数 学 年 刊
2009,30A(6):857–868

一类同余方程解数的上界估计

王 赟 杰*

提要 主要研究形如 $\prod_{i=1}^{r}(X+m_i)\equiv\prod_{j=r+1}^{2r}(X+m_j)\pmod{p^\mu}$ 的同余方程关于 $\mathbf{m}=(m_1,\cdots,m_{2r})$ 解数估计问题，并得出当 $r=4,5$ 时，该同余方程解数的上界估计．前者可改进 Dodd 的结论，而后者则可应用于对另一类同余方程组解数的上界估计．

关键词 同余方程的解数， p-adic 指数赋值，特征和
MR (2000) 主题分类 11A07, 11S99, 11L40
中图法分类 O156
文献标志码 A
文章编号 1000-8314(2009)06-0857-12

1 引 言

在本文中，假设 X 是未定元，对每一个向量 $\mathbf{m}=(m_1,\cdots,m_{2r})\in Z^{2r}$, 满足 $0<m_i\leqslant h$, 定义

$$f_1(X)=\prod_{i=1}^{r}(X+m_i),\quad f_2(X)=\prod_{i=r+1}^{2r}(X+m_i).$$

对形如 $f_1(X)\equiv f_2(X)\pmod{p^\mu}$ 的同余方程解数作上界估计，在数论尤其是在估计非完整特征和 $S(N,H)=\sum_{n=N}^{N+H}\chi(n)$ 上界理论中，有着重要的应用.

设 $S(r)=\{\mathbf{m}:0<m_i\leqslant h,\ i=1,\cdots,2r, f_1(X)\equiv f_2(X)\pmod{p^\mu}\}$, Burgess 在 [1] 的定理 8 中，首先完成了对 $\#S(3)$ 的上界估计，并通过这一结论，得到

$$S(N,H)=\sum_{n=N}^{N+H}\chi(n)\ll H^{1-\frac{1}{r}}q^{\frac{r+1}{4r^2}+\varepsilon}. \tag{1.1}$$

在 "$r=3,\ q=p^\alpha$ ($p>3$, p 是素数)" 时成立的结论 (其中 $\chi(n)$ 是模 q 的特征), 并在此基础上，进一步地在文 [2] 中，得到 $S(N,H)\ll H^{1-\frac{1}{r}}q^{\frac{r+1}{4r^2}+\varepsilon}$ 当 "$r=3$" 时总成立的结论.

而 $S(N,H)\ll H^{1-\frac{1}{r}}q^{\frac{r+1}{4r^2}+\varepsilon}$ 在 "$r\geqslant 4$" 时是否成立，至今尚不可知 (Burgess 只是在文 [3] 中，得到某些特殊的结论). 为证明 $r=4$ 时类似于 (1.1) 的结论，作为其中一个步骤， Dodd 在 [4] 中，通过对集合进行分拆的方法，完成了对 $\#S(4)$ 的上界估计：

$$\#S(4)\ll\mu^6\Big(\frac{h^8}{p^{3\mu+[\frac{\mu}{2}]-[\frac{\mu}{4}]}}+\frac{h^6}{p^{\mu+[\frac{\mu}{2}]-[\frac{\mu}{4}]}}+\frac{h^5}{p^{\mu-[\frac{\mu}{2}]}}+h^4\Big). \tag{1.2}$$

本文目的在于，通过引入 p-adic 指数赋值的方法，来研究同余方程 $\prod_{i=1}^{r}(X+m_i)\equiv\prod_{i=r+1}^{2r}(X+m_i)\pmod{p^\mu}$ 的解数，并得到

本文 2008 年 2 月 5 日收到， 2009 年 5 月 17 日收到修改稿.
*上海交通大学数学系，上海 200240. E-mail: himmelwangyj@163.com

定理 1.1 设 p 为大于 5 的素数，μ 为任意的正整数，则

$$\#S(4)\ll \frac{h^8}{p^{4\mu-[\frac{\mu}{2}]-\frac{3}{2}[\frac{\mu}{4}]}}+\frac{h^7}{p^{3\mu-[\frac{\mu}{2}]-\frac{3}{2}[\frac{\mu}{4}]}}+\frac{h^5}{p^{\mu-[\frac{\mu}{2}]}}+h^4.$$

作为证明 $r=4$ 时，使 (1.1) 成立的一个步骤，与文 [1] 第 11 节中证明 $\sum\limits_m \#A_{38}$ 的过程类似. 由于此时，h,μ 满足 "$h\leqslant p^{\frac{\alpha}{8}},[\frac{1}{2}\zeta]+1\leqslant\mu\leqslant\zeta$ (其中 $\zeta=\alpha-[\frac{3}{4}\alpha]$)", 所以当 μ 满足 "$\frac{\alpha}{8}<2\mu-\frac{11}{4}[\frac{\mu}{2}]+[\frac{\mu}{4}]+6\log_p\mu$" 或 "$\frac{\alpha}{8}\geqslant 2\mu-\frac{11}{4}[\frac{\mu}{2}]+[\frac{\mu}{4}]+6\log_p\mu,\ \mu\geqslant[\frac{\alpha-[3\alpha/4]}{2}]+1$ 且 $h<\mu^6p^{2\mu-\frac{11}{4}[\frac{\mu}{2}]+[\frac{\mu}{4}]}$" 这两个条件中的任何一个时，定理 1.1 的结论比 Dodd 在 [4] 中得到的结论 (1.2) 更好.

同样，对于 $r=5$ 时的情形，不难得到

定理 1.2 设 p 为大于 5 的素数，μ 为任意的正整数，则

$$\#S(5)\ll \frac{h^{10}}{p^{\frac{11}{2}\mu-2[\frac{3}{4}\mu]-[\frac{3}{8}\mu]}}+\frac{h^9}{p^{\frac{9}{2}\mu-2[\frac{3}{4}\mu]-[\frac{3}{8}\mu]}}+\frac{h^8}{p^{\frac{7}{2}\mu-2[\frac{3}{4}\mu]-[\frac{\mu}{8}]}}+\frac{h^6}{p^{\mu-[\frac{\mu}{2}]}}+h^5.$$

同时，我们还可将该定理用于估计同余方程组 $x_1^w+\cdots+x_d^w\equiv y_1^w+\cdots+y_d^w\pmod{p^\vartheta}$ 的解数 (其中 $1\leqslant w\leqslant w_0,\ d,w_0,\vartheta$ 取定某些固定的值，并且满足 $d\geqslant w_0\geqslant 4,\ \vartheta\geqslant w_0^2$). 在第 4 节中，我们将取 $d=w_0=5,\ \vartheta=25$, 以此为例进行说明.

2 基 本 命 题

本节中, 我们将给出一些在下文中被多次使用并起重要作用的基本命题和相关证明, 这些结论本身都具有独立的意义.

首先，对同余方程 $f_1(X)\equiv f_2(X)\pmod{p^\mu}$, 作替换 $M_i=m_i-m_1\ (2\leqslant i\leqslant 10)$, $Y=X+m_1$, 则 $f_1(X)\equiv f_2(X)\pmod{p^\mu}$ 成立当且仅当以下同余方程组成立：

$$\begin{aligned}
&M_2+M_3+M_4+M_5\equiv M_6+M_7+M_8+M_9+M_{10}\pmod{p^\mu}, &(2.1)\\
&M_2M_3+M_2M_4+M_2M_5+M_3M_4+M_3M_5+M_4M_5\\
\equiv\ &M_6M_7+M_6M_8+M_6M_9+M_6M_{10}+M_7M_8+M_7M_9\\
&+M_7M_{10}+M_8M_9+M_8M_{10}+M_9M_{10}\pmod{p^\mu}, &(2.2)\\
&M_2M_3M_4+M_2M_3M_5+M_2M_4M_5+M_3M_4M_5\\
\equiv\ &M_6M_7M_8+M_6M_7M_9+M_6M_7M_{10}+M_6M_8M_9+M_6M_8M_{10}\\
&+M_6M_9M_{10}+M_7M_8M_9+M_7M_8M_{10}+M_7M_9M_{10}\\
&+M_8M_9M_{10}\pmod{p^\mu}, &(2.3)\\
M_2M_3M_4M_5\equiv\ &M_6M_7M_8M_9+M_6M_7M_8M_{10}+M_6M_7M_9M_{10}\\
&+M_6M_8M_9M_{10}+M_7M_8M_9M_{10}\pmod{p^\mu}, &(2.4)\\
0\equiv\ &M_6M_7M_8M_9M_{10}\pmod{p^\mu}. &(2.5)
\end{aligned}$$

