

# An Estimate For Heilbronn's Exponential Sum

D.R. Heath-Brown  
Magdalen College, Oxford

*For Heini Halberstam,  
on his retirement*

Let  $p$  be a prime, and set  $e(x) = \exp(2\pi ix)$ . Heilbronn's exponential sum is defined by

$$S(a) = \sum_{n=1}^p e\left(\frac{an^p}{p^2}\right),$$

for any integer  $a$  coprime to  $p$ . It is important to note here that if  $n \equiv n' \pmod{p}$ , then  $n^p \equiv n'^p \pmod{p^2}$ . Thus the summand in  $S(a)$  has period  $p$  with respect to  $n$ , so that  $S(a)$  is a 'complete sum' to modulus  $p$ .

It was a favourite problem of Heilbronn, and later of Davenport, to show that  $S(a) = o(p)$  as  $p \rightarrow \infty$ . Odni [3] examined sums related to  $S(a)$ , and showed that they are  $O(p^{1/2})$  in a suitable average sense. However his argument fails to give a non-trivial upper bound for an individual value of  $S(a)$ . Indeed he shows how Weil's approach leads only to the estimate  $S(a) = O(p^{3/2})$ , which is worse than the trivial bound!

We can now answer Heilbronn's question with the following theorem.

**Theorem 1** *If  $p$  is a prime and  $p \nmid a$  then  $S(a) \ll p^{11/12}$ , uniformly in  $a$ .*

As a corollary one can handle sums over arbitrary intervals.

**Corollary** *If  $p$  is a prime and  $p \nmid a$  then*

$$\sum_{\substack{M < n \leq M+N \\ p \nmid n}} e\left(\frac{an^p}{p^2}\right) \ll p^{11/12} \log p,$$

*uniformly in  $a$ , for all  $M$  and for all  $N \leq p$ .*

In particular one sees, by Weyl's criterion, that the numbers  $n^p$  are uniformly distributed modulo  $p^2$  for large  $p$ .

Since the deduction of the corollary is very straightforward we shall present it here. We have

$$\begin{aligned} \sum_{\substack{M < n \leq M+N \\ p \nmid n}} e\left(\frac{an^p}{p^2}\right) &= p^{-1} \sum_{r=1}^p \sum_{s=1}^p e\left(\frac{as^p}{p^2}\right) \sum_{M < n \leq M+N} e\left(\frac{r(s-n)}{p}\right) \\ &\ll p^{-1} \left\{ N + \sum_{r=1}^{p-1} \left| \operatorname{cosec}\left(\frac{\pi r}{p}\right) \right| \right\} \max_r \left| \sum_{s=1}^p e\left(\frac{as^p}{p^2}\right) e\left(\frac{rs}{p}\right) \right|, \end{aligned}$$

on using the estimate

$$\sum_{M < n \leq M+N} e\left(\frac{-rn}{p}\right) \ll \begin{cases} N, & p \mid r, \\ \left| \operatorname{cosec}\left(\frac{\pi r}{p}\right) \right|, & p \nmid r. \end{cases}$$

Since  $N \leq p$  and

$$\sum_{r=1}^{p-1} \left| \operatorname{cosec}\left(\frac{\pi r}{p}\right) \right| \ll p \log p,$$

we deduce that

$$\sum_{\substack{M < n \leq M+N \\ p \nmid n}} e\left(\frac{an^p}{p^2}\right) \ll (\log p) \max_r \left| \sum_{s=1}^p e\left(\frac{as^p}{p^2}\right) e\left(\frac{rs}{p}\right) \right|.$$

However, since  $s \equiv s^p \pmod{p}$ , we have

$$e\left(\frac{as^p}{p^2}\right) e\left(\frac{rs}{p}\right) = e\left(\frac{(a+pr)s^p}{p^2}\right),$$

whence

$$\sum_{s=1}^p e\left(\frac{as^p}{p^2}\right) e\left(\frac{rs}{p}\right) = S(a+pr) \ll p^{11/12},$$

by Theorem 1. This bound holds uniformly in  $r$ , of course, so that the corollary follows.

