ACTA ARITHMETICA
LXXI.4 (1995)

On the last factor of the period polynomial for finite fields

by

S. Gurak (San Diego, Cal.)

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 fix $\theta = \exp(2\pi i/p)$, a primitive pth root of unity. Put

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

and let C_e denote the group of eth powers in $\mathbb{F}_q^*$. The Gauss periods are

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

and satisfy the period polynomial

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

In the classical case $q = p$, Gauss showed that $\Phi(x)$ is irreducible over $\mathbb{Q}$ and determined its coefficients for small values of e and f. In 1982 I determined how to compute the beginning coefficients of $\Phi(x)$ for the classical case when f is fixed [4]. (See also [3].)

G. Myerson [7] has shown that for the general case $q \ne p$, $\Phi(x)$ splits over $\mathbb{Q}$ into δ factors, each of degree e/δ. To be precise,

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

where

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

Each of the factors $\Phi^{(w)}(x)$ is irreducible or a power of an irreducible polynomial over $\mathbb{Q}$. Explaining patterns of additional reducibility that occur for $\Phi^{(w)}(x)$ was the primary focus of recent work of mine [5]. Here I consider instead the problem of computing the coefficients of a given factor $\Phi^{(w)}(x)$, particularly when $w = \delta$. I determine in Section 3 how to compute the beginning coefficients of the last factor $\Phi^{(\delta)}(x)$ in (3) in a manner analogous to that known for the case $q = p$ in [3] and [4].

2. Computations of the coefficients of $\Phi^{(w)}(x)$. Here I first express the coefficients $a_r = a_r(w)$ of a factor

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

of the period polynomial (3) for fixed w, $1 \le w \le \delta$, in terms of the symmetric power sums

$$S_n = S_n(w) = \sum_{k=0}^{e/\delta-1} (\eta_{k\delta+w})^n. \tag{6}$$

Specifically, this is given by Newton's identities

$$S_r + a_1 S_{r-1} + a_2 S_{r-2} + \ldots + a_{r-1} S_1 + r a_r = 0 \quad (1 \le r \le e/\delta). \tag{7}$$

To obtain a computationally practical formula for S_n, I introduce a certain counting function $t_w(n)$ as follows. For a fixed integer w and any $n > 0$, let $t_w(n)$ count the number of n-tuples $(x_1, \ldots, x_n)$ in $(C_e)^n$ for which $\mathrm{Tr}(g^w(x_1 + \ldots + x_n)) = 0$. I assert that

$$S_n(w) = -R\, f^{n-1} + p(e/\delta) t_w(n)/(p-1) \tag{8}$$

in (6) for $n > 0$. To see this, first write $\delta = c(q-1)/(p-1) + he$ for integers h and c. Then for any fixed j, $g^{\delta j + w} = G^{cj} g^{hej+w}$, $0 \le j < e/\delta$, where $G = g^{(q-1)/(p-1)}$ generates $\mathbb{F}_p^*$. Now $t_w(n)$ also counts the number of n-tuples in $(C_e)^n$ with $\mathrm{Tr}(g^{\delta j+w}(x_1 + \ldots + x_n)) = 0$ since $\mathrm{Tr}(g^{\delta j+w}(x_1 + \ldots + x_n)) = G^{cj}\,\mathrm{Tr}(g^w g^{hej}(x_1 + \ldots + x_n))$, so

$$t_v(n) = t_w(n) \quad \text{for } v \equiv w \pmod{\delta}. \tag{9}$$

In particular, $t_w(n)$ counts the number of ones (θ^0) occurring in the multinomial expansion of any $\eta^n_{k\delta+w} = (\sum_{x \in C_e} \theta^{\mathrm{Tr}\, g^{k\delta+w} x})^n$. A simple counting argument similar to that used in [4, p. 349] now yields (8). In particular, one finds $a_1 = R - p(e/\delta) t_w(1)/(p-1)$ from (7). A much tidier expression for a_1 is given below.

