ACTA ARITHMETICA
LXXIX.4 (1997)

On the average of character sums for a group of characters

by

D. A. Burgess (Nottingham)

To J. W. S. Cassels

1. Introduction. Let r, k, h be positive integers. For any Dirichlet character χ modulo k write

$$W_r(\chi) = \sum_{x=1}^{k} \Big| \sum_{m=1}^{h} \chi(x+m) \Big|^{2r}.$$

In [2] it was shown that, if χ is a primitive character, then

$$W_2(\chi) \ll kh^2 + k^{1/2+\varepsilon} h^4, \tag{1}$$

which implies that

$$W_2(\chi) \ll k^{1+\varepsilon} h^2 \tag{2}$$

for $h \le k^{1/4}$. In [6] it was shown that

$$\sum_{\text{primitive}\,\chi\,(\text{mod}\,k)} W_2(\chi) \ll k^{2+\varepsilon} h^2, \tag{3}$$

so that (2) holds for all h, on average for all primitive characters modulo k. Thus it is reasonable to conjecture that (2) might hold for some $h > k^{1/4}$, on average for the primitive characters of a large subgroup of the characters modulo k. In [8] such a result was obtained, it being shown that, for any prime p,

$$\sum_{\substack{\chi \bmod p^3 \\ \chi^{p^2} = \chi_0}} W_2(\chi) \ll p^5 h^2 + p^3 h^4, \tag{4}$$

where χ_0 is the principal character, and thus (2) holds for $h \le k^{1/3}$, on average for the characters modulo $k = p^3$ in the group of order p^2.

1991 *Mathematics Subject Classification*: Primary 11L40.

In this paper the argument is strengthened to show in the following theorem that, for the non-principal characters of this group, (2) remains true for $h \le k^{1/2}$, on average.

THEOREM 1. *Let p be an odd prime number. Let*

$$S = \sum_{\substack{\chi \bmod p^3 \\ \chi^{p^2}=\chi_0 \\ \chi \ne \chi_0}} \sum_{x=1}^{p^3} \Big| \sum_{m=1}^{h} \chi(x+m) \Big|^{2r}.$$

Then in the case $r = 2$ we have

$$S \ll p^2 h^4 + p^5 h^2.$$

From [1] it follows that if k is prime then

$$W_3(\chi) \ll kh^3 + k^{1/2} h^6 \tag{5}$$

for all positive h. By the methods of this paper it is shown that (5) can be improved for $h > p^{3/4}$, on average for the non-principal characters modulo $k = p^3$ in the group of order p^2.

THEOREM 2. *Let p be an odd prime number. Let*

$$S = \sum_{\substack{\chi \bmod p^3 \\ \chi^{p^2}=\chi_0 \\ \chi \ne \chi_0}} \sum_{x=1}^{p^3} \Big| \sum_{m=1}^{h} \chi(x+m) \Big|^{2r}.$$

Then in the case $r = 3$ we have

$$S \ll p^2 h^6 + \min(h,p)^3 p^5 h + \min(h,p)^2 p^6.$$

In Section 8 we shall describe some corollaries of these theorems.

2. Preliminary transformation of the problem. For S as in the statement of both theorems, we have

$$S = \sum_{\substack{\chi \bmod p^3 \\ \chi^{p^2}=\chi_0}} \sum_{x=1}^{p^3} \Big| \sum_{m=1}^{h} \chi(x+m) \Big|^{2r} - \sum_{x=1}^{p^3} \Big(\sum_{m=1}^{h} \chi_0(x+m) \Big)^{2r} = S_1 - S_2, \tag{6}$$

say.

Now

$$S_2 = \sum_{\boldsymbol{m}} \sum_{x=1}^{p^3} \chi_0(f_1(x)) \chi_0(f_2(x)),$$

where $\boldsymbol{m} \in \mathbb{Z}^{2r}$ satisfies $0 < m_i \le h$ for $1 \le i \le 2r$, and

$$f_1(x) = (x+m_1)\dots(x+m_r), \qquad f_2(x) = (x+m_{r+1})\dots(x+m_{2r}).$$

Thus

$$S_2 = \sum_{\boldsymbol{m}} \sum_{\substack{x=1 \\ x\not\equiv -m_i \ (\mathrm{mod}\, p)}}^{p^3} 1 = \sum_{\boldsymbol{m}} p^2 \#\{x : 1 \le x \le p,\ p \nmid f_1(x) f_2(x)\}. \tag{7}$$

We also have

$$S_1 = \sum_{\boldsymbol{m}} \sum_{x=1}^{p^3} \sum_{\chi^{p^2}=\chi_0} \chi(f_1(x))\overline{\chi}(f_2(x)) = \sum_{\boldsymbol{m}} \sum_{\substack{x=1 \\ p\nmid f_1(x)f_2(x)}}^{p^3} \sum_{\chi^{p^2}=\chi_0} \chi\left(\frac{f_1(x)}{f_2(x)}\right)$$

$$= p^2 \sum_{\boldsymbol{m}} \#\{1 \le x \le p^3, 1 \le z < p : p \nmid f_1(x) f_2(x),$$
$$f_1(x) - z^{p^2} f_2(x) \equiv 0 \ (\mathrm{mod}\, p^3)\}.$$

Thus, writing

$$f_{(z)}(x) = f_1(x) - z^{p^2} f_2(x), \tag{8}$$

we have

$$S_1 = S_3 + S_4, \tag{9}$$

where

$$S_3 = p^2 \sum_{\boldsymbol{m}} \sum_{z=1}^{p-1} \#\{1 \le x \le p^3 : x \not\equiv -m_i \ (\mathrm{mod}\, p),$$
$$f_{(z)}(x) \equiv 0 \ (\mathrm{mod}\, p^3),\ f'_{(z)}(x) \not\equiv 0 \ (\mathrm{mod}\, p)\} \tag{10}$$

and

$$S_4 = p^2 \sum_{\boldsymbol{m}} \sum_{z=1}^{p-1} \#\{1 \le x \le p^3 : x \not\equiv -m_i \ (\mathrm{mod}\, p),$$
$$f_{(z)}(x) \equiv 0 \ (\mathrm{mod}\, p^3),\ f'_{(z)}(x) \equiv 0 \ (\mathrm{mod}\, p)\}. \tag{11}$$

We consider the non-singular roots of $f_{(z)}$. Since the numbers of non-singular roots modulo p^3 and p are the same we have from (10) that

$$S_3 \le p^2 \sum_{\boldsymbol{m}} \sum_{z=1}^{p-1} \#\{1 \le x \le p : p \nmid f_1(x) f_2(x),\ f_{(z)}(x) \equiv 0 \ (\mathrm{mod}\, p)\}$$

$$= p^2 \sum_{\boldsymbol{m}} \sum_{\substack{x=1 \\ p\nmid f_1(x)f_2(x)}}^{p} \#\{1 \le z < p : f_1(x) - z f_2(x) \equiv 0 \ (\mathrm{mod}\, p)\}$$

$$= p^2 \sum_{\boldsymbol{m}} \#\{1 \le x \le p : p \nmid f_1(x) f_2(x)\} = S_2$$

from (7). Now from (6) and (9) we have

$$S \le S_4. \tag{12}$$

3. Estimates for solution sets of polynomials. In the proof of our theorems we shall require some lemmas concerning the number of solutions of congruences to a prime power modulus. We shall use the following generalisation of the well known estimate for the number of non-singular roots of a congruence.

