-\ell+1)/(\ell-1))),
\end{aligned}$$

since $R/f=1$ here. Replacing X by $\frac{\ell-1}{m}X$ yields the desired formula.

For $d\,|\,p-1$, let $f_d(x)$ denote the minimal polynomial for the ordinary cyclotomic period $\zeta_p^z+\ldots+\zeta_p^{z^d}$, 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 $m\,|\,\ell-1$ and $f=\ell^\nu$ or $2\ell^\nu$. If $p\,|\,\frac{a}{b}$ then $\Phi^{(j\delta/m)}(x)=(x-f)^{e/\delta}$ else*

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

P r o o f. First note that the element $g^{\delta/m}$ has order $mR(p-1)$ dividing p^b-1 since $p\equiv 1 \pmod m$, $m\,|\,\ell-1\,|\,b$ and $R=\ell^\nu$ here. Thus each of the traces $\operatorname{Tr} g^{j\delta/m}x=0$ for $x\in C_e$ if $p\,|\,\frac{a}{b}$, 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 $p\nmid\frac{a}{b}$. In view of Proposition 3, it is enough to show in this case that $\eta_{j\delta/m}$ is a conjugate of $(\ell^\nu-\ell+1)+\frac{\ell-1}{m}(\zeta_p^z+\ldots+\zeta_p^{z^m})$ if $f=\ell^\nu$ or a conjugate of $2(\ell^\nu-\ell+1)+\frac{\ell-1}{m}(\zeta_p^z+\ldots+\zeta_p^{z^m}+\zeta_p^{-z}+\ldots+\zeta_p^{-z^m})$ 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 $\operatorname{Tr} g^{ey+j\delta/m}$ ($1\le y\le R$). In particular, let N count the number of non-zero values among $\operatorname{Tr} g^{ey+j\delta/m}$ ($1\le y\le R$) and n_t count the number of times $\operatorname{Tr} g^{ey+j\delta/m}$ for $1\le y\le R$ lies in the coset $G^t(\mathbb{F}_p^*)^{e/\delta}$ ($1\le t\le e/\delta$), where $G=g^{(q-1)/(p-1)}$. Then

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

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/δ. 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 $g^{ey+j\delta/m} = g^{ey'+j\delta Rv/m}$ where $y' = y + ju$. Without loss of generality one may use the traces $\mathrm{Tr}\, g^{j\delta Rv/m+ey'}$ $(1 \le y' \le R)$ instead to find N and n_t. Now $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^{\ell-1}}} g^{j\delta Rv/m+ey'} = \frac{a}{b} G^{jv/m}\, \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{p^{\ell-1}}} g^{ey'} = 0$ if $\ell^{\nu-1} \nmid y'$, since $g^{j\delta Rv/m} = G^{jv/m}$ lies in $\mathbb{F}_{p^{\ell-1}}$ and g^e is a primitive f-root of unity. In particular, the proof of the theorem when $p \nmid \frac{a}{b}$ is reduced to the case $\nu = 1$ where $a = b = \ell - 1$. For this case one has traces

$$\mathrm{Tr}_{\mathbb{F}_{p^{\ell-1}}/\mathbb{F}_p} G^{jv/m} g^{ey'} = G^{jv/m} g^{ey'} + G^{jvp/m} g^{epy'} + \ldots + G^{jvp^{\ell-1}/m} g^{ep^{\ell-1}y'}$$

or

$$G^{jv/m}[g^{ey'} + G^{\frac{p-1}{m}jv} g^{epy'} + \ldots + G^{\frac{p-1}{m}jv(\ell-1)} g^{ep^{\ell-1}y'}] \tag{22}$$

for $1 \le y' \le \ell$ since $p \equiv 1 \pmod{m}$. Taking g^e as ζ_f^μ and $G^{(p-1)/m} = g^{(q-1)/m}$ as ζ_m^R modulo P in the residue field of $L = \mathbb{Q}(\zeta_f, \zeta_m)$ 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

$$\zeta_f^{\mu y'} + \zeta_m^{Rjv} \zeta_f^{\mu p y'} + \ldots + \zeta_m^{Rjv(\ell-1)} \zeta_f^{\mu p^{\ell-1} y'}. \tag{23}$$

