ACTA ARITHMETICA
LXVI.4 (1994)

An upper bound for the number of solutions of a system of congruences

by

Lyn Dodd (Nottingham)

1. Introduction. Let X denote an indeterminate. For each vector $\mathbf{m} \in \mathbb{Z}^{2r}$ with components satisfying $0 < m_i \le h$ define

$$f_1(X) = \prod_{i=1}^{r}(X + m_i) \qquad \text{and} \qquad f_2(X) = \prod_{i=r+1}^{2r}(X + m_i) .$$

In [1] Burgess showed that, for any prime $p > 3$ and primitive character $\chi \pmod{p^\alpha}$, the estimate

$$\Big|\sum_{n=N+1}^{N+H} \chi(n)\Big| = O(H^{1-1/r} p^{\alpha(r+1)/4r^2+\varepsilon})$$

holds in the case $r = 3$. This inequality was obtained by estimating

$$\sum_{\mathbf{m}} \Big| \sum_{x\in A_1} \chi\Big(\frac{f_1}{f_2}(x)\Big)\Big|$$

where

$$A_1 = \{x : 0 \le x < p^\alpha,\ p \nmid f_1(x) f_2(x)\} .$$

In order to do this, Burgess found estimates for the inner summation over various subsets of A_1 and then counted the number of $\mathbf{m}$ for which these subsets were non-empty. The counting process was carried out using different methods, one of which concerned the estimation of the cardinality of

$$S = \{\mathbf{m} : 0 < m_i \le h,\ f_1(X) \equiv f_2(X) \pmod{p^\mu}\} .$$

The estimation of such character sums in the case $r = 2$ is contained in [2]. The case $r = 4$ has yet to be proved. This paper estimates $\#S$ when $r = 4$, as a step in the direction of a proof. The result obtained is given by the following theorem.

The contents of this paper formed part of the author's PhD thesis (Nottingham University, 1991) which was supported by Science and Engineering Research Council.

Theorem 1. *Suppose p is a prime greater than 5 and μ is a positive integer. If*

$$H = \{\mathbf{m} : 0 < m_i \le h \text{ for } i = 1, \ldots, 8 \text{ and } f_1(X) \equiv f_2(X) \pmod{p^\mu}\}$$

then

$$\#H \ll \mu^6 \left(\frac{h^8}{p^{3\mu+[\mu/2]-[\mu/4]}}\text{‘} + \frac{h^6}{p^{\mu+[\mu/2]-[\mu/4]}} + \frac{h^5}{p^{\mu-[\mu/2]}} + h^4 \right).$$

In [4] Hua and Min obtain an asymptotic formula for the number of solutions of the system

$$x_1^h + \ldots + x_s^h \equiv y_1^h + \ldots + y_s^h \pmod{p^l} \qquad (1 \le h \le k)$$

where s, k, h, l are integers such that $s \ge k \ge 4$, $l \ge k^2$ and p is a prime greater than k. Assuming that $p \ne 5$ and letting $s_r(\mathbf{x}) = \sum_{i=1}^4 x_i^r$, in the particular case $s = k = 4$, $l = 16$ the number of solutions of the system

$$\left.\begin{aligned} s_1(\mathbf{x}) &\equiv s_1(\mathbf{y}) \\ s_2(\mathbf{x}) &\equiv s_2(\mathbf{y}) \\ s_3(\mathbf{x}) &\equiv s_3(\mathbf{y}) \\ s_4(\mathbf{x}) &\equiv s_4(\mathbf{y}) \end{aligned}\right\} \pmod{p^{16}} \tag{1}$$

is $p^{76}(1 + O(p^{-1/4}))$. Writing

$$\begin{aligned} \sigma_1(\mathbf{x}) &= x_1 + x_2 + x_3 + x_4\,, \\ \sigma_2(\mathbf{x}) &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4\,, \\ \sigma_3(\mathbf{x}) &= x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4\,, \\ \sigma_4(\mathbf{x}) &= x_1x_2x_3x_4\,, \end{aligned}$$

it follows that

$$\begin{aligned} s_1(\mathbf{x}) &= \sigma_1(\mathbf{x})\,, \\ s_2(\mathbf{x}) &= (\sigma_1(\mathbf{x}))^2 - 2\sigma_2(\mathbf{x})\,, \\ s_3(\mathbf{x}) &= (\sigma_1(\mathbf{x}))^3 - 3\sigma_1(\mathbf{x})\sigma_2(\mathbf{x}) + 3\sigma_3(\mathbf{x})\,, \\ s_4(\mathbf{x}) &= (\sigma_1(\mathbf{x}))^4 - 4(\sigma_1(\mathbf{x}))^2\sigma_2(\mathbf{x}) \\ &\qquad + 4\sigma_1(\mathbf{x})\sigma_3(\mathbf{x}) + 2(\sigma_2(\mathbf{x}))^2 - 4\sigma_4(\mathbf{x})\,. \end{aligned}$$

Since $p > 5$ the systems (1) and

$$\left.\begin{aligned} \sigma_1(\mathbf{x}) &\equiv \sigma_1(\mathbf{y}) \\ \sigma_2(\mathbf{x}) &\equiv \sigma_2(\mathbf{y}) \\ \sigma_3(\mathbf{x}) &\equiv \sigma_3(\mathbf{y}) \\ \sigma_4(\mathbf{x}) &\equiv \sigma_4(\mathbf{y}) \end{aligned}\right\} \pmod{p^{16}} \tag{2}$$

are equivalent. But (2) holds if and only if

$$\prod_{i=1}^{4}(X+x_i) \equiv \prod_{i=1}^{4}(X+y_i) \pmod{p^{16}}$$

for indeterminate X, which, by Theorem 1, has $\ll p^{76}$ solutions in one complete system of residues. A comparison with the result of Min and Hua shows that, in this case, Theorem 1 is essentially best possible.

2. Basic estimates. The basic tools used in proving Theorem 1 are the well-known estimate in Lemma 2 and Proposition 3 which is reproduced from [3]. The notation $\lceil x\rceil$ denotes the least integer greater than or equal to x and $p^\alpha \parallel x$ means $p^\alpha \mid x$, $p^{\alpha+1}\nmid x$.

LEMMA 2. *Suppose p is an odd prime and ν is a positive integer. If $0<x\le h$ then the number of solutions of the congruence $x^2+Ax+B\equiv 0 \pmod{p^\nu}$ is $\ll h/p^{[(\nu+1)/2]}+1$.*

PROPOSITION 3. *Let f be a polynomial of degree n having integer coefficients. Let p be a prime, d be a positive integer, and α, β and γ be non-negative integers satisfying $\gamma=\lceil\alpha/d\rceil$. If $T=\{x\in$ a complete set of residues $\pmod{p^\gamma} : p^{\alpha+\beta}\mid f(x),\ p^\beta \parallel f^{(d)}(x)\}$ then $\#T\ll n$.*

If $g(x)$ is a polynomial with integer coefficients such that $p^\delta\parallel g^{(d)}(x)$ then it follows from Proposition 3 that the number of x satisfying $0<x\le h$ and $g(x)\equiv 0 \pmod{p^\mu}$ is $\ll h/p^{\mu-\delta}+1$ if $d=1$ and $\ll h/p^{[(\mu-\delta+1)/2]}+1$ if $d=2$. The proof of Theorem 1 will be given by a series of lemmas. Throughout we shall use the fact that the conditions $A_1+\ldots+A_n\equiv 0 \pmod{p^\alpha}$ and $p^{a_j}\parallel A_j$ for $j=1,\ldots,n$ imply that $a_k\ge\min(\min_{j\ne k}a_j,\alpha)$ for $k=1,\ldots,n$.

3. Initial transformations. Making the substitution $M_i=m_i-m_1$ for $i=2,\ldots,8$ we see that $f_1(X)\equiv f_2(X) \pmod{p^\mu}$ if and only if the following congruences hold simultaneously:

$$M_2+M_3+M_4\equiv M_5+M_6+M_7+M_8 \pmod{p^\mu}, \tag{3}$$

$$M_2M_3+M_2M_4+M_3M_4$$
$$\equiv M_5M_6+M_5M_7+M_5M_8+M_6M_7+M_6M_8+M_7M_8 \pmod{p^\mu},$$

$$M_2M_3M_4\equiv M_5M_6M_7+M_5M_6M_8+M_5M_7M_8+M_6M_7M_8 \pmod{p^\mu},$$

$$0\equiv M_5M_6M_7M_8 \pmod{p^\mu}. \tag{4}$$

Eliminating M_2 from the second and third congruences of the above system produces the pair of congruences

$$(M_3+M_4)(M_5+M_6+M_7+M_8-M_4)-M_3^2 \tag{5}$$

$$\equiv M_5M_6 + M_5M_7 + M_5M_8 + M_6M_7 + M_6M_8 + M_7M_8 \pmod{p^\mu}$$

and

$$\begin{aligned} &M_3M_4(M_5 + M_6 + M_7 + M_8 - M_3 - M_4) \\ &\qquad \equiv M_5M_6M_7 + M_5M_6M_8 + M_5M_7M_8 + M_6M_7M_8 \pmod{p^\mu}, \end{aligned}$$

which together imply that

$$\begin{aligned} &(M_4 - M_8)(M_5M_6 + M_5M_7 + M_6M_7 + M_4^2 - M_4(M_5 + M_6 + M_7)) \\ &\qquad \equiv M_5M_6M_7 \pmod{p^\mu}. \end{aligned} \tag{6}$$

Define $\gamma_5, \gamma_6, \gamma_7, \gamma_8$ by

$$\begin{gathered} p^{\gamma_5} \parallel (M_5, p^\mu), \qquad p^{\gamma_5+\gamma_6} \parallel (M_5M_6, p^\mu), \\ p^{\gamma_5+\gamma_6+\gamma_7} \parallel (M_5M_6M_7, p^\mu), \qquad \gamma_5 + \gamma_6 + \gamma_7 + \gamma_8 = \mu. \end{gathered} \tag{7}$$

It may be assumed that $\gamma_5 \ge \gamma_6 \ge \gamma_7 \ge \gamma_8 \ge 0$, by re-ordering M_5, M_6, M_7, M_8 if necessary, and that for $i = 5, 6, 7$ any power of p dividing M_{i+1} also divides M_i. Let ε, k, m be given by

$$p^\varepsilon \parallel (M_5M_6 + M_5M_7 + M_6M_7 + M_4^2 - M_4(M_5 + M_6 + M_7), p^\mu), \tag{8}$$

$$p^k \parallel (2M_3 + M_4 - M_5 - M_6 - M_7, p^\mu) \tag{9}$$

and

$$p^m \parallel (2M_4 - M_5 - M_6 - M_7, p^\mu). \tag{10}$$

Writing $M_1 = m_1$ it follows that the number of $\mathbf{m} = (m_1, \ldots, m_8)$ satisfying $f_1(X) \equiv f_2(X) \pmod{p^\mu}$ is less than or equal to the number of solutions in $M_1, \ldots, M_8$ of (3)–(6) with $|M_i| < h$ for $i = 1, \ldots, 8$. We now present the lemmas which together provide the proof of Theorem 1. In all cases there are h possible values for m_1. Given $M_3, \ldots, M_8$ there are $\ll h/p^\mu + 1$ choices for M_2 from (3). We have $\ll h/p^{\max(\mu-k,k)} + 1$ choices for M_3 from (5) and (9), given $M_4, \ldots, M_8$. The following notation will be used:

$$A = \frac{h^8}{p^{3\mu+[\mu/2]-[\mu/4]}} + \frac{h^6}{p^{\mu+[\mu/2]-[\mu/4]}} + \frac{h^5}{p^{\mu-[\mu/2]}} + h^4$$

and

$$S = \text{“}M_1, \ldots, M_8 : |M_i| < h \text{ for } i = 1, \ldots, 8 \text{ and (3)–(10) hold”}.$$

4. Extending the conditions S. In this section we obtain the required estimate except for the set $\{S : 0 < m < \mu - [\mu/4],\ \varepsilon < \mu,\ [\mu/4] < k \le [\mu/2],\ \gamma_8 > 0 \text{ and } p \mid M_4\}$.