对该同余方程组，代入消元后可得：

$$\begin{aligned}
&M_3^2+(M_4+M_5-\tau_1)M_3+(M_4^2+M_4M_5+M_5^2)-\tau_1(M_4+M_5)+\tau_2\\
\equiv\ &0\pmod{p^\mu}, &(2.6)
\end{aligned}$$

$$M_4^3+(M_5-\tau_1)M_4^2+(M_5^2-\tau_1M_5+\tau_2)M_4+(M_5^3-\tau_1M_5^2+\tau_2M_5-\tau_3)$$
$$\equiv 0 \pmod{p^\mu}, \tag{2.7}$$
$$M_5^4-\tau_1M_5^3+\tau_2M_5^2-\tau_3M_5+\tau_4\equiv 0 \pmod{p^\mu}, \tag{2.8}$$

其中 $\tau_1=M_6+M_7+M_8+M_9+M_{10}$, $\tau_2=M_6M_7+M_6M_8+M_6M_9+M_6M_{10}+M_7M_8+M_7M_9+M_7M_{10}+M_8M_9+M_8M_{10}+M_9M_{10}$, $\tau_3=M_6M_7M_8+M_6M_7M_9+M_6M_7M_{10}+M_6M_8M_9+M_6M_8M_{10}+M_6M_9M_{10}+M_7M_8M_9+M_7M_8M_{10}+M_7M_9M_{10}+M_8M_9M_{10}$, $\tau_4=M_6M_7M_8M_9+M_6M_7M_8M_{10}+M_6M_7M_9M_{10}+M_6M_8M_9M_{10}+M_7M_8M_9M_{10}$.

对 $\gamma_2,\cdots,\gamma_{10}$ 可作如下定义：$M_i=k_ip^{\gamma_i}$, 其中 $(k_i,p)=1$, 由 (2.5) 不难发现

$$\gamma_6+\gamma_7+\gamma_8+\gamma_9+\gamma_{10}\geqslant\mu.$$

这时不妨设为 $\gamma_2\geqslant\gamma_3\geqslant\gamma_4\geqslant\gamma_5\geqslant 0$, $\gamma_6\geqslant\gamma_7\geqslant\gamma_8\geqslant\gamma_9\geqslant\gamma_{10}\geqslant 0$, 并设向量 $\mathbf{M}=(M_2,M_3,M_4,M_5,M_6,M_7,M_8,M_9,M_{10})$. 记 $A_1=\{\mathbf{m}=(m_1,m_2,m_3,m_4,m_5,m_6,m_7,m_8,m_9,m_{10}):0<m_1\leqslant h,0\leqslant|M_i|<h\ (2\leqslant i\leqslant 10)$, (2.1)–(2.5)$\}$, $A_1'=\{\mathbf{m}:0<m_1\leqslant h,0\leqslant|M_i|<h\,(2\leqslant i\leqslant 10)$, (2.1), (2.5)–(2.8)$\}$, 则 $A_1=A_1'$, $\#S(5)=\#A_1=\#A_1'$.

由于以上消元求解过程关于 M_i $(i=2,3,4,5)$ 对称，于是不难得出比 (2.6)–(2.8) 更一般的同余方程组：

$$M_{i_1}^2+(M_{i_2}+M_{i_3}-\tau_1)M_{i_1}+(M_{i_2}^2+M_{i_2}M_{i_3}+M_{i_3}^2)-\tau_1(M_{i_2}+M_{i_3})+\tau_2$$
$$\equiv 0 \pmod{p^\mu}, \tag{2.9}$$
$$M_{i_2}^3+(M_{i_3}-\tau_1)M_{i_2}^2+(M_{i_3}^2-\tau_1M_{i_3}+\tau_2)M_{i_2}+(M_{i_3}^3-\tau_1M_{i_3}^2+\tau_2M_{i_3}-\tau_3)$$
$$\equiv 0 \pmod{p^\mu}, \tag{2.10}$$
$$M_{i_3}^4-\tau_1M_{i_3}^3+\tau_2M_{i_3}^2-\tau_3M_{i_3}+\tau_4\equiv 0 \pmod{p^\mu}, \tag{2.11}$$

其中 i_1, i_2, i_3 可取 $\{2,3,4,5\}$ 中的任意 3 个数. 因此，即得

命题 2.1　设 $A_1''=\{\mathbf{m}:0<m_1\leqslant h,0\leqslant|M_i|<h\ (2\leqslant i\leqslant 10)$, (2.1), (2.5), (2.9)–(2.11)$\}$, 则 $A_1=A_1'=A_1''$, $\#S(5)=\#A_1''$.

命题 2.2 (见 [5, 命题 1])　设 $f(x)$ 是次数给定的整系数多项式，p 是奇素数，d 是正整数，则 $\#\{x \pmod{p^\nu}:p^\alpha|f(x),p\nmid f^{(d)}(x)\}\ll\deg f(x)$ (其中 $\nu=\alpha-[\frac{d-1}{d}\alpha]$).

3 主要结论的证明

由于定理 1.1 、 1.2 的证明过程基本相似，并且定理 1.2 的证明较定理 1.1 更具一般性，因此本文以定理 1.2 为例，作详细的展开证明；而对于定理 1.1, 重复同样的方法可得相应结论.

设 p 为素数, 以 $\mathrm{ord}_p(\cdot)$ 表示 p-adic 指数赋值 (即若 $a=p^ka'$, $(p,a')=1$, 则 $\mathrm{ord}_pa=k$). 本章通过比较 $\mathrm{ord}_p(M_i)$ $(M_i=m_i-m_1,\ 2\leqslant i\leqslant 10)$ 的方法以得到定理 1.2.

同时, 在证明定理 1.2 的过程中, 不难发现, 在任何情况下, 当取定 $M_i=m_i-m_1$ $(10\geqslant i\geqslant 2)$ 时，m_1 的解数总是 $\ll h$; 而对 M_2, 由 (2.1), 当 M_3, M_4, M_5, M_6, M_7, M_8, M_9, M_{10} 给定时，总有 M_2 解数 $\ll\frac{h}{p^\mu}+1$. 此外，可设 $T=\frac{h^{10}}{p^{\frac{11}{2}\mu-2[\frac{3}{4}\mu]-\frac{3}{4}[\frac{\mu}{2}]}}+\frac{h^9}{p^{\frac{9}{2}\mu-2[\frac{3}{4}\mu]-\frac{3}{4}[\frac{\mu}{2}]}}+\frac{h^8}{p^{\frac{7}{2}\mu-2[\frac{3}{4}\mu]-\frac{1}{2}[\frac{\mu}{4}]}}+\frac{h^7}{p^{\frac{3}{2}\mu-[\frac{\mu}{5}]}}+\frac{h^6}{p^{\mu-[\frac{\mu}{2}]}}+h^5$.

3.1 $\gamma_8+\gamma_9+\gamma_{10}\geqslant\mu$ 情形

在本节中，我们通过分别估计 $\#\{\mathbf{m}\in A_1:\gamma_{10}\geqslant\mu\}$, $\#\{\mathbf{m}\in A_1:\gamma_{10}<\mu$ 且 $\gamma_{10}+\gamma_9\geqslant\mu\}$, $\#\{\mathbf{m}\in A_1:\gamma_{10}+\gamma_9<\mu$ 且 $\gamma_{10}+\gamma_9+\gamma_8\geqslant\mu\}$ 的上界，来完成对 $\#\{\mathbf{m}\in A_1:\gamma_{10}+\gamma_9+\gamma_8\geqslant\mu\}$ 的上界估计.

引理 3.1 设 $A_2=\{\mathbf{m}\in A_1:\gamma_{10}<\mu,\gamma_{10}+\gamma_9<\mu$ 且 $\gamma_{10}+\gamma_9+\gamma_8\geqslant\mu\}$, 则 $\#A_2\ll T$.

证 设 $T(x)=x^2+(M_4+M_5-\tau_1)x+(M_4^2+M_4M_5+M_5^2)-\tau_1(M_4+M_5)+\tau_2$, 由 (2.6), 不难得出 $p^\mu\mid T(M_3)$ 且 $p\nmid T''(M_3)$. 根据命题 2.2, 给定 M_4, M_5, M_6, M_7, M_8, M_9, M_{10} 后， M_3 解数 $\ll\frac{h}{p^{\mu-[\frac{\mu}{2}]}}+1$; 对于 M_4, M_5, 由 (2.7), (2.8), 同理可得：给定 M_5, M_6, M_7, M_8, M_9, M_{10} 后， M_4 解数 $\ll\frac{h}{p^{\mu-[\frac{2}{3}\mu]}}+1$; 给定 M_6, M_7, M_8, M_9, M_{10} 后， M_5 解数 $\ll\frac{h}{p^{\mu-[\frac{3}{4}\mu]}}+1$.

