Canad. Math. Bull. Vol. **28** (4), 1985

ON A CONGRUENCE RELATED TO CHARACTER SUMS

BY

J. H. H. CHALK

In memory of my late colleague R. A. Smith

ABSTRACT. If χ is a Dirichlet character to a prime-power modulus p^α, then the problem of estimating an incomplete character sum of the form $\sum_{1 \le x \le h} \chi(x)$ by the method of D. A. Burgess leads to a consideration of congruences of the type

$$f(x)g'(x) - f'(x)g(x) \equiv 0(p^\alpha),$$

where $fg(x) \not\equiv 0(p)$ and f, g are monic polynomials of equal degree with coefficients in $\mathbf{Z}$. Here, a characterization of the solution-set for cubics is given in terms of explicit arithmetic progressions.

1. **Introduction and notation**. Let $p^n (p > 3$ prime, $n \ge 2)$ be a fixed prime-power, congruences to the modulus m will be denoted by (m) and $\text{ord}_p\, m$ will signify the integer ν for which $p^\nu | m, p^{\nu+1} \nmid m$. The symbol $[[x]]$ for $x \in \boldsymbol{R}$ will denote the least integer $\ge x$, i.e., $[[x]] = -[-x]$. Let f, g denote monic polynomials in $\boldsymbol{Z}[X]$ of equal degree r say, and suppose that they satisfy the mild restriction, modulo p^n:

$$(1) \qquad lf(X) + mg(X) \not\equiv 0, \quad (p^n)$$

for all pairs $(l, m) \in \boldsymbol{Z}^2$ with $(l, m) \not\equiv (0, 0)$, (p). Let

$$(2) \qquad J(f, g, X) = f(X)g'(X) - f'(X)g(X).$$

Then J is a combinative invariant of the pencil $f + \lambda g$ with the properties

$$(3) \qquad J(f + \lambda g, g, X) = J(f, g, X)$$

$$(4) \qquad J'(f, g, X) = f(X)g''(X) - f''(X)g(X).$$

Let

$$(5) \qquad S_n(f, g) = \{x \in \boldsymbol{Z} : fg(x) \not\equiv 0(p), \quad J(f, g, x) \equiv 0(p^n)\}.$$

Our purpose is to identify and classify the elements of $S_n(f, g)$ and, after some preparatory material on certain invariants of the pencil $f + \lambda g$, this is presented in the theorem for the case $r = 3$ (cf. §3). Apart from elements derivable by reduction (p^n) from such roots of $J(f, g, x) = 0$ as lie in $\boldsymbol{Z}_p$, the remaining elements of $S_n(f, g)$ form a set which is a union of at most 4 arithmetic progressions. Congruences of the type

Received by the editors August 28, 1984 and, in final revised form, February 18, 1985.
AMS Subject Classification: 10A10, 10G05.

https://doi.org/10.4153/CMB-1985-052-x Published online by Cambridge University Press

in (5) have acquired significance in the problem of estimating incomplete character sums of the type $\sum_{1\le x\le h}\chi(x)$, where χ is a (primitive) character to a prime-power modulus p^{α}. The methods of Davenport-Erdös [2] and of Burgess [1] lead directly to a consideration of sums of the form (cf. [1], Lemma 2):

$$\sigma(p^{\alpha}) = p^{\alpha-\gamma} \sum_{\substack{1\le x\le p^{\gamma}\\ J(f,g,x)\equiv 0(p^{\alpha-\gamma})\\ fg(x)\not\equiv 0(p)}} \chi[f/g(x)], \quad (\gamma \ge \tfrac{1}{2}\alpha)$$

and, by the theorem ($r = 3$), it is now possible, for example, to give precise estimates for the number of terms in such sums. It may be remarked that while previous work on general polynomial congruences (cf. [3], for references) is effective for the case $r = 2$ (cf. [2]) it is difficult to apply for $r \ge 3$.