PROPOSITION 1. *For $1 \le w \le \delta$, let $T(w)$ count the number of times $\mathrm{Tr}\, g^{\delta\nu+w} = 0$ for $1 \le \nu \le R$. Then $a_1 = R - pT(w)$ in (5).*

Proof. It suffices to show that $t_w(1) = \delta(p-1)T(w)/e$. I first assert that $T(w)$ also counts the number of times $\mathrm{Tr}\, g^{l\delta\nu+w} = 0$ $(1 \le \nu \le R)$

for any integer l prime to R. To see this, note that for $\nu \equiv \nu' \pmod R$, $\operatorname{Tr} g^{\delta\nu+w} = 0 \Leftrightarrow \operatorname{Tr} g^{\delta\nu'+w} = 0$, as $g^{\delta\nu'+w} = g^{\delta\nu+w} \cdot G^t$ if $\nu' = \nu + tR$. Since $l\nu$ runs through a complete set of residues modulo R for $1 \le \nu \le R$, the assertion about $T(w)$ follows. In particular, $T(w)$ counts the number of times $\operatorname{Tr} g^{e\nu+w} = 0$ $(1 \le \nu \le R)$ since $(e/\delta, R) = 1$. Hence $\delta(p-1)T(w)/e$ counts the number of times $\operatorname{Tr} g^{e\nu+w} = 0$ $(1 \le \nu \le (q-1)/e)$ which is just $t_w(1)$.

An immediate consequence of Proposition 1 is the following reducibility criterion for $\Phi^{(w)}(x)$.

Corollary 1. *If $T(w) = 0$ then $\Phi^{(w)}(x)$ is irreducible over $\mathbb{Q}$.*

P r o o f. When $T(w) = 0$, $a_1 = R$ is prime to e/δ, the degree of $\Phi^{(w)}(x)$. Hence, since $\Phi^{(w)}(x)$ is some power of an irreducible, $\Phi^{(w)}(x)$ itself must be irreducible. (This is essentially how Myerson argues the irreducibility of $\Phi(x)$ when $\delta = 1$ in [7, Theorem 6].)

A few comments are in order when $p \equiv 1 \pmod f$. Then e is a multiple of $(q-1)/(p-1)$ so $\delta = (q-1)/(p-1)$, $R = 1$ and $e/\delta = (p-1)/f$. In particular $C_e \subseteq \mathbb{F}_p^*$, so $t_w(n)$ counts the number of tuples $(x_1, \ldots, x_n)$ in C_e^n satisfying $\operatorname{Tr} g^w(x_1 + \ldots + x_n) = (\operatorname{Tr} g^w)(x_1 + \ldots + x_n) = 0$. If $\operatorname{Tr} g^w \neq 0$ then $t_w(n)$ coincides with the counting function $\beta_{p,f}(n)$ in [3, p. 392], so $S_n(w) = (-f^n + p\beta_{p,f}(n))/f$ in (8), and hence $\Phi^{(w)}(x)$ is the ordinary cyclotomic period polynomial for $\mathbb{F}_p$ of degree e/δ [4, p. 349]. On the other hand, if $\operatorname{Tr} g^w = 0$ then $t_w(n) = f^n$ so $S_n(w) = (e/\delta)f^n$ in (8), and thus $\Phi^{(w)}(x) = (x-f)^{e/\delta}$. To summarize, I have shown:

Proposition 2. *Suppose $p \equiv 1 \pmod f$ and $1 \le w \le \delta$. If $\operatorname{Tr} g^w = 0$ then $\Phi^{(w)}(x) = (x-f)^{e/\delta}$ else $\Phi^{(w)}(x)$ is the ordinary cyclotomic period polynomial of degree e/δ.*

In the general case $p \not\equiv 1 \pmod f$ there seems to be no nice interpretation of $t_w(n)$ as above, except for special values of the form $w = k\delta/m$ for fixed $m \mid \delta$ and $1 \le k \le m$. In the next section, I treat the simplest such case $w = \delta$ and describe how to compute the beginning coefficients of $\Phi^{(\delta)}(x)$ in a manner analogous to that for ordinary cyclotomic period polynomials [3, 4]. The methods used may be extended to handle other cases $w = k\delta/m$, with $m > 1$, but not without additional difficulties.