而由于 $\gamma_6\geqslant\gamma_7\geqslant\gamma_8\geqslant\frac{\mu}{3}$, M_6, M_7 的解数 $\ll\frac{h}{p^{\frac{\mu}{3}}}+1$. 另外， M_8 解数 $\ll\frac{h}{p^{\gamma_8}}+1$, M_9 解数 $\ll\frac{h}{p^{\gamma_9}}+1$, M_{10} 解数 $\ll\frac{h}{p^{\gamma_{10}}}+1$. 由于 $\gamma_8+\gamma_9+\gamma_{10}\geqslant\mu$, 可得

$$\begin{aligned}\#A_2\ll{}&h\Big(\frac{h}{p^\mu}+1\Big)\Big(\frac{h}{p^{\mu-[\frac{\mu}{2}]}}+1\Big)\Big(\frac{h}{p^{\mu-[\frac{2}{3}\mu]}}+1\Big)\Big(\frac{h}{p^{\mu-[\frac{3}{4}\mu]}}+1\Big)\Big(\frac{h}{p^{\frac{\mu}{3}}}+1\Big)\Big(\frac{h}{p^{\frac{\mu}{3}}}+1\Big)\\&\cdot\Big(\frac{h}{p^{\gamma_8}}+1\Big)\Big(\frac{h}{p^{\gamma_9}}+1\Big)\Big(\frac{h}{p^{\gamma_{10}}}+1\Big)\ll T.\end{aligned}$$

引理 3.2 设 $A_3=\{\mathbf{m}\in A_1:\gamma_{10}<\mu$ 且 $\gamma_{10}+\gamma_9\geqslant\mu\}$, 则 $\#A_3\ll T$.

证 与引理 3.1 的证明过程类似，唯一不同在于：此时 $\gamma_6\geqslant\gamma_7\geqslant\gamma_8\geqslant\gamma_9\geqslant\frac{\mu}{2}$, 所以 M_6, M_7, M_8 的解数 $\ll\frac{h}{p^{\frac{\mu}{2}}}+1$; 由于 $\gamma_9+\gamma_{10}\geqslant\mu$, 不难得到

$$\begin{aligned}\#A_3\ll{}&h\Big(\frac{h}{p^\mu}+1\Big)\Big(\frac{h}{p^{\mu-[\frac{\mu}{2}]}}+1\Big)\Big(\frac{h}{p^{\mu-[\frac{2}{3}\mu]}}+1\Big)\Big(\frac{h}{p^{\mu-[\frac{3}{4}\mu]}}+1\Big)\Big(\frac{h}{p^{\frac{\mu}{2}}}+1\Big)\Big(\frac{h}{p^{\frac{\mu}{2}}}+1\Big)\\&\cdot\Big(\frac{h}{p^{\frac{\mu}{2}}}+1\Big)\Big(\frac{h}{p^{\gamma_9}}+1\Big)\Big(\frac{h}{p^{\gamma_{10}}}+1\Big)\ll T.\end{aligned}$$

引理 3.3 设 $A_4=\{\mathbf{m}\in A_1:\gamma_{10}\geqslant\mu\}$, 则 $\#A_4\ll T$.

证 与引理 3.1 的证法类似，不难得到

$$\begin{aligned}\#A_4\ll{}&h\Big(\frac{h}{p^\mu}+1\Big)\Big(\frac{h}{p^{\mu-[\frac{\mu}{2}]}}+1\Big)\Big(\frac{h}{p^{\mu-[\frac{2}{3}\mu]}}+1\Big)\Big(\frac{h}{p^{\mu-[\frac{3}{4}\mu]}}+1\Big)\Big(\frac{h}{p^\mu}+1\Big)\Big(\frac{h}{p^\mu}+1\Big)\\&\cdot\Big(\frac{h}{p^\mu}+1\Big)\Big(\frac{h}{p^\mu}+1\Big)\Big(\frac{h}{p^\mu}+1\Big)\ll T.\end{aligned}$$

3.2 $\gamma_{10}+\gamma_9+\gamma_8<\mu$ 且 $\gamma_{10}+\gamma_9+\gamma_8+\gamma_7\geqslant\mu$ 情形

设 $A_5=\{\mathbf{m}\in A_1:\gamma_{10}+\gamma_9+\gamma_8<\mu$ 且 $\gamma_{10}+\gamma_9+\gamma_8+\gamma_7\geqslant\mu\}$, $A_6=\{\mathbf{m}\in A_5:\gamma_{10}=\gamma_5\}$, 此时总有 $\gamma_6\geqslant\gamma_7\geqslant\mu-[\frac{3}{4}\mu]$. 而对于 M_i $(i=6,7,8,9,10)$, M_i 解数 $\ll\frac{h}{p^{\gamma_i}}+1$.

本节中，我们先将集合 A_5 分解为 $\{\mathbf{m}\in A_5:\gamma_5<\gamma_{10}\}\cup\{\mathbf{m}\in A_5:\gamma_5>\gamma_{10}\}\cup A_6$, 并通过分别估计各集合的势的上界，来完成对 $\#A_5$ 的上界估计.

引理 3.4 设 $A_7=\{\mathbf{m}\in A_6:\gamma_2\geqslant\gamma_3>\gamma_4=\gamma_5\}$, 则 $\#A_7\ll T$.

证 对集合 A_7 中的元素，可分以下两类讨论：

(1) 若 $M_4 \not\equiv M_5 \pmod{p^{\gamma_{10}+1}}$, 根据命题 2.1, 可取 $i_1=5$, $i_2=4$, $i_3=3$. 对于 (2.9), 有同余方程

$$\begin{aligned} &{M_5'}^2+(M_3'+M_4'-\tau_1')M_5'+({M_3'}^2+M_3'M_4'+{M_4'}^2)-\tau_1'(M_3'+M_4')+\tau_2' \\ &\equiv 0 \pmod{p^{\mu-2\gamma_{10}}}, \end{aligned}$$

其中 $M_i'=\frac{M_i}{p^{\gamma_{10}}}$, $\tau_1'=\frac{\tau_1}{p^{\gamma_{10}}}$, $\tau_2'=\frac{\tau_2}{p^{2\gamma_{10}}}$. 设 $f(M_5')={M_5'}^2+(M_3'+M_4'-\tau_1')M_5'+({M_3'}^2+M_3'M_4'+{M_4'}^2)-\tau_1'(M_3'+M_4')+\tau_2'$, 由 (2.1), 不难发现 $f'(M_5')\equiv 2M_5'+M_4'-\tau_1'\equiv M_5'\not\equiv 0 \pmod p$, 因此, 同余方程 $f(M_5')\equiv 0 \pmod{p^{\mu-2\gamma_{10}}}$ 和 $f(M_5')\equiv 0 \pmod p$ 的解数一样多. 于是, 给定 M_3, M_4, M_6, M_7, M_8, M_9, M_{10} 后, M_5 的解数 $\ll \frac{h}{p^{\mu-\gamma_{10}}}+1$.

同样, 对于 M_4, 可设 $h(M_4')={M_4'}^3+(M_3'-\tau_1'){M_4'}^2+({M_3'}^2-\tau_1'M_3'+\tau_2')M_4'+({M_3'}^3-\tau_1'{M_3'}^2+\tau_2'M_3'-\tau_3')$, 与上文类似, 由 (2.10), 同理 $h(M_4')\equiv 0 \pmod p$ 和 $h(M_4')\equiv 0 \pmod{p^{\mu-3\gamma_{10}}}$ 的解数同样多. 所以, 给定 M_3, M_6, M_7, M_8, M_9, M_{10}, 则 M_4 的解数为 $\ll \frac{h}{p^{\mu-2\gamma_{10}}}+1$.

