arXiv:2302.02725v2 [math.NT] 4 Apr 2024

小集合上的模形式同余类

SUBHAM BHAKTA、S. KRISHNAMOORTHY 和 R. MUNEESWARAN

摘要：J.P. Serre 证明，对于任意整数 m，几乎所有 n 都有 a(n) $\equiv 0 \pmod m$，其中 a(n) 是任意一个具有有理系数的模形式的第 n^{th} 个傅里叶系数。本文中，我们考察一类特定的尖点形式，并研究在素因子个数为 O(1) 的整数集合上，$\#\{a(n) \pmod m\}_{n\le x}$ 的分布。此外，我们证明，任意剩余类 $a \in \mathbb{Z}/m\mathbb{Z}$ 都可以表示为至多十三个傅里叶系数之和，且这些系数关于 m 多项式有界。

1. 引言

设 f(z) 是一个权为 $k \in 2\mathbb{Z}$、层为 N 的模形式，其傅里叶展开为

$$f(z) = \sum_{n=1}^{\infty} a(n) e^{2\pi i n z}, \quad \Im(z) \geq 0,$$

其中 $a(n)$ 是第 n^{th} 个傅里叶系数。本文中，我们假设所有傅里叶系数 $a(n) \in \mathbb{Q}$. J.P. Serre 在 [17] 中证明，如果存在一个素数 $p \nmid 2$使得 a(p) (模 m)，那么我们就有一个渐近展开

$$\#\{n \leq x \mid a(n) \not\equiv 0 \pmod m\} = c\frac{x}{\log^{\alpha(m)} x},$$

对于某个 $c > 0$, $0 < \alpha(m) < 1$. 另一方面，他还证明，若存在素数 p，使得对所有 $p \nmid 2N$，$a(p) \equiv 0 \pmod m$，则存在 $c' > 0$ 使得

$$\#\{n \leq x \mid a(n) \not\equiv 0 \pmod m\} = c'\sqrt{x}.$$

这些结果基本上可由 Delange 对 Wiener-Ikehara 塔伯定理的推广 [4], 以及考察环$\mathbb{Z}/m\mathbb{Z}$. 上的相应 L 函数得出。特别地，这表明，对几乎所有 n，$a(n) \equiv 0 \pmod m$，而其他剩余类出现得相当罕见。然而，我们不知道每个非零剩余类 $a \in \mathbb{Z}/m\mathbb{Z}$ 是否都能以相同比例写成 a(n) (mod m)。Serre 在 [17] 第 20 页中提到，对于任意奇数 m 和非零 $a \in \mathbb{Z}/m\mathbb{Z}$,

$$\#\{n \leq x \mid a(n) \equiv a \pmod m,\ \omega(n) = M\} \gg \frac{x}{\log x}(\log\log x)^M.$$

这些论证的证明基于如下事实：对于正密度的素数 $p \equiv 1 \pmod m$ 和 $q \equiv -1 \pmod m$，相应的 Hecke 算子 T_p 和 T_q

日期：2024年4月5日。2020年数学主题分类。主要分类：11G05、11F11；次要分类：11P05、11B37、11F80。关键词和短语：线性递推数列、指数和、模形式、伽罗瓦表示。

分别在所有系数取值于 $\mathbb{Q}$.的全纯模形式的 $\mathbb{Z}$-模上作用为 2 和 0

在这方面，我们研究 {a(n) (mod m)} 在具有 O(1) 个素因子的整数上的分布，并证明如下结论。

定理 1. 设 M ≥ 1 是任意整数，f 是任意不具有复乘的新形式，且其系数属于 $\mathbb{Q}$.。那么，在关于 m 的某些假设下，对于任意元组，以下渐近公式成立

$$\frac{\#\{n \leq x \mid a(n) \equiv a \pmod{m},\ \omega(n) = M\}}{\#\{n \leq x \mid \omega(n) = M\}} \sim d_a(m)\frac{1}{m^M},$$

其中 $d_a(m) > 0$ 是一个有效可计算常数。

我们将在定理 4 中给出一个更精确的版本，并将其推广至范围更广的尖点形式族。尽管这保证了方程 a(n) ≡a (mod m) 存在解，但这样的 n 可能很大。首先，方程 a(n) (mod m) 的一个解，也是对任意素数 $\ell \mid m$，方程 a(n) (mod ℓ) 的一个解。读者可参阅 [20]，了解 m 为素数时最小此类 n 的上界。Thorner 和 Zaman 假设 f (z) 是不具有复乘的新形式，且其权 k 满足 (k − 1, m − 1) = 1，相应伽罗瓦表示的像为 $GL_2(\mathbb{Z}/m\mathbb{Z})$。Thorner 和 Zaman 给出了满足 a(n) ≡a (mod m) 的最小素数 n 的上界。然而，这实际上等价于一般情形。例如，若 n_0 是最小解，则写作 $n_0 = \prod_{i=1}^{t} p^{e_i}$i,0，我们有 $\prod_{i=1}^{t}$a(p^{e_i}i,0) ≡ a (mod m)。令 a(p^{e_i} i,0) = a_i，并将 a(p^{e_i}i,0) 写成 a(p_i,0) 的多项式（由于 p_i,0 固定），可知 a(p_i,0) (mod ℓ) $\ell \mid m$ 是 $\mathbb{F}_\ell[x]$. 上一个多项式的根。接着，我们寻找满足 a(p_i) ≡a(p_i, 0) (mod ℓ) 的最小素数 p_i，由此可见，只需寻找最小素数。

特别地，我们发现，任何满足 a(n) ≡a (mod m) 的此类 n，其增长速度都可能关于 m 呈指数级。不过，事实证明，如果允许增加若干项，我们就能得到多项式上界。更准确地说，我们研究方程

$$\sum_{i=1}^{O(1)} a(n_i) \equiv a \pmod{m},\ n_i = m^{O(1)}.$$

在 [19], Shparlinski 证明，对于 Ramanujan τ 函数 τ，集合 $\{\tau(n)\}_{n\geq 1}$是模任意素数 ℓ的加法基；也就是说，存在一个绝对常数 s，使得华林型同余

$$\tau(n_1) + \cdots + \tau(n_s) \equiv a \pmod{\ell}$$

对任意剩余类 a (mod ℓ) 都有解。此外，Shparlinski 证明，每个这样的 n_i 至多为 O(ℓ^4)，且至多有 4 个素因子。他的论证依赖于对指数和

$$\sum_{\substack{u_1 \in U_1, u_2 \in U_2 \\ a(n) = u_1 u_2 \pmod{\ell}}} \mathbf{e}_\ell(\lambda(u-a)),\ \forall \lambda \in \mathbb{F}_\ell^*,$$

在 $\mathbb{F}_\ell \times \mathbb{F}_\ell$ 的一个足够大的子集 $U_1 \times U_2$ 上，该子集满足 $\#U_1 \#U_2 > \ell^{1+c}$，其中 $c > 0$. 为某个常数

最近，Bajpai、García 和第一作者在 [1] 中证明，当 f 是一个不具有复乘且傅里叶系数为有理数的新形式时，存在一个绝对常数 s_0，使得 $\mathbb{F}_\ell$ 中的任意元素都可以写成至多 s_0 个集合 $\{a(p^n)\}_{n\geq 0}$，对几乎所有素数 p 以及 ℓ都成立。此外，s_0 不依赖于 f 的选取。 为证明这一点，他们研究了指数和

$$\sum_{n\leq \Gamma} \mathbf{e}_\ell(\lambda a(p^n)),\ \forall \lambda \in \mathbb{F}_\ell^*,$$

其中 Γ 是依赖于序列 $\{a(p^n) \pmod{\ell}\}$. 的适当参数。尽管这样得到的解更多，但在这种情况下，系数可能会随着 ℓ.的变化呈指数增长。

本文以如下形式证明了对 Shparlinski 主要结果的改进。

定理 2. 设 f (z) 是任意一个有理系数尖点形式。设 $0<\varepsilon、\gamma<1$为任意给定的正实数。设 S_1,S_2 为任意一个具有正密度的素数集，且 $S_1\cap S_2=\phi$. 那么存在一个整数 $N_{S_1,\ S_2}$ 使得对于所有素因子均大于 $N_{S_1,\ S_2}$，且满足 $L^\gamma \geq m/L$ 的任意整数 m，其中 L 是 m 的最大素因子，均有如下结论。

(a) 若 f(z) 是海克特征形式，则对于任意 $a \in \mathbb{Z}/m\mathbb{Z}$，我们可以写成

$$\sum_{i=1}^{s} a(n_i) \equiv a \pmod{m},\ n_i \leq m^{4\varepsilon},\ \forall 1\leq i\leq s,$$

对于某个 $s=O_{\varepsilon,\ \gamma}(1)$。此外，任意这样的 n_i 的所有素因子都是 $O(m^\varepsilon)$，且属于 $S_1\cup S_2$.

(b) 一般而言，若 f (z) 具有 $\sum_{i=1}^{r} c_i f_i$ 的形式，其中 $c_i\in\mathbb{Q}$、f_i 是不含复乘的新形式，且 $\sum \sigma_i c_i \not\equiv 0 \pmod{m}$ $\sigma_i\in\{\pm 1\}$.。如果相应的伽罗瓦表示 $\rho_{f_{i_1}}$、$f_{i_2}\cdots$、f_{i_s}、m 均没有像 $\Delta^{(s)}k$ (m)（对任意子集 $I=\{i_1,i_2,\cdots,i_s\}$ of $\{1,2,\cdots,r\}$ with $\#I\geq 2$.），则对任意 $a\in\mathbb{Z}/m\mathbb{Z}$，我们可以写成

$$\sum_{i=1}^{s} a(n_i) \equiv a \pmod{m},\ n_i \leq m^{4\varepsilon},\ \forall 1\leq i\leq s,$$

其中 s 与 (a) 部分中的相同，任意这样的 n_i 的所有素因子都是 $O(m^\varepsilon)$，且属于 $S_1\cup S_2$.