3. Beginning coefficients of the last factor $\Phi^{(\delta)}(x)$. Retaining the notation of the previous section, I determine here how to compute the beginning coefficients of the last factor $\Phi^{(\delta)}(x)$ in (5), or equivalently those of

$$\mathbf{F}(X) = X^{e/\delta}\Phi^{(\delta)}(X^{-1}) = 1 + a_1 X + \ldots + a_{e/\delta} X^{e/\delta}, \tag{10}$$

for fixed $f > 1$. My goal is to generalize the results known in the classical case $q = p$ [3, 4] by exhibiting a suitable counting function which coincides with $t_\delta(n)$ in (8) for all sufficiently large p. For this purpose fix an integer r prime to f satisfying $1 \le r \le f$, say with $\mathrm{ord}_f\, r = b$, and consider primes $p \equiv r \pmod f$. One finds then that $e/\delta = (p-1)/(p-1,f)$ and $R = f/(p-1,f)$. Further, all such primes have common decomposition field K in $\mathbb{Q}(\zeta)$, where $\zeta = \exp(2\pi i/f)$, with $[\mathbb{Q}(\zeta) : K] = b$. (The field K is that subfield of $\mathbb{Q}(\zeta)$ fixed by the action $\zeta \to \zeta^r$.) For $n > 0$, let $\beta_K(n)$ count the number of times $\mathrm{Tr}_{\mathbb{Q}(\zeta)/K}(x_1 + \ldots + x_n) = 0$ for choice of f-roots of unity $x_1, \ldots, x_n$ lying in $\mathbb{Q}(\zeta)$. That $\beta_K(n) = t_\delta(n)$ for large enough p is demonstrated next.

PROPOSITION 3. *If $p > (bn)^{\phi(f)/b}$ and $p \nmid a$, then $t_\delta(n) = \beta_K(n)$. (Here ϕ is Euler's totient function.)*

Proof. Since $p^b \equiv 1 \pmod f$ the element g^e lies in $\mathbb{F}_{p^b} \subseteq \mathbb{F}_q$. Thus, one may identify $\mathbb{F}_{p^b}/\mathbb{F}_p$ as the residue field extension at p for the extension $\mathbb{Q}(\zeta)/K$ for some prime P lying above p in $\mathbb{Q}(\zeta)$ where g^e corresponds to $\zeta \pmod P$. The condition $p > (bn)^{\phi(f)/b}$ ensures that for $0 \le \alpha_i < f$ $(1 \le i \le n)$, $\mathrm{Tr}_{\mathbb{F}_{p^b}/\mathbb{F}_p}(g^{e\alpha_1} + \ldots + g^{e\alpha_n}) \ne 0$ unless $\mathrm{Tr}_{\mathbb{Q}(\zeta)/K}(\zeta^{\alpha_1} + \ldots + \zeta^{\alpha_n}) = 0$; otherwise $P \mid \mathrm{Tr}_{\mathbb{Q}(\zeta)/K}(\zeta^{\alpha_1} + \ldots + \zeta^{\alpha_n})$, which implies

$$p \le |N_{K/\mathbb{Q}}(\mathrm{Tr}_{\mathbb{Q}(\zeta)/K}(\zeta^{\alpha_1} + \ldots + \zeta^{\alpha_n}))| \le (bn)^{\phi(f)/b}.$$

Thus $\beta_K(n)$ counts the number of times $\mathrm{Tr}_{\mathbb{F}_{p^b}/\mathbb{F}_p}(x_1 + \ldots + x_n) = 0$ for $x_i \in C_e$ $(1 \le i \le n)$. Now, in addition,

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x_1 + \ldots + x_n) = \frac{a}{b}\,\mathrm{Tr}_{\mathbb{F}_{p^b}/\mathbb{F}_p}(x_1 + \ldots + x_n) \quad \text{for } x_i \in C_e.$$

Hence, if $p \nmid a$ then $\beta_K(n) = t_0(n)$, which is the same as $t_\delta(n)$ by (9).