If $f = \ell$, the sum (23) is just $\tau_{\mu y'}(\chi^j)$ in (20), with χ determined by the condition $\chi(p) = \zeta_m^{Rv}$. A routine calculation now shows that the trace values in (22) consist of one zero and $(\ell-1)/m$ repetitions of each of the non-zero values $G^{jv/m}\tau_\mu(\chi^j), G^{(jv-(p-1))/m}\tau_\mu(\chi^j), \ldots, G^{(jv-(m-1)(p-1))/m}\tau_\mu(\chi^j)$ in this case, so

$$\eta_{j\delta/m} = 1 + \frac{\ell-1}{m}(\zeta_p^\lambda + \zeta_p^{\lambda G^{-(p-1)/m}} + \ldots + \zeta_p^{\lambda G^{-(m-1)(p-1)/m}})$$

in (21) where $\lambda = G^{jv/m}\tau_\mu(\chi^j)$ in $\mathbb{F}_p$. The conclusion of the theorem now follows when $f = \ell$ (and more generally when $f = \ell^\nu$).

For $f = 2\ell$, the sum (23) equals $\tau_{\mu y'/2}(\chi^j)$ in (20) if y' is even, and $-\tau_{\mu(y'+\ell)/2}(\chi^j)$ if y' is odd. A routine calculation shows that the trace values in (22) consist of one zero and $(\ell-1)/m$ repetitions from each of the cosets $\pm G^{jv/m}\tau_\mu(\chi^j)$, $\pm G^{(jv-(p-1))/m}\tau_\mu(\chi^j)$, $\ldots$, $\pm G^{(jv-(m-1)(p-1))/m}\tau_\mu(\chi^j)$ of $\mathbb{F}_p^*/(\pm 1)$. (Note that when m is even, each coset listed actually appears twice since $G^{(p-1)/2} = -1$.) Since $e/\delta = (p-1)/2$, $\psi_t = \zeta_p^{G^t} + \zeta_p^{-G^t}$ in (21) in this case, so

$$\eta_{j\delta/m} = 2 + \frac{\ell-1}{m}(\zeta_p^\lambda + \zeta_p^{-\lambda} + \zeta_p^{\lambda G^{-(p-1)/m}} + \zeta_p^{-\lambda G^{-(p-1)/m}} + \ldots + \zeta_p^{\lambda G^{-(m-1)(p-1)/m}} + \zeta_p^{-\lambda G^{-(m-1)(p-1)/m}})$$

from (21) where $\lambda = G^{jv/m}\tau_\mu(\chi^j)$ in $\mathbb{F}_p$. The conclusion of the theorem now holds when $f = 2\ell$ (and more generally when $f = 2\ell^\nu$), 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 $\Phi^{(\delta/2)}(x)$ is determined explicitly since $f_2(x)$ is given by (10).

References

[1] Z. Borevich and I. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

[2] S. Gupta and D. Zagier, *On the coefficients of the minimal polynomial of Gaussian periods*, Math. Comp. 60 (1993), 385–398.

[3] S. Gurak, *Minimal polynomials for Gauss circulants and cyclotomic units*, Pacific J. Math. 102 (1982), 347–353.

[4] —, *Factors of period polynomials for finite fields*, *II*, in: Contemp. Math. 168, Amer. Math. Soc., 1994, 127–138.

[5] —, *On the last factor of the period polynomial for finite fields*, Acta Arith. 71 (1995), 391–400.

[6] —, *On the minimal polynomials for certain Gauss periods over finite fields*, in: Finite Fields and their Applications, S. Cohen and H. Niederreiter (eds.), Cambridge Univ. Press, 1996, 85–96.

[7] —, *On the middle factor of the period polynomial for finite fields*, CMR Proceedings and Lecture Notes 19 (1999), 121–131.

[8] G. Myerson, *Period polynomials and Gauss sums for finite fields*, Acta Arith. 39 (1981), 251–264.

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 (3433)