LEMMA 4. *If $H_1 = \{S : m = 0\}$ then $\#H_1 \ll \mu^5 A$.*

Proof. Given M_4, M_5, M_6, M_7 there are $\ll h/p^{\mu-\varepsilon} + 1$ choices for M_8 from (6) and (8). Since $m = 0$ there are only non-singular solutions for M_4

from (8) and so we have $\ll h/p^{\varepsilon}+1$ choices for M_4 given M_5, M_6, M_7. By (7) it follows that

$$\begin{aligned}\#H_1 &\ll h\Big(\frac{h}{p^{\mu}}+1\Big)\sum_k\Big(\frac{h}{p^{\max(\mu-k,k)}}+1\Big)\\ &\quad\times\sum_{\gamma_5,\gamma_6,\gamma_7}\Big(\frac{h}{p^{\gamma_5}}+1\Big)\Big(\frac{h}{p^{\gamma_6}}+1\Big)\Big(\frac{h}{p^{\gamma_7}}+1\Big)\sum_{\varepsilon}\Big(\frac{h}{p^{\varepsilon}}+1\Big)\Big(\frac{h}{p^{\mu-\varepsilon}}+1\Big)\\ &\ll \mu^5 A\,. \ \blacksquare\end{aligned}$$

LEMMA 5. *If* $H_2=\{S: m>0$ *and* $p\nmid M_4\}$ *then* $\#H_2\ll\mu^4A$.

Proof. Given M_4, M_5, M_6, M_7 there are $\ll h/p^{\mu-\varepsilon}+1$ choices for M_8 from (6) and (8). By (8) and (10) there are $\ll h/p^{\max(\varepsilon-m,m)}+1$ choices for M_4 given M_5, M_6, M_7. Since $p\nmid M_4$, (7) and (10) imply that $p\nmid M_7$ and so $\gamma_7=0$ and $\gamma_5+\gamma_6=\mu$. From (10) it can be seen that $2M_4=M_5+M_6+M_7+Rp^m$ for some $R\in\mathbb{Z}$. Substituting for M_4 in (8) produces

$$4(M_5M_6+M_5M_7+M_6M_7)\equiv(M_5+M_6+M_7)^2 \pmod{p^{\min(2m,\varepsilon)}},$$

from which we have $\ll h/p^{\min(m,[(\varepsilon+1)/2])}+1$ choices for M_7, given M_5, M_6. Therefore

$$\begin{aligned}\#H_2 &\ll h\Big(\frac{h}{p^{\mu}}+1\Big)\sum_k\Big(\frac{h}{p^{\max(\mu-k,k)}}+1\Big)\\ &\quad\times\sum_{\varepsilon,m}\Big(\frac{h}{p^{\max(\varepsilon-m,m)}}+1\Big)\Big(\frac{h}{p^{\min(m,[(\varepsilon+1)/2])}}+1\Big)\\ &\quad\times\Big(\frac{h}{p^{\mu-\varepsilon}}+1\Big)\sum_{\gamma_5}\Big(\frac{h}{p^{\gamma_5}}+1\Big)\Big(\frac{h}{p^{\mu-\gamma_5}}+1\Big)\\ &\ll \mu^4 A\,. \ \blacksquare\end{aligned}$$

Multiplying (5) by 4 and then rearranging yields

$$(2M_3-\Sigma_1+M_4)^2\equiv 4M_4(\Sigma_1-M_4)-4\Sigma_2+(\Sigma_1-M_4)^2 \pmod{p^{\mu}}$$

where $\Sigma_1=M_5+M_6+M_7+M_8$ and $\Sigma_2=M_5M_6+M_5M_7+M_5M_8+M_6M_7+M_6M_8+M_7M_8$. Hence it follows from (9) that

$$p^{\min(2k,\mu)}\mid 4M_4(\Sigma_1-M_4)-4\Sigma_2+(\Sigma_1-M_4)^2$$

and so

$$\begin{aligned}&(11)\quad (M_4+M_8-M_5-M_6-M_7)^2\\ &\equiv 4(M_5M_6+M_5M_7+M_6M_7+M_4^2-M_4(M_5+M_6+M_7)) \pmod{p^{\min(2k,\mu)}}.\end{aligned}$$

Lemma 6. *If* $H_3 = \{S : m > 0,\ p \mid M_4$ *and* $\varepsilon = \mu\}$ *then* $\#H_3 \ll \mu^3 A$.

Proof. From (6) and (8) we know that $M_5M_6M_7 \equiv 0 \pmod{p^\mu}$ and so, by (7), $\gamma_5 + \gamma_6 + \gamma_7 = \mu$. Using (8) and (11) we obtain

$$M_4 + M_8 - M_5 - M_6 - M_7 \equiv 0 \pmod{p^{\min(k,[(\mu+1)/2])}},$$

from which we have $\ll h/p^{\min(k,[(\mu+1)/2])} + 1$ choices for M_8 given M_4, M_5, M_6, M_7. There are $\ll h/p^{[(\mu+1)/2]} + 1$ choices for M_4 from (8), given M_5, M_6, M_7. Thus

$$\begin{aligned}\#H_3 &\ll h\left(\frac{h}{p^\mu}+1\right)\left(\frac{h}{p^{\mu-[\mu/2]}}+1\right)\\ &\quad\times \sum_{\gamma_5,\gamma_6}\left(\frac{h}{p^{\gamma_5}}+1\right)\left(\frac{h}{p^{\gamma_6}}+1\right)\left(\frac{h}{p^{\mu-\gamma_5-\gamma_6}}+1\right)\\ &\quad\times \sum_{k}\left(\frac{h}{p^{\max(\mu-k,k)}}+1\right)\left(\frac{h}{p^{\min(k,[(\mu+1)/2])}}+1\right)\\ &\ll \mu^3 A.\ \blacksquare\end{aligned}$$

Lemma 7. *If* $H_4 = \{S : k > [\mu/2],\ m > 0,\ \varepsilon < \mu$ *and* $p \mid M_4\}$ *then* $\#H_4 \ll \mu^5 A$.

Proof. As $\varepsilon < \mu$ it follows from (8) that $p^\varepsilon \parallel \mathrm{RHS}$ and thus $p^\varepsilon \parallel \mathrm{LHS}$ of (11). Hence ε must be even and $p^{\varepsilon/2} \parallel M_4 + M_8 - M_5 - M_6 - M_7$. Together with (11) this gives $\ll h/p^{\mu-\varepsilon/2} + 1$ choices for M_8 given M_4, M_5, M_6, M_7. There are $\ll h/p^{\varepsilon/2} + 1$ choices for M_4 from (8), given M_5, M_6, M_7. Therefore

$$\begin{aligned}\#H_4 &\ll h\left(\frac{h}{p^\mu}+1\right)\sum_k\left(\frac{h}{p^k}+1\right)\sum_{\gamma_5,\gamma_6,\gamma_7}\left(\frac{h}{p^{\gamma_5}}+1\right)\left(\frac{h}{p^{\gamma_6}}+1\right)\\ &\quad\times\left(\frac{h}{p^{\gamma_7}}+1\right)\sum_{\varepsilon}\left(\frac{h}{p^{\varepsilon/2}}+1\right)\left(\frac{h}{p^{\mu-\varepsilon/2}}+1\right)\\ &\ll \mu^5 A.\ \blacksquare\end{aligned}$$

Lemma 8. *If* $H_5 = \{S : 0 \le k \le [\mu/4],\ m > 0,\ \varepsilon < \mu$ *and* $p \mid M_4\}$ *then* $\#H_5 \ll \mu^5 A$.

Proof. There are $\ll h/p^{\mu-\varepsilon} + 1$ choices for M_8 from (6) and (8), given M_4, M_5, M_6, M_7, and $\ll h/p^{\max(\varepsilon-m,m)} + 1$ choices for M_4 from (8) and (10), given M_5, M_6, M_7. As in Lemma 5 we have $\ll h/p^{\min(m,[(\varepsilon+1)/2])} + 1$ choices for M_7, given M_5, M_6, and thus

$$\begin{aligned}\#H_5 &\ll h\Big(\frac{h}{p^{\mu}}+1\Big)\sum_k\Big(\frac{h}{p^{\mu-k}}+1\Big)\\ &\quad\times\sum_{\varepsilon,m}\Big(\frac{h}{p^{\max(\varepsilon-m,m)}}+1\Big)\Big(\frac{h}{p^{\min(m,[(\varepsilon+1)/2])}}+1\Big)\\ &\quad\times\Big(\frac{h}{p^{\mu-\varepsilon}}+1\Big)\sum_{\gamma_5,\gamma_6}\Big(\frac{h}{p^{\gamma_5}}+1\Big)\Big(\frac{h}{p^{\gamma_6}}+1\Big)\\ &\ll \mu^5 A\,. \ \blacksquare\end{aligned}$$

LEMMA 9. *If* $H_6=\{S:[\mu/4]<k\le[\mu/2],\ m>0,\ \varepsilon<\mu,\ \gamma_8=0$ *and* $p\mid M_4\}$ *then* $\#H_6\ll\mu^4A$.

Proof. Given M_4, M_5, M_6, M_7 we have $\ll h/p^{\max(\mu-\varepsilon,k)}+1$ choices for M_8 from (6), (8) and (11). From (8) there are $\ll h/p^{[(\varepsilon+1)/2]}+1$ choices for M_4 given M_5, M_6, M_7. Hence, using (7),

$$\begin{aligned}\#H_6 &\ll h\Big(\frac{h}{p^{\mu}}+1\Big)\sum_{\gamma_5,\gamma_6}\Big(\frac{h}{p^{\gamma_5}}+1\Big)\Big(\frac{h}{p^{\gamma_6}}+1\Big)\Big(\frac{h}{p^{\mu-\gamma_5-\gamma_6}}+1\Big)\\ &\quad\times\sum_{\varepsilon,k}\Big(\frac{h}{p^{[(\varepsilon+1)/2]}}+1\Big)\Big(\frac{h}{p^{\mu-k}}+1\Big)\Big(\frac{h}{p^{\max(\mu-\varepsilon,k)}}+1\Big)\\ &\ll \mu^4 A\,. \ \blacksquare\end{aligned}$$

LEMMA 10. *If* $H_7=\{S:[\mu/4]<k\le[\mu/2],\ m\ge\mu-[\mu/4],\ \varepsilon<\mu,\ \gamma_8>0$ *and* $p\mid M_4\}$ *then* $\#H_7\ll\mu^5A$.