证明定理2 的关键工具之一，是关于双线性指数和的以下估计，其内容如下：

$$\max_{\lambda\in\mathbb{Z}/m\mathbb{Z}} \left| \sum_{a_1\in A_1} \sum_{a_2\in A_2} \mathbf{e}_m(\lambda a_1 a_2) \right| \leq \sqrt{m\#A_1\#A_2},$$

对于任意子集 A_1,A_2 的 $\mathbb{Z}/m\mathbb{Z}$。我们将在第 3 节简要讨论双线性和多线性指数和。利用上述无条件指数界以及有限域子集的 和积估计 ，我们可以在定理 2 的证明中使所有结果都明确化，并得到以下结论。

推论 1. 设 f (z) 是任意一个有理系数的海克特征形式，且 S_1,S_2是任意一个具有正密度的素数集，其中 $S_1 \cap S_2 = \phi$. 那么存在整数 $N_{S_1,\ S_2}$ 使得对于任意所有素因子都大于 $N_{S_1,\ S_2}$,且满足 $L^{1/77} \geq m/L$ 的整数 m（其中 L 是 m 的最大素因子），以及任意 $a \in \mathbb{Z}/m\mathbb{Z}$，我们可以写成

$$\sum_{i=1}^{s} a(n_i) \equiv a \pmod{m},\ n_i \leq m^{130/33},\ \forall 1 \leq i \leq 13,$$

对于某个 $s \leq 52$。此外，任何此类 n_i 的所有素因子均为 $O(m^{65/66})$，且在 $S_1 \cup S_2$. 中

现在，很自然会问，能否得到素因子更小的解。在定理 2 中，我们假设 m 的所有素因子都足够大，且 m 的最大素因子大于其他素因子。当然，任何素数 m 都满足这些条件。为了得到素因子较小的合数的解，我们假设 m 无平方因子。对此，我们证明如下结果。

定理 3. 设 f (z) 为任意具有有理系数的尖点形式，$0 < \varepsilon, \gamma < 1$ 为任意给定的实数，m 为无平方因子正整数，且 S_1,$S_2, \cdots, S_\omega$ 为任意具有正密度的素数集，其中 $\varepsilon(2 + \frac{\omega-2}{81}) > 2(\gamma + 1)$ 且 $S_i \cap S_j = \phi, i \neq j$。则存在整数 $N_{S_1,S_2,\cdots,S_\omega,\varepsilon}$ ，使得对于任意整数 m，若 m 的所有素因子均大于 $N_{S_1,S_2,\cdots,S_\omega,\varepsilon}$，$m^{\varepsilon/2} = o(L)$ 且 $L^{\gamma} \geq m/L$ 对某个 $\gamma > 0$ 成立，则有以下结论。

(a) 若 f(z) 是海克特征形式，则对任意 $a \in \mathbb{Z}/m\mathbb{Z}$，我们可以写成

$$\sum_{i=1}^{s} a(n_i) \equiv a \pmod{m},\ n_i \leq m^{2\varepsilon\omega},\ \forall 1 \leq i \leq s,$$

其中 s 是可计算的，并且取决于 ε、ω、γ. 。此外，任意此类 n_i 的所有素因子ω均小于或等于 m^{ε}，且属于 $\bigcup_{i=1} S_i$.

r (b) 一般而言，若 f(z) 的形式为 $\sum c_i f_i$，其中 $c_i \in \mathbb{Q}$、f_i 是不带复乘的 新形式 $_{i=1}$，且 $\sum \sigma_i c_i \neq 0 \pmod{m}$ $\sigma_i \in \{\pm 1\}$. 。若对应的伽罗瓦表示$\rho_{f_1,f_2\cdots,f_r,m}$ 的像不含 $\Delta^{(r)}$k (m)，则对任意 $a \in \mathbb{Z}/m\mathbb{Z}$，我们可以写成

$$\sum_{i=1}^{s} a(n_i) \equiv a \pmod{\ell},\ n_i \leq m^{2\varepsilon\omega},\ \forall 1 \leq i \leq s,$$

其中 s 与 (a) 中相同。此外，任意此类 n_i 的所有素因子均ω小于或等于 m^{ε}，且属于 $\bigcup_{i=1} S_i$.

在上述两个定理的 (b) 部分中，我们讨论的是一类更广的尖点形式，其中的形式不一定是海克特征形式。我们知道，任意尖点形式 f (z) 都可以唯一地写成一组两两正交的海克特征形式的 a $\mathbb{C}$-线性组合，其傅里叶系数来自 $\mathbb{C}$。关于模形式的海克理论，简要回顾请见 [5,Chapter 5] 。我们关注的是所有这类尖点形式，

它们都可以唯一地写成一组两两正交的特征形式的 a $\mathbb{Q}$-线性组合，其傅里叶系数来自 $\mathbb{Q}$. 。读者可能会注意到，并非每个具有有理系数的权 k 尖点形式都具有这一性质。[1]

1.1. 记号。我们用 $O_{s_1,\ s_2,\ \cdots,\ s_k}(B)$ 表示绝对值至多为 cB 的量，其中 c 是仅依赖于 S1,⋯,S_K 的某个正常数；若省略下标，则隐含常数为绝对常数。我们记 $A \ll_{s_1,\ s_2,\ \cdots,\ s_k} B$ 表示 $A = O_{s_1,\ s_2,\ \cdots,\ s_k}(B)$，而 $A = o(B)$ 表示 $A/B \to 0$。

对于任意整数 n，我们记 ω(n) 为 n 的不同素因子的个数，记 μ(n) 为莫比乌斯函数。我们还记 $(\mathbb{Z}/m\mathbb{Z})^*$ 为模 m 的乘法群，记 $((\mathbb{Z}/m\mathbb{Z})^*)^k$ 为 $(\mathbb{Z}/m\mathbb{Z})^*$. 中元素的 k^{th} 次幂

2. 小集合上的分布

在本节中，我们将讨论证明主要结果所需的预备事实。

2.1. 伽罗瓦表示及其像。设 f(z) 是任意一个权为 k、层为 N 的新形式。根据 Deligne-Serre 对应，我们有一个相关的伽罗瓦表示

$$\rho_f^{(\ell)} : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \longrightarrow \mathrm{GL}_2\left(\mathbb{F}_\ell\right)$$

使得对于任意素数 $p \nmid N\ell.$，$a(p) \pmod{\ell} \equiv \mathrm{tr}\left(\rho^{(\ell)}{}_f(\mathrm{Frob}_p)\right)$ 显然，$\rho^{(\ell)}{}_f(\mathrm{Frob}_p) \pmod{\ell}$ 的特征多项式与 $x^2 - a(p)x + p^{k-1} \pmod{\ell}$ 相同。当 f 不具有复乘时，由 Ribet [14, 定理 3.1] 可知，该表示的像为

$$\mathrm{Im}\left(\rho_f^{\ell}\right) = \Delta_k(\ell) = \left\{A \in \mathrm{GL}_2\left(\mathbb{F}_\ell\right) \mid \det(A) \in \left(\mathbb{F}_\ell^*\right)^{k-1}\right\},$$

除了有限多个素数 $\ell.$ 之外。对于任意整数 $e \geq 1$，我们有一个伽罗瓦表示

$$\rho_{f,\ell^e} : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \longrightarrow \mathrm{GL}_2\left(\mathbb{F}_{\ell^e}\right)$$

满足 $a(p) \pmod{\ell^e} \equiv \mathrm{tr}\left(\rho_{f,\ \ell^e}(\mathrm{Frob}_p)\right)$，且

$$\mathrm{Im}(\rho_{f,\ell^e}) = \Delta_k(\ell^e) := \{A \in \mathrm{GL}_2\left(\mathbb{F}_{\ell^e}\right) \mid \det(A) \in \left(\mathbb{F}_{\ell^e}^*\right)^{k-1}\}.$$

现在，给定任意合数 m，我们可以自然地关联一个伽罗瓦表示 $\rho_{f,\ m} := \prod_{\ell^e \| m} \rho_{f,\ \ell^e}$，并将其像记为 $G_{f,\ m}$。根据 Ribet 的结果，我们立即得到以下推论。

推论 2. 假设 f(z) 是任意一个不具有复乘的新形式。那么，存在一个有限素数集 S_f，使得

$$G_m = \Delta_k(m) = \{A \in \mathrm{GL}_2\left(\mathbb{Z}/m\mathbb{Z}\right) \mid \det(A) \in \left((\mathbb{Z}/m\mathbb{Z})^*\right)^{k-1}\},$$

对于任意与 S 中任一素数互素的整数 m_f·

[1]例如，读者可以参阅 Jeremy Rouse 在 https://mathoverflow.net/questions/364763/cusp-forms-with-integer-fourier-coefficients 上的回答。

考虑素因数分解 $m = \prod_{\ell|m} \ell^e$. 取任意剩余类 $a \in \mathbb{Z}/\ell^e\mathbb{Z}$以及 $\lambda \in (\mathbb{Z}/\ell^e\mathbb{Z})^*$. 记 $N_{a,\lambda}(\ell^e)$ 为 $\Delta_k(\ell^e)$ 中迹为 a且行列式为 λ. 由 [11,推论 6.0.7] 可知

$$N_{a,\lambda}(\ell^e) = \begin{cases} \ell^{2e}, \text{ if } a^2 - 4\lambda = 0. \\ \ell^e(\ell^e + 1), \text{ if } a^2 - 4\lambda \text{ is a non-zero square in } \mathbb{Z}/\ell^e\mathbb{Z}. \\ \ell^e(\ell^e - 1) \text{ if } a^2 - 4\lambda \text{ is not a square in } \mathbb{Z}/\ell^e\mathbb{Z}. \end{cases} \tag{1}$$

引理 1. 设 $m = \prod_{\ell|m} \ell^e$ 为任意整数，a 为 $\mathbb{Z}/m\mathbb{Z}$ 中的任意剩余类，且$\lambda \in (\mathbb{Z}/m\mathbb{Z})^*$. 那么我们有，

$$N_{a,\lambda}(m) := \#\{A \in \Delta_k(m) \mid \mathrm{tr}(A) = a,\ \det(A) = \lambda\} = m^2 + O\left(\frac{2^{\omega(m)}m^2}{\mathscr{L}}\right),$$

其中 $\mathscr{L}$是 m 的最小素因子。

证明。根据中国剩余定理，我们可以写成

$$\Delta_k(m) = \prod_{\ell^e||m} \Delta_k(\ell^e).$$

因此，只需证明当 m 是素数幂时结论成立。由 (1) 即可得出结论。□

注 1. 特别地，对于素因子足够大的任意 m， $\Delta_k(m)$ 中矩阵的迹值在 $\mathbb{Z}/m\mathbb{Z}$ 中等分布。我们用 $\mathbb{Z}/m\mathbb{Z}$ 上的密度测度来描述等分布，其定义为，

$$A \mapsto \frac{\#A}{\mathbb{Z}/m\mathbb{Z}} = \frac{\#A}{m},\ \forall A \subseteq \mathbb{Z}/m\mathbb{Z}.$$

现在设 $f_1, f2, \cdots, f_r$ 是一组新形式，其权分别为 $k_1, k2, \cdots, k_r$。那么我们可以通过映射关联一个伽罗瓦表示 $\rho_{f_1,\ f_2,\ \cdots,\ f_r,\ m}$: 伽罗瓦群 $\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to$一般线性群$_{2r}(\mathbb{Z}/m\mathbb{Z})$

$$\sigma \mapsto \begin{pmatrix} \rho_{f_{1,\ell}}(\sigma) & & & \\ & \rho_{f_{2,\ell}}(\sigma) & & \\ & & \ddots & \\ & & & \rho_{f_{r,\ell}}(\sigma) \end{pmatrix}. \tag{2}$$

使得像 $G_{f_1,f_2,\ \ldots,\ f_r,\ m}$包含于 $\Delta_{k_1,\ k_2,\ \cdots,\ k_r}(m)$，其中 $\Delta_{k_1,\ k_2,\ \cdots,\ k_r}(m)$ 表示一般线性群$_2(\mathbb{Z}/m\mathbb{Z})$ 中所有大小为 2×2 的分块矩阵构成的集合，其中每个分块的行列式都是乘法群 $(\mathbb{Z}/m\mathbb{Z})^*$. 中某个元素的 $k_i - 1^{th}$ 次幂

定义 1. 设 ℓ 为素数。若存在一个二次特征，使得权和层分别为 k_i, k j 和 N_i, N_j 的两个新形式 f_i 和 f_j 满足，则称它们为 ℓ-等价，即 $f_i \sim_\ell$ f j,

$$\chi : (\mathbb{Z}/N_iN_j\ell\mathbb{Z})^* \to \mathbb{C}^*,$$

满足对任意素数 $p \nmid N_1N_2$. 都有 $a_f(p) = \chi(p)a_g(p) \pmod{\ell}$。此外，我们称 f_i和 f j 扭曲等价，即 $f_i \sim f_j$，如果存在一个二次特征 χ，使得对任意素数 $p \nmid N_iN_j$，都有 a f (p) $= \chi(p)a_g(p)$。