We take this opportunity to record an estimate for a second sum which involves the distribution modulo  $p^2$  of  $n^{p-1}$  rather than  $n^p$ . For  $p \nmid n$  we shall set

$$q(n) = \frac{n^{p-1} - 1}{p}.$$

This has sometimes been called the ‘Fermat quotient’. Our result shows that  $q(n)$  is uniformly distributed modulo  $p$  for  $1 \leq n < p$ .

**Theorem 2** For any integer  $a$  coprime to  $p$  we have

$$\sum_{\substack{M < n \leq M+N \\ p \nmid n}} e\left(\frac{aq(n)}{p}\right) \ll N^{1/2} p^{3/8},$$

uniformly for  $M, N \geq 1$ . In particular

$$\sum_{n=1}^{p-1} e\left(\frac{aq(n)}{p}\right) \ll p^{7/8},$$

uniformly for  $p \nmid a$ .

The proof of Theorem 2 is quite straightforward, and we present it here. We observe that  $q(mn) = q(m)n^{p-1} + q(n)$ , whence  $q(mn) \equiv q(m) + q(n) \pmod{p}$ , for  $p \nmid mn$ . Thus

$$\chi(n) = \begin{cases} 0, & p \mid n, \\ e\left(\frac{aq(n)}{p}\right), & p \nmid n, \end{cases}$$

is a non-principal character to modulus  $p^2$ , of order  $p$ . The sum in Theorem 2 can therefore be written as

$$\sum_{M < n \leq M+N} \chi(n),$$

and the required result follows by an estimate of Burgess [1]. (Actually the result stated by Burgess contains a factor  $k^{3/16+\varepsilon}$  for characters to modulus  $k$ , but it is easy to remove the exponent  $\varepsilon$  when  $k = p^2$ .)

We now return to Theorem 1, with which we shall be concerned for the remainder of the paper. Our treatment begins with some elementary manipulations of a type which would have been quite familiar to Heilbronn, which lead to the following result.

**Lemma 1** Let

$$f(X) = X + \frac{X^2}{2} + \frac{X^3}{3} + \dots + \frac{X^{p-1}}{p-1} \in \mathbb{Z}_p[X],$$

and write

$$S_r = \{k \in \mathbb{Z}_p - \{0, 1\} : f(k) = r\},$$

$$N_r = \#S_r.$$

Then there is a value of  $r$  for which

$$S(a) \ll p^{3/4} N_r^{1/4}.$$

The trivial bound  $N_r \ll p$  leads to the estimate  $S(a) \ll p$ , so that nothing has been lost up to this point. On the other hand, it is not so clear how any non-trivial estimate for  $N_r$  may be obtained.

It turns out that ideas from the work of Stepanov [4] provide the necessary tool. Stepanov was concerned with proving Weil's theorem on the number of points on a curve over a finite field, rather than bounding the number of zeros of a polynomial in one variable. The method shows strong links with ideas from transcendence theory, where one constructs an auxiliary polynomial which vanishes to high order at the points of interest. The resemblance between  $f(X)$  and the function

$$-\log(1 - X) = X + \frac{X^2}{2} + \frac{X^3}{3} + \dots \in \mathbb{Q}[[X]]$$

serves as a guide during the argument. To construct the auxiliary polynomial one uses the fact that  $f$  satisfies a simple differential equation. This is expressed by the following lemma.

**Lemma 2** *For any positive integer  $r$  there exist polynomials  $q_r(X)$  and  $h_r(X)$  in  $\mathbb{Z}_p[X]$ , of degrees at most  $r + 1$  and  $r - 1$  respectively, such that*

$$\{X(1 - X)\}^r \left(\frac{d}{dX}\right)^r f(X) = q_r(X) + (X^p - X)h_r(X).$$

In effect the lemma converts  $f(X)$ , which has large degree, into  $q_r(X)$ , which has small degree.