Proof. Given M_5, M_6, M_7, M_8 there are $\ll h/p^m+1$ choices for M_4 from (10). By (7) it follows that

$$\begin{aligned}\#H_7 &\ll h\Big(\frac{h}{p^{\mu}}+1\Big)\sum_{\gamma_5,\gamma_6,\gamma_7}\Big(\frac{h}{p^{\gamma_5}}+1\Big)\Big(\frac{h}{p^{\gamma_6}}+1\Big)\Big(\frac{h}{p^{\gamma_7}}+1\Big)\Big(\frac{h}{p^{\mu-\gamma_5-\gamma_6-\gamma_7}}+1\Big)\\ &\quad\times\sum_k\Big(\frac{h}{p^{\mu-k}}+1\Big)\sum_m\Big(\frac{h}{p^m}+1\Big)\\ &\ll \mu^5 A\,. \ \blacksquare\end{aligned}$$

The conditions S have now been extended as follows:

$$S' = \text{“}S: 0<m<\mu-[\mu/4],\ \varepsilon<\mu,\ [\mu/4]<k\le[\mu/2],\ \gamma_8>0 \text{ and } p\mid M_4\text{”}\,.$$

This notation will be used in the next section.

5. Extending the conditions S'. In all the remaining cases we obtain an expression of the form

$$\#H_i \ll h\left(\frac{h}{p^{\mu}}+1\right)\sum\left(\frac{h^6}{p^{D_a}}+\frac{h^5}{p^{D_b}}+\frac{h^4}{p^{D_c}}+h^3\right),$$

where the sum is over a maximum of six variables. It is sufficient to show that $D_a \ge 2\mu+[\mu/2]-[\mu/4]$, $D_b \ge \mu+[\mu/2]-[\mu/4]$ and $D_c \ge \mu-[\mu/2]$ since

$$h\left(\frac{h}{p^{\mu}}+1\right)\left(\frac{h^6}{p^{2\mu+[\mu/2]-[\mu/4]}}+\frac{h^5}{p^{\mu+[\mu/2]-[\mu/4]}}+\frac{h^4}{p^{\mu-[\mu/2]}}+h^3\right)\ll A\,.$$

We now continue with further steps in the proof of Theorem 1.

Lemma 11. *If $H_8=\{S' : 2k\le \varepsilon\}$ then $\#H_8 \ll \mu^6 A$.*

Proof. From (8) and (11) we know that $p^k \mid M_4+M_8-M_5-M_6-M_7$. By (10), this implies that $p^{\min(m,k)} \mid M_4-M_8$. Hence, by (6) and (7), it follows that

$$\varepsilon+\min(m,k)\le \gamma_5+\gamma_6+\gamma_7<\mu\,. \tag{12}$$

There are $\ll h/p^{\mu-\varepsilon}+1$ choices for M_8 from (6) and (8), given M_4, M_5, M_6, M_7, and $\ll h/p^{\max(\varepsilon-m,m)}+1$ choices for M_4 from (8) and (10), given M_5, M_6, M_7. Therefore

$$\begin{aligned}\#H_8 &\ll h\left(\frac{h}{p^{\mu}}+1\right)\sum_{k,\varepsilon,m}\left(\frac{h}{p^{\mu-k}}+1\right)\left(\frac{h}{p^{\mu-\varepsilon}}+1\right)\left(\frac{h}{p^{\max(\varepsilon-m,m)}}+1\right)\\
&\qquad\times\sum_{\gamma_5,\gamma_6,\gamma_7}\left(\frac{h}{p^{\gamma_5}}+1\right)\left(\frac{h}{p^{\gamma_6}}+1\right)\left(\frac{h}{p^{\gamma_7}}+1\right)\\
&\ll h\left(\frac{h}{p^{\mu}}+1\right)\sum_{\substack{k,\varepsilon,m\\ \gamma_5,\gamma_6,\gamma_7}}\left(\frac{h^6}{p^{D_1}}+\frac{h^5}{p^{D_2}}+\frac{h^4}{p^{D_3}}+h^3\right),\end{aligned}$$

where

$$\begin{aligned}D_1 &= 2\mu-k-\varepsilon+\max(\varepsilon-m,m)+\gamma_5+\gamma_6+\gamma_7\,,\\
D_2 &= \min(2\mu-k-\varepsilon+\max(\varepsilon-m,m), 2\mu-k-\varepsilon+\gamma_5+\gamma_6+\gamma_7\,,\\
&\qquad\qquad \mu-\varepsilon+\max(\varepsilon-m,m)+\gamma_5+\gamma_6+\gamma_7)\,,\\
D_3 &= \min(\mu-\varepsilon+\max(\varepsilon-m,m), \mu-\varepsilon+\gamma_5+\gamma_6+\gamma_7, 2\mu-k-\varepsilon\,,\\
&\qquad\qquad \gamma_5+\gamma_6+\gamma_7+\max(\varepsilon-m,m))\,.\end{aligned}$$

It can be seen from (12) that $D_1 \ge 2\mu-k+\max(\varepsilon-m,m)+\min(m,k)\ge 2\mu+[\mu/2]-[\mu/4]$. By (7) we know that $\gamma_5+\gamma_6+\gamma_7\ge \mu-[\mu/4]>\mu-k$. Also, if $\max(\varepsilon-m,m)>\gamma_5+\gamma_6+\gamma_7$ then $\varepsilon-m>\gamma_5+\gamma_6+\gamma_7$. This is possible only if $m<[\mu/4]$, in which case (12) implies that $\varepsilon+m\le\gamma_5+\gamma_6+\gamma_7<\varepsilon-m$, a contradiction. We conclude that $\max(\varepsilon-m,m)\le\gamma_5+\gamma_6+\gamma_7$. Hence $D_3=\min(\mu-\varepsilon+\max(\varepsilon-m,m),\ 2\mu-k-\varepsilon)\ge\mu-[\varepsilon/2]\ge\mu-[\mu/2]$ and $D_2=2\mu-k-\varepsilon+\max(\varepsilon-m,m)$. If $\varepsilon>[\mu/2]+[\mu/4]$ then (12) implies that $m\le[\mu/4]$ and so $D_2=2\mu-k-m\ge 2\mu-[\mu/2]-[\mu/4]$. If $\varepsilon\le[\mu/2]+[\mu/4]$ then, as $k\le\max(\varepsilon-m,m)$, we have $D_2\ge 2\mu-\varepsilon\ge 2\mu-[\mu/2]-[\mu/4]$. ∎

It may now be assumed that $\mu\ge 2k>\varepsilon$. Consequently, it follows from (8) and (11) that ε is even and

$$p^{\varepsilon/2}\,\|\,M_4+M_8-M_5-M_6-M_7\,. \tag{13}$$

Denote by Q the expression

$$Q=M_5M_6+M_5M_7+M_6M_7+M_4^2-M_4(M_5+M_6+M_7)\,. \tag{14}$$

LEMMA 12. *If $H_9=\{S':2k>\varepsilon,2m>\varepsilon\}$ then $\#H_9\ll\mu^5A$.*

Proof. Given M_4,M_5,M_6,M_7 there are $\ll h/p^{\max(\mu-\varepsilon,2k-\varepsilon/2)}+1$ choices for M_8 from (6), (8), (11) and (13). By (10), $p^{2m}\,\|\,(2M_4-M_5-M_6-M_7)^2$ and so

$$4Q\equiv 2(M_5M_6+M_5M_7+M_6M_7)-M_5^2-M_6^2-M_7^2 \pmod{p^{2m}}\,.$$

As $p^\varepsilon\,\|\,Q$ we deduce that

$$p^\varepsilon\,\|\,M_5^2+M_6^2+M_7^2-2(M_5M_6+M_5M_7+M_6M_7)\,. \tag{15}$$

It follows from (10) and (13) that $p^{\varepsilon/2}\mid M_4-M_8$, which, together with (6) and (7), implies that

$$3\varepsilon/2\le\gamma_5+\gamma_6+\gamma_7<\mu\,. \tag{16}$$

Thus from (6) we obtain

$$\frac{Q}{p^\varepsilon}\cdot\frac{M_4-M_8}{p^{\varepsilon/2}}\equiv\frac{M_5M_6M_7}{p^{3\varepsilon/2}} \pmod{p^{\mu-3\varepsilon/2}}$$

and from (11) and (13) we have

$$\left(\frac{Q}{p^\varepsilon}\cdot\frac{M_4+M_8-M_5-M_6-M_7}{p^{\varepsilon/2}}\right)^2\equiv\frac{4Q^3}{p^{3\varepsilon}} \pmod{p^{2k-\varepsilon}}\,.$$

Since $M_4+M_8-M_5-M_6-M_7=2M_4-M_5-M_6-M_7-(M_4-M_8)$, combining the above two congruences produces

$$\left(\frac{Q(2M_4-M_5-M_6-M_7)-M_5M_6M_7}{p^{3\varepsilon/2}}\right)^2\equiv\frac{4Q^3}{p^{3\varepsilon}} \pmod{p^{\min(\mu-3\varepsilon/2,\,2k-\varepsilon)}},$$

which simplifies to

$$\begin{aligned}(17)\qquad & Q^2(M_5^2+M_6^2+M_7^2-2(M_5M_6+M_5M_7+M_6M_7))\\ &\equiv M_5M_6M_7(2Q(2M_4-M_5-M_6-M_7)-M_5M_6M_7) \pmod{p^{\min(\mu+3\varepsilon/2,\,2k+2\varepsilon)}}.\end{aligned}$$

From (15) it can be seen that $p^{3\varepsilon} \parallel$ LHS of (17). By (16) we must have $\min(\mu + 3\varepsilon/2,\ 2k + 2\varepsilon) > 3\varepsilon$ and thus $p^{3\varepsilon} \parallel$ RHS of (17), or

$$p^{3\varepsilon-\gamma_5-\gamma_6-\gamma_7} \parallel 2Q(2M_4 - M_5 - M_6 - M_7) - M_5M_6M_7\,.$$

This together with (10) implies that

$$3\varepsilon - \gamma_5 - \gamma_6 - \gamma_7 \ge \min(\varepsilon + m, \gamma_5 + \gamma_6 + \gamma_7)\,.$$

If $\varepsilon + m \le \gamma_5 + \gamma_6 + \gamma_7$ then $2\varepsilon - m \ge \gamma_5 + \gamma_6 + \gamma_7 \ge \varepsilon + m$, contradicting $2m > \varepsilon$. Hence, from (7), (16) and the above we conclude that

$$\mu - \left[\frac{\mu}{4}\right] \le \frac{3\varepsilon}{2} = \gamma_5 + \gamma_6 + \gamma_7 < \mu\,. \tag{18}$$

It follows from (8), (10) and (18) that

$$\begin{aligned}p^{5\varepsilon/2} \parallel 2Q(2M_4-M_5-M_6-M_7)(M_5^2+M_6^2+M_7^2-2(M_5M_6+M_5M_7+M_6M_7))\\ -2M_5M_6M_7(2Q + (2M_4 - M_5 - M_6 - M_7)^2)\,.\end{aligned}$$