而对于 M_3, 由 (2.11), $p^\mu \mid \ell(M_3)=M_3^4-\tau_1M_3^3+\tau_2M_3^2-\tau_3M_3+\tau_4$, 根据命题 2.2, 给定的 M_6, M_7, M_8, M_9, M_{10}, 则 M_3 的解数 $\ll \frac{h}{p^{\mu-[\frac{3}{4}\mu]}}+1$. 于是

$$\begin{aligned} \#A_7 &\ll h\Big(\frac{h}{p^\mu}+1\Big)\Big(\frac{h}{p^{\mu-\gamma_{10}}}+1\Big)\Big(\frac{h}{p^{\mu-2\gamma_{10}}}+1\Big)\Big(\frac{h}{p^{\mu-[\frac{3}{4}\mu]}}+1\Big)\Big(\frac{h}{p^{\gamma_6}}+1\Big)\Big(\frac{h}{p^{\gamma_7}}+1\Big) \\ &\quad\cdot\Big(\frac{h}{p^{\gamma_8}}+1\Big)\Big(\frac{h}{p^{\gamma_9}}+1\Big)\Big(\frac{h}{p^{\gamma_{10}}}+1\Big) \\ &= \frac{h^{10}}{p^{6\mu-3[\frac{3}{4}\mu]}}+\frac{h^9}{p^{5\mu-3[\frac{3}{4}\mu]}}+\frac{h^8}{p^{4\mu-[\frac{\mu}{2}]-2[\frac{3}{4}\mu]}}+\frac{h^7}{p^{3\mu-2[\frac{3}{4}\mu]}}+\frac{h^6}{p^{2\mu-[\frac{3}{4}\mu]}}+\frac{h^5}{p^{\mu-[\frac{3}{4}\mu]}}\ll T. \end{aligned}$$

(2) 若 $M_4\equiv M_5 \pmod{p^{\gamma_{10}+1}}$, 则 M_3, M_5 解数的估计过程与 (1) 中类似, 唯一不同在于 M_4 的估计: 由于此时 $M_4\equiv M_5 \pmod{p^{\gamma_{10}+1}}$, 因此 $h''(M_4')\not\equiv 0 \pmod p$, 应用命题 2.2, 给定 M_3, M_6, M_7, M_8, M_9, M_{10} 后, M_4 的解数 $\ll \frac{h}{p^{\mu-\gamma_{10}-[\frac{\mu-\gamma_{10}}{2}]}}+1$. 此时

$$\begin{aligned} \#A_7 &\ll h\Big(\frac{h}{p^\mu}+1\Big)\Big(\frac{h}{p^{\mu-\gamma_{10}}}+1\Big)\Big(\frac{h}{p^{\mu-\gamma_{10}-[\frac{\mu-\gamma_{10}}{2}]}}+1\Big)\Big(\frac{h}{p^{\mu-[\frac{3}{4}\mu]}}+1\Big)\Big(\frac{h}{p^{\gamma_6}}+1\Big) \\ &\quad\cdot\Big(\frac{h}{p^{\gamma_7}}+1\Big)\Big(\frac{h}{p^{\gamma_8}}+1\Big)\Big(\frac{h}{p^{\gamma_9}}+1\Big)\Big(\frac{h}{p^{\gamma_{10}}}+1\Big)\ll T. \end{aligned}$$

综合 (1), (2), 可得 $\#A_7\ll T$.

引理 3.5　设 $A_8=\{\mathbf{m}\in A_6:\gamma_2>\gamma_3=\gamma_4=\gamma_5\}$, 则 $\#A_8\ll T$.

证　对集合 A_8 中的元素, 可分以下两类讨论:

(1) 若 $\exists i,j\in\{3,4,5\}$, 使 $M_i\not\equiv M_j \pmod{p^{\gamma_5+1}}$, 不妨设 $i=4$, $j=5$, 则与引理 3.4 情形 (1) 中的过程类似, 此时取 $i_1=5$, $i_2=4$, $i_3=3$, 同理可得

$$\begin{aligned} \#A_8 &\ll h\Big(\frac{h}{p^\mu}+1\Big)\Big(\frac{h}{p^{\mu-[\frac{3}{4}\mu]}}+1\Big)\Big(\frac{h}{p^{\mu-2\gamma_{10}}}+1\Big)\Big(\frac{h}{p^{\mu-\gamma_{10}}}+1\Big)\Big(\frac{h}{p^{\gamma_6}}+1\Big) \\ &\quad\cdot\Big(\frac{h}{p^{\gamma_7}}+1\Big)\Big(\frac{h}{p^{\gamma_8}}+1\Big)\Big(\frac{h}{p^{\gamma_9}}+1\Big)\Big(\frac{h}{p^{\gamma_{10}}}+1\Big)\ll T. \end{aligned}$$

(2) 若 $M_3\equiv M_4\equiv M_5 \pmod{p^{\gamma_5+1}}$, 则可回到第 2 节中, 对同余方程 $f_1(X)\equiv f_2(X) \pmod{p^\mu}$, 重新选取 $Y=X+m_5$, 则 $f_1(X)\equiv f_2(X) \pmod{p^\mu}$ 等价于 $Y(Y+\widetilde{M_2})(Y+\widetilde{M_3})(Y+\widetilde{M_4})(Y+\widetilde{M_5})\equiv(Y+\widetilde{M_6})(Y+\widetilde{M_7})(Y+\widetilde{M_8})(Y+\widetilde{M_9})(Y+\widetilde{M_{10}}) \pmod{p^\mu}$, 其

中 $\widetilde{M}_2,\cdots,\widetilde{M}_{10}$ 分别取为 m_3-m_5, m_4-m_5, m_1-m_5, m_2-m_5, $m_{10}-m_5$, m_9-m_5, m_8-m_5, m_7-m_5, m_6-m_5 (不妨假设 $\mathrm{ord}_p(M_3-M_5)\geqslant\mathrm{ord}_p(M_4-M_5)$, $\mathrm{ord}_p(M_{10}-M_5)\geqslant\mathrm{ord}_p(M_9-M_5)\geqslant\mathrm{ord}_p(M_8-M_5)\geqslant\mathrm{ord}_p(M_7-M_5)\geqslant\mathrm{ord}_p(M_6-M_5)$), 此时显然有 $M_i-M_j=m_i-m_j$ $(i,j\geqslant 2)$ 且 $m_1-m_5=-M_5=\widetilde{M}_4$, 而 $\mathrm{ord}_p(\widetilde{M}_2)\geqslant\mathrm{ord}_p(\widetilde{M}_3)>\mathrm{ord}_p(\widetilde{M}_4)=\mathrm{ord}_p(\widetilde{M}_5)=\mathrm{ord}_p(\widetilde{M}_{10})$ 且 $\mathrm{ord}_p(\widetilde{M}_{10})+\mathrm{ord}_p(\widetilde{M}_9)+\mathrm{ord}_p(\widetilde{M}_8)+\mathrm{ord}_p(\widetilde{M}_7)\geqslant\mu$.

设 $\gamma_i'=\mathrm{ord}_p(\widetilde{M}_i)$, $A_8'=\{\mathbf{m}\in A_1:\gamma_2'\geqslant\gamma_3'>\gamma_4'=\gamma_5'=\gamma_{10}',\gamma_{10}'+\gamma_9'+\gamma_8'+\gamma_7'\geqslant\mu\}$, 则此时总有 $\{\mathbf{m}\in A_8:M_3\equiv M_4\equiv M_5\pmod{p^{\gamma_5+1}}\}\subset A_8'$. 而对于集合 A_8', 由引理 3.1, 3.2, 3.3, 可得 $\#\{\mathbf{m}\in A_8':\gamma_{10}'+\gamma_9'+\gamma_8'\geqslant\mu\}\ll T$; 由引理 3.4, 可得 $\#\{\mathbf{m}\in A_8':\gamma_{10}'+\gamma_9'+\gamma_8'<\mu\}\ll T$. 所以 $\#\{\mathbf{m}\in A_8:M_3\equiv M_4\equiv M_5\pmod{p^{\gamma_5+1}}\}\leqslant\#A_8'\ll T$.

所以 $\#A_8\ll T$.

引理 3.6 设 $A_9=\{\mathbf{m}\in A_6:\gamma_2\geqslant\gamma_3>\gamma_4>\gamma_5$ 或 $\gamma_2>\gamma_3=\gamma_4>\gamma_5\}$, 则 $\#A_9\ll T$.