2. Invariants of the pencil $f + \lambda g$.

DEFINITION. *Let*

(6) $$\mu = \mu(f,g) = \text{ord}_p[f(X) - g(X)]$$

Then, by (1),

(7) $$0 \le \mu < n$$

and, from the definition of $J(f,g,X)$,

(8) $$J(f,g,X) \equiv J'(f,g,X) \equiv 0 \quad (p^{\mu}).$$

We assume henceforth that

(9) $$S_n(f,g) \ne \emptyset.$$

Then it follows that there is a $t \in \mathbf{Z}$ *with* $fg(t) \not\equiv 0(p)$ *for which*

(10) $$f(t) + \lambda g(t) \equiv f'(t) + \lambda g'(t) \equiv 0(p^n),$$

where $(\lambda,p) = 1$ *and*

(11) $$-\lambda \equiv f/g(t), \quad (p^n).$$

By Taylor's theorem, applied to $f(X) + \lambda g(X)$, we have

(12) $$f(X) + \lambda g(X) \equiv u(X-t)^2[w(X-t) + v], \quad (p^n)$$

where $u = u(t)$, $w = w(t)$, $v = v(t)$ are constants depending on the choice of t which we can suppose, without loss of generality, to satisfy

(13) $gcd(v,w,p) = 1$, $w = 1$ if $\text{ord}_p w = 0$ and $v = 1$ if $\text{ord}_p w > 0$.

We show firstly that $\text{ord}_p u = \mu$. For, if $\text{ord}_p w = 0$ so that $w = 1$, then $1 + \lambda \equiv u(p^n)$, by comparing the coefficients of X^3 in (12). But by $(10)_1$ and (6), $f(t) + \lambda g(t) \equiv (1+\lambda)f(t)$, (p^{μ}) and so $1 + \lambda \equiv 0(p^{\mu})$, $u \equiv 0(p^{\mu})$. However, if $u \equiv 0(p^{\mu+1})$, then

https://doi.org/10.4153/CMB-1985-052-x Published online by Cambridge University Press

$1 + \lambda \equiv 0(p^{\mu+1})$ and $f(X) + \lambda g(X) \equiv 0(p^{\mu+1})$, contrary to the definition of μ in (6). Now, if $\text{ord}_p w > 0$ so that $v = 1$, then again on comparing coefficients of X^3 in (12), we have $1 + \lambda \equiv uw(p^n)$. But then

$$(14) \qquad f(X) - g(X) \equiv u[-wg(X) + w(X - t)^3 + (X - t)^2], \quad (p^n)$$

and now it is clear that $\text{ord}_p(f(X) - g(X)) = \text{ord}_p u$, since the polynomial on the right of (14) is primitive (p). Next, by means of a transformation $t \rightarrow T$ of the form

$$T = t + zp^l \quad (z \in \mathbf{Z}),$$

where $l = [[\frac{1}{2}m]]$, $m = n - \mu \geq 1$ and λ, u and w are kept fixed, we can ensure that, if

$$\nu = \nu(t) = \text{ord}_p v \geq [[\tfrac{1}{2}m]],$$

then $\nu(T) = \text{ord}_p v(T) = [[\frac{1}{2}m]]$, for a suitable choice of z.

Thus, we may suppose that t is chosen initially to satisfy

$$(15) \qquad \nu = \nu(t) = \text{ord}_p v \leq [[\tfrac{1}{2}m]].$$

Let

$$(16) \qquad F_\lambda(X) = f(X) + \lambda g(X),$$

then it suffices to check $F_\lambda(T)$ and $F'_\lambda(T)$ and note that since $\nu \geq 1$, we have $w = 1$ and so $u \equiv 1 + \lambda(p^n)$, from (12). But

$$F_\lambda(T) = F_\lambda(t) + zp^l F'_\lambda(t) + \frac{z^2}{2} p^{2l} F''_\lambda(t) + \frac{z^3}{6} p^{3l} F'''_\lambda(t)$$

$$F'_\lambda(t) = F'_\lambda(t) + zp^l F''_\lambda(t) + \frac{z^2}{2} p^{2l} F'''_\lambda(t),$$

since $F^{(iv)}(X) = 0$ and $F'''(X) = 6(1 + \lambda)$. Now,

$$F''_\lambda(t) \equiv 2uv(p^n), \text{ by (12)}$$

and so, by (13), either

$$\text{ord}_p F''_\lambda(t) = \mu + \nu(t)$$

or $\mu + \nu(t) \geq n$, $\text{ord}_p F''_\lambda(t) \geq n$. Then

$$(17) \qquad F_\lambda(T) \equiv F'_\lambda(T) \equiv 0(p^n)$$

if both the inequalities

$$l + \mu + \nu(t) \geq n$$
$$2l + \text{ord}_p(1 + \lambda) \geq n$$

hold. But

$$l + \mu + \nu(t) \geq [[\tfrac{1}{2}m]] + \mu + [\tfrac{1}{2}m] = m + \mu = n$$

$$2l + \text{ord}_p(1+\lambda) \geq 2l + \mu \geq 2\frac{m}{2} + \mu = n,$$

and so (17) holds. Now

$$\begin{aligned} F''_\lambda(T) &= F''_\lambda(t) + zp^l \cdot F'''_\lambda(t) \\ &\equiv 2uv(t) + 6zp^l u \quad (p^n) \\ &= 2u[v(t) + 3zp^l] \quad (p^n) \\ &= 2up^l[p^{-l}v(t) + 3z] \quad (p^n) \end{aligned}$$