LEMMA 1. *Let F be a polynomial of degree n having integer coefficients. Let p be a prime, d a positive integer, and α, β and γ be non-negative integers satisfying $\gamma = \lceil \alpha/d \rceil$. Then*

$$\#\{1 \le x \le p^{\gamma} : p^{\alpha+\beta} \mid F(x),\ p^{\beta} \parallel F^{(d)}(x)\} \le n.$$

Proof. This is Proposition 1 of [7].

We shall require an estimate for the number of solutions of a congruence in many variables to a prime modulus. The following will suffice.

LEMMA 2. *Let G be a polynomial in $x_1, \ldots, x_t$ which is not identically zero modulo the prime p. Let $0 < h_i \le p$ for all i. Then the number of $\boldsymbol{x}$, satisfying $0 < x_i \le h_i$ for all i, for which $G(\boldsymbol{x}) \equiv 0 \pmod p$ is $O((\prod h_i)/\min h_i)$.*

Proof. This is an easy modification of Lemma 5 of [4].

We shall also use the following estimate which, under favourable conditions, can provide an optimal estimate for the average number of singular roots of a set of polynomials.

LEMMA 3. *Let $F_i(\boldsymbol{y})$ $(0 < i \le n)$ be polynomials in ν variables y_k $(0 < k \le \nu)$. Let p be a prime and $2\beta \ge \alpha_1 \ge \ldots \ge \alpha_m > \beta \ge \alpha_{m+1} \ge \ldots \ge \alpha_n$ be positive integers. Let $\boldsymbol{H} \in \mathbb{N}^{\nu}$. Write*

$$N = \#\{\boldsymbol{y} : \forall k \le \nu\ 0 < y_k \le H_k,\ \forall i\ F_i(\boldsymbol{y}) \equiv 0 \pmod{p^{\alpha_i}}\}.$$

Put $\lambda_k = \lceil H_k/p^{\beta} \rceil$ for all $k \le \nu$. Then

$$N \ll \sum_{\substack{\boldsymbol{B} \\ \forall k \le \nu\ |B_k| < \lambda_k}} \#\bigg\{\boldsymbol{y} : \forall k \le \nu\ 0 < y_k \le p^{\beta},\ \forall i \le m\ F_i(\boldsymbol{y}) \equiv 0 \pmod{p^{\beta}},$$

$$\forall i > m\ F_i(\boldsymbol{y}) \equiv 0 \pmod{p^{\alpha_i}},\ \forall i \le m\ \sum_{k=1}^{\nu} B_k \frac{\partial F_i}{\partial y_k}(\boldsymbol{y}) \equiv 0 \pmod{p^{\alpha_i - \beta}}\bigg\}.$$

Proof. Clearly

$$N \le \#\{\boldsymbol{y} : \forall k \le \nu\ 0 < y_k \le \lambda_k p^{\beta},\ \forall i\ F_i(\boldsymbol{y}) \equiv 0 \pmod{p^{\alpha_i}}\}.$$

For $1 \le k \le \nu$ write $y_k = a_k + p^\beta b_k$, where $0 < a_k \le p^\beta$, $0 \le b_k < \lambda_k$. Then, for $m < i \le n$, $F_i(\boldsymbol{y}) \equiv 0 \pmod{p^{\alpha_i}}$ becomes

$$F_i(\boldsymbol{a}) \equiv 0 \pmod{p^{\alpha_i}},$$

while for $i \le m$, $F_i(\boldsymbol{y}) \equiv 0 \pmod{p^{\alpha_i}}$ becomes

$$F_i(\boldsymbol{a}) + \sum_{k=1}^{\nu} \frac{\partial F_i}{\partial y_k}(\boldsymbol{a}) b_k p^\beta \equiv 0 \pmod{p^{\alpha_i}}.$$

The latter congruences imply, for $i \le m$,

$$F_i(\boldsymbol{a}) \equiv 0 \pmod{p^\beta}$$

so that, say,

$$\forall i \le m \quad F_i(\boldsymbol{a}) = c_i(\boldsymbol{a}) p^\beta.$$

Thus we have

$$N \le \sum_{\substack{\boldsymbol{a} \\ \forall i \le m\ F_i(\boldsymbol{a}) \equiv 0 \pmod{p^\beta} \\ \forall i > m\ F_i(\boldsymbol{a}) \equiv 0 \pmod{p^{\alpha_i}}}} \#\Big\{\boldsymbol{b} : \forall k \le \nu\ 0 \le b_k < \lambda_k,\ \forall i \le m\ \sum_{k=1}^{\nu} \frac{\partial F_i}{\partial y_k}(\boldsymbol{a}) b_k \equiv -c_k(\boldsymbol{a}) \pmod{p^{\alpha_i - \beta}}\Big\}.$$

Now the number of solutions of the inhomogeneous congruences

$$\forall i \le m \quad \sum_{k=1}^{\nu} \frac{\partial F_i}{\partial y_k}(\boldsymbol{a}) b_k \equiv -c_k(\boldsymbol{a}) \pmod{p^{\alpha_i - \beta}}$$

in the variables $\boldsymbol{b}$ satisfying $0 \le b_k < \lambda_k$ for all $k \le \nu$ is at most the number of solutions of the homogeneous congruences

$$\forall i \le m \quad \sum_{k=1}^{\nu} \frac{\partial F_i}{\partial y_k}(\boldsymbol{a}) B_k \equiv 0 \pmod{p^{\alpha_i - \beta}}$$

in the variables $\boldsymbol{B}$ satisfying $|B_k| < \lambda_k$ for all $k \le \nu$. Thus we have

$$N \le \sum_{\substack{\boldsymbol{a} \\ \forall i \le m\ F_i(\boldsymbol{a}) \equiv 0 \pmod{p^\beta} \\ \forall i > m\ F_i(\boldsymbol{a}) \equiv 0 \pmod{p^{\alpha_i}}}} \#\Big\{\boldsymbol{B} : \forall k \le \nu\ |B_k| < \lambda_k,\ \forall i \le m\ \sum_{k=1}^{\nu} \frac{\partial F_i}{\partial y_k}(\boldsymbol{a}) B_k \equiv 0 \pmod{p^{\alpha_i - \beta}}\Big\}$$

$$\le \sum_{\substack{\boldsymbol{B} \\ \forall k \le \nu\ |B_k| < \lambda_k}} \#\Big\{\boldsymbol{a} : \forall k \le \nu\ 0 < a_k \le p^\beta,\ \forall i \le m\ F_i(\boldsymbol{a}) \equiv 0 \pmod{p^\beta},\ \forall i > m\ F_i(\boldsymbol{a}) \equiv 0 \pmod{p^{\alpha_i}},\ \forall i \le m\ \sum_{k=1}^{\nu} B_k \frac{\partial F_i}{\partial y_k}(\boldsymbol{a}) \equiv 0 \pmod{p^{\alpha_i - \beta}}\Big\}.$$

4. Proof of Theorem 1. Clearly in proving the theorem we may suppose that $p > 2$. We consider here the case $r = 2$.

It remains to consider the singular roots. Noting (11) we write

$$S_4 = S_5 + S_6, \tag{13}$$

where

$$S_5 = p^2 \sum_{\boldsymbol{m}} \#\{1 \le x \le p^3,\ 1 \le z < p : x \not\equiv -m_i \pmod p,$$
$$f_{(z)}(x) \equiv 0 \pmod{p^3},\ f'_{(z)}(x) \equiv 0 \pmod p,\ f''_{(z)}(x) \equiv 0 \pmod p\},$$

and

$$S_6 = p^2 \sum_{\boldsymbol{m}} \sum_{z=2}^{p-1} \#\{1 \le x \le p^3 : x \not\equiv -m_i \pmod p,\ f_{(z)}(x) \equiv 0 \pmod{p^3},$$
$$f'_{(z)}(x) \equiv 0 \pmod p,\ f''_{(z)}(x) \not\equiv 0 \pmod p\}.$$