读者可能会注意到，如果 $f_i \sim f_j$，那么它们的权 k_i 和 k_j 应该相同。更重要的是，我们有以下结论。

引理 2. 如果两个新形式 f_i、f_j 不扭等价，那么它们仅对有限多个素数 ℓ 是 ℓ-等价的

证明。为导出矛盾，假设 $f_i \sim_\ell f_j$ 对无限多个素数 ℓ 成立。于是，对每个素数 $p \nmid N_i N_j$，都存在无限多个素数 $\ell > N_1 N_2 p$ 满足 $a_i(p) \equiv \pm a_j(p) \pmod{\ell}$。显然，对于某个符号 $\sigma_p \in \{\pm 1\}$，我们有 $a_p(p) = \sigma_p a_j(p)$。现在定义一个模 $N_i N_j$ 的二次狄利克雷特征 χ，使得 $\chi(p) := \sigma_p$. □

现在我们回顾 Masser 和 Wüstholz 在 [10], 中给出的主要结果，他们研究的是椭圆曲线乘积的像。换言之，当所有 f_i 在（2）中的权为 2，且 m 是素数时。在合数模数的情形下，我们有如下推广。

引理 3. 令 $f_1, f_2、\cdots、f_r$ 为任意一组不含复乘且两两扭曲不等价的新形式。则存在一个有限素数集 S_f，使得，$G_{f_1, f_2、\cdots、f_r, m}$ 对于与 S_f 中的任意素数互素的整数 m，均包含 $SL_2(\mathbb{Z}/m\mathbb{Z})^r$

在证明这一点之前，令 G 为任意有限群，并记 $\mathrm{Occ}(G)$ 为非阿贝尔单群的同构类；这些群是 G 的复合因子的商群。

证明. 由引理 2 可知，存在一个有限素数集 P_f，使得对于任意素数 $\ell \notin P_f$，任意 f_i、f_j 都不 ℓ 等价。然后，如有必要，我们扩大 P_f，以确保每个 ρ_{f_i}、ℓ 的像为 $\Delta_{k_i}(\ell)$，特别地包含 $SL_2(\mathbb{Z}/\ell\mathbb{Z})$。现在，应用 [10] 中的引理 5.1 并取 $e = \ell - 1$，可知 G_{f_i}、f_i、ℓ 的像包含 $SL_2(\mathbb{Z}/\mathbb{Z}\ell)^2$，对于任意 $\ell \notin P_f$ 均如此。再由[13]中的引理 5.2.2 可知，G_{f_1}, f2、…、ℓ 包含 $SL_2(\mathbb{Z}/\ell\mathbb{Z})^r$，因为对于任意素数 $\ell \geq 5$，$SL_2(\mathbb{Z}/\ell\mathbb{Z})$ 都是自身换位子，所以该像包含任意形如 (I, I …、$SL_2(\mathbb{Z}/\ell\mathbb{Z})$、I …、I) 的矩阵。

此外，只要 m 的所有素因子都大于 5，对于任意这样的整数 m，$G_{f_1, f_2, \cdots, f_r, m}$ 中都含有 (I, I …, $PSL_2(\mathbb{Z}/\ell\mathbb{Z})$, I …, I) $\in$ Occ。于是，由 [3] 的附录中的定理 2 可知，$G_{f_1, f_2, \cdots, f_r, m}$ 含有 (I, I …, $PSL_2(\mathbb{Z}/m\mathbb{Z})$, I …, I)，由此证明完毕。□

现在，我们还需要一个引理来证明本章节的主要结果。

引理 4。设 $f_1, f_2, \cdots, f_r$ 是权为 k 且无复乘的两两扭曲不等价的新形式。那么存在一个有限素数集 S_f，使得，

$$G_{f_1, \cdots, f_r, m} = \Delta_k^{(r)}(m) := \left\{ \begin{pmatrix} A_1 & & \\ & A_2 & \\ & & \ddots \\ & & & A_r \end{pmatrix} \mid \det(A_1) = \cdots = \det(A_r) \in (\mathbb{Z}/m\mathbb{Z}^*)^{k-1} \right\}.$$

对于任意与 S_f 中任一素数互素的整数 m

证明。 由推论 2可知，并通过归纳法可得，每个投影

$$\pi_i : G_{f_1, \cdots, f_r, m} \to GL_2(\mathbb{Z}/m\mathbb{Z})$$

都具有如下性质：$\mathrm{Im}(\pi_i) = \Delta_k(m)\ \ \forall 1 \le i \le r$。对于 $r = 2$，结合 [8], 中的引理 3.3 的证明与引理 3，即可得到结论。注意，我们使用引理 3 排除 [8]中引理 3.3 的情形 (b)。

现在，根据归纳法，

$$G_{f_1,\cdots,f_{r-1},m} = \left\{ \begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_r \end{pmatrix} \mid \det(A_1) = \cdots = \det(A_{r-1}) \in (\mathbb{Z}/m\mathbb{Z}^*)^{k-1} \right\}$$

以及 G f,m $= \Delta_k$(m)。如果 G f1,⋯, f,m 不具有所需的像，那么根据 Goursat 引理（ [8] 中的引理 3.2），存在 G f1,⋯, f_{r-1},m 的正规子群 N_1 和 G f,m 的正规子群 N_2，以及一个同构 ψ : G f1,⋯, f_{r-1},m/N_1 →G f,m/N_2，使得

$$G_{f_1,\cdots,f_r,m} = \{(g_1, g_2) \mid \psi(g_1 N_1) = g_2 N_2\}.$$

如果 N_2 包含 $SL_2(\mathbb{Z}/m\mathbb{Z})$，那么显然 N_1 包含于 $SL_2(\mathbb{Z}/m\mathbb{Z})^{r-1}$，因为

$$N_1 \times SL_2(\mathbb{Z}/m\mathbb{Z}) \subseteq N_1 \times N_2 \subseteq \Delta_k^{(r)}(m).$$

由于同构 ψ，我们有 N_1 =$SL_2(\mathbb{Z}/m\mathbb{Z})^{r-1}$ 和 $N_2 = SL_2(\mathbb{Z}/m\mathbb{Z})$。特别地，

$$G_{f_1,\cdots,f_{r-1},m}/N_1 = G_{f_r,m}/N_2 = (\mathbb{Z}/m\mathbb{Z})^*.$$

这意味着 ψ 必须是恒等映射，因为 G $_{f1,\cdots,fr,m}$是 ψ 的图像，当然它包含于 $\Delta^{(r)}{}_k$ (m) 中。证明至此完成。□

至此，我们已完成证明本章节主要结果所需的全部准备工作。

2.2. 傅里叶系数的分布。本节研究 $\{a(n)$ (模 $m)\}$当n 只有有限个素因子时的情形。只有一个素因子的情形，可由引理 4 以及切博塔廖夫密度定理立即推出，其中 a由一个新形式给出。对于更大的尖点形式族，研究满足 n 且 $\omega(n) = 1$的情形时，有如下结果。

命题 1. 设 f $= c_1 f_1 + c_2 f_2 \cdots + c_r f_r$是一个系数属于 $\mathbb{Q}$.的任意尖点形式。假设所有 f_i 都是权为同一个 k 且无复乘的两两扭曲不等价的新形式。那么存在一个整数 N f，使得对于任意与 N_f互素的整数 m ∼ ϕ满足 m (m)，且 $2^{\omega(m)+r} = o(\mathscr{L})$，其中 $\mathscr{L}$是 m 的最小素因子时，集合

$$\{a(p) \pmod m \mid p, \text{ prime}\},$$

在模 m 下于剩余类中等分布。

证明。取任意剩余类 a ∈ $\mathbb{Z}$/m$\mathbb{Z}$. 。根据引理 1 可知，对于每个元组 (a_1,a2,⋯, a_r) ∈$(\mathbb{Z}/m\mathbb{Z})^r$ 和 ($\lambda_1,\lambda_2,\cdots,\lambda_r$) ∈$((\mathbb{Z}/m\mathbb{Z})^*)^r$,

$$\#\{\mathrm{diag}(A_1,\cdots,A_r) \in (GL_2(\mathbb{Z}/m\mathbb{Z}))^r \mid \det(A_i) = \lambda_i,\ \mathrm{tr}(A_i) = a_i\ \forall 1 \le i \le r\}.$$

为 $m^{2r} + O(2^{r+\omega(m)} m^{2r}/\ell)$，其中 ℓ 是 m 的最小素因子。特别地，

(3)

$$\#\{A \in \Delta_k^{(r)}(m) \mid \mathrm{tr}(A_1) = a_1, \cdots, \mathrm{tr}(A_r) = a_r\} = \frac{\phi(m)}{(\phi(m), k-1)}(m^{2r} + O(2^{r+\omega(m)} m^{2r}/\ell)).$$

因此，该集合

$$\{p \mid a_1(p) = a_1,\ a_2(p) = a_2, \cdots a_r(p) = a_r\}$$

密度为 $\phi(m)/(\phi(m),k^{-1})(m^{2r}+O(2^{r+\omega(m)}m^{2r}/\ell))\ \#\Delta^{(r)}\ k\ (m)$ ，这恰好是 $m^{2r}+O(2^{r+\omega(m)}m^{2r}/\ell)\ \#SL_2(\mathbb{Z}/m\mathbb{Z})^r$ 。现在，满足 $c_1a_1+c_2a_2\cdots+c_ra_r = a$ 的元组 $(a_1,a2,\cdots,a_r)$ 的数量为 m^{r-1}.。因此，对于一个密度为

$$m^{r-1}\frac{m^{2r}+O(2^{r+\omega(m)}m^{2r}/\ell)}{\#SL_2(\mathbb{Z}/m\mathbb{Z})^r} \sim \frac{1}{m}, \tag{4}$$

对于任何满足 $n \sim \phi(m)$ 且 $2^{\omega(m)+r} = o(\mathscr{L})$ 的 m，其中 $\mathscr{L}$ 是 m 的最小素因子.