As is usual in transcendence proofs, we have also to show that our auxiliary polynomial does not vanish identically. This is accomplished in our case via the observation that  $f(X)$  is almost equal to a transcendental function,  $-\log(1 - X)$ , so that it cannot satisfy an algebraic relation. The following lemma expresses this principle.

**Lemma 3** *Let  $F(X, Y) \in \mathbb{Z}_p[X, Y]$  have degree less than  $A$  with respect to  $X$ , and degree less than  $B$  with respect to  $Y$ . Then if  $F$  does not vanish identically we will have  $X^p \nmid F(X, f(X))$ , providing only that  $AB \leq p$ .*

This result is remarkably sharp. Indeed if  $AB > p$ , the polynomial  $F$  will have enough coefficients to ensure that  $X^p \mid F(X, f(X))$  is possible. Specifically, one may note that the coefficients of  $F(X, f(X))$  are linear functions of the coefficients of  $F(X, Y)$ . To make  $X^p \mid F(X, f(X))$  we must arrange that  $p$  such linear functions vanish, and we have  $AB$  variables at our disposal. Hence if  $AB > p$  a suitable polynomial  $F(X, Y)$  can be found.

With the help of Lemmas 2 and 3, Stepanov's method enables us to give the following bound for  $N_r$ .

**Lemma 4** *We have  $N_r = O(p^{2/3})$  uniformly in  $r$ .*

Theorem 1 now follows, via Lemma 1.

After the original version of this paper was submitted, the referee kindly pointed out that Lemma 4 appears already in a paper of Mit'kin [2]. Indeed Mit'kin shows an analogous result for the polynomial

$$f(X) = 1 + X + \frac{X^2}{2!} + \frac{X^3}{3!} + \dots + \frac{X^{p-1}}{(p-1)!} \in \mathbb{Z}_p[X],$$

as well.

## 1 Preliminaries

In this section we shall prove Lemma 1. We begin by writing

$$S_0(a) = \sum_{n=1}^{p-1} e\left(\frac{an^p}{p^2}\right)$$

so that  $S(a) = 1 + S_0(a)$ . Then

$$|S_0(a)|^2 = \sum_{m,n=1}^{p-1} e\left(\frac{a(m^p - n^p)}{p^2}\right).$$

When  $m \neq n$  we set  $m - n \equiv b \pmod{p}$  and  $m \equiv kb$ ,  $n \equiv (k-1)b \pmod{p}$ , so that  $b$  runs over the residues  $1, \dots, p-1$  modulo  $p$  and  $k$  runs similarly over the residues  $2, \dots, p-1$ . This yields

$$\begin{aligned} |S_0(a)|^2 &= (p-1) + \sum_{b=1}^{p-1} \sum_{k=2}^{p-1} e\left(\frac{ab^p\{k^p - (k-1)^p\}}{p^2}\right) \\ &= (p-1) + \sum_k S(a\{k^p - (k-1)^p\}). \end{aligned}$$

We now observe that

$$k^p - (k-1)^p = \sum_{l=1}^p (-1)^{l-1} \binom{p}{l} k^{p-l} \equiv 1 - pf(k) \pmod{p^2},$$

whence

$$|S_0(a)|^2 = (p-1) + \sum_{r=1}^p N_r S(a(1-pr)).$$

Cauchy's inequality then leads to the estimate

$$|S_0(a)|^4 \ll p^2 + \left\{ \sum_{r=1}^p N_r^2 \right\} \left\{ \sum_{r=1}^p |S(a(1-pr))|^2 \right\}.$$

Here  $\sum_r N_r$  is just the number of available integers  $k$ , namely  $p - 2$ . Moreover

$$\sum_{r=1}^p |S_0(a(1 - pr))|^2 = \sum_{m,n=1}^{p-1} e\left(\frac{a(m^p - n^p)}{p^2}\right) \sum_{r=1}^p e\left(\frac{ar(n^p - m^p)}{p}\right).$$

The inner sum vanishes unless  $p|n^p - m^p$ , but this implies that  $n \equiv m \pmod{p}$ . Thus

$$\sum_{r=1}^p |S_0(a(1 - pr))|^2 = p(p - 1),$$

so that

$$|S_0(a)|^4 \ll p^2 + (p - 2)p(p - 1) \max_r N_r.$$

Since  $\max_r N_r \geq 1$  we deduce that

$$S(a) \ll 1 + p^{1/2} + p^{3/4}(\max_r N_r)^{1/4} \ll p^{3/4}(\max_r N_r)^{1/4},$$

as required for Lemma 1.