证 对集合 A_9 中的元素, 以 "$\gamma_2>\gamma_3>\gamma_4>\gamma_5$" 为例 (其他情况同理可得), 可作以下讨论:

(1) 若 $\gamma_4\leqslant\gamma_9$, 对 M_5, 与引理 3.4 情形 (1) 中的过程类似, 此时取 $i_1=5$, $i_2=4$, $i_3=3$, 同理可得

$$\begin{aligned}\#A_9\ll h&\Big(\frac{h}{p^{\mu}}+1\Big)\Big(\frac{h}{p^{\mu-[\frac{3}{4}\mu]}}+1\Big)\Big(\frac{h}{p^{\mu-\gamma_{10}-\gamma_9}}+1\Big)\Big(\frac{h}{p^{\mu-\gamma_{10}}}+1\Big)\Big(\frac{h}{p^{\gamma_6}}+1\Big)\\&\cdot\Big(\frac{h}{p^{\gamma_7}}+1\Big)\Big(\frac{h}{p^{\gamma_8}}+1\Big)\Big(\frac{h}{p^{\gamma_9}}+1\Big)\Big(\frac{h}{p^{\gamma_{10}}}+1\Big)\ll T.\end{aligned}$$

(2) 若 $\gamma_4>\gamma_9$, 则当 $\gamma_4\geqslant\frac{\mu-\gamma_{10}}{2}$ ($\frac{\mu-\gamma_{10}}{2}>\gamma_9$ 显然成立) 时, M_4 的解数显然是 $\ll\frac{h}{p^{\frac{\mu-\gamma_{10}}{2}}}+1$; 当 $\gamma_4<\frac{\mu-\gamma_{10}}{2}$ 时, 则与情形 (1) 中估计 M_4 解数的过程类似 (其中, 给定 M_3, M_6, M_7, M_8, M_9, M_{10}, 则 M_4 的解数 $\ll\frac{h}{p^{\mu-\gamma_{10}-\gamma_4}}+1\leqslant\frac{h}{p^{\mu-\gamma_{10}-[\frac{\mu-\gamma_{10}}{2}]}}+1$). 因此

$$\begin{aligned}\#A_9\ll h&\Big(\frac{h}{p^{\mu}}+1\Big)\Big(\frac{h}{p^{\mu-[\frac{3}{4}\mu]}}+1\Big)\Big(\frac{h}{p^{\mu-\gamma_{10}-[\frac{\mu-\gamma_{10}}{2}]}}+1\Big)\Big(\frac{h}{p^{\mu-\gamma_{10}}}+1\Big)\Big(\frac{h}{p^{\gamma_6}}+1\Big)\\&\cdot\Big(\frac{h}{p^{\gamma_7}}+1\Big)\Big(\frac{h}{p^{\gamma_8}}+1\Big)\Big(\frac{h}{p^{\gamma_9}}+1\Big)\Big(\frac{h}{p^{\gamma_{10}}}+1\Big)\ll T.\end{aligned}$$

而对于 "$\gamma_2>\gamma_3>\gamma_4>\gamma_5$" 和 "$\gamma_2>\gamma_3=\gamma_4>\gamma_5$" 的情形, 同理可得. 因此, 总有 $\#A_9\ll T$.

引理 3.7 设 $A_{10}=\{\mathbf{m}\in A_6:\gamma_2=\gamma_3=\gamma_4>\gamma_5\}$, 则 $\#A_{10}\ll T$.

证 对集合 A_{10} 中的元素, 可分以下两类讨论:

(1) 若 $\exists i,j\in\{2,3,4\}$, 使 $M_i\not\equiv M_j\pmod{p^{\gamma_4+1}}$ (不妨设 $i=2$, $j=4$), 则与引理 3.6 中的证明过程类似, 可得

$$\begin{aligned}\#A_{10}\ll h&\Big(\frac{h}{p^{\mu}}+1\Big)\Big(\frac{h}{p^{\mu-[\frac{3}{4}\mu]}}+1\Big)\Big(\frac{h}{p^{\mu-\gamma_{10}-\gamma_9}}+1\Big)\Big(\frac{h}{p^{\mu-\gamma_{10}}}+1\Big)\Big(\frac{h}{p^{\gamma_6}}+1\Big)\\&\cdot\Big(\frac{h}{p^{\gamma_7}}+1\Big)\Big(\frac{h}{p^{\gamma_8}}+1\Big)\Big(\frac{h}{p^{\gamma_9}}+1\Big)\Big(\frac{h}{p^{\gamma_{10}}}+1\Big)\ll T.\end{aligned}$$

(2) 若 $M_2\equiv M_3\equiv M_4\pmod{p^{\gamma_4+1}}$, 则与引理 3.5 情形 (2) 中过程类似, 对同余方程 $f_1(X)\equiv f_2(X)\pmod{p^{\mu}}$, 重新选取 $Y=X+m_4$, 此时显然有而 $\mathrm{ord}_p(\widetilde{M}_2)\geqslant\mathrm{ord}_p(\widetilde{M}_3)>\mathrm{ord}_p(\widetilde{M}_4)>\mathrm{ord}_p(\widetilde{M}_5)=\mathrm{ord}_p(\widetilde{M}_{10})$ 且 $\mathrm{ord}_p(\widetilde{M}_{10})+\mathrm{ord}_p(\widetilde{M}_9)+\mathrm{ord}_p(\widetilde{M}_8)+\mathrm{ord}_p(\widetilde{M}_7)\geqslant\mu$.

设 $A'_{10}=\{\mathbf{m}\in A_1:\gamma'_2\geqslant\gamma'_3>\gamma'_4>\gamma'_5=\gamma'_{10},\gamma'_{10}+\gamma'_9+\gamma'_8+\gamma'_7\geqslant\mu\}$ (其中 $\gamma'_i=\mathrm{ord}_p(\widetilde{M_i})$), 于是由引理 3.1–3.3, 引理 3.6, 不难得到 $\#\{\mathbf{m}\in A_{10}:M_2\equiv M_3\equiv M_4\pmod{p^{\gamma_4+1}}\}\leqslant\#A'_{10}\leqslant\#\{\mathbf{m}\in A'_{10}:\gamma'_{10}+\gamma'_9+\gamma'_8\geqslant\mu\}+\#\{\mathbf{m}\in A'_{10}:\gamma'_{10}+\gamma'_9+\gamma'_8<\mu,\gamma'_{10}+\gamma'_9+\gamma'_8+\gamma'_7\geqslant\mu\}\ll T$.

所以仍然有 $\#A_{10}\ll T$.

引理 3.8　设 $A_{11}=\{\mathbf{m}\in A_6:\gamma_2=\gamma_3=\gamma_4=\gamma_5\}$, 则 $\#A_{11}\ll T$.

证　由于此时 $\gamma_{10}+\gamma_9+\gamma_8+\gamma_7\geqslant\mu$, 所以必有 $\gamma_5\geqslant\frac{\mu}{4}$, 于是, 可对 A_{11} 中元素分以下两类讨论:

(1) 若 $\forall i,j\in\{2,3,4,5\}$, 成立 $M_i\not\equiv M_j\pmod{p^{\gamma_5+1}}$, 则与引理 3.4 情形 (1) 中的估计过程相同, 此时仍然有

$$\#A_{11}\ll T.$$

(2) 若 $\exists i,j\in\{2,3,4,5\}$, 使 $M_i\equiv M_j\pmod{p^{\gamma_5+1}}$, 不妨设 $i=5$, 则与引理 3.5 情形 (2) 中的证明过程类似, 对同余方程 $f_1(X)\equiv f_2(X)\pmod{p^\mu}$, 可重新选取 $Y=X+m_5$, 同样, 由引理 3.1 ∼ 3.7 不难发现, $\#\{\mathbf{m}\in A_{11}:\exists i,j\in\{2,3,4,5\}$, 使 $M_i\equiv M_j\pmod{p^{\gamma_5+1}}\}\ll T$.

所以 $\#A_{11}\ll T$.

引理 3.9　设 $A_{12}=\{\mathbf{m}\in A_5:\gamma_5<\gamma_{10}\}$, 则 $\#A_{12}\ll T$.

证　对 A_{12} 可分以下几种情况讨论:

(1) 若 $\gamma_5<\gamma_{10}$ 且 $\exists i,j\in\{2,3,4,5\}$, 使得 $\gamma_i\neq\gamma_j$, 则由 (2.1)–(2.3) 可发现, 与 γ_i 的定义矛盾. 以情形 $\gamma_4>\gamma_5<\gamma_{10}$ 为例: 由于此时 $\gamma_{10}+\gamma_9+\gamma_8<\mu$, 所以 $\gamma_5<\gamma_{10}<\frac{\mu}{3}$, 由 (2.1), $M_5\equiv0\pmod{p^{\gamma_5+1}}$, 与 γ_5 的定义矛盾, 故不可能.

(2) 若 $\gamma_2=\gamma_3=\gamma_4=\gamma_5<\gamma_{10}$, 由 (2.4), 此时必有 $\gamma_5\geqslant\frac{\mu}{4}$, 则与引理 3.5 情形 (2) 中的求解过程类似, 对同余方程 $f_1(X)\equiv f_2(X)\pmod{p^\mu}$, 可重新选取 $Y=X+m_5$, 则 $\mathrm{ord}_p(m_5-m_{10})=\gamma_5=\mathrm{ord}_p(m_1-m_5)$, 所以 γ'_i 满足 $\gamma'_5=\gamma'_{10}$ (其中 γ'_i 定义与前文相同). 由引理 3.1–3.8, 不难得到 $\#\{\mathbf{m}\in A_{12}:\gamma_2=\gamma_3=\gamma_4=\gamma_5<\gamma_{10}\}\ll T$.