This is the derivative of (17) with respect to M_4 and so there are $\ll h/p^{\min(\mu-\varepsilon,\, 2k-\varepsilon/2)} + 1$ choices for M_4 given M_5, M_6, M_7. By (7) and (18) it follows that

$$\begin{aligned}\#H_9 &\ll h\left(\frac{h}{p^{\mu}} + 1\right)\sum_{k,\varepsilon}\left(\frac{h}{p^{\min(\mu-\varepsilon,2k-\varepsilon/2)}} + 1\right)\left(\frac{h}{p^{\max(\mu-\varepsilon,2k-\varepsilon/2)}} + 1\right)\\ &\quad\times\left(\frac{h}{p^{\mu-k}} + 1\right)\sum_{\gamma_5,\gamma_6,\gamma_7}\left(\frac{h}{p^{\gamma_5}} + 1\right)\left(\frac{h}{p^{\gamma_6}} + 1\right)\left(\frac{h}{p^{\gamma_7}} + 1\right)\\ &\ll \mu^3 h\left(\frac{h}{p^{\mu}} + 1\right)\sum_{k,\varepsilon}\left(\frac{h^6}{p^{D_4}} + \frac{h^5}{p^{D_5}} + \frac{h^4}{p^{D^6}} + h^3\right),\end{aligned}$$

where

$$\begin{aligned}D_4 &= 2\mu + k \ge 2\mu + \left[\frac{\mu}{2}\right] - \left[\frac{\mu}{4}\right],\\ D_5 &= \min\left(2\mu + k - \frac{3\varepsilon}{2}, 2\mu - k + \frac{\varepsilon}{2}, \mu + k + \varepsilon\right)\\ &> \min(2\mu - \varepsilon, \mu + k) \ge \mu + \left[\frac{\mu}{2}\right] - \left[\frac{\mu}{4}\right],\\ D_6 &= \min\left(\mu + 2k - \frac{3\varepsilon}{2}, 2\mu - k - \varepsilon, \mu + k - \frac{\varepsilon}{2}, \mu - k + \frac{3\varepsilon}{2}\right)\\ &> \mu - k \ge \mu - \left[\frac{\mu}{2}\right]. \ \blacksquare\end{aligned}$$

Lemma 13. *If* $H_{10} = \{S' : 2k > \varepsilon > 2m\}$ *then* $\#H_{10} \ll \mu^6 A$.

Proof. Given M_4, M_5, M_6, M_7 there are $\ll h/p^{\max(\mu-\varepsilon, 2k-\varepsilon/2)} + 1$ choices for M_8 from (6), (8), (11) and (13). Since $p \neq 2$, from (8) and (14) we know that $p^\varepsilon \parallel 4Q$. This can be rewritten as

$$(2M_4 - M_5 - M_6 - M_7)^2 \equiv M_5^2 + M_6^2 + M_7^2 - 2(M_5M_6 + M_5M_7 + M_6M_7) \pmod{p^\varepsilon},$$

which, together with (10), implies that

$$p^{2m} \parallel M_5^2 + M_6^2 + M_7^2 - 2(M_5M_6 + M_5M_7 + M_6M_7). \tag{19}$$

From (10) and (13) we see that $p^m \mid M_4 - M_8$ and so from (6) and (7) we have

$$\varepsilon + m \le \gamma_5 + \gamma_6 + \gamma_7 < \mu. \tag{20}$$

Using (6), (11), (13) and (20) we deduce that

$$\frac{Q}{p^\varepsilon} \cdot \frac{M_4 - M_8}{p^m} \equiv \frac{M_5M_6M_7}{p^{\varepsilon+m}} \pmod{p^{\mu-\varepsilon-m}}$$

and

$$\left(\frac{Q}{p^\varepsilon} \cdot \frac{M_4 + M_8 - M_5 - M_6 - M_7}{p^m}\right)^2 \equiv \frac{4Q^3}{p^{2\varepsilon+2m}} \pmod{p^{2k-2m}}.$$

Combining these two congruences as in the previous lemma, we obtain

$$\begin{aligned} &Q^2(M_5^2 + M_6^2 + M_7^2 - 2(M_5M_6 + M_5M_7 + M_6M_7)) \\ &\equiv M_5M_6M_7(2Q(2M_4 - M_5 - M_6 - M_7) - M_5M_6M_7) \pmod{p^{\min(\mu+\varepsilon+m, 2k+2\varepsilon)}}. \end{aligned} \tag{21}$$

By (8) and (19), $p^{2\varepsilon+2m} \parallel$ LHS of (21). But from (20) we know that $\min(\mu + \varepsilon + m, 2k + 2\varepsilon) > 2\varepsilon + 2m$ and so $p^{2\varepsilon+2m} \parallel$ RHS of (21), or

$$p^{2\varepsilon+2m-\gamma_5-\gamma_6-\gamma_7} \parallel 2Q(2M_4 - M_5 - M_6 - M_7) - M_5M_6M_7.$$

Hence, by (10), we see that $2\varepsilon + 2m - \gamma_5 - \gamma_6 - \gamma_7 \ge \min(\varepsilon + m, \gamma_5 + \gamma_6 + \gamma_7)$, which, together with (7) and (20), implies that

$$\mu - \left[\frac{\mu}{4}\right] \le \varepsilon + m = \gamma_5 + \gamma_6 + \gamma_7 < \mu. \tag{22}$$

Also, from (10), (19) and (22) it can be seen that

$$\begin{aligned} p^{4m} \parallel\, &(2(2M_4 - M_5 - M_6 - M_7)^2 + 4Q)(M_5^2 + M_6^2 + M_7^2 \\ &- 2(M_5M_6 + M_5M_7 + M_6M_7)) - 12M_5M_6M_7(2M_4 - M_5 - M_6 - M_7). \end{aligned}$$

This expression is the second derivative of (21) with respect to M_4 and so there are $\ll h/p^{[(\min(\mu+\varepsilon-3m, 2k+2\varepsilon-4m)+1)/2]} + 1$ choices for M_4, given

M_5, M_6, M_7. Hence, by (22),

$$\begin{aligned}
\#H_{10} &\ll h\biggl(\frac{h}{p^{\mu}}+1\biggr)\\
&\qquad \times \sum_{k,\varepsilon,m}\biggl(\frac{h}{p^{\max(\mu-\varepsilon,2k-\varepsilon/2)}}+1\biggr)\biggl(\frac{h}{p^{\min([(\mu+\varepsilon-3m+1)/2],k+\varepsilon-2m)}}+1\biggr)\\
&\qquad \times \biggl(\frac{h}{p^{\mu-k}}+1\biggr)\sum_{\gamma_5,\gamma_6,\gamma_7}\biggl(\frac{h}{p^{\gamma_5}}+1\biggr)\biggl(\frac{h}{p^{\gamma_6}}+1\biggr)\biggl(\frac{h}{p^{\gamma_7}}+1\biggr)\\
&\ll \mu^3 h\biggl(\frac{h}{p^{\mu}}+1\biggr)\sum_{k,\varepsilon,m}\biggl(\frac{h^6}{p^{D_7}}+\frac{h^5}{p^{D_8}}+\frac{h^4}{p^{D_9}}+h^3\biggr),
\end{aligned}$$

where

$$\begin{aligned}
D_7 &= \max\Bigl(2\mu-k,\mu+k+\frac{\varepsilon}{2}\Bigr)+\min\Bigl(\Bigl[\frac{\mu+\varepsilon-m+1}{2}\Bigr],k+\varepsilon-m\Bigr)\\
&\ge 2\mu+\frac{\varepsilon}{2}\ge 2\mu+\Bigl[\frac{\mu}{2}\Bigr]-\Bigl[\frac{\mu}{4}\Bigr],\\
D_8 &= \mu-k+\min\Bigl(\max\Bigl(\mu-\frac{\varepsilon}{2},2k\Bigr)+\min\Bigl(\Bigl[\frac{\mu-3m+1}{2}\Bigr],k+\frac{\varepsilon}{2}-2m\Bigr),\\
&\qquad \max\Bigl(\mu+m,2k+\frac{\varepsilon}{2}+m\Bigr),\\
&\qquad \varepsilon+\min\Bigl(\Bigl[\frac{\mu+\varepsilon-m+1}{2}\Bigr],k+\varepsilon-m\Bigr)\Bigr)\\
&> \mu+k\ge \mu+\Bigl[\frac{\mu}{2}\Bigr]-\Bigl[\frac{\mu}{4}\Bigr],\\
D_9 &= \min\Bigl(\mu-k+\min\Bigl(\varepsilon+m,\max\Bigl(\mu-\varepsilon,2k-\frac{\varepsilon}{2}\Bigr),\\
&\qquad \min\Bigl(\Bigl[\frac{\mu+\varepsilon-3m+1}{2}\Bigr],k+\varepsilon-2m\Bigr)\Bigr),\\
&\qquad \min\Bigl(\Bigl[\frac{\mu-3m+1}{2}\Bigr],k+\frac{\varepsilon}{2}-2m\Bigr)+\max\Bigl(\mu-\frac{\varepsilon}{2},2k\Bigr)\Bigr)\\
&> \mu-k\ge \mu-\Bigl[\frac{\mu}{2}\Bigr]. \ \blacksquare
\end{aligned}$$

It may now be assumed that $\varepsilon = 2m$. There are $\ll h/p^{\max(\mu-2m,2k-m)}+1$ choices for M_8 from (6), (8), (11) and (13) given M_4, M_5, M_6, M_7.

Lemma 14. *If* $H_{11} = \{S' : 2k > \varepsilon = 2m$ *and* $\gamma_5+\gamma_6+\gamma_7 \ge 2k+m\}$ *then* $\#H_{11} \ll \mu^5 A$.

P r o o f. From (10) there are $\ll h/p^m+1$ choices for M_4 given M_5, M_6, M_7 and it follows that

$$\#H_{11} \ll h\Big(\frac{h}{p^\mu}+1\Big)\sum_{k,m}\Big(\frac{h}{p^{\max(\mu-2m,2k-m)}}+1\Big)\Big(\frac{h}{p^{\mu-k}}+1\Big)\Big(\frac{h}{p^m}+1\Big)$$
$$\times\sum_{\gamma_5,\gamma_6,\gamma_7}\Big(\frac{h}{p^{\gamma_5}}+1\Big)\Big(\frac{h}{p^{\gamma_6}}+1\Big)\Big(\frac{h}{p^{\gamma_7}}+1\Big)$$
$$\ll \mu^3 h\Big(\frac{h}{p^\mu}+1\Big)\sum_{k,m}\Big(\frac{h^6}{p^{D_{10}}}+\frac{h^5}{p^{D_{11}}}+\frac{h^4}{p^{D_{12}}}+h^3\Big),$$

where

$$D_{10}=\mu+k+2m+\max(\mu-2m,2k-m)\ge 2\mu+k\ge 2\mu+\Big[\frac{\mu}{2}\Big]-\Big[\frac{\mu}{4}\Big],$$
$$D_{11}=\min(\mu+k+2m,\min(\mu-k+m,2k+2m)+\max(\mu-2m,2k-m))$$
$$\ge \mu+k\ge\mu+\Big[\frac{\mu}{2}\Big]-\Big[\frac{\mu}{4}\Big],$$
$$D_{12}=\min(\max(\mu-m,2k),\mu-k+m,2k+2m)$$
$$\ge\min(\mu-k,2k)\ge\mu-\Big[\frac{\mu}{2}\Big].\ \blacksquare$$

By (10) and (13) we know that $p^m \mid M_4-M_8$ and so, by (6), (7) and (8),

$$3m\le\gamma_5+\gamma_6+\gamma_7<\mu. \tag{23}$$

Also, with Q given by (14), from (6), (11) and (13) we obtain

$$\frac{Q}{p^{2m}}\cdot\frac{M_4-M_8}{p^m}\equiv\frac{M_5M_6M_7}{p^{3m}}\pmod{p^{\mu-3m}}$$

and

$$\Big(\frac{Q}{p^{2m}}\cdot\frac{M_4+M_8-M_5-M_6-M_7}{p^m}\Big)^2\equiv\frac{4Q^3}{p^{6m}}\pmod{p^{2k-2m}}.$$