## 2 Stepanov's Method

We shall begin by taking a polynomial  $\Phi(X, Y, Z) \in \mathbb{Z}_p[X, Y, Z]$ , for which

$$\deg_X \Phi < A, \deg_Y \Phi < B, \deg_Z \Phi < C.$$

The underlying idea is to arrange that the polynomial  $\Psi(X) = \Phi(X, f(X), X^p)$  has a zero of order at least  $D$ , say, at each point  $k \in S_r$ . We will therefore be able to conclude that  $DN_r \leq \deg \Psi(X)$ , providing that  $\Psi$  does not vanish identically. We note that

$$\deg \Psi \leq (\deg_X \Phi) + (\deg f)(\deg_Y \Phi) + (\deg X^p)(\deg_Z \Phi) < A + (p - 1)B + pC,$$

whence

$$DN_r \ll A + p(B + C), \tag{1}$$

providing that  $\Psi$  does not vanish.

In order for  $\Psi$  to have a zero of order at least  $D$  at a point  $k$  we need

$$\left. \frac{d^n \Psi(X)}{dX^n} \right|_{X=k} = 0 \quad \text{for } n < D.$$

Since  $k \neq 0, 1$  in our application, this will be equivalent to

$$\{X(1 - X)\}^n \left. \frac{d^n \Psi(X)}{dX^n} \right|_{X=k} = 0. \tag{2}$$

For any term  $X^a f(X)^b X^{pc}$  we have

$$\begin{aligned} \{X(1-X)\}^n \left(\frac{d}{dX}\right)^n \{X^a f(X)^b X^{pc}\} \\ = X^{pc} \{X(1-X)\}^n \left(\frac{d}{dX}\right)^n \{X^a f(X)^b\}. \end{aligned}$$

We may now apply Leibnitz' formula, using Lemma 2 together with the fact that

$$\{X(1-X)\}^g \left(\frac{d}{dX}\right)^g X^a$$

either vanishes (if  $g > a$ ) or is a polynomial of degree  $a + g$ . It follows that  $\{X(1-X)\}^n \left(\frac{d}{dX}\right)^n \{X^a f(X)^b\}$  is a linear combination of terms

$$\hat{q}(X) q_{g_1}(X) \dots q_{g_l}(X) f(X)^{b-l}$$

modulo  $X^p - X$ , where

$$0 \leq l \leq \min(b, n),$$

$$\deg q_{g_i}(X) \leq g_i + 1, \quad (1 \leq i \leq l),$$

and

$$\deg \hat{q}(X) = a + n - g_1 - \dots - g_l.$$

Since  $X^{pc} \equiv X^c \pmod{X^p - X}$  we can now write

$$\begin{aligned} \{X(1-X)\}^n \left(\frac{d}{dX}\right)^n \{X^a f(X)^b X^{pc}\} \\ \equiv \sum_{0 \leq \beta < B} P_\beta(X; a, b, c, n) f(X)^\beta \pmod{X^p - X}, \end{aligned}$$

with  $\deg P_\beta(X) < A + 2n + C$ . Hence if

$$P(X; a, b, c, n, r) = \sum_{0 \leq \beta < B} P_\beta(X; a, b, c, n) r^\beta$$

we deduce that

$$\left. \{X(1-X)\}^n \frac{d^n}{dX^n} \{X^a f(X)^b X^{pc}\} \right|_{X=k} = P(k; a, b, c, n, r)$$

for any  $k \in S_r$ . Here we use the observation that  $k^p - k = 0$  for any such  $k$ .