现在，为了研究 $\{a(n) \pmod m\}$，其中 n 有多个素因子。对于任意整数 $M \geq 1$，记

$$N_M(x) = \{n \leq x \mid \omega(n) = M\}.$$

这是一个经典结果：[12]当 $\#N_M(x) \sim \frac{1}{(M-1)!}x(\log x)(\log\log x)^{M-1}$。现在我们需要下面这个推广。[2]

引理 5. 设 $P_1,\ldots,P_r$ 是素数的互不相交子集，其密度分别为 $\alpha_1,\ldots,\alpha_r$。令 $N(M;a_1,\ldots,a_r)$ 表示由 M 个素数相乘得到、且其中恰有 a_j 个素数选自集合 P_j 的整数集合。假设所有 $\alpha_j \geq 0$, $a_j \geq 1$，那么对于固定的任意 M，当 $x \to \infty$

$$\sum_{\substack{n\leq x\\ n\in N(M;a_1,\ldots,a_r)}} 1 \sim M\left(\prod_{j=1}^{r}\frac{\alpha_j^{a_j}}{(a_j)!}\right)\frac{x}{(\log x)}(\log\log x)^{M-1}.$$

现在考虑将任意 $a \in \mathbb{Z}/m\mathbb{Z}$ 分解为 M 个项的情形。将一个分解写作 $a = a_1a_2\cdots a_M$。这个分解中某些 a_i 可能重复。给定任意元组 $\vec{a} = (a_1,a2,\cdots,a_M) \in (\mathbb{Z}/m\mathbb{Z})^M$，记 $p(\vec{a}) = a_1a_2\cdots a_M$.。我们称两个向量 $\vec{a}_1$ 和 $\vec{a}_2$ 等价，即 $\vec{a}_1 \sim_{S_M} \vec{a}_2$，当且仅当它们相差一个 S_M 中的置换。给定任意元素 $\vec{a} \in (\mathbb{Z}/m\mathbb{Z})^M$，记 $n_{\vec{a}} = \prod_{1\leq i\leq k} n_i!$ ，其中 $a_1,a2,\cdots,a_k$ 是 $\vec{a}$ 中出现的所有不同项，且 a_i 出现 n_i 次。特别地，我们有 $\sum_{1\leq i\leq k} n_i = M$。我们将在下一个定理中用这些记号研究新形式的情形。

为了推广这一点，我们需要研究 $M_{r\times M}(\mathbb{Z}/m\mathbb{Z})$，即由 $\mathbb{Z}/m\mathbb{Z}$ 上的矩阵构成、具有 r 行和 M 列的矩阵环。接着，我们考虑 S_M 在 $M_{r\times M}(\mathbb{Z}/m\mathbb{Z})$ 的列上的自然作用。给定任意元素 $A \in M_{r\times M}(\mathbb{Z}/m\mathbb{Z})$，分别用 $C_1(A)$、$C_2(A)\cdots C_M(A)$ 和 $R_1(A)$、$R_2(A)\cdots R_r(A)$ 表示 A 的列和行。此外，令 n_A 表示数值 $\prod_{1\leq i\leq k} n_i!$，其中 $C_1,C2,\cdots,C_k$ 是 A 中出现的所有不同列组成的集合，且 C_i 出现 n_i 次。

定理 4. 设 $M \geq 1$ 为任意整数，且 $f = c_1f_1+c_2f_2\cdots+c_rf_r$ 为任意一个系数属于 $\mathbb{Q}$. 的尖点形式。假设所有 f_i 都是权 k 相同且无复乘的两两扭曲不等价的新形式。那么存在一个整数 N_f ，使得对于任意

[2]关于证明，t 读者可参阅 https://mathoverflow.net/questions/156982/chebotarev-density-theorem-for-k-almost-prim es.

与 N_f 互素且满足 $m \sim \phi(m)$，以及 $2^{\omega(m)+r} = o(\mathscr{L})$ 的整数 m，其中 $\mathscr{L}$ 是 m 的最小素因子，以下渐近公式对任意元组 $\vec{a} = (a_1, a_2, \cdots, a_r) \in (\mathbb{Z}/m\mathbb{Z})^r$ 成立。

$$\frac{\#\{n \in N_M(x) \mid a_1(n) = a_1, a_2(n) = a_2 \cdots, a_r(n) = a_r\}}{\#N_M(x)} \sim d_{\vec{a}}(m)\frac{1}{m^{rM}},$$

对于某个 $d_{\vec{a}}(m) > 0$，它是一个有效可计算常数。

证明。 我们先处理 $r = 1$ 的情形。我们使用引理 5 和命题 1 得到

$$\frac{\#\{n \in N_M(x) \mid a(n) = a\}}{\#N_M(x)} \sim \frac{1}{m^M} \sum_{\substack{\vec{a} \in (\mathbb{Z}/m\mathbb{Z})^M/S_M \\ p(\vec{a}) = a}} \frac{M!}{n_{\vec{a}}}. \tag{5}$$

现在对于 $r \geq 1$ 的情形，我们对 $r \geq 1$ 使用命题 1 的证明。更确切地说，对于每个元组 $(a^{(1)}、a^{(2)}、\cdots、a^{(r)}) \in (\mathbb{Z}/m\mathbb{Z})^r$，集合

$$\{p \mid a_1(p) = a^{(1)}, a_2(p) = a^{(2)}, \cdots, a_r(p) = a^{(r)}\}$$

具有密度 $\sim \frac{1}{m^r}$。类似地，如同 $r = 1$ 的情形，根据引理 5 可知，所需比例为

$$\frac{1}{m^{rM}} \sum_{\substack{A \in M_{r\times M}(\mathbb{Z}/m\mathbb{Z})/S_M \\ p(R_1(A))=a_1,\ p(R_2(A))=a_2, \cdots p(R_r(A))=a_r}} \frac{M!}{n_A},$$

取 $d_{\vec{a}}(m)$ 为上面一行中的求和式，证明即告完成。

□

注 2。读者或许会注意到，我们在（5）中得到的比例确实小于 1，因为 $\#\{\vec{a} \in (\mathbb{Z}/m\mathbb{Z})^M/S_M\} \ll m^M/M!$，且所有 $n_{\vec{a}} \geq 1$。此外，条件 $p(\vec{a}) = a$ 大致应以比例 $\frac{1}{m}$ 成立。因此，5 中的比例大致应为 $\frac{1}{m}$。

注 3。将 $m = \ell_1^{e_1}\ell_2^{e_2}\ldots\ell^{e_s}{}_s$，写成任意 $a \in \mathbb{Z}/m\mathbb{Z}$，我们在 $\mathbb{Z}/\ell_1^{e_1}\mathbb{Z} \times \mathbb{Z}/\ell_2^{e_2}\mathbb{Z} \times \ldots \times \mathbb{Z}/\ell^{e_s}{}_s\mathbb{Z}$ 中有一个形如 $(u_1\ell_1^{n_1}, u_2\ell_2^{n_2}, \ldots, u_s\ell^{n_s}{}_s)$ 的元素，其中 u_i 是 $\mathbb{Z}/\ell^{e_i}{}_i$ 中的单位元，且 $0 \leq n_i \leq e_i$. 那么，将 a 写成 $(\mathbb{Z}/m\mathbb{Z})$ 中 M 个元素的乘积（允许重复）的方式数为

$$\phi(m)^{M-1}\prod_{j=1}^{s}\left(\sum_{i_{M-2}=0}^{n_j}\sum_{i_{M-3}=0}^{i_{M-2}}\ldots\sum_{i=0}^{i_1}1\right).$$

我们先考察 $M = 2$ 且 $m = \ell^e$. 的情形。设 $a = u\ell^n$，其中 u 是 $\mathbb{Z}/\ell^e\mathbb{Z}$ 中的单位元，且 $n \in \{0, 1, 2, \ldots, e\}$.。那么，将 a 写成 M 项乘积的次数，与将 ℓ^n 写成 M 项乘积的次数相同。因此，只需计算在 ℓ^n. 中将 a 写成两个项的乘积的方式数。任意 ℓ^n 都可以按以下方式写成两个项的乘积

$$\ell^n = u(u^{-1}l^n) = (u\ell)(u^{-1}\ell^{n-1})\ldots = (u\ell^{n-1})(u^{-1}\ell) = (u\ell^n)u^{-1},$$

对于任意单位元 u，$\in \mathbb{Z}/\ell^e\mathbb{Z}$. 因此，$\ell^n$ 可以写成两个项的乘积的次数为 $(n+1)\phi(\ell^e)$。

一般而言，a 可以写成 M 个项的乘积的次数为

$$\left(\sum_{i_{M-2}=0}^{n}\sum_{i_{M-3}=0}^{i_{M-2}}\cdots\sum_{i=0}^{i_1}1\right)\phi\left(\ell^e\right)^{M-1},$$

注意到，M 项的乘积也可以写成两个项的乘积，其中一项是 M 个 -1 项的乘积。于是，对于任意 $a\in\mathbb{Z}/m\mathbb{Z}$，在$\mathbb{Z}/\ell_1^{e_1}\mathbb{Z}\times\mathbb{Z}/\ell_2^{e_2}\mathbb{Z}\times\ldots\times\mathbb{Z}/\ell^{e_s}{}_s\mathbb{Z}$下，依据自然同构，可得一个元素，例如 $(u_1\ell_1^{n_1}, u_2\ell_2^{n_2}, ..., u^s\ell^{n_s}{}_s)\in\mathbb{Z}/\ell_1^{e_1}\mathbb{Z}\times\mathbb{Z}/\ell_2^{e_2}\mathbb{Z}\times\ldots\times\mathbb{Z}/\ell^{e_s}{}_s\mathbb{Z}$，其中 u_i是单位元，且 $0\le n_i\le e_{i\cdot}$。将 a 写成 M 项乘积的方法数，等于将 a 的每个坐标分别写成 M 项乘积的方法数之乘积。

3. 关于剩余类

设 f (z) 是一个系数属于 $\mathbb{Q}$的尖点形式，m 是任意整数。本节中，我们给出集合 $\{a(n) \pmod m\}_{n\in I}$ 中元素个数的一个下界，其中 I 是某个小集合。我们从第 2 节得知，当 I 是一个大集合且 f (z) 属于某种特定类型时，该集合为 $\mathbb{Z}/m\mathbb{Z}$。本节中，我们将考察一个小集合 I。Shparlinski 在 [19]中对 Ramanujan τ 函数进行了研究。沿着相同思路推理，我们首先得到以下推广。

引理 6。设 f(z) 为任意海克特征形式，m 为任意整数。对于任意素数集 S，考虑

$$N_{f,m,S}(x)=\#\{a(p^i)\pmod m \mid p\in S,\ p\le\sqrt{x},\ i=1,2\}.$$

如果 S 具有正密度，那么对于任意 $x\ge 1$，

$$N_{f,m,S}(x)\gg_S x^{1/4+o(1)},$$

前提是 $x^{1/2}\le L$，其中 L 是 m 的最大素因子。更准确地说，

$$\#\{a(p)\pmod m \mid p\in S,\ p\le\sqrt{x}\}\gg_S x^{1/4+o(1)}$$

or

$$\#\{a(p^2)\pmod m \mid p\in S,\ p\le\sqrt{x}\}\gg_S x^{1/4+o(1)}.$$

特别地，对于任意 $0<\varepsilon<1$，只要 $m^\varepsilon\le L$，就有 $N_f,\ L,\ S(m^{2\varepsilon})\gg_S m^{\frac{\varepsilon}{2}+o(1)}$。

证明与 [19] 中的基本相同。这是由 Hecke 关系 $a(p^2)=a(p)^2-p^{k-1}$，以及不同的剩余类 $p^{k-1}(\mathrm{mod}\ m)$、$p\le\sqrt{x}\le L$ 的数量为 $\gg\sqrt{x}$ 这一事实得到的。给定任意整数 m，条件 $m^\varepsilon\le L$ 显然对于任意较小的 $\varepsilon>0$. 都满足。然而，如果我们希望取任意 $1/2\le\varepsilon<1$，则应有 $\nu_L(m)=1$，并且 L 要充分大于 m 的其他素因子。

设 $f_1, f2, \cdots, f_r$ 是一组具有相同权 k 和层 N 的特征形式，并考虑

(6)
$$\mathscr{S}_{f_1,f_2,\cdots,f_r,m}=\left\{p\mid a_1(p)\equiv a_2(p)\cdots\equiv a_r(p)\pmod m,\ p^{k-1}\equiv 1\pmod m\right\}.$$

于是我们得到如下结论。

引理 7. 若所有的 $f_1, f_2, \cdots, f_r$ 都是不带复乘的新形式，则 $\mathscr{S}_{f_1,f_2,\cdots,f_r,m}$ 的素数集合若非空，则具有正密度。否则，存在一个整数 N_f，使得对于任意与 N_f 互素的整数 m，

$$a_i(p) \equiv \pm a_j(p) \pmod{m},\ p^{k-1} \equiv 1 \pmod{m}\ \forall\ 1 \le i, j \le r,$$