Proceeding as in Lemma 12, these two congruences combine to produce

$$Q^2(M_5^2+M_6^2+M_7^2-2(M_5M_6+M_5M_7+M_6M_7))$$
$$\equiv M_5M_6M_7(2Q(2M_4-M_5-M_6-M_7)-M_5M_6M_7)\pmod{p^{\min(2k+4m,\mu+3m)}}. \tag{24}$$

Define x by

$$p^x \,\|\, (M_5^2+M_6^2+M_7^2-2(M_5M_6+M_5M_7+M_6M_7),p^\mu). \tag{25}$$

Lemma 15. *If $H_{12}=\{S' : (25)$ holds, $x\ge 2k>\varepsilon=2m$ and $2k+m>\gamma_5+\gamma_6+\gamma_7\}$ then $\#H_{12}\ll\mu^5A$.*

Proof. Since $p^{2m} \parallel Q$ (25) implies that $p^{\min(2k+4m,\mu+3m)} \mid$ RHS of (24) or, by (7),

$$4Q(2M_4-M_5-M_6-M_7) \equiv 2M_5M_6M_7 \pmod{p^{\min(2k+4m,\mu+3m)-\gamma_5-\gamma_6-\gamma_7}}.$$

We know that $\min(2k+4m,\mu+3m)-\gamma_5-\gamma_6-\gamma_7 > 3m$. Since $p^{3m} \parallel$ LHS and $p^{\gamma_5+\gamma_6+\gamma_7} \parallel$ RHS of the above we conclude that

$$\mu - \left[\frac{\mu}{4}\right] \le 3m = \gamma_5+\gamma_6+\gamma_7 < \mu\,. \tag{26}$$

As $4Q = (2M_4-M_5-M_6-M_7)^2-M_5^2-M_6^2-M_7^2+2(M_5M_6+M_5M_7+M_6M_7)$ we can rewrite the above as

$$\begin{aligned}(2M_4 - M_5 - M_6 - M_7)((2M_4 - M_5 - M_6 - M_7)^2 \\ - M_5^2 - M_6^2 - M_7^2 + 2(M_5M_6 + M_5M_7 + M_6M_7)) \\ \equiv 2M_5M_6M_7 \pmod{p^{\min(2k+m,\mu)}}\,.\end{aligned}$$

By (10) and (25) it follows that

$$\begin{aligned}p^{2m} \parallel 6(2M_4 - M_5 - M_6 - M_7)^2 \\ -2(M_5^2 + M_6^2 + M_7^2 - 2(M_5M_6 + M_5M_7 + M_6M_7))\,.\end{aligned}$$

This is the derivative of the above expression with respect to M_4 and so there are $\ll h/p^{\min(2k-m,\mu-2m)}+1$ choices for M_4 given M_5, M_6, M_7. Therefore

$$\begin{aligned}\#H_{12} \ll h\left(\frac{h}{p^{\mu}}+1\right)\sum_{k,m}\left(\frac{h}{p^{\min(2k-m,\mu-2m)}}+1\right) \\ \times\left(\frac{h}{p^{\max(2k-m,\mu-2m)}}+1\right)\left(\frac{h}{p^{\mu-k}}+1\right) \\ \times\sum_{\gamma_5,\gamma_6,\gamma_7}\left(\frac{h}{p^{\gamma_5}}+1\right)\left(\frac{h}{p^{\gamma_6}}+1\right)\left(\frac{h}{p^{\gamma_7}}+1\right).\end{aligned}$$

As (26) holds, the result follows by comparison with Lemma 12. ∎

LEMMA 16. *If* $H_{13} = \{S' : (25)$ *holds*, $2k > x \ge \mu - m$, $2k > \varepsilon = 2m$ *and* $2k+m > \gamma_5+\gamma_6+\gamma_7\}$ *then* $\#H_{13} \ll \mu^5 A$.

Proof. There are $\ll h/p^m+1$ choices for M_4 from (10) given M_5, M_6, M_7 and $\ll h/p^{[(x+1)/2]}+1$ choices for M_7 from (25) given M_5, M_6. By (7) and (23),

$$\begin{aligned}\#H_{13} \ll h\left(\frac{h}{p^{\mu}}+1\right) \\ \times\sum_{k,m,x}\left(\frac{h}{p^{\mu-k}}+1\right)\left(\frac{h}{p^{m}}+1\right)\left(\frac{h}{p^{2k-m}}+1\right)\left(\frac{h}{p^{[(x+1)/2]}}+1\right)\end{aligned}$$

$$\times \sum_{\gamma_5,\gamma_6} \left(\frac{h}{p^{\gamma_5}}+1\right)\left(\frac{h}{p^{\gamma_6}}+1\right)$$
$$\ll \mu h\left(\frac{h}{p^{\mu}}+1\right) \sum_{\substack{k,m\\ \gamma_5,\gamma_6}} \left(\frac{h^6}{p^{D_{13}}}+\frac{h^5}{p^{D_{14}}}+\frac{h^4}{p^{D_{15}}}+h^3\right),$$

where

$$\begin{aligned} D_{13} &= \mu + k + \gamma_5 + \gamma_6 + \left[\frac{\mu - m + 1}{2}\right] \\ &\ge \mu + 2\left[\frac{\mu - m+1}{2}\right] + \max\left(2m, \mu - \left[\frac{\mu}{2}\right]\right), \\ D_{14} &= \left[\frac{\mu - m + 1}{2}\right] + \min(\mu + k, \gamma_5 + \gamma_6 + \min(\mu - k + m, 2k)) \\ &\ge \mu + \left[\frac{\mu - m + 1}{2}\right] > \mu + \left[\frac{\mu}{2}\right] - \left[\frac{\mu}{4}\right], \\ D_{15} &= \min\left(\mu + k, \left[\frac{\mu - m + 1}{2}\right] + \min(2k, \gamma_5 + \gamma_6 + m, \mu - k + m)\right) \\ &> \mu - \left[\frac{\mu}{2}\right]. \end{aligned}$$

If $m > [\mu/4]$ then $D_{13} \ge 2\mu + m \ge 2\mu + [\mu/2] - [\mu/4]$ and if $m \le [\mu/4]$ then $D_{13} \ge 3\mu - m - [\mu/2] \ge 3\mu - [\mu/2] - [\mu/4]$. ∎

It remains to consider $\min(2k, \mu - m) > x$. From (8), (14) and (25) we see that $p^{x+4m} \parallel$ LHS of (24) and thus

$$p^{x+4m} \parallel M_5M_6M_7(2Q(2M_4 - M_5 - M_6 - M_7) - M_5M_6M_7).$$

This together with (23) implies that $x + 4m \ge \gamma_5 + \gamma_6 + \gamma_7 + 3m$, or

$$x \ge \gamma_5 + \gamma_6 + \gamma_7 - m. \tag{27}$$

We now look at the derivatives of (24) with respect to M_4. Define T, U and V by

$$\begin{aligned} p^T \parallel (&Q(2M_4 - M_5 - M_6 - M_7) \\ &\times (M_5^2 + M_6^2 + M_7^2 - 2(M_5M_6 + M_5M_7 + M_6M_7)) \\ &- M_5M_6M_7(2Q + (2M_4 - M_5 - M_6 - M_7)^2), p^{\min(2k+4m,\mu+3m)}), \end{aligned} \tag{28}$$

$$\begin{aligned} p^U \parallel (&(2Q + (2M_4 - M_5 - M_6 - M_7)^2) \\ &\times (M_5^2 + M_6^2 + M_7^2 - 2(M_5M_6 + M_5M_7 + M_6M_7)) \\ &- 6M_5M_6M_7(2M_4 - M_5 - M_6 - M_7), p^{\min(2k+4m,\mu+3m)}) \end{aligned} \tag{29}$$

and

$$p^V \parallel ((2M_4 - M_5 - M_6 - M_7) \times (M_5^2 + M_6^2 + M_7^2 - 2(M_5M_6 + M_5M_7 + M_6M_7)) - 2M_5M_6M_7, p^{\min(2k+4m,\mu+3m)}) \tag{30}$$

By (7), (10), (25) and (27) it can be seen that

$$T \ge \gamma_5 + \gamma_6 + \gamma_7 + 2m\,, \qquad U \ge \gamma_5 + \gamma_6 + \gamma_7 + m\,, \qquad V \ge \gamma_5 + \gamma_6 + \gamma_7\,. \tag{31}$$

The conditions S' have now been extended. In the final section the following notation will be used:

$$S'' = \text{“}S' : (25), (28), (29), (30) \text{ hold, } \min(2k, \mu - m) > x \ge \gamma_5 + \gamma_6 + \gamma_7 - m \text{ and } 2k > \varepsilon = 2m\text{”}.$$

6. Completion of the proof. The following five lemmas conclude the proof of Theorem 1.

LEMMA 17. *If* $H_{14} = \{S'' : T = \gamma_5 + \gamma_6 + \gamma_7 + 2m\}$ *then* $\#H_{14} \ll \mu^5 A$.

Proof. Given M_5, M_6, M_7 there are $\ll h/p^{\min(2k+4m,\mu+3m)-\gamma_5-\gamma_6-\gamma_7-2m} + 1$ choices for M_4 from (24) and (28). Hence

$$\#H_{14} \ll h\left(\frac{h}{p^\mu} + 1\right) \times \sum_{k,m}\left(\frac{h}{p^{\max(\mu-2m,2k-m)}} + 1\right)\left(\frac{h}{p^{\min(2k+2m,\mu+m)-\gamma_5-\gamma_6-\gamma_7}} + 1\right) \times \left(\frac{h}{p^{\mu-k}} + 1\right)\sum_{\gamma_5,\gamma_6,\gamma_7}\left(\frac{h}{p^{\gamma_5}} + 1\right)\left(\frac{h}{p^{\gamma_6}} + 1\right)\left(\frac{h}{p^{\gamma_7}} + 1\right).$$

By (23) we know that $\min(2k+2m, \mu+m) - \gamma_5 - \gamma_6 - \gamma_7 \le \min(2k-m, \mu-2m) \le \max(2k-m, \mu-2m)$ and so the above becomes

$$\#H_{14} \ll h\left(\frac{h}{p^\mu} + 1\right)\sum_{\substack{k,m\\ \gamma_5,\gamma_6,\gamma_7}}\left(\frac{h^6}{p^{D_{16}}} + \frac{h^5}{p^{D_{17}}} + \frac{h^4}{p^{D_{18}}} + h^3\right),$$

where

$$D_{16} = 2\mu + k \ge 2\mu + \left[\frac{\mu}{2}\right] - \left[\frac{\mu}{4}\right],$$

$$D_{17} = \min(2\mu + k - \gamma_5 - \gamma_6 - \gamma_7, \mu + k + 2m, 2\mu + m - k) > \mu + k \ge \mu + \left[\frac{\mu}{2}\right] - \left[\frac{\mu}{4}\right],$$

$$D_{18} = \min(\mu - k + \gamma_5 + \gamma_6 + \gamma_7,\\ \min(\mu + 2k, \mu + k + 2m, 2\mu - k + m) - \gamma_5 - \gamma_6 - \gamma_7) \\ > \mu - k \geq \mu - \left[\frac{\mu}{2}\right]. \ \blacksquare$$

LEMMA 18. *If* $H_{15} = \{S'' : T > \gamma_5+\gamma_6+\gamma_7+2m$ *and* $U = \gamma_5+\gamma_6+\gamma_7+m\}$ *then* $\#H_{15} \ll \mu^5 A$.