引理 3.10　设 $A_{13}=\{\mathbf{m}\in A_5:\gamma_5>\gamma_{10}\}$, 则 $\#A_{13}\ll T$.

证　与引理 3.9 的证明过程类似:

(1) 若 $\gamma_5>\gamma_{10}$ 且 $\exists i,j\in\{7,8,9,10\}$, 使得 $\gamma_i\neq\gamma_j$, 则由 (2.1)–(2.3) 可发现矛盾.

(2) 若 $\gamma_5>\gamma_{10}=\gamma_9=\gamma_8=\gamma_7\leqslant\gamma_6$, 由 (2.4), 此时必有 $\gamma_5\geqslant\frac{\mu}{4}$, 则与引理 3.5 情形 (2) 中的证明过程类似, 对同余方程 $f_1(X)\equiv f_2(X)\pmod{p^\mu}$, 可重新选取 $Y=X+m_{10}$, 同理 γ'_i 满足 $\gamma'_5=\gamma'_{10}$. 由引理 3.1–3.8, 不难得到 $\#\{\mathbf{m}\in A_{13}:\gamma_5>\gamma_{10}=\gamma_9=\gamma_8=\gamma_7\leqslant\gamma_6\}\ll T$.

引理 3.11　$\#A_5\ll T$.

证　由引理 3.4–3.10 不难证得.

3.3　$\gamma_{10}+\gamma_9+\gamma_8+\gamma_7<\mu$ 且 $\gamma_{10}+\gamma_9+\gamma_8+\gamma_7+\gamma_6\geqslant\mu$ 情形

这时, 与 "$\gamma_{10}+\gamma_9+\gamma_8+\gamma_7\geqslant\mu$ 且 $\gamma_{10}+\gamma_9+\gamma_8<\mu$" 情形时所用的证明方法类似 (但需作一些改动), 设 $A_{14}=\{\mathbf{m}\in A_1:\gamma_{10}+\gamma_9+\gamma_8+\gamma_7+\gamma_6\geqslant\mu$ 且 $\gamma_{10}+\gamma_9+\gamma_8+\gamma_7<\mu\}$,

$A_{15}=\{\mathbf{m}\in A_{14}:\gamma_{10}=\gamma_5\}$, $A_{16}=\{\mathbf{m}\in A_{15}:\gamma_4>\gamma_5\}$, $A_{17}=\{\mathbf{m}\in A_{16}:\gamma_4\leqslant\gamma_9\}$.

我们先将集合 A_{14} 分解为 $\{\mathbf{m}\in A_{14}:\gamma_5<\gamma_{10}\}\cup\{\mathbf{m}\in A_{14}:\gamma_5>\gamma_{10}\}\cup\{\mathbf{m}\in A_{15}:\gamma_4=\gamma_5\}\cup A_{16}$, 并通过分别估计各集合势的上界，来完成对 $\#A_{14}$ 的上界估计.

引理 3.12 设 $A_{18}=\{\mathbf{m}\in A_{17}:\gamma_2>\gamma_3>\gamma_4>\gamma_5\}$, 则 $\#A_{18}\ll T$.

证 由于此时 $\gamma_5=\gamma_{10}<\gamma_4\leqslant\gamma_9$, 与引理 3.6 情形 (2) 过程类似，此时

$$\#A_{18}\ll h\Big(\frac{h}{p^{\mu}}+1\Big)\Big(\frac{h}{p^{\frac{\mu-\gamma_{10}-\gamma_9}{2}}}+1\Big)\Big(\frac{h}{p^{\mu-\gamma_{10}-\gamma_9}}+1\Big)\Big(\frac{h}{p^{\mu-\gamma_{10}}}+1\Big)\Big(\frac{h}{p^{\gamma_6}}+1\Big)\cdot\Big(\frac{h}{p^{\gamma_7}}+1\Big)\Big(\frac{h}{p^{\gamma_8}}+1\Big)\Big(\frac{h}{p^{\gamma_9}}+1\Big)\Big(\frac{h}{p^{\gamma_{10}}}+1\Big)\ll T.$$

所以 $\#A_{18}\ll T$.

引理 3.13 设 $A_{19}=\{\mathbf{m}\in A_{17}:\gamma_2>\gamma_3=\gamma_4>\gamma_5\}$, 则 $\#A_{19}\ll T$.

证 这时，对集合 A_{19} 中的元素，与引理 3.4 的过程类似 (分 $M_3\not\equiv M_4\pmod{p^{\gamma_4+1}}$, $M_3\equiv M_4\pmod{p^{\gamma_4+1}}$ 两类情况讨论), 则同样有

$$\#A_{19}\ll h\Big(\frac{h}{p^{\mu}}+1\Big)\Big(\frac{h}{p^{\mu-\gamma_{10}}}+1\Big)\Big(\frac{h}{p^{\mu-\gamma_{10}-\gamma_9}}+1\Big)\Big(\frac{h}{p^{\frac{\mu-\gamma_{10}-\gamma_9}{2}}}+1\Big)\Big(\frac{h}{p^{\gamma_6}}+1\Big)\cdot\Big(\frac{h}{p^{\gamma_7}}+1\Big)\Big(\frac{h}{p^{\gamma_8}}+1\Big)\Big(\frac{h}{p^{\gamma_9}}+1\Big)\Big(\frac{h}{p^{\gamma_{10}}}+1\Big)\ll T.$$

引理 3.14 设 $A_{20}=\{\mathbf{m}\in A_{17}:\gamma_2=\gamma_3>\gamma_4>\gamma_5\}$, 则 $\#A_{20}\ll T$.

证 这时, 对集合 A_{20} 中的元素, 与引理 3.5 的证明过程类似, 分 $M_2\not\equiv M_3\,(\mathrm{mod}\,p^{\gamma_3+1})$, $M_2\equiv M_3\pmod{p^{\gamma_3+1}}$ 两类情况讨论，对后者，可重新选取 $Y=X+m_3$, 同理可得 $\#A_{20}\ll T$.

引理 3.15 设 $A_{21}=\{\mathbf{m}\in A_{17}:\gamma_2=\gamma_3=\gamma_4>\gamma_5\}$, 则 $\#A_{21}\ll T$.

证 与引理 3.5 的证明过程类似, 分 $\exists i,j\in\{2,3,4\}$, 使 $M_i\not\equiv M_j\pmod{p^{\gamma_4+1}}$ $(i\neq j)$, 与 $\exists i,j\in\{2,3,4\}$, 使 $M_i\equiv M_j\pmod{p^{\gamma_4+1}}$ $(i\neq j)$ 两类情况讨论，对后者 (此时不妨设 $i=3$, $j=4$), 可重新选取 $Y=X+m_4$, 同理可得 $\#A_{21}\ll T$.

引理 3.16 $\#A_{17}\ll T$.

证 由引理 3.12–3.15 立即可得.

设 $A_{22}=\{\mathbf{m}\in A_{16}:\gamma_4>\gamma_9\}$, 则接下来只需估计 A_{16} 中满足条件 $\gamma_4>\gamma_9$ 的元素个数.

引理 3.17 若 $A_{23}=\{\mathbf{m}\in A_{22}:\gamma_2\geqslant\gamma_3\geqslant\gamma_4>\gamma_5=\gamma_{10}\leqslant\gamma_9=\gamma_8=\gamma_7=\gamma_6\}$, 则 $A_{22}\subset A_{23}$.

证 对于 A_{22} 中的元素，以 "$\gamma_2>\gamma_3>\gamma_4>\gamma_5=\gamma_{10}$" 为例，此时，若 $\gamma_{10}\leqslant\gamma_9=\gamma_8=\gamma_7=\gamma_6$ 不成立，则由 (2.2)–(2.4), 可导出矛盾 (以情形 $\gamma_4>\gamma_5=\gamma_{10}=\gamma_9<\gamma_8$ 为例，由 (2.2), $M_9M_{10}\equiv 0\pmod{p^{2\gamma_{10}+1}}$, 与 γ_{10} 的定义相矛盾，故不可能).

因此，只剩余 $\gamma_4>\gamma_5=\gamma_{10}\leqslant\gamma_9=\gamma_8=\gamma_7=\gamma_6$ 两种情形. 而对 A_{22} 中其余情况 (即 $\gamma_2\geqslant\gamma_3=\gamma_4>\gamma_5=\gamma_{10}$ 或 $\gamma_2>\gamma_3=\gamma_4>\gamma_5=\gamma_{10}$), 重复以上讨论，同理可得.

所以，此时即有 $A_{22}\subset A_{23}$.

引理 3.18　设 $A_{24}=\{\mathbf{m}\in A_{14}:\gamma_{10}<\gamma_9=\gamma_8=\gamma_7=\gamma_6\}$, 则 $\#A_{24}\ll T$.