对于一个具有正密度的素数集 p。

证明。 我们先回顾一下（2）中的伽罗瓦表示。

$$\rho_{f_1,f_2,\cdots,f_r,m} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_{2r}(\mathbb{Z}/m\mathbb{Z}).$$

现在考虑

$$C = \left\{ \begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_r \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})^r \;\middle|\; \mathrm{tr}(A_1) = \mathrm{tr}(A_2) = \cdots = \mathrm{tr}(A_r) \right\}.$$

如果 $\mathscr{S}_{f_1,f_2,\cdots,f_r,m}$ 非空，那么 C $\cap$ im($\rho_{f_1,f_2,\cdots,f_r,m}$) 也非空，并且根据切博塔廖夫密度定理，我们得到所需的正密度。

另一方面，如果 $\mathscr{S}_{f_1,f2,\cdots,f_r,m}$ 为空，那么由 (1) 可知，G $f_{1,}f2,\cdots, f_r,m$ 不包含 $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})^r$. 。于是引理 4 表明，集合 $\{f_1, f2, \cdots, f_r\}$. 中有多个等价类。令 f_{i_1}, $f_{i_2}, \cdots, f_{i_{r'}}$ 为每个类中的代表元。再次应用引理 4，可知 G f_{i_1}, $f_{i_2},\cdots, f_{i_{r'}},m$ 包含 $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})^{r'}$。由 (1) 即得证明。此外，条件 $p^{k-1} \equiv 1 \pmod{m}$ 得到满足，这是因为我们讨论的是 $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$

. □ 中的共轭类。

现在考虑 f_1, f2, ..., f_r 是海克特征形式，其傅里叶展开为$\infty f_i(z) = \sum a_i(n)z^n$，且 $a_i(n) \in \mathbb{Q}$, $\forall 1 \le i \le r$。对于任意齐次多项式 $n=1 P(x_1, x2, ..., x_r)$，若 $P(\pm1, \pm1, ..., \pm1) \neq 0$，令 $a(n) = P(a_1(n), a_2(n) ..., a_r(n))$。考虑引理 6 中的量 N_f,m,S(x)。由于我们假设

$$P(\pm1, \pm1, ..., \pm1) \neq 0,$$

我们也可以假设，对于任意具有充分大素因子的整数 m，$P(\pm1, \pm1, ..., \pm1) \not\equiv 0 \pmod{m}$。

推论 3. 假设 $f_1, f_2, \cdots, f_r$ 均为无复乘的新形式。令 m 为任意具有充分大素因子的整数，且满足 $P(\pm1, \pm1, ..., \pm1) \not\equiv 0 \pmod{m}$；令 L 为 m 的最大素因子，满足对于某个$0 < \varepsilon < 1$. 有 $m^\varepsilon \le L$。于是我们有，

$$N_{f,L,S}(m^{2\varepsilon}) \gg \frac{m^{\varepsilon/2+o(1)}}{d},\ d = \deg(P).$$

证明。 如果集合 $\mathscr{S}_{f_1,f_2,\ \cdots,\ f_r,\ m}$ 属于 (6) 非空，那么根据切博塔廖夫密度定理可知，对于任意 $n \ge 1$,

$$a(p^n) \equiv P(a_1(p^n), a_1(p^n), \cdots a_1(p^n)) \pmod{m},$$

对于一个具有正密度的素数集 p。由于 $P(x_1, x2, \cdots x_r)$ 是一个齐次多项式，我们有

$$P(a_1(p^n), a_1(p^n), \cdots a_1(p^n)) \equiv P(1, 1, \cdots, 1)a_1(p^n)^d \pmod{m},$$

其中 d 是 P 的次数。另一方面，对于任意一个不属于 $\mathscr{S}_{f_1,f_2,\cdots,f_r,m}$ 的素数 p,

$$a(p^n) \equiv Q(a_1(p^n), a_1(p^n), \cdots a_1(p^n)) \pmod{m}, \forall n \geq 1$$

对于一个具有正密度的素数集 p，其中 Q(x_1,x2, ..., x_r) ≡P(±x1,±x2,⋯,±x_r)。由于 P(x_1,x2, .., x_r) 是齐次的，Q(x_1,x2, ..., x_r) 是次数为 d =deg(P) 的齐次多项式。因此我们得到,

$$Q(a_1(p^n), a_1(p^n), ...a_1(p^n)) \equiv P(\pm 1, \pm 1, \cdots, \pm 1) a_1(p^n)^d \pmod{m}.$$

证明可由引理 6以及以下假设立即得出：$P(\pm 1, \pm 1, \cdots, \pm 1) \not\equiv 0$. 注意，因子 $1/d$的出现是因为方程$x^d \equiv a$（模 L）在 $\mathbb{F}_L$上至多有 d 个根。□

注 4。这里我们始终讨论所有 c_i 都属于 $\mathbb{Q}$. 的情形。高度至多为 H 的元组 (c_1,c2,⋯, c_r) 的数量为 $\sim(2H/\zeta(2))^r$，见 [7,定理 B.6。2]其中，满足 $\sum_{i=1}^m \pm c_i = 0$ 的元组 (c_1,c2,⋯, c_r) 的数量为 $\sim H^{r-1}$. 从高度的意义上说，我们表示，几乎所有形如 $\sum c_i f_i$, $c_i \in$ 的 $S_k(\mathbb{Q}, N)$ 中的 f $\mathbb{Q}$，满足推论 3。

现在，为了研究并非所有 f_i 都是不含复乘的新形式的情形，我们需要计算某些超曲面交集上的点数。在这种情况下，指数较小，因此我们得到的下界较弱。

r 引理 8. 考虑 a(n) = $\sum a_i(n)$，则对于任意整数 m ≥ 1，和 $\sum_{i=1}^{r} a_i(p)^m$ 都可以写成 a($p^{m'}$) $0 \leq m' \leq m$ 的线性组合，其中 i=1系数是以 p 为变量、系数取自 $\mathbb{Q}$ 的多项式。此外，当 m 为奇数（分别为偶数）时，与 1（分别为 a(p)）关联的系数次数最高。

证明. 根据 Hecke 算子的性质，我们有

$$a_i(p^{2\beta}) = a_i(p)^{2\beta} - \binom{2\beta-1}{1} p^{12} a_i(p)^{2\beta-2} + \cdots + (-1)^{\beta-1} \binom{\beta+1}{2} p^{12\beta-12} a_i(p)^2 + \\ + (-1)^{\beta} p^{(k-1)\beta},$$

and

$$a_i(p^{2\beta+1}) = a_i(p)^{2\beta+1} - \binom{2\beta}{1} p^{12} a_i(p)^{2\beta-1} + \cdots + (-1)^{\beta-1} \binom{\beta+2}{3} p^{12\beta-12} a_i(p)^3 + \\ + (-1)^{\beta} \binom{\beta+1}{1} p^{(k-1)\beta} a_i(p),$$

$_r$对于任意 $\beta \in \mathbb{N}$ 和 $i \in \{1,2,\cdots,r\}$.，记 $\sum a_i(p)^m = A_m$，可知 a(p^n)$_{i=1}$ 可以写成 A_1,A2,⋯,A_n 的线性组合，其系数是 p 的多项式。根据 A_1 =a(p), 即可通过归纳法得证。

□

引理 9. 设 $a_1, a_2, ..., a_r$ 是任意 r 个实数，$s_j = \sum a^j_i$ ，并考虑 $f(x) = \prod_{i=1}(x^r + q_1x^{r-1} + q_2x^{r-2} + ... + q_{r-1}x + q_r$，它是根为 $a_1, a_2, a_3, ..., a_r$ 的多项式。那么，每个系数 q_k 都可以表示为 $\{s_j\}_{j\in\{1,2,...,r\}}$ 的多项式。

证明。该证明可由对称多项式的牛顿恒等式立即得出。更确切地说，我们有

$$q_k = \frac{(-1)^k}{k!} B_k(-s_1, -1!s_2, \cdots, -(k-1)!s_k),$$

对于某个多项式 $B_k \in \mathbb{Q}[x_1, x2, \cdots, x_k]$.

□

命题2。设 $f \in S(\mathbb{Q}, N)$ 是任意一个形如 $c_1f_1 + c_2f_2 + \cdots c_rf_r$，其中 $c_i \in \mathbb{Q}$，且所有 f_i 都是海克特征形式。对于任意素数集 S 和任意整数 m，考虑

$$N_{f,m,S}(x) = \#\{a(p^i) \pmod m \mid p \in S,\ p \le x^{\frac{1}{2r}},\ i = 1, 2, 3, ..., 2r\}.$$

假设 S 具有正密度。那么对于任意 $\delta > 0$，以及任意充分大的 $x \ge 1$，我们有

$$N_{f,m,S}(x) \gg_S x^{\frac{1}{4r^2} - \delta},$$

前提是 $x^{1/2r} \le L$，其中 L 是 m 的最大素因子。特别地，对于任意 $\varepsilon > 0$，若 $m^{\varepsilon/r^2} \le L$，则 $N_{f,\ L,\ S}(m^{2\varepsilon}) \gg_S m^{\frac{\varepsilon}{2r^2} - \delta}$。

证明。设 $y > 0$ 是任意给定的实数，满足 $N_{f,\ m,\ S}(x) \le y$。特别地，#{a(p)（模 m）：$p \le x^{1/2r}$} $\le y$，因此存在某个 a_1，使得对于至少 $x^{1/2r + o(1)}y$ 个不超过 $x^{1/2r}$ 的素数，有 $a(p) \equiv a_1$（模 m）。现在考虑集合

$$S_{a_1} = \{p : a(p) \equiv a_1 \pmod m,\ p \le x^{\frac{1}{2r}}\}.$$

我们有 #{a(p^2)（模 m）：$p \in S_{a_1}(x)$} $< y$，则存在某个 a_2，使得对于至少 $\#S_{a_1}(x)y = x^{1/2r + o(1)}y^2$ 个不超过 $x^{1/2r}$ 的素数，有 $a(p^2) \equiv a_2$（模 m）。于是我们考虑

$$S_{a_1,a_2}(x) = \{p : a(p^2) \equiv a_2 \pmod m,\ p \in S_{a_1}(x)\}.$$

由于 $\{a(p^3) \pmod m : p \in S_{a_1,\ a_2}(x)\} < y$，所以存在一个 a_3，使得对于至少 $\#S_{a_1,\ a_2}(x)y = x^{1/2r + o(1)}y^3$ 个不超过 $x^{1/2r}$ 的素数，$a(p^3) \equiv a_3 \pmod m$。递归论证可得

$$a(p) = a_1 \pmod m,\ a(p^2) = a_2 \pmod m, \cdots, a(p^{2r}) = a_{2r} \pmod m,$$

对于至少 $x^{1/2r + o(1)}y^{2r}$ 个不超过 $x^{1/2r}$ 的素数，并将这个素数集记为 $S_{a_1,\ a_2,\ldots a_{2r}}(x)$。

现在，数列 $\{a_i(p^n)\}$ 的特征多项式为 $x^2 - a_i(p)x + p^{k-1}$，因此 $\{a(p^n)\}$ 是一个特征多项式为 $p(T) = \prod_{i=1}^{r}(T^2 - a_i(p)T + p^{k-1})$.[3] 的线性递推数列。由引理 8 和引理 9 可知，

[3]作为参考，读者可参阅 https://math.stackexchange.com/questions/1348838/sum-and-product-of-linear-recurrences.