Clearly we have

$$S_5 \le p^2 \sum_{\boldsymbol{m}} \#\{1 \le x \le p^3 :$$
$$(m_1 + m_2 - m_3 - m_4)x + (m_1 m_2 - m_3 m_4) \equiv 0 \pmod{p^3},$$
$$(m_1 + m_2 - m_3 - m_4) \equiv 0 \pmod p\}.$$

Write

$$p^\delta = \text{highest common factor}(p^3, m_1 + m_2 - m_3 - m_4), \tag{14}$$

where $1 \le \delta \le 3$. For solubility of the congruence

$$(m_1 + m_2 - m_3 - m_4)x + (m_1 m_2 - m_3 m_4) \equiv 0 \pmod{p^3}$$

we require also

$$p^\delta \mid (m_1 m_2 - m_3 m_4). \tag{15}$$

The congruence then has at most p^δ solutions satisfying $1 \le x \le p^3$. (14) and (15) imply

$$(m_1 - m_3)(m_2 - m_3) \equiv 0 \pmod{p^\delta}.$$

Suppose that $p^\varepsilon \mid (m_1 - m_3)$ and $p^{\delta-\varepsilon} \mid (m_2 - m_3)$. Then the number of such $\boldsymbol{m}$ is

$$O\biggl(h\biggl(1 + \frac{h}{p^\varepsilon}\biggr)\biggl(1 + \frac{h}{p^{\delta-\varepsilon}}\biggr)\biggl(1 + \frac{h}{p^\delta}\biggr)\biggr) = O\biggl(\frac{h^4}{p^{2\delta}} + h^2\biggr).$$

Thus

$$S_5 \ll p^2 \sum_{\delta,\varepsilon} p^\delta \biggl(\frac{h^4}{p^{2\delta}} + h^2\biggr) \ll ph^4 + p^5 h^2. \tag{16}$$

On the other hand, we have

$$S_6 \ll p^2 \sum_{\boldsymbol{m}} \sum_{z=2}^{p-1} \#\{1 \le x \le p^3 : f_{(z)}(x) \equiv 0 \pmod{p^3},$$
$$f'_{(z)}(x) \equiv 0 \pmod{p},\ f''_{(z)}(x) \not\equiv 0 \pmod{p}\}.$$

Thus, by Lemma 1,

$$S_6 \ll p^3 \#\{\boldsymbol{m}, 1 < z < p : \exists x\ f_{(z)}(x) \equiv 0 \pmod{p^2},\ f'_{(z)}(x) \equiv 0 \pmod{p}\}.$$

Thus

$$\text{(17)}\qquad S_6 \ll p^3 \#\{\boldsymbol{m}, z, x : \forall i\ 0 < m_i \le h,\ 0 < x \le p,\ 0 < z < p,$$
$$f_{(z)}(x) \equiv 0 \pmod{p^2},\ f'_{(z)}(x) \equiv 0 \pmod{p}\}.$$

Put

$$\text{(18)}\qquad \lambda = \left\lceil \frac{h}{p} \right\rceil, \qquad \mu = \begin{cases} p & \text{if } \lambda > 1, \\ h & \text{if } \lambda = 1. \end{cases}$$

Now we apply Lemma 3, treating x, z as constants and the m_i as our variables, to obtain

$$\text{(19)}\qquad S_6 \ll p^3 \sum_{\substack{\boldsymbol{B} \\ \forall k \le 4\, |B_k| < \lambda}} \#\Big\{\boldsymbol{a}, x, z : \forall k \le 4\ 0 < a_k \le \mu,\ 0 < x \le p,$$
$$0 < z < p,\ f_{(z)}(x) \equiv 0 \pmod{p},$$
$$f'_{(z)}(x) \equiv 0 \pmod{p},\ \sum_{k=1}^{4} B_k \frac{\partial f_{(z)}}{\partial m_k}(x) \equiv 0 \pmod{p}\Big\}$$

if $\lambda > 1$, while if $\lambda = 1$ this follows immediately from (17).

Given $\boldsymbol{B}, x, z, a_3, a_4$ we have, from (19),

$$f'_{(z)}(x) \equiv 2(1-z)x + (a_1 + a_2 - za_3 - za_4) \equiv 0 \pmod{p},$$

from which $a_1 + a_2$ is determined modulo p. Then also from (19) we have

$$f_{(z)}(x) \equiv (1-z)x^2 + (a_1 + a_2 - za_3 - za_4)x + (a_1a_2 - za_3a_4) \equiv 0 \pmod{p},$$

and so a_1a_2 is also determined modulo p. Thus there are at most two choices for a_1, a_2. Use these congruences to eliminate a_1, a_2. We have on writing

$$\pi_1 = a_1 + a_2, \quad \pi_2 = a_1a_2, \quad \varrho_1 = a_3 + a_4, \quad \varrho_2 = a_3a_4,$$

the identity

$$(\pi_1^2 - 4\pi_2)(B_1 - B_2)^2 - (2B_2a_1 + 2B_1a_2 - \pi_1(B_1 + B_2))^2 = 0.$$

Now from (19) we have

$$\sum_{k=1}^{4} B_k \frac{\partial f_{(z)}(x)}{\partial m_k} \equiv (B_1 + B_2 - zB_3 - zB_4)x + (a_1B_2 + a_2B_1 - za_3B_4 - za_4B_3) \equiv 0 \pmod p.$$

Thus eliminating a_1, a_2 we have

(20) $$(z^2\varrho_1^2 - 4z\varrho_1(1-z)x - 4x^2z(1-z) - 4z\varrho_2)(B_1 - B_2)^2 - z^2(2(B_3a_4 + B_4a_3) + 2x(B_3 + B_4) - (\varrho_1 + 2x)(B_1 + B_2))^2 \equiv 0 \pmod p.$$

Thus from (19),

(21) $$S_6 \ll p^3 \sum_{\boldsymbol{B}} \#\{x, z, a_3, a_4 : (z^2\varrho_1^2 - 4z\varrho_1(1-z)x - 4x^2z(1-z) - 4z\varrho_2)(B_1 - B_2)^2 - z^2(2(B_3a_4 + B_4a_3) + 2x(B_3 + B_4) - (\varrho_1 + 2x)(B_1 + B_2))^2 \equiv 0 \pmod p\}.$$

By Lemma 2, for a given choice of $\boldsymbol{B}$, (20) has at most $O(p^2\mu)$ solutions in x, z, a_3, a_4, unless this polynomial is identically zero modulo p. If the coefficient of za_3a_4 is zero we have

$$-4(B_1 - B_2)^2 \equiv 0 \pmod p,$$

and thus $B_1 \equiv B_2 \pmod p$. Under this condition if the coefficient of $z^2a_3^2$ is zero we have

$$-(2B_4 - B_1 - B_2)^2 \equiv 0 \pmod p,$$

and if the coefficient of $z^2a_4^2$ is zero we have

$$-(2B_3 - B_1 - B_2)^2 \equiv 0 \pmod p.$$

Thus if the polynomial is identically zero modulo p we have

$$B_1 \equiv B_2 \equiv B_3 \equiv B_4 \pmod p.$$

Hence the number of such cases is $O(\lambda(1 + \lambda/p)^3)$.

Consequently, from (21) we have

$$S_6 \ll p^3\left(\lambda^4p^2\mu + \left(\lambda + \frac{\lambda^4}{p^3}\right)p^2\mu^2\right) \ll p^2h^4 + p^5h^2.$$

The theorem follows from (12), (13) and (16).