Proof. From (24) and (29) there are

$$\ll h/p^{[(\min(2k+4m,\mu+3m)-\gamma_5-\gamma_6-\gamma_7-m+1)/2]} + 1$$

choices for M_4 given M_5, M_6, M_7. Therefore

$$\#H_{15} \ll h\left(\frac{h}{p^{\mu}} + 1\right) \\ \times \sum_{k,m}\left(\frac{h}{p^{[(\min(2k+3m,\mu+2m)-\gamma_5-\gamma_6-\gamma_7+1)/2]}} + 1\right) \\ \times \left(\frac{h}{p^{\max(\mu-2m,2k-m)}} + 1\right)\left(\frac{h}{p^{\mu-k}} + 1\right) \\ \times \sum_{\gamma_5,\gamma_6,\gamma_7}\left(\frac{h}{p^{\gamma_5}} + 1\right)\left(\frac{h}{p^{\gamma_6}} + 1\right)\left(\frac{h}{p^{\gamma_7}} + 1\right).$$

By (23) we see that

$$\left[\frac{\min(2k + 3m, \mu + 2m) - \gamma_5 - \gamma_6 - \gamma_7 + 1}{2}\right] \leq \left[\frac{\min(2k, \mu - m) + 1}{2}\right] \\ < \max(\mu - 2m, 2k - m)$$

and so

$$\#H_{15} \ll h\left(\frac{h}{p^{\mu}} + 1\right) \sum_{\substack{k,m \\ \gamma_5,\gamma_6,\gamma_7}} \left(\frac{h^6}{p^{D_{19}}} + \frac{h^5}{p^{D_{20}}} + \frac{h^4}{p^{D_{21}}} + h^3\right),$$

where

$$D_{19} = \left[\frac{\min(2k + 3m, \mu + 2m) + \gamma_5 + \gamma_6 + \gamma_7 + 1}{2}\right] \\ + \max(2\mu - 2m - k, \mu + k - m),$$

$$D_{20} = \left[\frac{\min(2k + 3m, \mu + 2m) - \gamma_5 - \gamma_6 - \gamma_7 + 1}{2}\right] \\ + \min(\mu - k + \gamma_5 + \gamma_6 + \gamma_7, \max(\mu + k - m, 2\mu - k - 2m)) \\ > m + \min\left(2\mu - k - \left[\frac{\mu}{4}\right], \mu + k - m\right) \geq \mu + \left[\frac{\mu}{2}\right] - \left[\frac{\mu}{4}\right],$$

$$D_{21} = \min\Big(\Big[\frac{\min(2k+3m, \mu+2m) - \gamma_5 - \gamma_6 - \gamma_7 + 1}{2}\Big] + \min(\mu - k, \max(\mu - 2m, 2k - m))\,, \mu - k + \gamma_5 + \gamma_6 + \gamma_7\Big) > \mu - k \geq \mu - \Big[\frac{\mu}{2}\Big]\,.$$

From (7) and (23) it follows that if $2k \leq \mu - m$ then

$$D_{19} \geq 2\mu + \Big[\frac{\gamma_5 + \gamma_6 + \gamma_7 - m + 1}{2}\Big] \geq 2\mu + \Big[\frac{\max(3m, \mu - [\mu/4]) - m + 1}{2}\Big] \geq 2\mu + \Big[\frac{\mu}{2}\Big] - \Big[\frac{\mu}{4}\Big]$$

and if $2k > \mu - m$ then

$$D_{19} \geq \mu + \Big[\frac{\mu - m + 1}{2}\Big] + \Big[\frac{\mu + \max(3m, \mu - [\mu/4]) + 1}{2}\Big] \geq 2\mu + \Big[\frac{\mu}{2}\Big] - \Big[\frac{\mu}{4}\Big]\,. \ \blacksquare$$

It may now be assumed that

(32) $$T > \gamma_5 + \gamma_6 + \gamma_7 + 2m, \quad U > \gamma_5 + \gamma_6 + \gamma_7 + m\,.$$

From (30) it follows that $(2M_4 - M_5 - M_6 - M_7)(M_5^2 + M_6^2 + M_7^2 - 2(M_5M_6 + M_5M_7 + M_6M_7)) = Hp^V + 2M_5M_6M_7$ for some $H \in \mathbb{Z}$ with $p \nmid H$. Substituting this into (28) gives

$$QHp^V \equiv M_5M_6M_7(2M_4 - M_5 - M_6 - M_7)^2 \pmod{p^T}\,.$$

By (7) and (10) we know that $p^{\gamma_5+\gamma_6+\gamma_7+2m} \parallel$ RHS of the above and thus, by (32), $p^{\gamma_5+\gamma_6+\gamma_7+2m} \parallel QHp^V$, from which we conclude

(33) $$V = \gamma_5 + \gamma_6 + \gamma_7\,.$$

It can be seen from (29) that

$$(M_5^2 + M_6^2 + M_7^2 - 2(M_5M_6 + M_5M_7 + M_6M_7))((2M_4 - M_5 - M_6 - M_7)^2 + 2Q) \equiv 6M_5M_6M_7(2M_4 - M_5 - M_6 - M_7) \pmod{p^U}\,.$$

By (7) and (10) $p^{\gamma_5+\gamma_6+\gamma_7+m} \parallel$ RHS and so, by (32), $p^{\gamma_5+\gamma_6+\gamma_7+m} \parallel$ LHS. Thus, using (10), (25) and (27), we deduce that $p^{2m} \parallel (2M_4 - M_5 - M_6 - M_7)^2 + 2Q$ and

(34) $$x = \gamma_5 + \gamma_6 + \gamma_7 - m\,.$$

From (28) we have

$$4Q(2M_4 - M_5 - M_6 - M_7)(M_5^2 + M_6^2 + M_7^2 - 2(M_5M_6 + M_5M_7 + M_6M_7)) - 2M_5M_6M_7(4Q + 2(2M_4 - M_5 - M_6 - M_7)^2) \equiv 0 \pmod{p^T}\,.$$

As

$$4Q=(2M_4-M_5-M_6-M_7)^2-(M_5^2+M_6^2+M_7^2-2(M_5M_6+M_5M_7+M_6M_7))$$

this can be rewritten as

$$\begin{aligned}((2M_4-M_5-M_6-M_7)^3+2M_5M_6M_7)\\ \times(M_5^2+M_6^2+M_7^2-2(M_5M_6+M_5M_7+M_6M_7))\\ -(2M_4-M_5-M_6-M_7)(M_5^2+M_6^2+M_7^2-2(M_5M_6+M_5M_7+M_6M_7))\\ -6M_5M_6M_7(2M_4-M_5-M_6-M_7)^2\equiv 0 \pmod{p^T}.\end{aligned}$$

It follows from (7), (10), (25) and (34) that

$$\begin{aligned}(2M_4-M_5-M_6-M_7)^3(M_5^2+M_6^2+M_7^2-2(M_5M_6+M_5M_7+M_6M_7))\\ -6M_5M_6M_7(2M_4-M_5-M_6-M_7)^2\equiv 0 \pmod{p^{\min(T,2(\gamma_5+\gamma_6+\gamma_7)-m)}},\end{aligned}$$

which, together with (10), implies that

$$\begin{aligned}(2M_4-M_5-M_6-M_7)(M_5^2+M_6^2+M_7^2-2(M_5M_6+M_5M_7+M_6M_7))\\ -6M_5M_6M_7\equiv 0 \pmod{p^{\min(T-2m,2(\gamma_5+\gamma_6+\gamma_7)-3m)}}.\end{aligned}\tag{35}$$

By (29),

$$\begin{aligned}(2(2M_4-M_5-M_6-M_7)^2+4Q)(M_5^2+M_6^2+M_7^2-2(M_5M_6+M_5M_7+M_6M_7))\\ -12M_5M_6M_7(2M_4-M_5-M_6-M_7)\equiv 0 \pmod{p^U}.\end{aligned}$$

Substituting for $4Q$ this becomes

$$\begin{aligned}3(2M_4-M_5-M_6-M_7)^2(M_5^2+M_6^2+M_7^2-2(M_5M_6+M_5M_7+M_6M_7))\\ -(M_5^2+M_6^2+M_7^2-2(M_5M_6+M_5M_7+M_6M_7))^2\\ -12M_5M_6M_7(2M_4-M_5-M_6-M_7)\equiv 0 \pmod{p^U},\end{aligned}$$

which, by (10), (25) and (34), reduces to

$$\begin{aligned}(2M_4-M_5-M_6-M_7)(M_5^2+M_6^2+M_7^2-2(M_5M_6+M_5M_7+M_6M_7))\\ -4M_5M_6M_7\equiv 0 \pmod{p^{\min(U-m,2(\gamma_5+\gamma_6+\gamma_7)-3m)}}.\end{aligned}$$

Subtracting (35) from the above congruence we obtain $2M_5M_6M_7\equiv 0 \pmod{p^{\min(U-m,T-2m,2(\gamma_5+\gamma_6+\gamma_7)-3m)}}$ and so, by (7), $\gamma_5+\gamma_6+\gamma_7\ge\min(U-m,T-2m,2(\gamma_5+\gamma_6+\gamma_7)-3m)$. This, together with (7), (23) and (32), implies that

$$\mu-\left[\frac{\mu}{4}\right]\le 3m=\gamma_5+\gamma_6+\gamma_7<\mu.\tag{36}$$

It follows from (36) that

$$\left[\frac{\mu}{2}\right]-\left[\frac{\mu}{4}\right]\le m<k\le\left[\frac{\mu}{2}\right]\le 2m.$$

LEMMA 19. *If* $H_{16} = \{S'' : (32)$ *holds and* $2U \ge \min(\mu + 5m, 2k + 6m)\}$ *then* $\#H_{16} \ll \mu^5 A$.