对于任意 p $\in S_{a_1,\ a_2,\ \ldots a_{2r}}$(x)，p(x) 的系数都是关于素数 p 的多项式。此外，次数最高的多项式仅出现一次，其次数为 (k $-$ 1)r。特别地，我们得到一个次数为 (k $-$ 1)r 的多项式 g(T)，它满足

$$g(p) \equiv 0 \pmod{m},\ \forall p \in S_{a_1,a_2,\ldots a_{2r}}(x).$$

特别地，对于至少$x^{12r^{-}} \leq L$ 的素数 p，有 g(p) $\equiv$0 (mod L)。取 y $= x^{14r^2-\delta}$，证明即可完成，因为仅有 O_g(1) 个 p $\leq$ L 满足 g(p) $\equiv$ 0 (mod L)。□

4. 模形式的华林型问题

本节的主要目标是将 Shparlinski 关于一大类尖点形式的主要结果加以推广，并为解产生许多其他 n_is。在某些情况下，我们还研究模合数的同一问题。首先讨论贯穿全文将要用到的工具。

4.1. 指数和与华林型问题。设 m、s $\omega \geq 1$ 为任意给定的整数，A_1,A2,$\cdots$,Aω 为 $\mathbb{Z}/m\mathbb{Z}$ 的一些子集，满足

$$\prod_{i=1}^{\omega} \#A_i \gg m^{1+\beta}, \tag{7}$$

对于某个 $\beta > 0.$，任意 a $\in \mathbb{Z}/m\mathbb{Z}$，我们记 T_s(a) 为方程的解的个数

$$\prod_{i=1}^{\omega} a_1^{(i)} + \prod_{i=1}^{\omega} a_2^{(i)} + \ldots + \prod_{i=1}^{\omega} a_s^{(i)} \equiv a \pmod{m},$$

其中 $a^{(i)}{}_j \in A_i$, $\forall 1 \leq j \leq s\ 1 \leq i \leq \omega.$。于是我们得到如下计数公式:

(8)

$$T_s(a) = \frac{(\#A_1\#A_2\cdots\#A_\omega)^s}{m} + O\left(\frac{1}{m}\sum_{\lambda=1}^{m-1}\left|\sum_{a^{(1)}\in A_1,\cdots,a^{(\omega)}\in A_\omega} \mathbf{e}_m\left(\lambda a^{(1)}a^{(2)}\cdots a^{(\omega)}\right)\right|^s\right).$$

当 $\omega = 2$时，《 [21] 第6章的习题14.a中提到的一个旧结果[2],q替换为m，并取$a := 1_{A_1}$，$b := 1_{A_2}$以及$\phi := \mathrm{e}_m$，按照《

$$\max_{\lambda\in\mathbb{Z}/m\mathbb{Z}}\left|\sum_{a_1\in A_1}\sum_{a_2\in A_2}\mathbf{e}_m(\lambda a_1 a_2)\right| \leq \sqrt{m\#A_1\#A_2}. \tag{9}$$

将（9）代入（8），得到如下结果。

推论 4. 对于 $\omega = 2$ 以及任意 s $> 2/\beta$，求和式

$$a_1^{(1)}a_1^{(2)} + a_2^{(1)}a_2^{(2)} + \cdots + a_s^{(1)}a_s^{(2)}$$

当 m 充分大时，在 $\mathbb{Z}/m\mathbb{Z}$ 中等分布，其中 β与（7）中的常数相同，并且 $a^{(1)}j \in A_1$,$a^{(2)}j \in A_2$,$\forall 1 \leq j \leq s$。

当 $\omega = 3$ 时，我们将使用 Shkredov 在 [18, 定理 5] 中给出的以下界。

定理 5. 设 $A_1,A_2,A_3 \subseteq \mathbb{F}_\ell$ 为任意集合，使得对于某个 $\delta > 0$，以下条件成立

$$|A_1||A_2||A_3| \geq \ell^{1+\beta}. \tag{10}$$

Then

$$\max_{\lambda \in (\mathbb{Z}/\ell\mathbb{Z})^*} \left| \sum_{a_1 \in A_1} \sum_{a_2 \in A_2} \sum_{a_3 \in A_3} \mathbf{e}_\ell(\lambda a_1 a_2 a_3) \right| \ll \frac{|A_1||A_2||A_3|}{\ell^{\frac{\beta}{8\log(8/\beta)+4}}}.$$

为了处理 $\omega > 3$ 的情形，Bourgain 和 Gilbichuck 在 [2,定理 2] 中给出的以下界对我们很有用。对于 $\omega = 3$，以下界同样成立，但我们只在 $\omega > 3$ 情形下使用它。

定理 6（Bourgain-Glibichuk）。设 $3 \leq \omega \ll \log\log\ell$ 为一个自然数，$\varepsilon > 0$ 为任意固定常数。对于任意子集 $A_1,A_2,\cdots,A_\omega \subset \mathbb{F}_\ell \setminus \{0\}$，满足

$$|A_1| \cdot |A_2| \cdot (|A_3| \cdots |A_\omega|)^{1/81} > \ell^{1+\beta}, \tag{11}$$

存在一个估计

$$\max_{\lambda \in (\mathbb{Z}/\ell\mathbb{Z})^*} \left| \sum_{a_1 \in A_1} \sum_{a_2 \in A_2} \cdots \sum_{a_\omega \in A_\omega} \mathbf{e}_\ell(\lambda a_1 a_2 \cdots a_\omega) \right| \ll \frac{|A_1||A_2| \cdots |A_\omega|}{\ell^{0.45\beta/2^\omega}}.$$

为了研究模合数的情形，我们需要研究任意有限域 $\mathbb{F}_q$. 上的这些指数和。对此，我们可以使用 Bourgain-Glibichuk 在 [2]中的定理 4。由此，假设对于任意 $d \in \mathbb{F}_q$ 以及任意真子域 S，$\mathbb{F}_q$，dS 与集合 A_i. 的交集都很小，A_i 就能得到一个非平凡界。不过在我们的情形中，每个集合 $\mathbb{F}_\ell$ 都属于一个素域，因此我们无法使用这个结果。不过，定理 6 可用于研究无平方因子整数。更具体地说，结合这两个结果，我们得到如下结论。

推论 5. 设 m 为任意无平方因子整数，且 $A_1,A_2, \cdots, A_\omega \subseteq (\mathbb{Z}/m\mathbb{Z})^*$ 满足

$$|A_1| \cdot |A_2| \cdot (|A_3| \cdots |A_\omega|)^{1/81} > m^{1+\beta}. \tag{12}$$

则我们有以下估计

$$\max_{\lambda \in (\mathbb{Z}/m\mathbb{Z})^*} \left| \sum_{a_1 \in A_1} \sum_{a_2 \in A_2} \cdots \sum_{a_\omega \in A_\omega} \mathbf{e}_m(\lambda a_1 a_2 \cdots a_\omega) \right| \ll \frac{|A_1||A_2| \cdots |A_\omega|}{\ell^{0.45\beta/2^\omega}},$$

其中某个素因子 ℓ 属于 m。

证明。注意到存在一个素数 $\ell \mid m$，使得

$$|A_1^{(\ell)}| \cdot |A_2^{(\ell)}| \cdot (|A_3^{(\ell)}| \cdots |A_\omega^{(\ell)}|)^{1/81} > \ell^{1+\beta},$$

其中 $A^{(\ell)}{}_i$ 表示 A_i, $\forall 1 \leq i \leq \omega$ 的 ℓ^{th} 分量。现在只需对 $\{A^{(\ell)}{}_i \}_{1 \leq i \leq \omega}$ 应用定理 6，并对与其他分量相关的指数和作平凡估计，即可得到证明。□

4.2. 海克特征形式的和。设 m 是任意给定的整数，f 是任意海克特征形式。我们要证明， $\{a(n) \pmod m\}_{n=m^{O(1)}}$ 是 $\mathbb{Z}/m\mathbb{Z}$. 的加法基。当 f 由 Ramanujan τ 函数给出且 m 为素数时，Shparlinski 已证明了这一点。对于任意 $\gamma > 0$，考虑

$$N_\gamma = \{m \in \mathbb{N} \mid \ell \text{ prime divides } m \implies m \le \ell^{1+\gamma}\}.$$

命题 3。设 ω 为任意整数， γ和β > 0 为任意实数。取任意两两不相交的素数集 $S_1, S_2, \cdots, S_\omega$ s，满足

$$\begin{cases} \#A_1 \#A_2 \cdots \#A_\omega \ge m^{1+\beta}, & \omega = 2,3 \\ \#A_1 \#A_2 (\#A_3 \cdots \#A_\omega)^{\frac{1}{81}} \ge m^{1+\beta}, & \omega \ge 4. \end{cases} \tag{13}$$

其中 $A_i = \{a(p), a(p^2) \pmod m \mid p \in S_i\}$. 令 $B\gamma(\ell) = \{m \in N\gamma$ 无平方因子，且 $p \mid m \implies p > \ell\}$. 存在 ℓ_β 使得

$$\sum_{i=1}^{s} a(n_i) \equiv a \pmod m$$

对任意整数 a，该方程均有解，并且

$$s > \begin{cases} \frac{2}{\beta}, & \omega = 2 \\ \frac{(1+\gamma)(8\log(\frac{8}{\beta})+4)}{\beta}, & \omega = 3, \quad m \in B_\gamma(\ell_\beta) \\ \frac{(1+\gamma)2^\omega}{0.45\beta}, & \omega \ge 4, \quad m \in B_\gamma(\ell_\beta). \end{cases} \tag{14}$$

在这两种情形下，任意这样的 n_i的素因子均只来自 $S_1, S_2, \cdots, S_\omega$.

证明。 对于情形 $\omega = 2$ 的证明由推论 4得出，因为 $a(\cdot)$ 具有乘法性，且 S_1, S_2 是两两不相交的素数集。

对于较大的 ω 值，我们假设 m 无平方因子。为证明 $\omega = 3$，注意存在一个素数 $\ell \mid m$，使得

$$|A_1^{(\ell)}||A_2^{(\ell)}| \cdots |A_3^{(\ell)}| \ge \ell^{1+\beta},$$

其中$A^{(\ell)}{}_i$ 是 ℓ^{th} A的分量。按照推论5的证明作类似论证，可由定理5得到以下结论。

$$\max_{\lambda \in (\mathbb{Z}/m\mathbb{Z})^*} \left| \sum_{a_1 \in A_1} \sum_{a_2 \in A_2} \sum_{a_3 \in A_3} \mathbf{e}_m(\lambda a_1 a_2 a_3) \right| \ll \frac{|A_1||A_2||A_3|}{\ell^{\frac{\beta}{8\log(8/\beta)+4}}}.$$

现在注意，存在 ℓ_β ，使得对于任意 m $\in B(\ell_\beta)$，以下结论成立：

$$O\left(\left(\frac{|A_1||A_2||A_3|}{\ell^{\frac{\beta}{8\log(8/\beta)+4}}}\right)^s\right) = o\left(\frac{(|A_1||A_2||A_3|)^s}{m}\right),$$