证　对集合 A_{24} 中的元素可分以下两种情况讨论:

(1) 若 $\forall u_1,u_2\in\{6,7,8,9\}$, $M_{u_1}\not\equiv M_{u_2}\pmod{p^{\gamma_9+1}}$ 或有且仅有一对 $u_1,u_2\in\{6,7,8,9\}$ 存在, 使得 $M_{u_1}\equiv M_{u_2}\pmod{p^{\gamma_9+1}}$ 成立 (这时不妨设 $u_1=6,u_2=7$), 则与引理 3.5 情形 (2) 中的过程类似, 重新选取 $Y=X+m_6$, 由引理 3.1–3.3, 3.11, 3.13, 3.15 可得, 此时 $\#A_{24}\ll T$.

(2) 否则, 在其余情形下, 与引理 3.17 的过程类似, 由 (2.2)–(2.4) 可得, 此时与 γ_i 的定义矛盾.

因此 $\#A_{24}\ll T$.

引理 3.19　设 $A_{25}=\{\mathbf{m}\in A_{23}:\gamma_{10}=\gamma_9=\gamma_8=\gamma_7=\gamma_6\}$, 则 $\#A_{25}\ll T$.

证　此时, 与引理 3.18 的证明过程类似, 对集合 A_{25} 中的元素可分两种情况讨论:

(1) 若 "$\forall i,j\in\{6,7,8,9,10\}$, 成立 $M_i\not\equiv M_j\pmod{p^{\gamma_{10}+1}}$" 或 "$\exists t_1,t_2\in\{6,7,8,9,10\}$, 使 $M_{t_1}\equiv M_{t_2}\pmod{p^{\gamma_{10}+1}}$, 且 $\forall t_0\in\{t_3,t_4,t_5\}$, 成立 $M_{t_0}\not\equiv M_{t_1}\pmod{p^{\gamma_{10}+1}}$ (不妨设 $t_1=6,t_2=7$)" 两者之一成立, 则与引理 3.5 情形 (2) 中的过程类似, 可选取 $Y=X+m_6$, 由引理 3.1–3.3, 3.11–3.13 可得, $\#A_{25}\ll T$.

(2) 否则, 在其余情形下, 与引理 3.17 的过程类似, 由 (2.2)–(2.4) 可得, 此时与 γ_i 的定义矛盾.

因此 $\#A_{25}\ll T$.

引理 3.20　$\#A_{16}\ll T$.

证　由引理 3.16–3.19 立即可得.

对于集合 A_{15} 中的元素, 当 $\gamma_4=\gamma_5$ 时, 同样可类似运用上述方法. 设 $A_{26}=\{\mathbf{m}\in A_{15}:\gamma_4=\gamma_5\}$, $A_{27}=\{\mathbf{m}\in A_{26}:\gamma_3\leqslant\gamma_8\}$.

引理 3.21　设 $A_{28}=\{\mathbf{m}\in A_{27}:\gamma_2\geqslant\gamma_3>\gamma_4=\gamma_5\}$, 则 $\#A_{28}\ll T$.

证　这时, 由 (2.2), 必有 $\gamma_4=\gamma_9$. 因此, 对集合 A_{28} 中的元素可分以下两类讨论:

(1) 若 $M_2\not\equiv M_3\pmod{p^{\gamma_3+1}}$, 则与引理 3.13 的过程类似, 不难得到 $\#A_{28}\ll T$.

(2) 若 $M_2\equiv M_3\pmod{p^{\gamma_3+1}}$, 与引理 3.5 情形 (2) 中的过程类似, 可选取 $Y=X+m_3$, 此时 γ_i' 满足 $\gamma_2'>\gamma_3'>\gamma_4'=\gamma_5'=\gamma_{10}'=\gamma_9'$. 由引理 3.1–3.3, 3.11, 3.21, 不难证得 $\#\{\mathbf{m}\in A_{28}:M_2\equiv M_3\pmod{p^{\gamma_3+1}}\}\leqslant\#A_{28}'\ll T$.

因此 $\#A_{28}\ll T$.

引理 3.22　设 $A_{29}=\{\mathbf{m}\in A_{27}:\gamma_2>\gamma_3=\gamma_4=\gamma_5$ 且存在 $i_1,i_2\in\{3,4,5\}$, 使得 $M_{i_1}\not\equiv M_{i_2}\pmod{p^{\gamma_5+1}}\}$, 则 $\#A_{29}\ll T$.

证　对集合 A_{29} 中的元素可分以下几类讨论:

(1) 若 M_3, M_4, M_5 间模 p^{γ_5+1} 互不同余, 则与引理 3.4 情形 (1) 中的证明过程类似, 根据命题 2.1, 取 $i_1=3$, $i_2=4$, $i_3=5$,

$$\begin{aligned}\#A_{29}\ll h\Big(\frac{h}{p^{\mu}}+1\Big)\Big(\frac{h}{p^{\mu-\gamma_{10}}}+1\Big)\Big(\frac{h}{p^{\mu-2\gamma_{10}}}+1\Big)\Big(\frac{h}{p^{\mu-3\gamma_{10}}}+1\Big)\Big(\frac{h}{p^{\gamma_6}}+1\Big)\\ \cdot\Big(\frac{h}{p^{\gamma_7}}+1\Big)\Big(\frac{h}{p^{\gamma_8}}+1\Big)\Big(\frac{h}{p^{\gamma_9}}+1\Big)\Big(\frac{h}{p^{\gamma_{10}}}+1\Big)\ll T.\end{aligned}$$

(2) 若 $\exists i,j,k\in\{3,4,5\}$, 使 $M_i\equiv M_j\not\equiv M_k\pmod{p^{\gamma_5+1}}$, 不妨设 $i=3$, $j=4$, $k=5$, 则同样根据命题 2.1, 取 $i_1=3$, $i_2=5$, $i_3=4$, 依然有 $\#A_{29}\ll T$.

引理 3.23 设 $A_{30}=\{\mathbf{m}\in A_{27}:\gamma_2=\gamma_3=\gamma_4=\gamma_5$ 且 M_2, M_3, M_4, M_5 间模 p^{γ_5+1} 互不同余$\}$, 则 $\#A_{30}\ll T$.

证 由于 M_2, M_3, M_4, M_5 间模 p^{γ_5+1} 互不同余, 则与引理 3.4 情形 (1) 中的证明过程类似, 根据命题 2.1, 取 $i_1=3$, $i_2=4$, $i_3=5$, 同理可得 $\#A_{30}\ll T$.

设 $A_{31}=\{\mathbf{m}\in A_{26}:\gamma_3>\gamma_8\}$, 与引理 3.17 的证明过程类似, 可得以下引理:

引理 3.24 若 $A_{32}=\{\mathbf{m}\in A_{26}:\gamma_2\geqslant\gamma_3>\gamma_4=\gamma_5=\gamma_{10}=\gamma_9\leqslant\gamma_8=\gamma_7=\gamma_6$ 且 $\gamma_8<\gamma_3\}$, 则 $A_{31}\subset A_{32}$.

同样, 与引理 3.18, 3.19 证明过程类似, 同理可得引理 3.25, 3.26.

引理 3.25 设 $A_{33}=\{\mathbf{m}\in A_{32}:M_4\not\equiv M_5\pmod{p^{\gamma_{10}+1}}\}$, 则 $\#A_{33}\ll T$.

引理 3.26 设 $A_{34}=\{\mathbf{m}\in A_{32}:M_4\equiv M_5\pmod{p^{\gamma_{10}+1}}\}$, 则 $\#A_{34}\ll T$.

引理 3.27 设 $A_{35}=\{\mathbf{m}\in A_{15}:\gamma_2\geqslant\gamma_3>\gamma_4=\gamma_5=\gamma_{10}\}$, 则 $\#A_{35}\ll T$.

证 由引理 3.21, 3.24–3.26 立即可得.

引理 3.28 设 $A_{36}=\{\mathbf{m}\in A_{15}:\gamma_2>\gamma_3=\gamma_4=\gamma_5=\gamma_{10}\}$, 则 $\#A_{36}\ll T$.

证 由引理 3.22, 不难发现, 只需再证 $M_3\equiv M_4\equiv M_5\pmod{p^{\gamma_5+1}}$ 时情形即可. 对此, 与引理 3.5 情形 (2) 中的过程类似, 可选取 $Y=X+m_5$, 则 γ_i' 满足 $\gamma_2'\geqslant\gamma_3'>\gamma_4'=\gamma_5'=\gamma_{10}'$.