P r o o f. Given M_5, M_6, M_7 there are $\ll h/p^{U-3m} + 1$ choices for M_4 from (29), (30), (33) and (36). As

$$U \ge \min\left(\left[\frac{\mu + 5m + 1}{2}\right], k + 3m\right)$$

we may take the number of M_4 to be $\ll h/p^{\min(k,[(\mu-m+1)/2])} + 1$. Using (36) it follows that

$$\begin{aligned}
\#H_{16} &\ll h\left(\frac{h}{p^{\mu}} + 1\right) \\
&\quad \times \sum_{k,m}\left(\frac{h}{p^{\min([(\mu-m+1)/2],k)}} + 1\right)\left(\frac{h}{p^{\max(\mu-2m,2k-m)}} + 1\right) \\
&\quad \times \left(\frac{h}{p^{\mu-k}} + 1\right)\sum_{\gamma_5,\gamma_6,\gamma_7}\left(\frac{h}{p^{\gamma_5}} + 1\right)\left(\frac{h}{p^{\gamma_6}} + 1\right)\left(\frac{h}{p^{\gamma_7}} + 1\right) \\
&\ll \mu^3 h\left(\frac{h}{p^{\mu}} + 1\right)\sum_{k,m}\left(\frac{h^6}{p^{D_{22}}} + \frac{h^5}{p^{D_{23}}} + \frac{h^4}{p^{D_{24}}} + h^3\right),
\end{aligned}$$

where

$$\begin{aligned}
D_{22} &= \mu - k + 3m + \min\left(k, \left[\frac{\mu - m + 1}{2}\right]\right) + \max(\mu - 2m, 2k - m) \\
&\ge 2\mu + m \ge 2\mu + \left[\frac{\mu}{2}\right] - \left[\frac{\mu}{4}\right], \\
D_{23} &= \min\left(k, \left[\frac{\mu - m + 1}{2}\right]\right) \\
&\quad + \min(\mu - k + 3m, \max(2\mu - k - 2m, \mu + k - m)) \\
&> \mu + \min\left(k, \left[\frac{\mu - m + 1}{2}\right]\right) > \mu + \left[\frac{\mu}{2}\right] - \left[\frac{\mu}{4}\right], \\
D_{24} &= \min\left(\mu - k + 3m, \min\left(k, \left[\frac{\mu - m + 1}{2}\right]\right)\right. \\
&\quad \left. + \min(\mu - k, \max(2k - m, \mu - 2m))\right) \\
&> \min(\mu - k, 2k) \ge \mu - \left[\frac{\mu}{2}\right]. \ \blacksquare
\end{aligned}$$

For the final two cases it may be assumed that

$$2U < \min(2k+6m, \mu+5m)\,. \tag{37}$$

We rewrite (24) as

$$A_4M_4^4 + A_3M_4^3 + A_2M_4^2 + A_1M_4 + A_0 \equiv 0 \pmod{p^{\min(2k+4m,\mu+3m)}}\,. \tag{38}$$

Hence (28) and (29) now become

$$p^T \parallel (4A_4M_4^3 + 3A_3M_4^2 + 2A_2M_4 + A_1, p^{\min(2k+4m,\mu+3m)}) \tag{39}$$

and

$$p^U \parallel (12A_4M_4^2 + 6A_3M_4 + 2A_2, p^{\min(2k+4m,\mu+3m)}) \tag{40}$$

where

$$\begin{aligned} A_4 &= \sigma_1^2 - 4\sigma_2 = M_5^2 + M_6^2 + M_7^2 - 2(M_5M_6 + M_5M_7 + M_6M_7)\,,\\ A_3 &= 8\sigma_1\sigma_2 - 2\sigma_1^3 - 4M_5M_6M_7\,,\\ A_2 &= \sigma_1^4 - 2\sigma_1^2\sigma_2 - 8\sigma_2^2 + 6M_5M_6M_7\sigma_1\,,\\ A_1 &= 8\sigma_1\sigma_2^2 - 2\sigma_1^3\sigma_2 - 4M_5M_6M_7\sigma_2 - 2M_5M_6M_7\sigma_1^2\,,\\ A_0 &= \sigma_1^2\sigma_2^2 - 4\sigma_2^3 + 2M_5M_6M_7\sigma_1\sigma_2 + M_5^2M_6^2M_7^2\,, \end{aligned} \tag{41}$$

and

$$\sigma_1 = M_5 + M_6 + M_7 \quad \text{and} \quad \sigma_2 = M_5M_6 + M_5M_7 + M_6M_7\,.$$

From (39) we see that for some $R \in \mathbb{Z}$, $p \nmid R$,

$$M_4^3 = \frac{Rp^T - 3A_3M_4^2 - 2A_2M_4 - A_1}{4A_4}\,.$$

This, in conjunction with (38), implies that

$$A_0 - \frac{A_1A_3}{16A_4} + \frac{A_3Rp^T}{16A_4} + M_4\left(\frac{Rp^T}{4} + \frac{3A_1}{4} - \frac{A_2A_3}{8A_4}\right) + M_4^2\left(\frac{A_2}{2} - \frac{3A_3^2}{16A_4}\right) \equiv 0 \pmod{p^{\min(2k+4m,\mu+3m)}}\,.$$

But from (25), (34) and (36) we know that $p^{2m} \parallel A_4$ and thus

$$\begin{aligned} &16A_0A_4 - A_1A_3 + A_3Rp^T + M_4(4A_4Rp^T + 12A_1A_4 - 2A_2A_3)\\ &\quad + M_4^2(8A_2A_4 - 3A_3^2) \equiv 0 \pmod{p^{\min(2k+6m,\mu+5m)}}\,. \end{aligned} \tag{42}$$

Clearly from (40), $p^U \parallel 6A_4M_4^2 + 3A_3M_4 + A_2$ and so

$$36A_4^2M_4^4 + 36A_3A_4M_4^3 + M_4^2(9A_3^2 + 12A_2A_4) + 6A_2A_3M_4 + A_2^2 \equiv 0 \pmod{p^{2U}}\,.$$

Also, by (38),

$$36A_4(A_4M_4^4 + A_3M_4^3 + A_2M_4^2 + A_1M_4 + A_0) \equiv 0 \pmod{p^{\min(2k+6m,\mu+5m)}}\,.$$

These two congruences and (37) imply that

$$M_4^2(24A_2A_4 - 9A_3^2) + M_4(36A_1A_4 - 6A_2A_3) + 36A_0A_4 - A_2^2 \equiv 0 \pmod{p^{2U}}\,.$$

Substituting this into (42) produces

$$12A_0A_4 - 3A_1A_3 + A_2^2 + 3Rp^T(A_3 + 4A_4M_4) \equiv 0 \pmod{p^{2U}}.$$

From (41) we know that

$$A_3 + 4A_4M_4 = 2A_4(2M_4 - M_5 - M_6 - M_7) - 4M_5M_6M_7.$$

Thus

$$12A_0A_4 - 3A_1A_3 + A_2^2 + 6Rp^T(A_4(2M_4 - M_5 - M_6 - M_7) - 2M_5M_6M_7) \equiv 0 \pmod{p^{2U}}$$

which, taken with (7), (10) and (36), implies that $p^{\min(T+3m,2U)} \mid 12A_0A_4 - 3A_1A_3 + A_2^2$. By (41) we can rewrite this as

$$A_4^4 + 24M_5^2M_6^2M_7^2A_4 \equiv 0 \pmod{p^{\min(T+3m,2U)}},$$

or

$$A_4^3 + 24M_5^2M_6^2M_7^2 \equiv 0 \pmod{p^{\min(T+m,2U-2m)}}. \tag{43}$$

It is now necessary to examine the derivatives of $A_4^3 + 24M_5^2M_6^2M_7^2$ with respect to M_7. Define

$$\begin{aligned} &p^{\delta_1} \parallel 3A_4^2(2M_7 - 2M_5 - 2M_6) + 48M_5^2M_6^2M_7, \\ &p^{\delta_2} \parallel 6A_4^2 + 6A_4(2M_7 - 2M_5 - 2M_6)^2 + 48M_5^2M_6^2, \\ &p^{\delta_3} \parallel 36A_4(2M_7 - 2M_5 - 2M_6) + 6(2M_7 - 2M_5 - 2M_6)^3, \\ &p^{\delta_4} \parallel 72A_4 + 72(2M_7 - 2M_5 - 2M_6)^2, \\ &p^{\delta_5} \parallel 720(M_7 - M_5 - M_6). \end{aligned} \tag{44}$$

By assumption $\gamma_5 \ge \gamma_6 \ge \gamma_7$ and so from (36) we have

$$\gamma_5 + \gamma_6 \ge 2m. \tag{45}$$

Therefore, as $p^{2m} \parallel A_4 = (M_7 - M_5 - M_6)^2 - 4M_5M_6$, it follows that $p^m \mid M_7 - M_5 - M_6$ and from (44) we deduce that

$$\delta_5 \ge m, \quad \delta_4 \ge 2m, \quad \delta_3 \ge 3m. \tag{46}$$

LEMMA 20. *If* $H_{17} = \{S'' : (32), (37)\text{–}(41)$ *and* (44) *hold and* $\delta_4 = 2m\}$ *then* $\#H_{17} \ll \mu^6 A$.

Proof. The proof is split into two cases according to the value of $\min(2U - 2m, T + m)$.

Case 1: $2U - 2m \le T + m$. Given M_5, M_6, M_7 there are

$$\ll h/p^{\max(\min(\mu+3m,2k+4m)-T,T-U)} + 1$$

choices for M_4 from (38), (39) and (40). Since

$$\max(\min(\mu+3m, 2k+4m) - T, T - U) \ge \left[\frac{\min(\mu + 3m, 2k + 4m) - U + 1}{2}\right]$$

we may take the number of M_4 to be $\ll h/p^{[(\min(\mu+3m,2k+4m)-U+1)/2]}+1$. Given M_5, M_6 there are $\ll h/p^W+1$ choices for M_7 from (43) and (44), where

$$W=\max(2U-2m-\delta_1,\delta_1-\delta_2,\delta_2-\delta_3,\delta_3-2m)\ge\left[\frac{U+1}{2}\right]-m\,.$$

Thus

$$\begin{aligned}\#H_{17}\ll{}& h\left(\frac{h}{p^{\mu}}+1\right)\\ &\times\sum_{k,m,U}\left(\frac{h}{p^{[(\min(\mu+3m,2k+4m)-U+1)/2]}}+1\right)\left(\frac{h}{p^{[(U+1)/2]-m}}+1\right)\\ &\times\left(\frac{h}{p^{\mu-k}}+1\right)\left(\frac{h}{p^{\max(\mu-2m,2k-m)}}+1\right)\sum_{\gamma_5,\gamma_6}\left(\frac{h}{p^{\gamma_5}}+1\right)\left(\frac{h}{p^{\gamma_6}}+1\right).\end{aligned}$$

By (37),

$$\left[\frac{\min(\mu+3m,2k+4m)-U+1}{2}\right]\ge\left[\frac{U+1}{2}\right]-m$$

and so, using (45), we obtain

$$\begin{aligned}\#H_{17}&\ll\mu^2h\left(\frac{h}{p^{\mu}}+1\right)\\ &\qquad\times\sum_{k,m,U}\left(\frac{h^2}{p^{\min([(\mu+m+1)/2],k+m)}}+\frac{h}{p^{[(U+1)/2]-m}}+1\right)\\ &\qquad\times\left(\frac{h^4}{p^{\max(2\mu-k,\mu+k+m)}}+\frac{h^3}{p^{\mu}}+\frac{h^2}{p^{k}}+h\right)\\ &\ll\mu^2h\left(\frac{h}{p^{\mu}}+1\right)\sum_{k,m,U}\left(\frac{h^6}{p^{D_{25}}}+\frac{h^5}{p^{D_{26}}}+\frac{h^4}{p^{D_{27}}}+h^3\right),\end{aligned}$$

where

$$\begin{aligned}D_{25}={}&\min\left(\left[\frac{\mu+m+1}{2}\right],k+m\right)+\max(2\mu-k,\mu+k+m)\\ &\ge2\mu+m\ge2\mu+\left[\frac{\mu}{2}\right]-\left[\frac{\mu}{4}\right],\\ D_{26}={}&\min\left(\mu+\min\left(\left[\frac{\mu+m+1}{2}\right],k+m\right),\right.\\ &\qquad\qquad\left.\left[\frac{U+1}{2}\right]-m+\max(2\mu-k,\mu+k+m)\right)\\ &>\mu+k>\mu+\left[\frac{\mu}{2}\right]-\left[\frac{\mu}{4}\right],\end{aligned}$$

$$D_{27} = \min\left(\mu + \left[\frac{U+1}{2}\right] - m, k + \min\left(\left[\frac{\mu+m+1}{2}\right], k+m\right),\right.$$
$$\left.\max(2\mu - k, \mu + k + m)\right) > \mu - \left[\frac{\mu}{2}\right].$$