由于$s\beta > (8\log(8/\beta) + 4)(1+\gamma)$ 根据假设。由此情形下公式（8）可得结果。

证明$\omega \ge 4$时，我们沿用前一种情形中的相同论证，并使用推论 5和（8）。

□

4.3. 更大类的和。现在考虑一个具有有理系数的模形式 f，其形式为 $c_1f_1+c_2f_2+\cdots+c_rf_r$，其中 $c_i\in$有理数域，且 f_i都是具有有理系数的海克特征形式。更一般地，对于任意具有有理系数的齐次多项式 $P(x_1,x2,\cdots,x_r)$，还可以考虑一个新序列 $a(n):=P(a_1(n),a_2(n)\cdots,a_r(n))$。我们立即遇到的第一个问题是，除非 P(·) 是单项式，否则 a(·) 不一定具有乘法性。即使在单项式的情形下，为了得到类似于命题 3 的结果，我们仍需确保

$$\#A_1\#A_2\cdots\#A_\omega\geq m^{1+\beta},$$

其中

$$A_i=\left\{P(a_1(p),\cdots,a_r(p)),\ P(a_1(p^2),\cdots,a_r(p^2))\pmod m\mid p\in S_i\right\},$$

对于某个素数集 S_i. 若 P 具有 x_i^e（其中某个 i）的形式，则结论显然成立。一般而言，我们有一个稍弱的结果，将在本章节中讨论。对于任意一个符号 r 元组$\vec{\sigma}$，考虑

$$\mathscr{S}_{\vec{\sigma},\vec{f},m}=\left\{p\mid \sigma_1a_1(p)=\cdots=\sigma_ra_r(p)\pmod m,\ p^{k-1}=1\pmod m\right\},$$

以及 $\mathscr{S}$-符号 $_{\vec{f},\ m}=\bigcup_{\vec{\sigma}\in\{\pm1\}^r}\mathscr{S}_{\vec{\sigma},\ \vec{f},\ m}$. 于是得到以下结论。

推论 6. 设 m ω,γ和 $\beta>0$如命题 *3* 所述。取任意两两不交的素数集 $S_1,S_2,\cdots,S_\omega$，满足

$$\begin{cases}\#A_1\#A_2\cdots\#A_\omega\geq m^{1+\beta},\omega=2,3\\ \#A_1\#A_2(\#A_3\cdots\#A_\omega)^{\frac{1}{81}}\geq m^{1+\beta},\omega\geq4.\end{cases}\tag{15}$$

其中 $A_i=\{a(p),a(p^2)\pmod m\mid p\in S_i\cap\mathscr{S}$-符号 $_{\vec{f},\ m}\}$. 假设对任意 $\vec{\sigma}\in\{\pm1\}^r$.，$(P(\vec{\sigma}),m)=1$。那么存在 $\beta'>0$（依赖于β），使得对于 $\omega=2$，分别有 3 和 $\omega\geq4$，且对于 $s>\frac{2}{\beta'}$，$\frac{(1+\gamma)8\log(8/\beta+4)}{\beta'}$，以及 $\frac{(1+\gamma2^\omega)}{0.45\beta'}$，~~任意 a~~ $\in\mathbb{Z}$ 均~~可写成~~

$$a(n_1)+a(n_2)+\ldots+a(n_s)\equiv a\pmod m,\ n_i\in\mathbb{N},\ i=1,2,\cdots,s,$$

对于任意充分大的 m。此外，任何这样的 n_i 的素因子都只来自 $S_1,S_2,\cdots,S\omega$.

证明。注意，对于任意 $p\in\mathscr{S}$-sign $_{f,m}$，我们有

$$a_i(p^2)=a_j(p^2),\ \forall\ 1\leq i,j\leq r.$$

特别地，对于任意这样的素数 p,

$$a(p)=P(\vec{\sigma})a_1(p)^d,\ a(p^2)=P(1,1,\cdots,1)a_1(p^2)^d,$$

对于某个 $\vec{\sigma}\in\{\pm1\}^r$，且 d 是 P 的次数。由于 $\#A_1\#A_2\cdots\#A_\omega\geq m^{1+\beta}$，对于某一类符号元组 $\vec{\sigma}:=(\sigma_1,\sigma_2,\cdots,\sigma_r)$，我们有

$$\#A_1'\#A_2'\cdots\#A_\omega'\geq\frac{m^{1+\beta}}{2^r},\ \omega=2,3$$

$$\#A_1'\#A_2'(\#A_3'\cdots\#A_\omega')^{\frac{1}{81}}\geq\frac{m^{1+\beta}}{2^r},\ \omega\geq4,$$

其中 $A_i' = \{a(p),\ a(p^2)\,(\text{模 } m) \mid p \in S^i \cap \mathscr{S}_{\vec{\sigma},\ \vec{f},\ m}\}$. 由命题 3可得证明，对于任意 β' 以及充分大的 m 满足 $m^{\beta-\beta'} \geq 2^r$。□

4.4. 主要结果的证明。 为证明定理 2，我们需要给出β在（13）中的一个明确值。我们将利用已知的有限域上和积问题的显式界来得到这一结果。例如，设 $m := \ell$ 是一个素数，且 $A \subset \mathbb{F}_\ell$是一个小集合。那么问题就是寻找 $\beta > 0$ 使得

$$\max\{|A+A|, |A\cdot A|\} \gg |A|^{1+\beta}.$$

Garaev 在 [6] 中证明了 β 可以取为 1/14；随后 Rudnev 在 [16] 中将其改进为 1/11，而据我们所知，根据目前最优的结果，β 的最优值由 1/5. 给出。这是 Roche-Newton、Shkredov 和 Rudnev 在 [15] 中得到的结果。

4.5. 定理 2 的证明。对于（a）部分的证明，注意到 #{a(p)（模 L），$p \in S_1, p \leq m^\varepsilon\}$或 #{$a(p^2)$（模 L），$p \in S_1, p \leq m^\varepsilon\} \gg_{S_1} m^{\frac{\varepsilon}{2}+o(1)} \geq L^{\frac{\varepsilon}{2}+o(1)}$。取其中规模较大的集合，并将其记为 A_1. 同样地，#{a(p)（模 L），$p \in S_2, p \leq m^\varepsilon$}或 #{$a(p^2)$（模 L），$p \in S_2, p \leq m^\varepsilon\} \gg_{S_2} m^{\frac{\varepsilon}{2}+o(1)} \geq L^{\frac{\varepsilon}{2}+o(1)}$，并将其中较大的集合记为 A_2. 现在我们对两个集合 A_1 和 A_2应用 [15, 定理 6] 。我们设 A_1'为 $A_1 \cdot A_1$或 $A_1 + A_1$, 中的一个，并设集合 A_2'为 $A_2 \cdot A_2$或 $A_2 + A_2$, 中的一个，使其满足

$$\#A_1' \gg_{S_1} L^{\frac{\varepsilon(1+\beta)}{2}+o(1)},\ A_2' \gg_{S_2} L^{\frac{\varepsilon(1+\beta)}{2}+o(1)},$$

当 L 足够大时，设 $L^\gamma \geq L'$。其中 $L' = m_L$，且 $(L, L') = 1$. 我们有

$$\#A_1' \cdot \#A_2' \gg_{S_1,S_2} L^{\varepsilon(1+\beta)+o(1)} = L^{(1+\gamma)(1+\beta')} \geq (LL')^{1+\beta'} = m^{1+\beta'+o(1)},$$

其中 $\beta' = \frac{\varepsilon(1+\beta)}{1+\gamma} - 1 + o(1)$。另一方面，将 A_1' 和 A_2' 视为 $\mathbb{Z}/m\mathbb{Z}$ 的子集，并通过自然包含映射 $\mathbb{Z}/L\mathbb{Z} \hookrightarrow \mathbb{Z}/m\mathbb{Z}$，对于任意 $s = 4\left(\lfloor \frac{2}{\beta'} \rfloor + 1\right)$，结论由推论 4 得出。这是因为 $A_1' \cdot A_2'$中的任意元素都具有如下形式：$a(n_1) + a(n_2) + a(n_3) + a(n_4)$，其中 $n_1, n_2, n_3, n_4 \leq m^{4\varepsilon}$，每个 n_i都含有一个来自 S_1, 的素因子和一个来自 S_2的素因子。此外，注意 s 确实是一个可计算的常数，它取决于 ε 和 γ；读者可以代入任何已知的 β 值，这些值在本章节的前言中已提及。

现在证明第 (b) 部分。根据引理 4，任意两个 f_i、f_j 相差一个二次特征。特别地，采用推论 6 证明中的相同论证，令 $d = 1$ 且 $P = \sum c_i x_i$，即可得到结论。

注 5。 代入 $\beta = \frac{1}{5}$， $\varepsilon = \frac{65}{66}$以及 $\gamma = \frac{1}{77}$，得到 $s = 52$， $n_i \leq \frac{260}{66}$， $\forall 1 \leq i \leq 52$, 并由定理 1推出推论 2。

4.6. 定理 3 的证明。我们先证明 (a)。任取给定的实数 $\varepsilon > 0$，以及任意两两不交且具有正密度的素数集 $S_1, S2, \cdots, S_\omega$，其中 $\varepsilon(2 + \frac{\omega-2}{81}) > 2$。我们在定理 2 中研究了 $\omega = 2$ 的情形。$\omega > 2$ 的情形可类似证明。由引理 6 可知，对每个 $1 \leq i \leq \omega$，有 #{a(p)

(mod L), p $\in S_i$, p $\leq m^{\varepsilon}\}$ or $\#\{a(p^2) \pmod L,\ p \in S_i,\ p \leq m^{\varepsilon}\} \gg_{S_i} L^{\varepsilon/2+o(1)}$.
记 A_i 为相应集合中基数较大的那个，则有

$$\#A_1\#A_2\Big(\prod_{3\leq i\leq \omega} \#A_i\Big)^{1/81} \gg_{S_1,S_2,\cdots,S_\omega} L^{\varepsilon(2+\frac{\omega-2}{81})/2+o(1)}.$$

记 $\beta = \varepsilon(2+\frac{\omega-2}{81})/2 + o(1) - 1$（根据对 ω 的假设，该值为正），并令 $m = LL'$，其中 $(L,L') = 1$，则有

$$L^{1+\beta} \geq m^{1+\beta'},$$

对任意 β' 满足 $L^{\frac{\beta-\beta'}{1+\beta'}} > m/L$。结论现由命题 3 推出，其中 $s > (1+\gamma)8\log(8/\beta' + 4)$，$\omega = 3$ 且 $s > \frac{2^\omega}{0.45\beta'}$，$\omega \geq 4$，其中 $\beta' = \frac{\beta-\gamma}{\gamma+1}$。
按照前一个证明中 (b) 部分的类似方法进行推导，可得本定理的 (b) 部分。

注 6。我们现将由定理 3 得到的具体数值列于下表。

ω	ε	γ	s
21	0.9	0.005	2^{31}
165	0.5	0.003	2^{180}
1461	0.1	0.0006	2^{1478}
16041	0.1	0.00006	2^{16062}
161841	0.001	0.000006	2^{161866}
1619841	0.0001	0.0000006	$2^{1619894}$
16199841	0.00001	0.00000006	$2^{16199872}$
161999841	0.000001	0.000000006	$2^{161999875}$

表 1：给定上界所需的项数

5. 进一步的问题与评论

5.1. 素数解。我们在定理 m中对合数 1 和定理 3中都作了一些假设。我们想知道是否可以去掉这些假设。我们还想问，是否可以得到方程的一个解

$$\sum_{i=1}^{O(1)} a(p_i) \equiv a \pmod m,\ p_i \leq m^{O(1)},$$

其中每个 p_i 都是素数。或者至少，是否 $\{a(n) \text{ (模 } m)\}_{\omega(n)=1}$ 是一个加法基$n\leq m^{O(1)}$