I should remark that the finite set ξ_n of exceptional primes for which $t_\delta(n) > \beta_K(n)$ can be determined in a manner analogous to the case $q = p$ [3] by finding the rational primes dividing any of the norms $N_{K/\mathbb{Q}}(\mathrm{Tr}_{\mathbb{Q}(\zeta)/K}(\zeta^{\alpha_1} + \ldots + \zeta^{\alpha_n}))$, where $0 \le \alpha_i < f$, $1 \le i \le n$.

In general the counting function $\beta_K(n)$ is difficult to determine. A simple closed formula for $\beta_K(n)$ in certain special cases is given by the following two propositions.

PROPOSITION 4. *If $f = l$, a prime, then*

$$\beta_K(n) = \begin{cases} b^{n(l-1)/l} \dfrac{n!}{(n/l)![(bn/l)!]^{(l-1)/b}} & \text{if } l \mid n, \\ 0 & \text{otherwise}. \end{cases}$$

Proof. When $l = 2$, one finds $b = 1$, $K = \mathbb{Q}$ and $\zeta = -1$. An easy counting argument shows $\beta_{\mathbb{Q}}(n) = 0$ or $\binom{n}{n/2}$ according as n is odd or even. Now consider the case l is an odd prime, and observe that then an integral linear combination $c_0 + c_1\zeta + \ldots + c_{l-1}\zeta^{l-1}$ equals zero if and only if

$c_0 = c_1 = \ldots = c_{l-1}$. A straightforward argument shows that $\mathrm{Tr}_{\mathbb{Q}(\zeta)/K}(\zeta^{\alpha_1} + \ldots + \zeta^{\alpha_n}) = 0$ for $0 \le \alpha_i < l$ $(1 \le i \le n)$ if and only if $l \mid n$ and n/l of the α's are zero, with the remaining $(n/l)(l-1)$ α's equally distributed among the $(l-1)/b$ cosets of the multiplicative subgroup $\langle r \rangle$ in $\mathbb{Z}_l^*$. For a fixed choice of coset representatives $T = \{t_1, \ldots, t_{(l-1)/b}\}$ there are

$$M = \frac{n!}{(n/l)![(bn/l)!]^{(l-1)/b}}$$

ways to choose the $(n/l)(l-1)$ non-zero α's from among T so that $\mathrm{Tr}_{\mathbb{Q}(\zeta)/K}(\zeta^{\alpha_1} + \ldots + \zeta^{\alpha_n}) = 0$. As each coset is of size $b = \mathrm{ord}_l\, r$ and the choice of a given $\alpha_i \ne 0$ in $\mathrm{Tr}_{\mathbb{Q}(\zeta)/K}(\zeta^{\alpha_1} + \ldots + \zeta^{\alpha_n})$ depends only on the coset it represents, one finds that $\beta_K(n) = b^{n(l-1)/l} M$ when $l \mid n$. The result stated in the proposition now follows.

PROPOSITION 5. (i) *For $f = 4$ and $r = 1$,*

$$\beta_K(n) = \begin{cases} \dfrac{(n!)^2}{[(n/2)!]^4} & \text{if } 2 \mid n, \\ 0 & \text{if } 2 \nmid n. \end{cases}$$

(ii) *For $f = 4$ and $r = 3$, $\beta_K(n) = \binom{2n}{n}$.*

Proof. In view of the result of Proposition 2, the counting function $\beta_K(n)$ in statement (i) is what Gupta and Zagier call $\beta_4(n)$ in [3]. Thus statement (i) is just equation (5) in [3, Theorem 2], which was first observed by D. H. and E. Lehmer [6].