Thus, with $z = 1$ if $\nu > l$ and $z = p$ if $\nu = l$

$$\text{ord}_p F''_\lambda(T) = \mu + l = \mu + [[\tfrac{1}{2}m]]$$

and so $\nu(T) = l = [[\frac{1}{2}m]]$.

We note, in passing, that we could equally well choose z so that $F''_\lambda(T) \equiv 0(p^n)$, in which case the pencil $f(X) + \lambda g(X)$ contains a perfect cube (p^n), for (12) becomes

(18) $$f(X) + \lambda g(X) \equiv (1+\lambda)(X-T)^3 \quad (p^n),$$

whenever $\nu = \nu(t) \geq [[\frac{1}{2}m]]$.

Henceforth, we shall assume that (12) holds with v chosen so that $\nu = \text{ord}_p\ v$ is *maximal*, subject to the condition $\nu \leq [[\frac{1}{2}m]]$.

3. **The reduction formulae**. By (2) and (5), and writing

(19) $$f_1(X) = (X-t)^2[w(X-t) + v],$$

(20) $$S_n(f,g) = S_m^*(f_1, g) \cup E_m^*(f_1, g),$$

where

(21) $$S_m^*(f_1,g) = \{x \in \mathbf{Z}: f_1 f g(x) \not\equiv 0(p), \quad J(f_1, g, x) \equiv 0(p^m)\}$$

and

(22) $$E_m^*(f_1, g) = \{x \in \mathbf{Z}: f_1(x) \equiv 0(p), \quad fg(x) \not\equiv (0(p), \quad J(f_1, g, x) \equiv 0(p^m)\}.$$

Here $S_m^*(f_1, g)$ is a modification of $S_m(f_1, g)$ for the special case $\mu = 0$, since

(23) $$S_m^*(f_1, g) = S_m(f_1, g) \text{ when } \mu > 0,$$

for $(\lambda, p) = 1$, $g(x) \equiv 0(p) \Rightarrow f(x) = -\lambda g(x) + uf_1(x) \equiv 0(p)$, if $\mu > 0$. The theorem may now be stated in terms of a 2-stage reduction formula:

THEOREM. *Let* $r = 3$

(i) *There is a* ν *with* $0 \leq \nu \leq [[\frac{1}{2}m]]$, *where* $m = n - \mu$, *for which*

$$S_n(f,g) = S_m^*(f_1, g) \cup A_m(\nu),$$

where $f_1(X)$ *is as defined in* (19) *and* $S_m^*(f_1, g)$ *in* (21). *Further*

$$A_m(0) = \{x \in \mathbf{Z}: x \equiv t(p^m)\}, \quad A_m([[\tfrac{m}{2}]]) = \{x \in \mathbf{Z}: x \equiv t(p^{[[m/2]]})\}$$

https://doi.org/10.4153/CMB-1985-052-x Published online by Cambridge University Press

and for $0 \le \nu \le [[\frac{1}{2}m]]$,

$$A_m(\nu) = A'_m(\nu) \cup A''_m(\nu),$$

where

$$A'_m(\nu) = \{x \in \mathbf{Z} : x \equiv t(p^{m-\nu})\}$$

$$A''_m(\nu) = \{x \in \mathbf{Z} : x = t + vz, z \equiv z_0(p^{m-2\nu})\},$$

and z_0 *is uniquely defined* $(p^{m-2\nu})$ *and satisfies* $3z_0 + 2 \equiv 0(p)$.