设 $A_{36}'=\{\mathbf{m}\in A_1:\gamma_2'\geqslant\gamma_3'>\gamma_4'=\gamma_5'=\gamma_{10}'\}$, 由引理 3.1–3.3, 3.11, 3.27, 同理可得 $\#\{\mathbf{m}\in A_{36}:M_3\equiv M_4\equiv M_5\pmod{p^{\gamma_5+1}}\}\leqslant\#A_{36}'\ll T$.

引理 3.29 设 $A_{37}=\{\mathbf{m}\in A_{15}:\gamma_2=\gamma_3=\gamma_4=\gamma_5=\gamma_{10}\}$, 则 $\#A_{37}\ll T$.

证 由引理 3.23, 不难发现, 只需再证 "$\exists k_1,k_2\in\{2,3,4,5\}$, 使 $M_{k_1}\equiv M_{k_2}\pmod{p^{\gamma_5+1}}$" 情形即可. 此时, 不妨假设 $k_2=5$, 则与引理 3.5 情形 (2) 中的过程类似, 选取 $Y=X+m_5$, 则 γ_i' 满足 $\gamma_2'\geqslant\gamma_3'\geqslant\gamma_4'>\gamma_5'=\gamma_{10}'$ 或 $\gamma_2'\geqslant\gamma_3'>\gamma_4'=\gamma_5'=\gamma_{10}'$ 或 $\gamma_2'>\gamma_3'=\gamma_4'=\gamma_5'=\gamma_{10}'$.

设 $A_{37}'=\{\mathbf{m}\in A_1:\gamma_2'\geqslant\gamma_3'\geqslant\gamma_4'>\gamma_5'=\gamma_{10}'$ 或 $\gamma_2'\geqslant\gamma_3'>\gamma_4'=\gamma_5'=\gamma_{10}'$ 或 $\gamma_2'>\gamma_3'=\gamma_4'=\gamma_5'=\gamma_{10}'\}$, 由引理 3.1–3.3, 3.11, 3.20, 3.27, 3.28, 同理可得 $\#\{\mathbf{m}\in A_{37}:\exists k_1\in\{2,3,4,5\}$, 使 $M_{k_1}\equiv M_5\pmod{p^{\gamma_5+1}}\}\leqslant\#A_{37}'\ll T$.

引理 3.30 设 $A_{38}=\{\mathbf{m}\in A_{14}:\gamma_5<\gamma_{10}\}$, 则 $\#A_{38}=0$.

证 此时, 与引理 3.9 情形 (1) 的讨论过程类似, 由 (2.1)–(2.4) 可得出矛盾. 因此 $\#A_{38}=0$.

引理 3.31 设 $A_{39}=\{\mathbf{m}\in A_{14}:\gamma_5>\gamma_{10}\}$, $\#A_{39}\ll T$.

证 该证明过程与引理 3.9 相似, 此时 $\#A_{39}=\#\{\mathbf{m}\in A_{39}:\gamma_5>\gamma_{10}=\gamma_9=\gamma_8=\gamma_7=\gamma_6\}$, 由引理 3.1–3.3, 3.11, 3.20, 3.27–3.29 可得结论.

4 关于定理 1.2 的证明及说明

由引理 3.1–3.3, 3.11, 3.20, 3.27–3.31 立即可得，定理 1.2 成立.

此外，与 Dodd 在 [4] 中过程类似，还可将定理 1.2 用于估计同余方程组

$$x_1^w+\cdots+x_d^w\equiv y_1^w+\cdots+y_d^w \pmod{p^\vartheta}$$

解数的上界 (其中 w,w_0,d,ϑ 满足 $1\leqslant w\leqslant w_0$, $d\geqslant w_0\geqslant 4$, $\vartheta\geqslant w_0^2$, p 是一个素数且 $p>k$).

以 $w_0=d=5$, $\vartheta=25$ 为例， $p>5$ 时同余方程组

$$\begin{cases} s_1(x)\equiv s_1(y) \pmod{p^{25}},\\ s_2(x)\equiv s_2(y) \pmod{p^{25}},\\ s_3(x)\equiv s_3(y) \pmod{p^{25}},\\ s_4(x)\equiv s_4(y) \pmod{p^{25}},\\ s_5(x)\equiv s_5(y) \pmod{p^{25}} \end{cases}$$

等价于同余方程组

$$\begin{cases} \sigma_1(x)\equiv \sigma_1(y) \pmod{p^{25}},\\ \sigma_2(x)\equiv \sigma_2(y) \pmod{p^{25}},\\ \sigma_3(x)\equiv \sigma_3(y) \pmod{p^{25}},\\ \sigma_4(x)\equiv \sigma_4(y) \pmod{p^{25}},\\ \sigma_5(x)\equiv \sigma_5(y) \pmod{p^{25}}, \end{cases} \tag{4.1}$$

其中

$$\begin{aligned} \sigma_1(x)&=x_1+x_2+x_3+x_4+x_5,\\ \sigma_2(x)&=x_1x_2+x_1x_3+x_1x_4+x_1x_5+x_2x_3+x_2x_4+x_2x_5+x_3x_4+x_3x_5+x_4x_5,\\ \sigma_3(x)&=x_1x_2x_3+x_1x_2x_4+x_1x_2x_5+x_1x_3x_4+x_1x_3x_5+x_1x_4x_5+x_2x_3x_4\\ &\quad+x_2x_3x_5+x_2x_4x_5+x_3x_4x_5,\\ \sigma_4(x)&=x_1x_2x_3x_4+x_1x_2x_3x_5+x_1x_2x_4x_5+x_1x_3x_4x_5+x_2x_3x_4x_5,\\ \sigma_5(x)&=x_1x_2x_3x_4x_5. \end{aligned}$$

由定理 1.2, 不难得到，该同余方程组解数 $\ll p^{\frac{315}{2}}$.

5 对 Dodd 结论的改进

当 $r=4$ 时，运用同样的方法，可得定理 1.1 的结论

$$\#S(4)\ll \frac{h^8}{p^{4\mu-\frac{7}{4}[\frac{\mu}{2}]}}+\frac{h^7}{p^{3\mu-\frac{7}{4}[\frac{\mu}{2}]}}+\frac{h^5}{p^{\mu-[\frac{\mu}{2}]}}+h^4, \tag{5.1}$$

其中 $S(4)=\{m:0<m_i\leqslant h, i=1,\cdots,8, f_1(X)\equiv f_2(X) \pmod{p^\mu}\}$.

对于该结论，与 Dodd 在 [4] 中得到的结论相比，当 μ 满足 "$\frac{\alpha}{8}<2\mu-\frac{11}{4}[\frac{\mu}{2}]+[\frac{\mu}{4}]+6\log_p\mu$", 或 "$\frac{\alpha}{8}\geqslant 2\mu-\frac{11}{4}[\frac{\mu}{2}]+[\frac{\mu}{4}]+6\log_p\mu$, $\mu\geqslant[\frac{\alpha-[\frac{3}{4}\alpha]}{2}]+1$ 且 $h<\mu^6p^{2\mu-\frac{11}{4}[\frac{\mu}{2}]+[\frac{\mu}{4}]}$" 这两个条件中的任何一个时，定理 1.1 的结论比 Dodd 在 [4] 中得到的结论 (1.2) 更好.

致谢 感谢陆鸣皋教授的悉心鼓励与指导.

参 考 文 献

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

[2] Burgess D. A., The character sum estimate with $r = 3$ [J], *J. London Math. Soc.*, 1986, 33(2):219–226.

[3] Burgess D. A., On a set of congruences related to character sums [J], *J. London Math. Soc.*, 1988, 37(2):385–394.

[4] Dodd L., An upper bound for the number of solutions of a system of congruences [J], *Acta Arithmetica*, 1994, 66(4):323–350.

[5] Burgess D. A., On a set of congruences related to character sums III [J], *J. London Math. Soc.*, 1992, 45(2):201–214.

The Estimation of an Upper Bound for the Number of Solutions of a Kind of Congruences

WANG Yunjie*

*Department of Mathematics, Shanghai Jiaotong University, Shanghai 200240, China. E-mail: himmelwangyj@163.com

Abstract This paper investigates the estimation of the solution number about $\mathbf{m} = (m_1, \cdots, m_{2r})$ of the congruences such as $\prod_{i=1}^{r}(X + m_i) \equiv \prod_{j=r+1}^{2r}(X + m_j) \pmod{p^\mu}$, and gets the upper bound of the solution number of such congruence when $r = 4$ and 5. The former result improves the Dodd's conclusion, and the latter can be used to estimate the solution number of the other kinds of congruences.

Keywords The number of solutions of congruences, p-adic exponential evalution, Character sums

2000 MR Subject Classification 11A07, 11S99, 11L40