To verify statement (ii) of the proposition note that $K = \mathbb{Q}$ here, so $\mathrm{Tr}_{\mathbb{Q}(\zeta)/K}(\zeta^{\alpha}) = 0$ if α is odd, else equals 2 or -2 according as $4 \mid \alpha$ or $2 \parallel \alpha$. Begin by encoding each fourth root of unity by a pair of ones and minus ones, so that ζ corresponds to the pair $(1, -1)$, ζ^2 to $(-1, -1)$, ζ^3 to $(-1, 1)$ and ζ^4 to $(1, 1)$. The encoding is such that the trace $\mathrm{Tr}_{\mathbb{Q}(\zeta)/K}(\zeta^{\alpha})$ equals the sum of its corresponding pair of values. Moreover, one may identify an n-tuple $(x_1, \ldots, x_n)$ of fourth roots of unity by a unique $2n$-tuple $(y_1, y_2, \ldots, y_{2n-1}, y_{2n})$ consisting of ones and minus ones, where x_j corresponds to the pair (y_{2j-1}, y_{2j}) $(1 \le j \le n)$ as described, and vice versa. The correspondence is such that each tuple $(x_1, \ldots, x_n)$ with $\mathrm{Tr}_{\mathbb{Q}(\zeta)/K}(x_1 + \ldots + x_n) = 0$ yields a tuple $(y_1, \ldots, y_{2n})$ with $y_1 + \ldots + y_{2n} = 0$, and vice versa. Thus $\beta_K(n) = \binom{2n}{n}$, the number of ways to fill a $2n$-tuple with an equal number of ones and minus ones.

Thus statement (ii) is verified and the proof of the proposition is now complete.

Now let h be the smallest positive integer for which $\beta_K(h) \ne 0$. Using (7), (8) and Proposition 2, one may obtain the following generalization of Theorem 1 in [4]. Since the argument is identical, I shall omit it here.

Theorem 1. *For all sufficiently large primes* $p \equiv r \pmod f$, *the coefficient* a_s *of the polynomial* $\Phi^{(\delta)}(x)$ *in* (5) (*or* $\mathbf{F}(X)$ *in* (10)) *satisfies* $a_s = \mho_s(p)$, *where* $\mho_s$ *is a polynomial of degree* $[s/h]$ *in* p.

The next examples illustrate the result above.

Example 1. Consider the case $f = 3$ and $r = 2$ with $q = p^2$ above in Theorem 1, so $R = 3$ and $e/\delta = p-1$ in (8). The decomposition field $K = \mathbb{Q}$ with

$$\beta_K(n) = \begin{cases} 4^{n/3}\binom{n}{n/3} & \text{if } 3 \mid n, \\ 0 & \text{otherwise} \end{cases}$$

from Proposition 4, so $h = 3$. One finds the following expressions for the coefficients a_s $(1 \le s \le 8)$ for $\Phi^{(\delta)}(x)$ from (7) and (8):

$$a_1 = 3, \quad a_2 = 9, \quad a_3 = -(4p-27) \qquad \text{for } p > 2,$$
$$a_4 = -(12p-81), \quad a_5 = -(36p-243), \quad a_6 = 8p^2 - 148p + 729 \qquad \text{for } p > 5,$$
$$a_7 = 24p^2 - 444p + 2187, \quad a_8 = 72p^2 - 1332p + 6561 \qquad \text{for } p > 11.$$

One observes that $\Phi^{(\delta)}(x)$ is always irreducible from Corollary 1.

Example 2. Consider next the case $f = 8$ and $r = 3$ or 7 with $q = p^2$ in Theorem 1, so $R = 4$ and $e/\delta = (p-1)/2$ in (8). The decomposition field K is $\mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{2})$, respectively, but it is easy to verify that the counting function $\beta_K(n)$ is the same in each case. For the first few values, one computes $\beta_K(1) = 2$, $\beta_K(2) = 14$, $\beta_K(3) = 68$ and $\beta_K(4) = 454$. Thus $h = 1$ and one finds the following expression for the coefficients a_s $(1 \le s \le 4)$ for $\Phi^{(\delta)}(x)$ from (7) and (8).

$$a_1 = -(p-4), \quad a_2 = \tfrac{1}{2}(p^2 - 15p + 48) \qquad \text{for } p > 3,$$
$$a_3 = -\tfrac{1}{6}(p^3 - 33p^2 + 296p - 960) \qquad \text{for } p > 7 \text{ and}$$
$$a_4 = \tfrac{1}{24}(p^4 - 58p^3 + 1043p^2 - 8306p + 26880) \qquad \text{for } p > 19.$$

The pattern of these coefficients is exhibited below for primes $p < 23$.