(ii) *If* $S^*_m(f_1, g) \neq \ominus$ *then either,* (a) *all solutions of* $J(f_1, g, x) \equiv 0(p^m)$ *are non-singular, or* (b) *there is a pair* (t_1, v_1) *with* $1 \le \nu_1 \le \nu$ *such that*

$$S^*_m(f_1, g) = A_m(\nu_1).$$

PROOF OF PART (i) OF THE THEOREM. Observe firstly that, from (22)

$$E^*_m(f_1, g) = E_m(f_1, g),$$

where

$$E_m(f_1, g) = \{x \in \mathbf{Z} : x \equiv t(p), \quad J(f_1, g, x) \equiv 0(p^m)\}, \tag{24}$$

since

$$J(f_1, g, x) \equiv f_1(x) \equiv 0(p) \Rightarrow f'_1(x) \equiv 0(p), \quad \text{as} \quad g(x) \not\equiv 0(p).$$

Thus $x \equiv t(p)$ and the condition $fg(x) \not\equiv 0(p)$ is redundant as $fg(t) \not\equiv 0(p)$. Next, we express $J(f_1, g, X)$ is alternative forms, using the notation:

$$f_1(X) = (X - t)^2 L(X), \text{ where } L(X) = w(X - t) + v, \tag{25}$$

$$J(f_1, g, X) = (X - t)^2 L(X) g'(X) - g(X)[(X - t)^2 L'(x) + 2(X - t)L(X)]$$

$$= (X - t)[(X - t) J(L, g, X) - 2L(X)g(X)], \tag{26}$$

$$= (X - t)\{(X - t)[J(L, g, X) - 2wg(X)] - 2vg(X)\}. \tag{27}$$

From (25), we see that in the case $\nu = 0$ the conditions $x \equiv t(p)$ and $J(f_1, g, x) \equiv 0(p^m)$ imply, by (26), that $x \equiv t(p^m)$, since $L(t)g(t) \not\equiv 0(p)$. It remains to consider the cases where $\nu > 0$, when $w = 1$.

For brevity, we write

$$Y = X - t \tag{28}$$

and then, by (27),

$$J(f_1, g, Y + t) = Y\{Yl(Y) - 2vg(Y + t)\}, \tag{29}$$

where

$$L(Y) = (Y + v)g'(Y + t) - 3g(Y + t). \tag{30}$$

https://doi.org/10.4153/CMB-1985-052-x Published online by Cambridge University Press

Note that

(31) $\quad y = x - t \equiv 0(p) \Rightarrow l(y) \equiv -3g(t) \not\equiv 0(p), \quad g(y+t) \not\equiv 0(p).$

Suppose firstly that $\nu = [[\frac{1}{2}m]]$. Then, by (30) and (31),

$$\begin{aligned} y \equiv 0(p), J(f_1, g, y+t) \equiv 0(p^m) &\Leftrightarrow [l(y) - vg(y+t)]^2 \equiv 0(p^m) \\ &\Leftrightarrow \text{ord}_p y \geq \tfrac{1}{2}m, \\ &\Leftrightarrow x \equiv t(p^{[[m/2]]}) \end{aligned}$$

as required. It now remains to consider the case

$$0 < \nu < \tfrac{1}{2}m.$$

Here the conditions on y are

(32) $\quad y \equiv 0(p), \quad y[yl(y) - 2vg(y+t)] \equiv 0(p^m)$

and clearly imply that

$$\text{ord}_p y \geq \nu.$$

Now, for the set of such y's with $\text{ord}_p y > \nu$, it is necessary and sufficient that $\text{ord}_p y \geq m - \nu, x \equiv t(p^{m-\nu})$. For the remaining set of y's, we have

$$\text{ord}_p y = \nu,$$

and this requires more detailed consideration. On putting

(33) $\quad Y = vZ$

our conditions become

(34) $\quad z \not\equiv 0(p), \quad J(f_1, g, t + vz) \equiv 0(p^m).$

But, with $X = t + vZ$,

$$f_1(X) = v^3(Z^3 + Z^2) = v^3 f_2(Z), \text{ say}$$

and

$$\begin{aligned} f_1'(X) &= v^3 f_2'(Z)v^{-1} = v^2 f_2'(Z) \\ g(X) &= g(t) + g'(t)vZ + \tfrac{1}{2}g''(t)v^2Z^2 + \tfrac{1}{6}g'''(t)v^3Z^3 \\ &= g_2(Z) \text{ say,} \\ g'(X) &= g_2'(Z)v^{-1}. \end{aligned}$$

Thus

$$\begin{aligned} J(f_1, g, X) &= v^3 f_2(Z)v^{-1}g_2'(Z) - v^2 f_2'(Z)g_2(Z) \\ &= v^2 J(f_2, g_2, Z). \end{aligned}$$

and our conditions (34) take the form

https://doi.org/10.4153/CMB-1985-052-x Published online by Cambridge University Press