5. Introduction to proof of Theorem 2. We may suppose that $p > 2$. We consider here the case $r = 3$. Noting (11) we write

$$S_7 = \sum_{\boldsymbol{m}} \#\{x, z : 0 < x \le p^3,\ 0 < z < p,\ f_1(x) f_2(x) \not\equiv 0 \ (\mathrm{mod}\, p), \\ f_{(z)}(x) \equiv 0 \ (\mathrm{mod}\, p^3),\ f'_{(z)}(x) \equiv 0 \ (\mathrm{mod}\, p), \\ \text{either } f'_{(z)} \not\equiv 0 \ (\mathrm{mod}\, p^2) \text{ or } f''_{(z)}(x) \not\equiv 0 \ (\mathrm{mod}\, p)\} \tag{22}$$

and

$$S_8 = \sum_{\boldsymbol{m}} \#\{x, z : 0 < x \le p^3,\ 0 < z < p,\ f_1(x) f_2(x) \not\equiv 0 \ (\mathrm{mod}\, p), \\ f_{(z)}(x) \equiv 0 \ (\mathrm{mod}\, p^3),\ f'_{(z)}(x) \equiv 0 \ (\mathrm{mod}\, p^2),\ f''_{(z)}(x) \equiv 0 \ (\mathrm{mod}\, p)\} \tag{23}$$

so that

$$S_4 = p^2 S_7 + p^2 S_8. \tag{24}$$

We estimate S_7 and S_8 in Section 7.

We shall use also the polynomials $g_i(x)$ given by

$$\forall i \le 3 \quad g_i(x) = f_1(x)/(x + m_i), \qquad \forall i \ge 4 \quad g_i(x) = f_2(x)/(x + m_i).$$

Thus we have, from (8),

$$f_{(z)}(x) = g_1(x)(x + m_1) - z^{p^2} g_4(x)(x + m_4)$$

and

$$f'_{(z)}(x) = g_1(x) + g_2(x) + g_3(x) - z^{p^2} g_4(x) - z^{p^2} g_5(x) - z^{p^2} g_6(x).$$

Write

$$\begin{aligned}
C_1(\boldsymbol{m}) &= g_1(x)(x + m_1) - z g_4(x)(x + m_4), \\
C_2(\boldsymbol{m}) &= (2x + m_2 + m_3)(x + m_1) - z(2x + m_5 + m_6)(x + m_4) \\
&\quad + (g_1(x) - z g_4(x)), \\
C_3(\boldsymbol{m}) &= 2(x + m_1) - 2z(x + m_4) \\
&\quad + ((4x + 2m_2 + 2m_3) - z(4x + 2m_5 + 2m_6)), \\
C_4(\boldsymbol{m}) &= b_1 g_1(x) + b_2 g_2(x) + b_3 g_3(x) - b_4 z g_4(x) - b_5 z g_5(x) - b_6 z g_6(x) \\
&= (b_2(x + m_3) + b_3(x + m_2))(x + m_1) \\
&\quad - z(b_5(x + m_6) + b_6(x + m_5))(x + m_4) + (b_1 g_1(x) - b_4 z g_4(x))
\end{aligned}$$

and

$$\begin{aligned}
C_5(\boldsymbol{m}) &= b_1(2x + m_2 + m_3) + b_2(2x + m_1 + m_3) + b_3(2x + m_1 + m_2) \\
&\quad - b_4 z(2x + m_5 + m_6) - b_5 z(2x + m_4 + m_6) \\
&\quad - b_6 z(2x + m_4 + m_5) \\
&= (b_2 + b_3)(x + m_1) - z(b_5 + b_6)(x + m_4) \\
&\quad + (b_1(2x + m_2 + m_3) + b_2(x + m_3) + b_3(x + m_2) \\
&\quad - z b_4(2x + m_5 + m_6) - z b_5(x + m_6) - z b_6(x + m_5)).
\end{aligned}$$

We define λ and μ by (18).

6. Minor lemmas

LEMMA 4. *Write*

$$D_1 = \begin{vmatrix} g_1(x) & -zg_4(x) \\ 2x+m_2+m_3 & -z(2x+m_5+m_6) \end{vmatrix}. \tag{25}$$

Then

$$\sum_{\substack{\boldsymbol{b} \\ \forall i\, |b_i|<\lambda}} \#\{\boldsymbol{m}, x, z : 0 < m_i \le \mu,\ 0 < x \le p,\ 0 < z < p,$$
$$f_1(x)f_2(x) \not\equiv 0 \pmod p,\ C_1(\boldsymbol{m}) \equiv C_2(\boldsymbol{m}) \equiv 0 \pmod p,\ D_1 \equiv 0 \pmod p\} \ll p\mu^4\lambda^6.$$

P r o o f. From $C_1(\boldsymbol{m}) \equiv C_2(\boldsymbol{m}) \equiv D_1 \equiv 0 \pmod p$ it follows that

$$g_1(x) \equiv zg_4(x) \pmod p,$$

from which z is uniquely determined. Then from $C_1(\boldsymbol{m}) \equiv 0 \pmod p$ it follows that $m_1 = m_4$. Finally,

$$D_1 = z((m_5+m_6-m_2-m_3)x^2 + 2(m_5m_6-m_2m_3)x + m_5m_6(m_2+m_3) - m_2m_3(m_5+m_6)),$$

so that, by Lemma 2, $D_1/z \equiv 0 \pmod p$ has $O(p\mu^3)$ solutions as a function of m_2, m_3, m_5, m_6, x. Thus the required estimate follows trivially.

LEMMA 5. *Write*

$$D_2 = \begin{vmatrix} m_2m_3 & -zm_5m_6 & 0 \\ m_2+m_3 & -z(m_5+m_6) & m_2m_3 - zm_5m_6 \\ b_2m_3+b_3m_2 & -zb_5m_6 - zb_6m_5 & b_1m_2m_3 - b_4zm_5m_6 \end{vmatrix}.$$

Then

$$\sum_{\substack{\boldsymbol{b} \\ \forall i\, |b_i|<\lambda \\ D_2 \text{ identically } 0 \pmod p}} \#\{m_2, m_3, m_5, m_6, x, z : 0 < m_i \le \mu,\ 0 < x \le p,\ 0 < z < p\} \ll p^2\mu^4\lambda\left(\frac{\lambda}{p}+1\right)^5.$$

P r o o f. We have

$$\begin{aligned} D_2 = {} & (b_6-b_1)zm_2^2m_3^2m_5 + (b_5-b_1)zm_2^2m_3^2m_6 + (b_1-b_3)zm_2^2m_3m_5m_6 \\ & + (b_1-b_2)zm_2m_3^2m_5m_6 + (b_4-b_6)z^2m_2m_3m_5^2m_6 \\ & + (b_4-b_5)z^2m_2m_3m_5m_6^2 + (b_3-b_4)z^2m_2m_5^2m_6^2 \\ & + (b_2-b_4)z^2m_3m_5^2m_6^2. \end{aligned}$$

This is identically $0 \pmod p$ only if

$$b_1 \equiv b_2 \equiv b_3 \equiv b_4 \equiv b_5 \equiv b_6 \pmod p.$$

The required estimate follows trivially.

LEMMA 6. *We have*

$$\sum_{\substack{\boldsymbol{b}\\ \forall i\,|b_i|<\lambda}} \#\{\boldsymbol{m}, x, z : 0 < m_i \le \mu,\ 0 < x \le p,\ 0 < z < p,\ f_1(x)f_2(x) \not\equiv 0 \ (\mathrm{mod}\, p),\ C_1(\boldsymbol{m}) \equiv C_2(\boldsymbol{m}) \equiv C_3(\boldsymbol{m}) \equiv 0 \ (\mathrm{mod}\, p),\ D_1 \equiv 0 \ (\mathrm{mod}\, p)\} \ll p\mu^3\lambda^6,$$

where D_1 is defined by (25).