Case 2: $T + M < 2U - 2m$. There are

$$\ll h/p^{\max(\min(\mu+3m,2k+4m)-T,U-3m)} + 1$$

choices for M_4 from (29), (30), (33), (36), (38) and (39), given M_5, M_6, M_7. Since

$$\max(\min(\mu + 3m, 2k + 4m) - T, U - 3m)$$
$$\geq \left[\frac{\min(\mu + 3m, 2k + 4m) - T + U - 3m + 1}{2}\right]$$

we may take the number of M_4 to be $\ll h/p^{[(\min(\mu,2k+m)-T+U+1)/2]} + 1$. Given M_5, M_6, there are $\ll h/p^Y + 1$ choices for M_7 from (43) and (44), where $Y = \max(T + m - \delta_1, \delta_1 - \delta_2, \delta_2 - \delta_3, \delta_3 - 2m) \geq [(T - m + 3)/4]$ and so

$$\#H_{17} \ll h\left(\frac{h}{p^\mu} + 1\right)$$
$$\times \sum_{\substack{k,m\\U,T}} \left(\frac{h}{p^{[(\min(\mu,2k+m)-T+U+1)/2]}} + 1\right)\left(\frac{h}{p^{[(T-m+3)/4]}} + 1\right)$$
$$\times \left(\frac{h}{p^{\mu-k}} + 1\right)\left(\frac{h}{p^{\max(\mu-2m,2k-m)}} + 1\right)$$
$$\times \sum_{\gamma_5,\gamma_6} \left(\frac{h}{p^{\gamma_5}} + 1\right)\left(\frac{h}{p^{\gamma_6}} + 1\right).$$

From (37),

$$\left[\frac{\min(\mu, 2k+m) - T + U + 1}{2}\right] + \left[\frac{T - m + 3}{4}\right]$$
$$\geq \left[\frac{\min(2\mu - m, 4k + m) + 2U - T}{4}\right]$$
$$\geq \min\left(k + m, \left[\frac{\mu+m}{2}\right]\right)$$

and

$$\left[\frac{\min(\mu, 2k+m) - T + U + 1}{2}\right] \geq \min\left(\left[\frac{k+m}{2}\right], \left[\frac{\mu+m}{4}\right]\right).$$

Also, (32) and (36) imply that $T > 5m$ and consequently $[(T-m+3)/4] > m$. Hence, by (45), it follows that

$$\begin{aligned}\#H_{17} &\ll \mu^4 h\Big(\frac{h}{p^\mu}+1\Big)\sum_{k,m}\bigg(\frac{h^2}{p^{\min([(\mu+m)/2],k+m)}}+\frac{h}{p^m}+1\bigg)\\ &\quad\times\bigg(\frac{h^4}{p^{\max(2\mu-k,\mu+k+m)}}+\frac{h^3}{p^\mu}+\frac{h^2}{p^k}+h\bigg)\\ &\ll \mu^4 h\Big(\frac{h}{p^\mu}+1\Big)\sum_{k,m}\bigg(\frac{h^6}{p^{D_{28}}}+\frac{h^5}{p^{D_{29}}}+\frac{h^4}{p^{D_{30}}}+h^3\bigg),\end{aligned}$$

where

$$\begin{aligned}D_{28} &= \min\bigg(\bigg[\frac{\mu+m}{2}\bigg],k+m\bigg)+\max(2\mu-k,\mu+k+m)\\ &\ge 2\mu+m\ge 2\mu+\bigg[\frac{\mu}{2}\bigg]-\bigg[\frac{\mu}{4}\bigg],\\ D_{29} &= \min\bigg(\mu+\min\bigg(\bigg[\frac{\mu+m}{2}\bigg],k+m\bigg),\\ &\qquad\qquad \max(2\mu-k+m,\mu+k+2m)\bigg)\\ &> \mu+k>\mu+\bigg[\frac{\mu}{2}\bigg]-\bigg[\frac{\mu}{4}\bigg],\\ D_{30} &= \min\bigg(\mu+m,k+\min\bigg(\bigg[\frac{\mu+m}{2}\bigg],k+m\bigg),\\ &\qquad\qquad \max(2\mu-k,\mu+k+m)\bigg)>\mu-\bigg[\frac{\mu}{2}\bigg].\ \blacksquare\end{aligned}$$

LEMMA 21. *If $H_{18}=\{S'' : (32), (37)–(41)$ and (44) hold and $\delta_4\ne 2m\}$ then $\#H_{18}\ll\mu^6 A$.*

P r o o f. By (46) we must have $\delta_4>2m$. Using (44) it follows that $A_4+(2M_7-2M_5-2M_6)^2\equiv 0\pmod{p^{\delta_4}}$ and so we deduce that

$$p^m \parallel M_7-M_5-M_6\,. \tag{47}$$

This together with (44) implies that $\delta_5=m$ and

$$6A_4+(2M_7-2M_5-2M_6)^2\equiv 0\pmod{p^{\delta_3-m}}\,.$$

It can also be seen from (44) that

$$6A_4+6(2M_7-2M_5-2M_6)^2\equiv 0\pmod{p^{\delta_4}}\,.$$

Combining these two congruences gives

$$5(2M_7-2M_5-2M_6)^2\equiv 0 \pmod{p^{\min(\delta_3-m,\delta_4)}},$$

which, by (47), implies that $2m\ge\min(\delta_3-m,\delta_4)$ and thus $\delta_3=3m$.

Case 1: $2U-2m\le T+m$. Given M_5,M_6,M_7 there are

$$\ll h/p^{[(\min(\mu+3m,2k+4m)-U+1)/2]}+1$$

choices for M_4 as in Lemma 20, Case 1. From (43) and (44) we have $\ll h/p^Z+1$ choices for M_7, given M_5,M_6, where

$$Z=\max(2U-2m-\delta_1,\delta_1-\delta_2,\delta_2-3m)\ge\left[\frac{2U-5m+2}{3}\right].$$

Therefore

$$\begin{aligned}\#H_{18}\ll{}& h\biggl(\frac{h}{p^\mu}+1\biggr)\\ &\times\sum_{k,m,U}\biggl(\frac{h}{p^{[(\min(\mu+3m,2k+4m)-U+1)/2]}}+1\biggr)\biggl(\frac{h}{p^{[(2U-5m+2)/3]}}+1\biggr)\\ &\times\biggl(\frac{h}{p^{\mu-k}}+1\biggr)\biggl(\frac{h}{p^{\max(\mu-2m,2k-m)}}+1\biggr)\sum_{\gamma_5,\gamma_6}\biggl(\frac{h}{p^{\gamma_5}}+1\biggr)\biggl(\frac{h}{p^{\gamma_6}}+1\biggr).\end{aligned}$$

It can be seen from (32) and (36) that $U>4m$, which in turn implies that $[(2U-5m+2)/3]>m$ and

$$\begin{aligned}\left[\frac{\min(\mu+3m,2k+4m)-U+1}{2}\right]+\left[\frac{2U-5m+2}{3}\right]&\\ \ge\left[\frac{\min(3\mu-m,6k+2m)+U}{6}\right]&\\ \ge\min\left(\left[\frac{\mu+m}{2}\right],k+m\right).&\end{aligned}$$

Also,

$$\left[\frac{\min(\mu+3m,2k+4m)-U+1}{2}\right]\ge\min\left(\left[\frac{k+m}{2}\right],\left[\frac{\mu+m}{4}\right]\right)$$

by (37). Using (45) it follows that

$$\begin{aligned}\#H_{18}&\ll\mu^3h\biggl(\frac{h}{p^\mu}+1\biggr)\sum_{k,m}\biggl(\frac{h^2}{p^{\min([(\mu+m)/2],k+m)}}+\frac{h}{p^m}+1\biggr)\\ &\quad\times\biggl(\frac{h^4}{p^{\max(2\mu-k,\mu+k+m)}}+\frac{h^3}{p^\mu}+\frac{h^2}{p^k}+h\biggr)\\ &\ll\mu^5A\end{aligned}$$

by comparison with Case 2 of the previous lemma.

Case 2: $T+m<2U-2m$. Given M_5, M_6, M_7 we have

$$\ll h/p^{[(\min(\mu,2k+m)-T+U+1)/2]}+1$$

choices for M_4 as in Case 2 of Lemma 20. By (43) and (44) we have $\ll h/p^L+1$ choices for M_7 given M_5, M_6, where

$$L=\max(T+m-\delta_1,\delta_1-\delta_2,\delta_2-3m)\ge\left[\frac{T-2m+2}{3}\right]$$

and so

$$\begin{aligned}\#H_{18}\ll h\Big(\frac{h}{p^\mu}+1\Big)&\\ \times\sum_{\substack{k,m\\U,T}}&\Big(\frac{h}{p^{[(\min(\mu,2k+m)-T+U+1)/2]}}+1\Big)\Big(\frac{h}{p^{[(T-2m+2)/3]}}+1\Big)\\ &\times\Big(\frac{h}{p^{\mu-k}}+1\Big)\Big(\frac{h}{p^{\max(\mu-2m,2k-m)}}+1\Big)\sum_{\gamma_5,\gamma_6}\Big(\frac{h}{p^{\gamma_5}}+1\Big)\Big(\frac{h}{p^{\gamma_6}}+1\Big).\end{aligned}$$

By (32) and (36), $T>5m$ and $U>4m$. Consequently, $[(T-2m+2)/3]>m$ and

$$\begin{aligned}\left[\frac{T-2m+2}{3}\right]&+\left[\frac{\min(\mu,2k+m)-T+U+1}{2}\right]\\ &\ge\left[\frac{\min(3\mu-m,6k+2m)+U}{6}\right]\ge\min\left(\left[\frac{\mu+m}{2}\right],k+m\right).\end{aligned}$$

As in Lemma 20, Case 2 we have

$$\begin{aligned}\#H_{18}&\ll\mu^4h\Big(\frac{h}{p^\mu}+1\Big)\sum_{k,m}\Big(\frac{h^2}{p^{\min([(\mu+m)/2],k+m)}}+\frac{h}{p^m}+1\Big)\\ &\qquad\times\Big(\frac{h^4}{p^{\max(2\mu-k,\mu+k+m)}}+\frac{h^3}{p^\mu}+\frac{h^2}{p^k}+h\Big)\\ &\ll\mu^6A.\ \blacksquare\end{aligned}$$

Since $\#H\ll\#\{\bigcup_{j=1}^{18}H_j\}$, Theorem 1 follows immediately from Lemmas 4 to 21.

References

[1] D. A. Burgess, *Estimation of character sums modulo a power of a prime*, Proc. London Math. Soc. (3) 52 (1986), 215–235.

[2] —, *On character sums and L-series*, ibid. 12 (1962), 193–206.

[3] D. A. Burgess, *On a set of congruences related to character sums III*, J. London Math. Soc. (2) 45 (1992), 201–214.
[4] L. K. Hua and S. H. Min, *An analogue of Tarry's problem*, Acad. Sinica Science Record 1 (1942), 26–29.

DEPARTMENT OF MATHEMATICS
NOTTINGHAM UNIVERSITY
UNIVERSITY PARK
NOTTINGHAM NG7 2RD
ENGLAND

Received on 7.9.1992
and in revised form on 20.7.1993 (2300)