p	Factor $\Phi^{(\delta)}(x)$
3	$x+1$
7	$x^3 - 3x^2 - 4x + 13$
11	$x^5 - 7x^4 + 2x^3 + 61x^2 - 123x + 67$
19	$x^9 - 15x^8 + 62x^7 + 65x^6 - 951x^5 + 1585x^4$ $+ 616x^3 - 1846x^2 - 583x - 37$

It is interesting to note that when $h > 1$, the polynomial $\Phi^{(\delta)}(x)$ is irreducible for sufficiently large p by Proposition 3 and the corollary to Proposition 1. In particular, $h > 1$ whenever f is square-free, since then $\mathrm{Tr}_{\mathbb{Q}(\zeta)/K}(\zeta^\alpha) \neq 0$ for any integer α.

To generalize Theorem 1 of S. Gupta and D. Zagier [3], I next introduce the rational power series

$$B_K(X) = \exp\Big(-R\sum_{n=1}^{\infty}\beta_K(n)\frac{X^n}{n}\Big) \tag{11}$$

and

$$A_{K,r}(X) = \exp\bigg(\frac{r}{f}\log B_K(X) - \frac{R}{f}\log(1-fX)\bigg), \tag{12}$$

defined in terms of the counting function $\beta_K(n)$.

The argument in the proof of Theorem 1 of [3] extends in a straightforward manner to yield the following general result here.

Theorem 2. *The power sums $B_K(X)$ and $A_{K,r}(X)$ above lie in $\mathbb{Z}[[X]]$ and satisfy*

$$(1-fX)^R A_{K,r}(X)^f = B_K(X)^r.$$

For any $N > 0$ there is a constant $p_0(N)$ such that for all primes $p \equiv r \pmod f$ with $p > p_0(N)$,

$$\mathbf{F}(X) \equiv A_{K,r}(X)B_K(X)^{(p-r)/f} \pmod{X^N}. \tag{13}$$

For Example 1, the relevant power series (11) and (12) are given by

$$B_K(X) = 1 - 12X^3 - 48X^6 + \ldots$$

and

$$A_{K,2}(X) = 1 + 3X + 9X^2 + 19X^3 + 57X^4 + 171X^5 + \ldots$$

respectively.

In Example 2, the power series (11) is given by

$$B_K(X) = 1 - 8X + 4X^2 + 48X^3 - 62X^4 + \ldots;$$

the corresponding series (12) are

$$A_{K,3}(X) = 1 + X + 6X^2 + 57X^3 + 411X^4 + \ldots$$

and

$$A_{K,7}(X) = 1 - 3X - 4X^2 + 27X^3 + 98X^4 + \ldots$$

For the case $f = 4$ and $r = 3$, one has $R = 2$, $K = \mathbb{Q}$ and $e/\delta = (p-1)/2$. From Proposition 3, for primes $p \equiv 3 \pmod 4$ and not dividing a, one finds $t_\delta(n) = \beta_K(n)$ for $1 \le n \le (p-1)/2$. In such cases one may take $N = (p+1)/2$ in (13) which completely determines $\mathbf{F}(X)$ or $\Phi^{(\delta)}(x)$. It is even possible to find a closed form formula for the coefficients a_s in (10);

namely, $a_s = (-1)^s\binom{p-1-s}{s}$ for $1 \le s \le (p-1)/2$. This result is proved in the section to follow. (Incidentally, if $p\,|\,a$ here, then it is easy to show that $\Phi^{(\delta)}(x) = (x-4)^{(p-1)/2}$ since $t_\delta(n) = 4^n$.)

4. The case $f = 4$ and $r = 3$. In order to derive the closed form formula mentioned at the end of the last section, the following well-known result will be needed.