We now write

$$\Phi(X, Y, Z) = \sum_{a,b,c} \lambda_{a,b,c} X^a f(X)^b X^{pc}$$

and

$$P_n(X) = \sum_{a,b,c} \lambda_{a,b,c} P(X; a, b, c, n, r),$$

so that  $\deg P_n(X) < A + 2n + C$  and

$$\{X(1-X)\}^n \frac{d^n}{dX^n} \Phi(X, f(X), X^p) \Big|_{X=k} = P_n(k)$$

for any  $k \in S_r$ . We shall arrange, by appropriate choice of the coefficients  $\lambda_{a,b,c}$ , that  $P_n(X)$  vanishes identically for  $n < D$ . This will ensure that (2) holds for  $k \in S_r$ . Each polynomial  $P_n(X)$  has at most  $A + 2n + C \leq A + 2D + C$  coefficients, which are linear forms in the original  $\lambda_{a,b,c}$ . Thus if

$$D(A + 2D + C) < ABC \tag{3}$$

there will be a set of coefficients  $\lambda_{a,b,c}$ , not all zero, for which the polynomials  $P_n(X)$  vanish for all  $n < D$ .

We must now consider whether  $\Phi(X, f(X), X^p)$  can vanish if  $\Phi(X, Y, Z)$  does not. We shall write

$$\Phi(X, Y, Z) = \sum_c F_c(X, Y) Z^c,$$

and take  $c_0$  to be the smallest value of  $c$  for which  $F_c(X, Y)$  is not identically zero. It follows that

$$\Phi(X, f(X), X^p) = X^{pc_0} \sum_{c_0 \leq c < C} F_c(X, f(X)) X^{p(c-c_0)},$$

so that if  $\Phi(X, f(X), X^p)$  is identically zero we must have

$$F_{c_0}(X, f(X)) \equiv 0 \pmod{X^p}.$$

This will contradict Lemma 3, providing that

$$AB \leq p, \tag{4}$$

as we now assume.

Finally we conclude that (1) holds, subject to the conditions (3) and (4). One readily sees that a suitable choice of parameters is

$$A = [p^{2/3}], \quad B = C = [p^{1/3}], \quad D = [\frac{1}{3}p^{2/3}].$$

These are satisfactory if  $p$  is large enough, and then (1) yields  $N_r \ll p^{2/3}$  as required for Lemma 4.

### 3 Proof of Lemmas 2 and 3

For the proof of Lemma 2 a simple induction argument suffices. For  $r = 1$  we have

$$X(1 - X) \frac{d}{dX} f(X) = X - X^p,$$

so that we may take  $q_1(X) = 0$  and  $h_1(X) = -1$ . For the general case we differentiate the formula

$$\{X(1 - X)\}^r \left(\frac{d}{dX}\right)^r f(X) = q_r(X) + (X^p - X)h_r(X)$$

and multiply by  $X(1 - X)$  to obtain

$$\begin{aligned} & \{X(1 - X)\}^{r+1} \left(\frac{d}{dX}\right)^{r+1} f(X) + r(1 - 2X)\{X(1 - X)\}^r \left(\frac{d}{dX}\right)^r f(X) \\ &= X(1 - X)q_r'(X) - X(1 - X)h_r(X) + (X^p - X)X(1 - X)h_r'(X). \end{aligned}$$

This allows us to set

$$q_{r+1}(X) = X(1 - X)q_r'(X) - X(1 - X)h_r(X) - r(1 - 2X)q_r(X)$$

and

$$h_{r+1}(X) = X(1 - X)h_r'(X) - r(1 - 2X)h_r(X).$$

The required bounds for  $\deg q_r(X)$  and  $\deg h_r(X)$  then follow by induction.

The proof of Lemma 3 is more difficult. We shall use the following auxilliary result.