(35) $$z \not\equiv 0(p), \quad J(f_2, g_2, z) \equiv 0(p^{m-2\nu}).$$

Now

$$J(f_2, g_2, Z) = Z[Z(Z+1)g_2'(Z) - (3Z+2)g_2(Z)],$$

where $g_2'(Z) \equiv 0(p^\nu)$ and $g_2(Z) \equiv g(t) \not\equiv 0(p)$ identically in Z. Thus (35) becomes the single condition

(36) $$F(z) \equiv 0\ (p^{m-2\nu}),$$

where

$$F(Z) = Z(Z+1)g_2'(Z) - (3Z+2)g_2(Z).$$

But

$$F(Z) \equiv -(3Z+2)g(t), \quad F'(Z) \equiv -3g(t) \not\equiv 0 \quad (p)$$

and so (36) has just one solution $z \equiv z_0(p^{m-2\nu})$, where $3z_0 + 2 \equiv 0\ (p)$.

This completes the proof of part (i) of the theorem. For part (ii), we shall need the following lemma to obtain the inequality $\nu_1 \le \nu$ in a second application of the reduction formula of part (i).

LEMMA. *Suppose that*

(37) $$f(X) + \lambda g(X) \equiv u f_1(X), \quad (p^n)$$

with $(\lambda, p) = 1$ *and* $f_1(X)$ *of the form in* (19). *If*

$$S_m^*(f_1, g) \neq \phi$$

there is a $t_1 \not\equiv t(p)$ *such that*

(38) $$g(X) + \lambda_1 f_1(X) \equiv u_1 g_1(X), (p^m), m = n - \mu,$$

where

(39) $$(\lambda_1, p) = 1, \quad f_1 f g(t_1) \not\equiv 0(p)$$

and

(40) $$g_1(X) = (X - t_1)^2[w_1(X - t_1) + v_1]$$

with

(41) $$gcd(v_1, w_1, p), \ w_1 = 1 \text{ if } \operatorname{ord}_p w_1 = 0 \text{ and } v_1 = 1 \text{ if } \operatorname{ord}_p w_1 > 0.$$

Moreover,

(42) $$f(X) + (\lambda + \lambda_1^{-1}u)g(X) \equiv \lambda_1^{-1}uu_1 g_1(X), \quad (p^n)$$

where

(43) $$\mu_1 = \operatorname{ord}_p u_1 = 0, \quad \lambda + \lambda_1^{-1}u \not\equiv 0(p), \quad \nu_1 = \operatorname{ord}_p v_1 \le \nu.$$

PROOF. From the definition of $S_m^*(f_1, g)$ in (21), it is clear that there is a $t_1 \not\equiv t(p)$ which satisfies (38), (39), (40) and (41). Now (42) is obtained from (37) and (38) by multiplying (38) by $u\lambda_1^{-1}$ and substituting $u\lambda_1^{-1}(u_1g_1(x) - g(x))$ for $uf_1(x)$ in (37). Note that, if $\lambda + \lambda_1^{-1}u \equiv 0(p)$, then

$$f(X) \equiv \lambda_1^{-1}uu_1g_1(X)\ (p), \text{ by (42)},$$

which is impossible since $g_1(t_1) \equiv 0(p), f(t_1) \not\equiv 0(p)$. Hence $\lambda + \lambda_1^{-1}u \not\equiv 0(p)$. Now, if $\text{ord}_p u_1 > 0$, then, by (42)

$$f(X) + (\lambda + \lambda_1^{-1}u)g(X) \equiv 0(p^{\mu+1})$$

and (by comparing coefficients of X^3) $\lambda + \lambda_1^{-1}u \equiv -1(p^{\mu+1})$, which implies that $f(X) \equiv g(X)\ (p^{\mu+1})$, contrary to the definition of μ. Hence $\text{ord}_p u_1 = 0$. Since the choice of t was taken so that $\nu = \text{ord}_p v \leq [[\frac{1}{2}m]]$ was maximal, it follows from (42) that $\nu_1 = \text{ord}_p v_1 \leq \nu$. This completes the proof of the lemma.