Proof. From $C_1(\boldsymbol{m}) \equiv C_2(\boldsymbol{m}) \equiv D_1 \equiv 0 \ (\mathrm{mod}\, p)$ it follows that

$$g_1(x) \equiv z g_4(x) \ (\mathrm{mod}\, p),$$

from which z is uniquely determined. Then from $C_1(\boldsymbol{m}) \equiv 0 \ (\mathrm{mod}\, p)$ it follows that $m_1 = m_4$ and, since $f_1(x)f_2(x) \not\equiv 0 \ (\mathrm{mod}\, p)$, from $C_2(\boldsymbol{m}) \equiv 0 \ (\mathrm{mod}\, p)$ that

$$(2x + m_2 + m_3) - z(2x + m_5 + m_6) \equiv 0 \ (\mathrm{mod}\, p).$$

Now substituting into $C_3(\boldsymbol{m}) \equiv 0 \ (\mathrm{mod}\, p)$ we obtain $z = 1$ and so also $m_2 + m_3 \equiv m_5 + m_6 \ (\mathrm{mod}\, p)$. But also we have $g_1(x) \equiv g_4(x) \ (\mathrm{mod}\, p)$ and so $m_2 m_3 \equiv m_5 m_6 \ (\mathrm{mod}\, p)$. Thus m_2, m_3 is a permutation of m_5, m_6. The required estimate follows trivially.

LEMMA 7. *Write*

$$D_3 = \begin{vmatrix} g_1(x) & g_4(x) & 0 \\ 2x + m_2 + m_3 & 2x + m_5 + m_6 & g_1(x) \\ 1 & 1 & 2x + m_2 + m_3 \end{vmatrix}$$

and

$$D_4 = \begin{vmatrix} g_1(x) & g_4(x) & 0 \\ 2x + m_2 + m_3 & 2x + m_5 + m_6 & g_4(x) \\ 1 & 1 & 2x + m_5 + m_6 \end{vmatrix}.$$

Then

$$\sum_{\substack{\boldsymbol{b}\\ \forall i\,|b_i|<\lambda}} \#\{m_2, m_3, m_5, m_6, x : 0 < m_i \le \mu,\ 0 < x \le p,\ D_3 \equiv D_4 \equiv 0 \ (\mathrm{mod}\, p)\} \ll p\mu^2\lambda^6.$$

Proof. The conditions $D_3 \equiv D_4 \equiv 0 \ (\mathrm{mod}\, p)$ expand to give

$$\begin{aligned}
&(g_1(x) - g_4(x))((2x + m_5 + m_6)(2x + m_2 + m_3) - g_1(x)) \\
&\qquad - g_4(x)(m_2 + m_3 - m_5 - m_6)(2x + m_2 + m_3) \\
&\equiv (g_1(x) - g_4(x))((2x + m_5 + m_6)^2 - g_4(x)) \\
&\qquad - g_4(x)(m_2 + m_3 - m_5 - m_6)(2x + m_5 + m_6) \equiv 0 \ (\mathrm{mod}\, p).
\end{aligned}$$

These will have only $O(1)$ solutions x unless both polynomials are identically $0 \pmod p$. But in the first of these the coefficient of x^3 is $m_2+m_3-m_5-m_6$, and if this is $0 \pmod p$ then the coefficient of x^2 is $3(m_2m_3-m_5m_6)$. Thus if both polynomials in x are identically $0 \pmod p$ then the pair m_2, m_3 is a permutation of m_5, m_6. This contributes

$$\ll \lambda^6 p \mu^2 \tag{26}$$

to our estimate.

Now consider the other case in which at least one of D_3 and D_4 is not identically $0 \pmod p$. Then there are only $O(1)$ values for x. The two polynomial congruences $D_3 \equiv D_4 \equiv 0 \pmod p$ are cubics. The difference between these polynomials is

$$\begin{vmatrix} g_1(x) & g_4(x) & 0 \\ 2x+m_2+m_3 & 2x+m_5+m_6 & g_1(x)-g_4(x) \\ 1 & 1 & m_2+m_3-m_5-m_6 \end{vmatrix}.$$

By row and column operations this simplifies to

$$\begin{vmatrix} m_2m_3 & m_5m_6 & 0 \\ m_2+m_3 & m_5+m_6 & m_2m_3-m_5m_6 \\ 1 & 1 & m_2+m_3-m_5-m_6 \end{vmatrix},$$

which is a polynomial in m_2, m_3, m_5, m_6. This polynomial is -1 when $m_2 = m_3 = 1$, $m_5 = m_6 = 0$. Thus it is not identically $0 \pmod p$ and so has $O(\mu^3)$ solutions in m_2, m_3, m_5, m_6. Thus this contributes

$$\ll \lambda^6 \mu^3 \tag{27}$$

to our estimate. The lemma follows from (26) and (27).

Lemma 8. *Write*

$$\begin{aligned} D_5 = &\begin{vmatrix} m_2m_3 & -m_5m_6 & 0 \\ m_2+m_3 & -(m_5+m_6) & m_2m_3 \\ b_2m_3+b_3m_2 & -b_5m_6-b_6m_5 & b_1m_2m_3 \end{vmatrix} \\ &\times \begin{vmatrix} m_2m_3-m_5m_6 & m_5m_6 & 0 \\ m_2+m_3-m_5-m_6 & m_5+m_6 & m_5m_6 \\ 0 & 1 & m_5+m_6 \end{vmatrix} \\ &- \begin{vmatrix} m_2m_3 & -m_5m_6 & 0 \\ m_2+m_3 & -(m_5+m_6) & m_5m_6 \\ b_2m_3+b_3m_2 & -b_5m_6-b_6m_5 & b_4m_5m_6 \end{vmatrix} \\ &\times \begin{vmatrix} m_2m_3-m_5m_6 & m_5m_6 & 0 \\ m_2+m_3-m_5-m_6 & m_5+m_6 & m_2m_3 \\ 0 & 1 & m_2+m_3 \end{vmatrix}. \end{aligned}$$

Then

$$\sum_{\substack{\boldsymbol{b}\\ \forall i\, |b_i|<\lambda\\ D_5\ \textit{identically}\ 0\ (\mathrm{mod}\ p)}} \#\{m_2, m_3, m_5, m_6 : 0 < m_i \le \mu\} \ll \mu^4 \lambda \Big(\frac{\lambda}{p} + 1\Big)^5.$$

Proof. Substitute $m_6 = 0$ in D_5 to obtain $(b_6 - b_1) m_2^3 m_3^3 m_5^3$. Thus if D_5 is identically $0 \pmod p$ then $b_6 \equiv b_1 \pmod p$. Similar arguments give

$$b_1 \equiv b_5 \equiv b_6, \qquad b_2 \equiv b_3 \equiv b_4 \pmod p.$$

Substituting this in D_5, and putting $m_2 = m_3 = m_5 = 1$ we obtain

$$-(b_4 - b_1)(1 - m_6)^2 m_6$$

also. The required estimate follows trivially.

7. Proof of Theorem 2

LEMMA 9. *We have*

$$S_7 \ll h^6 + p^3 h \mu^3,$$

where μ is defined by (18).