**Lemma 5** *Let  $F(X, Y) \in \mathbb{Z}_p[X, Y]$ . Let  $\deg_X F = m \geq 0$  and  $\deg_Y F = n \geq 1$  and suppose that  $m, n < p$ . Then*

$$(1 - X)^{m+1} \left(\frac{d}{dX}\right)^{m+1} F(X, f(X)) \equiv G(X, f(X)) \pmod{X^{p-1-m}},$$

for some  $G(X, Y) \in \mathbb{Z}_p[X, Y]$  with  $\deg_X G \leq m$  and  $\deg_Y G = n - 1$ . In particular  $G$  does not vanish identically.

To prove this result it will suffice to show that

$$\begin{aligned} & (1 - X)^{m+1} \left(\frac{d}{dX}\right)^{m+1} X^a f(X)^b \\ & \equiv G(X, f(X); a, b) \pmod{X^{p-1-m}}, \quad (a \leq m, b \leq n) \end{aligned} \quad (5)$$

with

$$\deg_X G(X, Y; a, b) \leq a, \quad \deg_Y G(X, Y; a, b) \leq b - 1,$$

and such that the coefficient of  $X^a Y^{b-1}$  in  $G(X, Y; a, b)$  is non-zero.

In order to establish (5) we apply Leibnitz' formula, observing that

$$(1 - X)^k \left(\frac{d}{dX}\right)^k X^a$$

is either identically zero (if  $k > a$ ) or is a polynomial of degree  $a$ , and that

$$\begin{aligned} (1 - X)^l \left(\frac{d}{dX}\right)^l f(X) &= (1 - X)^l \left(\frac{d}{dX}\right)^{l-1} \{1 + X + \dots + X^{p-2}\} \\ &= (1 - X)^l \left(\frac{d}{dX}\right)^{l-1} \left\{ \frac{1}{1 - X} + O(X^{p-1}) \right\} \\ &= (1 - X)^l \left\{ \frac{(l-1)!}{(1 - X)^l} + O(X^{p-l}) \right\} \\ &= (l-1)! + O(X^{p-l}) \end{aligned} \quad (6)$$

for  $l \geq 1$ . One can therefore see that

$$\deg_X G(X, Y; a, b) \leq a, \quad \deg_Y G(X, Y; a, b) \leq b,$$

in (5). To check that  $\deg_Y G(X, Y; a, b) \neq b$  we use Leibnitz' formula to write

$$\left(\frac{d}{dX}\right)^{m+1} X^a f(X)^b = \sum_{k=0}^{m+1} \binom{m+1}{k} \left(\frac{d}{dX}\right)^k X^a \left(\frac{d}{dX}\right)^{m+1-k} f(X)^b$$

and

$$\left(\frac{d}{dX}\right)^{m+1} f(X)^b = \sum_{k_1, \dots, k_b} \binom{m+1-k}{k_1, \dots, k_b} \left\{ \left(\frac{d}{dX}\right)^{k_1} f(X) \right\} \dots \left\{ \left(\frac{d}{dX}\right)^{k_b} f(X) \right\},$$

where  $k_1 + \dots + k_b = m + 1 - k$  and

$$\binom{m+1-k}{k_1, \dots, k_b} = \frac{(m+1-k)!}{k_1! \dots k_b!}$$

is a multinomial coefficient. We now see that terms with  $k > a$  vanish identically. Moreover, if  $k \leq a$  then  $m + 1 - k \geq m + 1 - a > 0$ , so that  $k_i > 0$  for some index  $i$ . It follows that there will be no term involving  $f(X)^b$  in (5).