PROOF OF PART (ii) OF THE THEOREM. Suppose that $S_m^*(f_1, g) \neq \ominus$; then there is a $t_1 \not\equiv t(p)$ such that $f_1fg(t_1) \not\equiv 0(p)$ and

$$g(t_1) + \lambda_1f_1(t_1) \equiv g'(t_1) + \lambda_1f_1(t_1) \equiv 0(p^m),$$

where $(\lambda_1, p) = 1$. Then, by Taylor's theorem applied to $g(X) + \lambda_1f_1(X)$, we have

$$g(X) + \lambda_1f_1(X) \equiv u_1g_1(X) \quad (p^m),$$

where $g_1(X)$ satisfies (40) and (41) of the lemma. Suppose first that, for *all* such choices of t_1, $J'(f_1, g, t_1) \not\equiv 0(p)$. Then all solutions of $J(f_1, g, x) \equiv 0(p^m)$ are non-singular and $S_m^*(f_1, g) \leq \deg J(f_1, g, X) \leq 4$, as required. If this is not the case, we may choose t_1 as above and satisfy the further condition

$$g''(t_1) + \lambda_1f_1''(t_1) \equiv 0(p) \tag{44}$$

since

$$J'(f_1, g, t_1) = J'(f_1, g + \lambda_1f_1, t_1) \equiv 0(p),$$

implies (44), as $f_1(t_1) \not\equiv 0(p)$ and $g(t_1) + \lambda_1f_1(t_1) \equiv 0(p^m)$, (cf. (4)). But by (38) and (40) of the lemma,

$$g''(t_1) + \lambda_1f_1''(t_1) \equiv 2u_1v_1\ (p)$$

whence

$$\nu \geq \nu_1 = \text{ord}_p v_1 \geqslant 1. \tag{45}$$

We can now prove that $S_m(f_1, g_1) = \ominus$. For

$$\begin{aligned} J(f_1, g_1, X) &\equiv 3\{(X - t)^3(X - t_1)^2 - (X - t_1)^3(X - t)^2\}\ (p) \\ &\equiv 3(t_1 - t)(X - t)^2(X - t_1)^2\ (p), \end{aligned}$$

where

$$f_1(x) \equiv (x - t)^3 \not\equiv 0(p), \quad g_1(x) \equiv (x - t_1)^3 \not\equiv 0(p)$$

by (45). Now, if $\mu \neq 0$, $S_m^*(f_1, g) = S_m(f_1, g)$ and the reduction formula of part (i) can be applied again to give

$$S_m^*(f_1, g) = S_m^*(f_1, g_1) \cup A_m(\nu_1)$$

and since $S_m^*(f_1, g_1) \subset S_m(f_1, g_1) = \Phi$, the proof is complete. For the case $\mu = 0$, we give a direct verification, using the formula

$$S_m^*(f_1, g) = S_m'(f_1, g_1) \cup E_m'(f_1, g_1),$$

where

$$S_m'(f_1, g_1) = \{x \in \mathbf{Z} : fgf_1g_1(x) \not\equiv 0(p), \quad J(f_1, g_1, x) \equiv 0(p^m)\}$$
$$E_m'(f_1, g_1) = \{x \in \mathbf{Z} : g_1(x) \equiv 0(p), \quad fgf_1(x) \not\equiv 0(p), \quad J(f_1, g_1, x) \equiv 0(p^m)\}.$$

Clearly, $S_m'(f_1, g_1) \subset S_m(f_1, g_1) = \Phi$, and

$$E_m'(f_1, g_1) = \{x \in \mathbf{Z} : x \equiv t(p), \quad J(f_1, g_1, x) \equiv 0(p^m)\},$$

since

$$J(f_1, g_1, x) \equiv g_1(x) \equiv 0(p), \quad f_1(x) \not\equiv 0(p) \Rightarrow g_1'(x) \equiv 0(p) \Rightarrow x \equiv t_1(p)$$

Thus the condition $fgf_1(x) \not\equiv 0(p)$ in $E_m'(f_1, g_1)$ is redundant and we obtain

$$E_m'(f_1, g_1) = E_m(f_1, g_1) = A_m(\nu_1),$$

as required.

References

1. D. A. Burgess, *On Character Sums and L-series*, Proc. London Math. Soc., (3), **12** (1962), pp. 193–196.

2. J. H. H. Chalk, *A New Proof of Burgess' Theorem on Character Sums*, C-R Math, Rep. Acad. Sci. Canada, No. 4 V (1983), pp. 163–168, (see Math. Reviews for a revised statement of the result).

3. J. H. H. Chalk and R. A. Smith, *Sándor's Theorem on Polynomial Congruences and Hensel's Lemma*, C-R Math. Rep. Acad. Sci. Canada, No. 1, II (1982), pp. 49–54.

4. H. Davenport and P. Erdös, *The Distribution of Quadratic and Higher Residues*, Publications Mathematicae, T-2, fasc., 3-4 (1952), pp. 252–265.

University of Toronto
Toronto, Canada