Proof. From Lemma 1 applied to (22) it follows that

$$S_7 \ll p \sum_{\boldsymbol{m}} \#\{z : 0 < z < p,\ \exists x\ f_1(x) f_2(x) \not\equiv 0 \ (\mathrm{mod}\, p),\\ f_{(z)}(x) \equiv 0 \ (\mathrm{mod}\, p^2),\ f'_{(z)}(x) \equiv 0 \ (\mathrm{mod}\, p)\}.$$

We can rewrite this as

$$\text{(28)}\qquad S_7 \ll p \sum_{x=1}^{p} \sum_{z=1}^{p-1} \#\{\boldsymbol{m} : f_1(x) f_2(x) \not\equiv 0 \ (\mathrm{mod}\, p),\\ f_{(z)}(x) \equiv 0 \ (\mathrm{mod}\, p^2),\ f'_{(z)}(x) \equiv 0 \ (\mathrm{mod}\, p)\},$$

say. Write

$$\text{(29)}\qquad N = \#\{\boldsymbol{m} : f_1(x) f_2(x) \not\equiv 0 \ (\mathrm{mod}\, p),\ f_{(z)}(x) \equiv 0 \ (\mathrm{mod}\, p^2),\\ f'_{(z)}(x) \equiv 0 \ (\mathrm{mod}\, p)\}.$$

Thus by Lemma 3,

$$\text{(30)}\qquad N \ll \sum_{\substack{\boldsymbol{b}\\ \forall i\, |b_i|<\lambda}} \#\{\boldsymbol{m} : \forall i\ 0 < m_i \le \mu,\ f_1(x) f_2(x) \not\equiv 0 \ (\mathrm{mod}\, p),\\ 0 \equiv C_1(\boldsymbol{m}) \equiv C_2(\boldsymbol{m}) \equiv C_4(\boldsymbol{m}) \ (\mathrm{mod}\, p)\}$$

if $\lambda > 1$, and follows immediately from (29) if $\lambda = 1$. Thus from (28) we have

$$S_7 \ll p \sum_{\substack{\boldsymbol{b}\\ \forall i\, |b_i|<\lambda}} \#\{\boldsymbol{m}, x, z : 0 < m_i \le \mu,\ 0 < x \le p,\ 0 < z < p,\\ f_1(x) f_2(x) \not\equiv 0 \ (\mathrm{mod}\, p),\ 0 \equiv C_1(\boldsymbol{m}) \equiv C_2(\boldsymbol{m}) \equiv C_4(\boldsymbol{m}) \ (\mathrm{mod}\, p)\}.$$

But by Lemma 4,

$$\sum_{\substack{\boldsymbol{b}\\ \forall i\, |b_i|<\lambda}} \#\{\boldsymbol{m},x,z : 0<m_i\le\mu,\ 0<x\le p,\ 0<z<p,$$
$$f_1(x)f_2(x)\not\equiv 0 \ (\operatorname{mod} p),\ 0\equiv C_1(\boldsymbol{m})\equiv C_2(\boldsymbol{m})\equiv D_1 \ (\operatorname{mod} p)\}$$
$$\ll p\mu^4\lambda^6 \ll \frac{h^6}{p}+ph^4.$$

Thus

$$S_7 \ll \Big(p \sum_{\substack{\boldsymbol{b}\\ \forall i\, |b_i|<\lambda}} \#W_1\Big) + h^6 + p^2h^4, \tag{31}$$

where

$$W_1 = \{\boldsymbol{m},x,z : 0<m_i\le\mu,\ 0<x\le p,\ 0<z<p,$$
$$f_1(x)f_2(x)\not\equiv 0 \ (\operatorname{mod} p),\ 0\equiv C_1(\boldsymbol{m})\equiv C_2(\boldsymbol{m})\equiv C_4(\boldsymbol{m})\not\equiv D_1 \ (\operatorname{mod} p)\}.$$

Consider $(\boldsymbol{m},x,z)\in W_1$. Given m_2,m_3,m_5,m_6,z,x, the values of m_1, m_4 are uniquely determined by $C_1(\boldsymbol{m})\equiv C_2(\boldsymbol{m})\equiv 0 \ (\operatorname{mod} p)$ since $D_1\not\equiv 0$ $(\operatorname{mod} p)$. Eliminating m_1,m_4 from $C_1(\boldsymbol{m})\equiv C_2(\boldsymbol{m})\equiv C_4(\boldsymbol{m})\equiv 0 \ (\operatorname{mod} p)$ we obtain

$$D(x) = \begin{vmatrix} g_1(x) & -zg_4(x) & 0 \\ 2x+m_2+m_3 & -z(2x+m_5+m_6) & g_1(x)-zg_4(x) \\ b_2(x+m_3)+b_3(x+m_2) & -zb_5(x+m_6)-zb_6(x+m_5) & b_1g_1(x)-b_4zg_4(x) \end{vmatrix}$$
$$\equiv 0 \ (\operatorname{mod} p).$$

By Lemma 2 this has $O(p^2\mu^3)$ solutions in m_2,m_3,m_5,m_6,z,x unless it is identically $0 \ (\operatorname{mod} p)$ as a polynomial in these variables. In the latter case $D(0)$ will also be identically $0 \ (\operatorname{mod} p)$. However, we have

$$D(0) = \begin{vmatrix} m_2m_3 & -zm_5m_6 & 0 \\ m_2+m_3 & -z(m_5+m_6) & m_2m_3-zm_5m_6 \\ b_2m_3+b_3m_2 & -zb_5m_6-zb_6m_5 & b_1m_2m_3-b_4zm_5m_6 \end{vmatrix},$$

and by Lemma 5,

$$\sum_{\substack{\boldsymbol{b}\\ \forall i\, |b_i|<\lambda \\ D(0) \text{ identically } 0 \ (\operatorname{mod} p)}} \#\{m_2,m_3,m_5,m_6,x,z :$$
$$0<m_i\le\mu,\ 0<x\le p,\ 0<z<p\}$$
$$\ll p^2\mu^4\lambda\Big(\frac{\lambda}{p}+1\Big)^5.$$

Thus, by (31),

$$S_7 \ll p\bigg(\lambda^6p^2\mu^3 + \lambda\Big(\frac{\lambda}{p}+1\Big)^5 p^2\mu^4\bigg) + h^6 + p^2h^4 \ll h^6 + p^3h\mu^3,$$

which completes the proof of the lemma.

LEMMA 10. *We have*

$$S_8 \ll h^6 + p^3 h\mu^3 + p^4\mu^2.$$

Proof. We have, from (23),

$$S_8 = p^2 \sum_{\boldsymbol{m}} \#\{x, z : 0 < x \le p,\ 0 < z < p,\ f_1(x)f_2(x) \not\equiv 0 \ (\mathrm{mod}\, p),$$
$$f_{(z)}(x) \equiv 0 \ (\mathrm{mod}\, p^3),\ f'_{(z)}(x) \equiv 0 \ (\mathrm{mod}\, p^2),\ f''_{(z)}(x) \equiv 0 \ (\mathrm{mod}\, p)\}.$$

Rewrite this as

$$S_8 \ll p^2 \sum_{x=1}^{p} \sum_{z=1}^{p-1} \#\{\boldsymbol{m} : f_1(x)f_2(x) \not\equiv 0 \ (\mathrm{mod}\, p), \tag{32}$$
$$f_{(z)}(x) \equiv 0 \ (\mathrm{mod}\, p^3),\ f'_{(z)}(x) \equiv 0 \ (\mathrm{mod}\, p^2),\ f''_{(z)}(x) \equiv 0 \ (\mathrm{mod}\, p)\}.$$

Write

$$N = \#\{\boldsymbol{m} : f_1(x)f_2(x) \not\equiv 0 \ (\mathrm{mod}\, p),\ f_{(z)}(x) \equiv 0 \ (\mathrm{mod}\, p^2),$$
$$f'_{(z)}(x) \equiv 0 \ (\mathrm{mod}\, p^2),\ f''_{(z)}(x) \equiv 0 \ (\mathrm{mod}\, p)\}.$$