Finally we have to examine the coefficient of  $X^a f(X)^{b-1}$ , which arises in the above formulae from those terms in which precisely one of the  $k_i$  is non-zero. Since  $k$  can be at most  $a$  if we are to have a non-zero contribution, we see, using (6), that the required coefficient is

$$\begin{aligned} b \sum_{k=0}^a \binom{m+1}{k} (-1)^k \frac{a!}{(a-k)!} (m-k)! \\ = b(m-a)! a! \sum_{k=0}^a (-1)^k \binom{m+1}{k} \binom{m-k}{m-a}. \end{aligned} \quad (7)$$

It remains to determine whether or not this expression vanishes in  $\mathbb{Z}_p$ . To this end we consider the expansion

$$\begin{aligned}
\frac{1 - X^{m+1}}{1 - X} &= (1 - X)^{-1} - \left(\frac{1}{1 - X} - 1\right)^{m+1} (1 - X)^m \\
&= (1 - X)^{-1} + \left\{ \sum_{k=0}^{m+1} (-1)^{m-k} \binom{m+1}{k} \left(\frac{1}{1 - X}\right)^k \right\} (1 - X)^m \\
&= \sum_{k=0}^m (-1)^{m-k} \binom{m+1}{k} (1 - X)^{m-k} \\
&= \sum_{k=0}^m (-1)^{m-k} \binom{m+1}{k} \sum_{j=0}^{m-k} (-1)^j \binom{m-k}{j} X^j.
\end{aligned}$$

Now the sum over  $k$  on the right of (7) is just the coefficient of  $X^{m-a}$  in the final expression above, apart from a factor  $(-1)^a$ . Moreover

$$\frac{1 - X^{m+1}}{1 - X} = 1 + X + \dots + X^m$$

so that the coefficient of  $X^{m-a}$  is just 1. We can therefore conclude that

$$b(m-a)! a! \sum_{k=0}^a (-1)^k \binom{m+1}{k} \binom{m-k}{m-a} = (-1)^a b(m-a)! a!.$$

Since this is non-zero in  $\mathbb{Z}_p$  for  $b, m < p$  the lemma now follows.

It remains to derive Lemma 3 from Lemma 5. We shall take a non-zero polynomial  $F(X, Y) \in \mathbb{Z}_p[X, Y]$  with  $\deg_X F = m$  and  $\deg_Y F = n$ . Using induction on  $n$  we shall show that  $X^{(m+1)(n+1)} \nmid F(X, f(X))$  providing that  $(m+1)(n+1) \leq p$ . This clearly suffices for Lemma 3. When  $n = 0$  the result is obvious. Suppose now that the result has been proved when  $n$  is replaced by  $n - 1$ . If  $F$  is as above but  $X^{(m+1)(n+1)} \mid F(X, f(X))$  then

$$X^{(m+1)n} \left| (1 - X)^{m+1} \left(\frac{d}{dX}\right)^{m+1} F(X, f(X)). \right.$$

In the notation of Lemma 5 this yields  $X^{(m+1)n} \mid G(X, f(X))$ , in view of the fact that  $(m+1)n \leq p - (m+1)$ . Moreover we will have  $\deg_X G = m' \leq m$ , and  $\deg_Y G = n - 1$ . However we now have  $X^{(m'+1)n} \mid G(X, f(X))$ , contradicting the induction hypothesis. It therefore follows that  $X^{(m+1)(n+1)} \nmid F(X, f(X))$  as required for the induction step. This completes the proof of our assertion, and with it the proof of Lemma 3.

## 4 Acknowledgement

This paper was prepared while the author was a guest of the Mathematics Department of Oklahoma State University. Their support is gratefully acknowledged.

## References

- [1] D.A. Burgess, On character sums and  $L$ -functions. II., *Proc. London Math. Soc.* (3), 13 (1963), 524-536.
- [2] D.A. Mit'kin, An estimate for the number of roots of some comparisons by the Stepanov method, *Mat. Zametki*, 51 (1992), 52-58, 157. (Translated as *Math. Notes*, 51 (1992), 565-570.)
- [3] R.W.K. Odoni, Trigonometric sums of Heilbronn's type, *Math. Proc. Camb. Phil. Soc.*, 98 (1985), 389-396.
- [4] S.A. Stepanov, The number of points of a hyperelliptic curve over a prime field, *Izv. Akad. Nauk SSSR Ser. Mat.*, 33 (1969), 1171-1181.