LEMMA. *Let d be a positive integer. For any polynomial $q(x)$ of degree less than d,*

$$\sum_{n=0}^{d}(-1)^n\binom{d}{n}q(n) = 0.$$

Returning to the situation at hand, first observe that the power series

$$C(X) = \exp\bigg(-\frac{1}{2}\sum_{n=1}^{\infty}\binom{2n}{n}\frac{X^n}{n}\bigg)$$

satisfies

$$\frac{C'(X)}{C(X)} = -\frac{1}{2}\sum_{n=1}^{\infty}\binom{2n}{n}X^{n-1} = \frac{1}{2X}\bigg(1-\frac{1}{\sqrt{1-4X}}\bigg).$$

One finds then $C(X) = \frac{1}{2}(1+\sqrt{1-4X})$. In particular, from Proposition 5(ii), the power series

$$B_K(X) = C(X)^4 = \frac{1}{2}(1-4X+2X^2+(1-2X)\sqrt{1-4X})$$

and

$$A_{K,3}(X) = \frac{C^3(X)}{\sqrt{1-4X}} = \frac{1}{2}\bigg(1-X+\frac{1-3X}{\sqrt{1-4X}}\bigg)$$

in (11) and (12), so

$$\mathbf{F}(X) \equiv A_{K,3}(X)B_K(X)^{(p-3)/4} \equiv \frac{C(X)^p}{\sqrt{1-4X}} \pmod{X^{(p+1)/2}}$$

in (13) where $p\nmid a$. But

$$\begin{aligned}
&(1-4X)^{-1/2}C(X)^p \\
&\quad = 2^{-p}(1-4X)^{-1/2}\sum_{n=0}^{p}\binom{p}{n}(1-4X)^{n/2} \\
&\quad = 2^{-p}\sum_{n=0}^{p}\binom{p}{n}(1-4X)^{(n-1)/2} \\
&\quad = 2^{-p}\sum_{s=0}^{\infty}(4X)^s\sum_{n=0}^{p}\frac{(-1)^s}{s!}\binom{p}{n}\binom{\frac{n-1}{2}}{}\binom{\frac{n-3}{2}}{}\cdots\binom{\frac{n-2s+1}{2}}{},
\end{aligned}$$

so the congruence above yields

$$a_s = \frac{(-1)^s}{2^{p-2s}s!} \sum_{n=0}^{p} \binom{p}{n} \left(\frac{n-1}{2}\right)\left(\frac{n-3}{2}\right)\cdots\left(\frac{n-2s+1}{2}\right) \tag{14}$$

in (10) for $1 \le s \le (p-1)/2$. Now Moriarty's identity (2.73) in [2] implies that

$$\frac{1}{2^{p-2s}} \sum_{\substack{n=0\\ n \text{ odd}}}^{p} \binom{p}{n}\binom{\frac{n-1}{2}}{s} = \frac{1}{2}\binom{p-s-1}{s}.$$

Since

$$\sum_{\substack{n=0\\ n \text{ odd}}}^{p} \binom{p}{n}\binom{\frac{n-1}{2}}{s} = \sum_{\substack{n=0\\ n \text{ even}}}^{p} \binom{p}{n}\binom{\frac{n-1}{2}}{s} \quad \text{for } s < p$$

by the Lemma, it follows from (14) that the coefficients a_s in (10) actually satisfy

$$a_s = (-1)^s \binom{p-s-1}{s} \quad (1 \le s \le (p-1)/2)$$

when $p \nmid a$. In view of the parenthetical remark made at the end of Section 3, I have shown

PROPOSITION 6. *Let $f = 4$ and $p \equiv 3 \pmod 4$ be prime. If $p \nmid a$ then*

$$\Phi^{(\delta)}(x) = \sum_{s=0}^{(p-1)/2} (-1)^s \binom{p-s-1}{s} x^{(p-1)/2-s},$$

else

$$\Phi^{(\delta)}(x) = (x-4)^{(p-1)/2}.$$

This concludes the discussion of the special case $f = 4$ and $r = 3$.

References

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

[2] G. P. Egorychev, *Integral Representations and the Computation of Combinatorical Sums*, Transl. Math. Monographs 39, Amer. Math. Soc., Providence, 1984.

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

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

[5] —, *Factors of period polynomials for finite fields, I*, to appear.

[6] D. H. Lehmer and E. Lehmer, *Cyclotomy with short periods*, Math. Comp. 41 (1983), 743–758.

[7] 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
5998 ALCALÁ PARK
SAN DIEGO, CALIFORNIA 92110-2492
U.S.A.

Received on 25.4.1994
and in revised form on 14.2.1995 (2604)