Define λ and μ by (18). Thus by Lemma 3 we have

$$N \ll \sum_{\substack{\boldsymbol{b} \\ \forall i\, |b_i| < \lambda}} \#\{\boldsymbol{m} : \forall i\, 0 < m_i \le \mu,\ f_1(x)f_2(x) \not\equiv 0 \ (\mathrm{mod}\, p),$$
$$0 \equiv C_1(\boldsymbol{m}) \equiv C_2(\boldsymbol{m}) \equiv C_3(\boldsymbol{m}) \equiv C_4(\boldsymbol{m}) \equiv C_5(\boldsymbol{m}) \ (\mathrm{mod}\, p)\}.$$

By Lemma 6,

$$\sum_{\substack{\boldsymbol{b} \\ \forall i\, |b_i| < \lambda}} \#\{\boldsymbol{m}, x, z : 0 < m_i \le \mu,\ 0 < x \le p,\ 0 < z < p,$$
$$f_1(x)f_2(x) \not\equiv 0 \ (\mathrm{mod}\, p),\ C_1(\boldsymbol{m}) \equiv C_2(\boldsymbol{m}) \equiv C_3(\boldsymbol{m}) \equiv D_1 \equiv 0 \ (\mathrm{mod}\, p)\}$$
$$\ll p\mu^3\lambda^6 \ll \frac{h^6}{p^2} + ph^3.$$

Thus by (32) we have

$$S_8 \ll \Big(p^2 \sum_{\substack{\boldsymbol{b} \\ \forall i\, |b_i| < \lambda}} \#W_2\Big) + h^6 + p^3\mu^3, \tag{33}$$

where

$$W_2 = \{\boldsymbol{m}, x, z : 0 < m_i \le \mu,\ 0 < x \le p,\ 0 < z < p,$$
$$f_1(x)f_2(x) \not\equiv 0 \ (\mathrm{mod}\, p),$$
$$0 \equiv C_1(\boldsymbol{m}) \equiv C_2(\boldsymbol{m}) \equiv C_3(\boldsymbol{m}) \equiv C_4(\boldsymbol{m}) \equiv C_5(\boldsymbol{m}) \not\equiv D_1 \ (\mathrm{mod}\, p)\}.$$

Consider $(\boldsymbol{m}, x, z) \in W_2$. Given m_2, m_3, m_5, m_6, z, x, the values of m_1, m_4 are uniquely determined by $C_1(\boldsymbol{m}) \equiv C_2(\boldsymbol{m}) \equiv 0 \ (\mathrm{mod}\, p)$ since $D_1 \not\equiv 0$

$(\bmod p)$. Eliminating m_1, m_4 from $C_1(\boldsymbol{m}) \equiv C_2(\boldsymbol{m}) \equiv C_4(\boldsymbol{m}) \equiv 0 \pmod p$ we obtain

(34)
$$E_1 = \begin{vmatrix} g_1(x) & -g_4(x) & 0 \\ 2x+m_2+m_3 & -(2x+m_5+m_6) & g_1(x)-zg_4(x) \\ b_2(x+m_3)+b_3(x+m_2) & -b_5(x+m_6)-b_6(x+m_5) & b_1g_1(x)-b_4zg_4(x) \end{vmatrix} \equiv 0 \pmod p.$$

Also eliminating m_1, m_4 from $C_1(\boldsymbol{m}) \equiv C_2(\boldsymbol{m}) \equiv C_3(\boldsymbol{m}) \equiv 0 \pmod p$ we obtain

(35)
$$E_2 = \begin{vmatrix} g_1(x) & -g_4(x) & 0 \\ 2x+m_2+m_3 & -(2x+m_5+m_6) & g_1(x)-zg_4(x) \\ 2 & -2 & 2((2x+m_2+m_3)-z(2x+m_5+m_6)) \end{vmatrix} \equiv 0 \pmod p,$$

which can be rewritten as

(36) $$D_3 \equiv zD_4 \pmod p.$$

But by Lemma 7,

$$\sum_{\substack{\boldsymbol{b} \\ \forall i\, |b_i|<\lambda}} \#\{m_2, m_3, m_5, m_6, x : 0 < m_i \le \mu,\ 0 < x \le p,\ D_3 \equiv D_4 \equiv 0 \pmod p\} \ll p\mu^2\lambda^6 \ll \frac{h^6}{p^3} + p\mu^2.$$

Thus, by (33),

(37) $$S_8 \ll p^2\Big(\sum_{\substack{\boldsymbol{b} \\ \forall i\, |b_i|<\lambda}} \#W_3\Big) + h^6 + p^4\mu^2,$$

where

$$W_3 = \{m_2, m_3, m_5, m_6, x, z : 0 < m_i \le \mu,\ 0 < x \le p,\ 0 < z < p,\ E_1 \equiv 0 \pmod p,\ D_3 \equiv zD_4 \pmod p,\ D_3, D_4 \text{ not both } 0 \pmod p\}.$$

Now, for $(m_2, m_3, m_5, m_6, x, z) \in W_3$, z is uniquely determined by (36). Also (34) can be rewritten as

$$D_6 \equiv zD_7 \pmod p$$

where

$$D_6 = \begin{vmatrix} g_1(x) & -g_4(x) & 0 \\ 2x+m_2+m_3 & -(2x+m_5+m_6) & g_1(x) \\ b_2(x+m_3)+b_3(x+m_2) & -b_5(x+m_6)-b_6(x+m_5) & b_1g_1(x) \end{vmatrix}$$

and

$$D_7 = \begin{vmatrix} g_1(x) & -g_4(x) & 0 \\ 2x + m_2 + m_3 & -(2x + m_5 + m_6) & g_4(x) \\ b_2(x + m_3) + b_3(x + m_2) & -b_5(x + m_6) - b_6(x + m_5) & b_4 g_4(x) \end{vmatrix}.$$

Thus, by (37), we have

$$S_8 \ll p^2\Big(\sum_{\substack{\boldsymbol{b} \\ \forall i\, |b_i|<\lambda}} \#W_4\Big) + h^6 + p^4\mu^2, \tag{38}$$

where

$$W_4 = \{m_2, m_3, m_5, m_6, x : 0 < m_i \le \mu,\ 0 < x \le p,\\ D_3D_7 \equiv D_4D_6 \pmod p\}.$$

Write

$$H(x) = D_3D_7 - D_4D_6.$$

Then $H(0) = D_5$ and so $H(x)$ can be identically 0 $(\operatorname{mod} p)$ only if D_5 is. But by Lemma 8,

$$\sum_{\substack{\boldsymbol{b} \\ \forall i\, |b_i|<\lambda}} \#\{m_2, m_3, m_5, m_6 : 0 < m_i \le \mu,\ H(x) \text{ is identically } 0 \pmod p\}\\ \ll \mu^4\lambda\Big(\frac{\lambda}{p} + 1\Big)^5 \ll \frac{h^6}{p^7} + h\mu^3.$$

Thus by (38)

$$S_8 \ll p^2\Big(\sum_{\substack{\boldsymbol{b} \\ \forall i\, |b_i|<\lambda \\ H(x) \text{ not identically } 0 \pmod p}} \#W_5\Big) + h^6 + p^3h\mu^3 + p^4\mu^2, \tag{39}$$

where

$$W_5 = \{m_2, m_3, m_5, m_6, x : 0 < m_i \le \mu,\ 0 < x \le p,\ H(x) \equiv 0 \pmod p\}.$$

By Lemma 2,

$$\#W_5 \ll p\mu^3,$$

and thus by (39),

$$S_8 \ll p^3\mu^3\lambda^6 + p^4\mu^2 + h^6 + p^3h\mu^3 \ll h^6 + p^3h\mu^3 + p^4\mu^2,$$

which completes the proof of the lemma.