对于 $\mathbb{Z}/m\mathbb{Z}$.，回想一下，Bajpai、García 和第一作者在 [1] 中研究过这个问题；然而，他们的方法无法使解呈现多项式增长。值得注意的是，对于某些 m，我们已经得到了具有多项式增长且含有 ω多个素因子的解。

5.2. 多项式值之和。 沿用章节 3 中的论证，可以研究方程 $o(1)\sum a(n_i)^d \equiv a \pmod m$ 的可解性，正如 Shparlin-Iski 在 [19] 中指出的那样。然而，命题 2 让我们有理由相信，也可以研究 $o(1)\sum p(a(n_i)) \equiv a \pmod m$，其中 $p(x) \in \mathbb{Q}[x]$. 是任意多项式。唯一的障碍是，对于任何乘性函数 $f(n)$，$p(f(n))$ 都可能不是乘性函数。我们也想知道是否有办法克服这一点。或许最有趣的情形是 P 的次数为 1。在这种情况下，$a(n) := P(a_1(n), a_2(n) \cdots, a_r(n))$ 是某个模形式的傅里叶系数。

5.3. 关于更大类的尖点形式。 我们预期，在命题 2 中，至少当 m 是素数时 ℓ，可以处理更大类的尖点形式。我们在推论 3 中讨论了其他一些族。本节将讨论我们关于如何扩展这些族的启发式想法。我们预期，在某些适当条件下，或许以下结论成立。

问题1. 设 ℓ 为任意素数，L 为其任意次幂。对于任意元组 $(c_i)_{1\le i\le r} \in \mathbb{F}_L^r$、$(a_i)_{1\le i\le r+1} \in \mathbb{F}_L^{r+1}$，方程组的解的数量是否

$$c_1x_1^i + c_2x_2^i + \cdots c_rx_r^i = a_i,\ \forall 1 \le i \le r+1,$$

至多为 $O_r(1)$?

例如，利用牛顿恒等式，很容易看出当所有 c_i 都相同时，这一结论成立。一般情况下，根据下面的推论，我们可以得到一个部分答案。

引理10. 设 ℓ 为任意素数，L 为其任意次幂。对于任意 $(c_1, c2, \cdots, cr) \in \mathbb{F}_L^r$，考虑 $f_i = c_1x_1^i + c_2x^i \cdots c_rx_r^i \in \mathbb{F}_L[x_1, x2, \cdots x_r]$，并令 V 为由 $f_1, f2, \cdots, f_r$ 生成的射影簇。那么 $\dim(V) = 0$，前提是对于任意 $i \in S$，$\sum c_i \ne 0$ 属于 $\mathbb{F}_\ell$

$S \subseteq \{1, 2, \cdots, r\}$.

证明. 只需证明 V 的坐标环中不存在非平凡素理想 I。假设存在这样的非平凡素理想 I。由恒等式 $f_r = \sum_{i=1}^r q_i f_{r-i}$ 可得 $(\sum_{i=1}^r c_i)x_1x_2\cdots x_r$ 属于 I，其中 q_i 是 $x_1, x2, \cdots, x_r$ 中的第 i^{th} 个初等对称多项式。由于 $\sum_{i=1}^r c_i \ne 0$，我们可以假设 $x_r \in$ 属于 I。然后重复同样的论证，并注意到任意和 $\sum_{i\in S} c_i \ne 0$，可知 $x_1, x2, \cdots, x_r$ 全都属于 I。特别地，这表明，

$$I = (f_1, f_2, \cdots, f_r) = (x_1, x_2, \cdots, x_r),$$

至此，证明完成。 □

注7. 条件 $\sum c_i \ne 0$ 很重要。例如，$\sum c_i = 0$ 蕴含 $i \in S$ $1\le i\le r$，这意味着 V 包含簇 $(x_1 - x_r, x_2 - x_r, \cdots x_{r-1} - x_r)$。特别地，V 的维数至少为 1。

由引理 10可知，当所有 1 个 a_i 都相等时，问题 [9,定理 21] 得到肯定的答案。证明可用

要完整解答问题 1 是多么有帮助。令 $f_1, f2, \cdots, f_r$ 为任意一组海克特征形式，并设

$$a_{P,\vec{f}}(n) = P(a_1(n), a_2(n), \cdots, a_r(n)),$$

其中，$P(x_1, x2, \cdots, x_r)$ 是一个含有 r 个变量的多项式。

推论7. 设 ℓ 为任意给定的素数，则对于任意素数集 S，考虑数量：

$$N_{S,P,\vec{f}}(x) = \#\{a_{P,\vec{f}}(n) \pmod{\ell} \mid p \text{ divides } n \implies p \in S,\ n \le x\}.$$

假设 S 具有正密度，则对于任意充分大的素数 ℓ 以及任意 $\delta > 0$，我们有以下估计

$$N_{S,P,\vec{f}}(x) \ge \min\left\{\ell^{\frac{1}{2}-\delta}, x^{\frac{1}{4r^2}-\delta}\right\}.$$

证明. 先将 $a_i(p^n) \pmod{\ell} = c_i\alpha_i^n + d_i\beta_i^n$ 写成，其中 α_i、$\beta_i \in \mathbb{F}_{\ell^2}$，并假设 P 是一个次数为 d 的齐次多项式。于是，$a^f(p^n)$ 是 $\left\{\prod_{i=1}^r \alpha^{nt_i}{}_i \ \beta^{n(d_i-}{}_{t_i)\,i}\right\}_{0\le t_i\le d\sum\ {}_i=\ {}^i dd}$ 的线性组合。令 $\vec{d} = (d_1, d2, \cdots, d_r)$ 表示 P 中一个单项式的次数。对于固定的元组 $(a_1, a2, \cdots, a_{r+1}) \in \mathbb{F}_\ell^{r+1}$，现在来考虑满足以下条件的素数 p 的个数

$$(a_{P,\vec{f}}(p), a_{P,\vec{f}}(p^2) \cdots, a_{P,\vec{f}}(p^{r+1})) \pmod{\ell} = (a_1, a_2, \cdots, a_{r+1}).$$

根据我们对问题 1 的预期，$\left\{\prod_{i=1}^r \alpha^{t_i}{}_i \ \beta^{d_i-}{}_{t_i i}\right\}_{0\le t_i\le d\sum\ {}_i=\ {}^i dd}$ 是 O(1)。

特别地，

$$\prod_{\sum d_i = d} \prod_{i=1}^{r} \prod_{0\le t_i\le d_i} \alpha_i^{t_i}\beta_i^{d_i-t_i} = O(1).$$

回忆一下，$\alpha_i\beta_i = p^{k_i-1}$ (模 ℓ)，因此

$$\prod_{\sum d_i = d} \prod_{i=1}^{r} \prod_{0\le t_i\le d_i} \alpha_i^{t_i}\beta_i^{d_i-t_i} = \prod_{\sum d_i = d} \prod_{i=1}^{r-1} p^{(k_i-1)\frac{d_i(d_i+1)}{2}} \pmod{\ell} = O(1).$$

这是不可能的，因为 S 是无限集，且任意 $k_i - 1$ 都严格为正。特别地，这表明满足以下条件的素数 p 的数量

$$(a_{P,\vec{f}}(p), a_{P,\vec{f}}(p^2) \cdots, a_{P,\vec{f}}(p^{r+1})) \pmod{\ell} = (a_1, a_2, \cdots, a_{r+1})$$

是 $O(1)$。 证明现在即可得出，论证方式与命题 2的证明类似 □

致谢

我们谨此感谢德国哥廷根乔治-奥古斯特大学为我们提供了优越的工作条件。本项目的大部分工作是在第一作者访问印度 IISER TVM 期间完成的。我们衷心感谢 IISER 提供的热情接待和经费支持。

第一作者获得 ERC Consolidator 资助项目 648329 以及 IISER TVM 的研究员资助。第三作者谨此感谢印度科学与工业研究理事会提供的经费支持。

参考文献

[1] J. Bajpai、S. Bhakta 和 Victor C. García，模形式在素域上的指数和，载于《研究数论》。 **8** 2022 18 32 3, 20 ( ) – 。 J. Bourgain 和 A. Glibichuk，《任意有限域中[2]子群上的指数和估计》，载于《数学分析杂志》115 (2011)，51–70。 15, 16[3] A.C. Cojocaru，《与非复乘椭圆曲线相关的伽罗瓦表示的满射性》，载于《加拿大数学通报》48 (2005)，16–31。 7[4] H. Delange，《池原定理的推广》，载于《高等师范学校科学年刊》71 (1954)，213–242。 1[5] F. Diamond 和 J. Shurman，《模形式入门》，数学研究生教材，第 **228**, 2005 4 卷，Springer-Verlag，纽约（）。M. Z. Garaev，在[6] $\mathbb{F}_p$ **11** 2007 19 中的[7]一个显式和积估计，载于《国际数学研究论文集》。（）。M. Hindry 和 J.H. Silverman，《丢番图几何：导论》，数学研究生教材，第 **201**, , 2013 13 卷，Springer Science &[8]Business Media（）。N. Jones，《具有最大伽罗瓦表示的椭圆曲线对》，载于《数论杂志》133 (2013)，3381–3393。 8[9] G. Lachaud 和 R. Rolland，《有限域上代数集的点数》，载于《纯粹与应用代数杂志》 **219** 2015 5117 5136 21 （），–。D. W. Masser 和 G.[10]Wüstholz，《椭圆曲线除法域的伽罗瓦性质》，载于《伦敦数学会通报》 **25** 1993 247 234 7 （），–。L. Mathewson，《gl2 (fq) 的类方程》，硕士[11]论文（导师：Jeb F. Willenbring），威斯康星大学密尔沃基分校，2012 6。H.L. Montgomery 和 R.C. Vaughan，《乘法数论》，[12]载于《数论基础》，I. 经典理论，剑桥高等数学研究丛书 **97**, 2007 9，剑[13]桥大学出版社，剑桥，（）。K.A. Ribet，《具有实乘法的阿贝尔簇除法点上的伽罗瓦作用》，载于《美国数学杂志》98 (1976)，751–804。 7[14] K.A. Ribet，《与模形式相关的 l 进表示。II》，载于《格拉斯哥数学杂志》27 (1985)，185–194。 5[15] O. Roche-Newton、M. Rudnev 和 I.D. Shkredov，《有限域上的新型和积估计》，载于《数学进展》293 (2016)，589–605。 19[16] M. Rudnev，《素数阶域中的一个改进和积不等式》，载于《国际数学研究论文集》16 (2012)，3693–3705。 19[17] J.P.Serre，《某些算术函数的整除性》，载于 Delange-Pisot-Poitou 研讨班，第16年，“数论”，分册 *1*, *20***16** 1974 75 1，报告编号（/）。I. D. Shkredov，[18]《若干和积问题中的渐近公式》，载于《莫斯科数学会汇刊》79 (2018)，231–281。 15[19] I.E. Shparlinski，《拉马努金函数的值集》，载于《数学档案（巴塞尔）》85 (2005)，508–513。 2,3,11,21[20] 2020 2 J. Thorner，《佐藤–泰[21]特猜想的有效形式》，载于 arXiv（）。I. M. Vinogradov，《数论基础》，Dover P ublications, Inc.，纽约（1954），S. Kravetz 译。 15

德国哥廷根乔治-奥古斯特大学数学研究所。电子邮箱：subham.bhakta@mathematik.uni-goettingen.de 印度科学教育与研究学院特里凡得琅分校，印度。电子邮箱：muneeswaran20@iisertvm.ac.in 印度科学教育与研究学院特里凡得琅分校，印度。电子邮箱：srilakshmi@iisertvm.ac.in