Proof of Theorem 2. Follows from Lemmas 9 and 10.

8. Corollaries. In [3] it was shown that from (1) it follows that

$$\Big|\sum_{x=N+1}^{N+H} \chi(x)\Big| \ll H^{1/2}k^{3/16+\varepsilon}.$$

More generally, in [3] it was shown that if k is cubefree and $r \ge 2$ then

$$\Big|\sum_{x=N+1}^{N+H}\chi(x)\Big| \ll H^{1-1/r}k^{(r+1)/(4r^2)+\varepsilon}.$$

It would follow from (3) that

$$\sum_{\text{primitive}\,\chi}\Big|\sum_{x=N+1}^{N+H}\chi(x)\Big| \ll kk^{1/4+\varepsilon}H^{1/4}.$$

Similarly from (4) it would follow that

$$\sum_{\substack{\chi \bmod p^3\\ \chi^{p^2}=\chi_0\\ \chi\ne\chi_0}}\Big|\sum_{x=N+1}^{N+H}\chi(x)\Big| \ll p^2p^{1/2+\varepsilon}H^{1/2}.$$

This estimate is improved by the following corollaries.

Corollary 1. *If $H \le p^{3/2}$ then*

$$\sum_{\substack{\chi \bmod p^3\\ \chi^{p^2}=\chi_0\\ \chi\ne\chi_0}}\Big|\sum_{x=N+1}^{N+H}\chi(x)\Big| \ll p^2p^{3/4}H^{1/4}.$$

Proof. From the proof of Lemma 2 of [5] we see that if $2^\nu < p^3$ then

$$\Big|\sum_{x=N+1}^{N+H}\chi(x)\Big| \le 2 + H^{3/4}2^{-\nu}\Big(\sum_{m=1}^{p^3}\Big|\sum_{x=m+1}^{x+2^\nu}\chi(x)\Big|^4\Big)^{1/4} + \sum_{\mu=0}^{\nu-1}2^{-\mu/4}\Big(\sum_{m=1}^{p^3}\Big|\sum_{x=m+1}^{x+2^\mu}\chi(x)\Big|^4\Big)^{1/4}.$$

Choose $H/2 < 2^\nu < H$. Then we have

$$\sum_{\substack{\chi \bmod p^3\\ \chi^{p^2}=\chi_0\\ \chi\ne\chi_0}}\Big|\sum_{x=N+1}^{N+H}\chi(x)\Big| \ll p^2 + H^{3/4}2^{-\nu}\sum_{\chi}\Big(\sum_{m=1}^{p^3}\Big|\sum_{x=m+1}^{x+2^\nu}\chi(x)\Big|^4\Big)^{1/4} + \sum_{\mu=0}^{\nu-1}2^{-\mu/4}\sum_{\chi}\Big(\sum_{m=1}^{p^3}\Big|\sum_{x=m+1}^{x+2^\mu}\chi(x)\Big|^4\Big)^{1/4}$$

$$\ll p^2 + H^{3/4}2^{-\nu}p^{3/2}\Big(\sum_{\chi}\sum_{m=1}^{p^3}\Big|\sum_{x=m+1}^{x+2^\nu}\chi(x)\Big|^4\Big)^{1/4}$$

$$+\sum_{\mu=0}^{\nu-1}2^{-\mu/4}p^{3/2}\Big(\sum_{\chi}\sum_{m=1}^{p^3}\Big|\sum_{x=m+1}^{x+2^\mu}\chi(x)\Big|^4\Big)^{1/4}$$

$$\ll p^2 + H^{3/4}2^{-\nu}p^{3/2}(p^2 2^{4\nu}+p^5 2^{2\nu})^{1/4}$$

$$+\sum_{\mu=0}^{\nu-1}2^{-\mu/4}p^{3/2}(p^2 2^{4\mu}+p^5 2^{2\mu})^{1/4}$$

$$\ll H^{1/4}p^{11/4}.$$

COROLLARY 2. *If $H \ge p^{3/2}$ then*

$$\sum_{\substack{\chi \bmod p^3\\ \chi^{p^2}=\chi_0\\ \chi\ne\chi_0}}\Big|\sum_{x=N+1}^{N+H}\chi(x)\Big| \ll p^2p^{3/8+\delta}H^{1/2}.$$

Proof. From Lemma 6 of [3], with $p^{3/2} < 2^\nu \le 2p^{3/2}$, it follows that for $p^{3/2+\delta} \le H \le p^{9/4-\delta}$ there is an h satisfying $1 \le h \le 2^\nu$ for which

$$\Big|\sum_{x=N+1}^{N+H}\chi(x)\Big| \ll \max\Big(H^{1/2}p^{-3/4}h^{-1/4}(\log p)\Big(\sum_{x=1}^{p^3}\Big|\sum_{m=1}^{h}\chi(x+m)\Big|^4\Big)^{1/4},\ Hp^{-3/2}\Big).$$

From this it follows that

$$\sum_{\substack{\chi \bmod p^3\\ \chi^{p^2}=\chi_0\\ \chi\ne\chi_0}}\Big|\sum_{x=N+1}^{N+H}\chi(x)\Big| \ll \sum_{\mu=0}^{\nu}H^{1/2}p^{-3/4}2^{-\mu/4}(\log p)p^{3/2}(p^2 2^{4\mu}+p^5 2^{2\mu})^{1/4}+Hp^{1/2}$$

$$\ll p^2p^{3/8}H^{1/2}\log p.$$

COROLLARY 3. *If $p < H < p^{6/5}$ then*

$$\sum_{\substack{\chi \bmod p^3\\ \chi^{p^2}=\chi_0\\ \chi\ne\chi_0}}\Big|\sum_{x=N+1}^{N+H}\chi(x)\Big| \ll p^2p^{1+\varepsilon}.$$

P r o o f. Choose $H/2 < 2^\nu \le H$ and apply Theorem 2 in the proof of Corollary 1.

COROLLARY 4. *If* $H \ge p^{6/5}$ *then*

$$\sum_{\substack{\chi \bmod p^3 \\ \chi^{p^2}=\chi_0 \\ \chi\ne\chi_0}} \Big|\sum_{x=N+1}^{N+H} \chi(x)\Big| \ll p^2 H^{2/3} p^{1/5+\varepsilon}.$$

P r o o f. Choose $p^{6/5} < 2^\nu \le 2p^{6/5}$ and apply Theorem 2 in the proof of Corollary 2.

References

[1] D. A. Burgess, *On character sums and primitive roots*, Proc. London Math. Soc. (3) 12 (1962), 179–192.
[2] —, *On character sums and L-series*, ibid. 12 (1962), 193–206.
[3] —, *On character sums and L-series II*, ibid. 13 (1963), 524–536.
[4] —, *Estimation of character sums modulo a small power of a prime*, J. London Math. Soc. (2) 30 (1984), 385–393.
[5] —, *Mean values of character sums*, Mathematika 33 (1986), 1–5.
[6] —, *Mean values of character sums II*, ibid. 34 (1987), 1–7.
[7] —, *On a set of congruences related to character sums III*, J. London Math. Soc. (2) 45 (1992), 201–214.
[8] —, *Mean values of character sums III*, Mathematika 42 (1995), 133–136.

Department of Mathematics
The University
Nottingham, NG7 2RD, U.K.
E-mail: dab@maths.nott.ac.uk

Received on 23.4.1996 (2972)