arXiv:2301.02381v1 [math.NT] 6 Jan 2023

有限域上具有两个指定迹的本原对的存在性

Aakash Choudhary*和 R. K. Sharma †

印度理工学院德里分校数学系，印度德里 110016

摘要

给定 $F = \mathbb{F}_{p^t}$，一个含有 p^t 个元素的域，其中 p 是素数幂，$t \geq 7$、n 是正整数，且 $f = f_1/f_2$ 是一个有理函数，其中 f_1、f_2 是互素的不可约多项式，满足 $deg(f_1) + deg(f_2) = n$ 属于 $F[x]$。我们构造了关于 (p,t) 的一个充分条件，保证存在本原配对 $(\epsilon, f(\epsilon))$，使其属于 F，且满足 $Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = a$ 以及 $Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(f(\epsilon)) = b$，其中 a、$b \in \mathbb{F}_p$ 为任意指定的迹。此外，我们证明，对任意正整数 n，当 t 足够大时，这样的配对必定存在。对于 $n = 2$ 的情形，我们单独进行了处理，并验证了对于所有 (p,t)，除 p 可能取的 71 个值外，这样的配对均存在。我们还给出了 $n = 3$ 情形下的一个结果。

关键词：特征标、有限域、本原元。2020年数学主题分类：12E20，11T23

1 引言

设 $\mathbb{F}_p$ 表示一个有限阶为 p 的域，其中 $p = q^r$，q 为某个素数，且 r 为正整数。$\mathbb{F}_p$ 的乘法群是循环的，记作 $\mathbb{F}_p^*$；$\mathbb{F}_p^*$ 的生成元称为 $\mathbb{F}_p$ 中的本原元。

*电子邮件：achoudhary1396@gmail.com

†电子邮件：rksharmaiitd@gmail.com

域 $\mathbb{F}_p$ 有 $\phi(p-1)$ 个本原元，其中 ϕ 是欧拉函数。设 $\mathbb{F}_{p^t}$ 表示 $\mathbb{F}_p$ 的一个扩域，其次数为 t，其中 t 为某个正整数。元素 $\epsilon \in \mathbb{F}_{p^t}^*$ 为本原元的充要条件是：它是 $\mathbb{F}_p$ 上一个次数为 t 的不可约多项式的根，而这样的不可约多项式称为本原多项式。对于 $\epsilon \in \mathbb{F}_{p^t}$，$\epsilon$ 在 $\mathbb{F}_p$ 上的迹记作 $Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon)$，定义为$Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = \epsilon + \epsilon^p + \epsilon^{p^2} + \cdots + \epsilon^{p^{t-1}}$。

在 ElGamal 加密方案和 Diffie–Hellman 密钥交换等密码方案中，本原元是基本构件。在编码理论和密码学中，本原元有许多应用 [10], ，因此本原元和本原多项式的研究成为一个活跃的研究领域。有关有限域中本原元存在性的更多信息，请参阅[9] 。对于任意有理函数 $f(x) \in \mathbb{F}_p(x)$和 $\epsilon \in \mathbb{F}_p$ ，如果对$(\epsilon, f(\epsilon))$中的两个元素 ϵ和 $f(\epsilon)$都是 $\mathbb{F}_p$中的本原元，我们就称该对为本原对。一般而言，如果 ϵ 是本原元， $f(\epsilon)$未必是本原元。例如，取$x^2 + 3x + 2 \in \mathbb{F}_7[x]$，则 3 和 5 是 $\mathbb{F}_7$ 中的本原元，但 $f(3)$和 $f(5)$都不是。

1985 年，Cohen [3] 引入了“本原对”这一术语，并验证了在 $\mathbb{F}_p$中存在本原对 $(\epsilon, f(\epsilon))$，其中对应一次多项式为 $f(x) = x + k \in \mathbb{F}_p[x]$。此后，许多研究者对这一领域进行了研究 [12, 13, 7, 14]。最近，Cohen、Sharma 和 Sharma [4]给出了一个条件，保证在$\mathbb{F}_p$中存在本原对 $(\epsilon, f(\epsilon))$，其中$\mathbb{F}_p$为非例外有理函数 f；也就是说， f不是 $cx^j g^k(x)$ 的形式，其中 $j \in \mathbb{Z}$, $k > 1$ 是整除 $p-1$ 和 $c \in \mathbb{F}_p^*$的 $g(x) \in \mathbb{F}_p(x)$。Jungnickel、Vanstone [8] 确定了一个充分条件，保证存在具有 ϵ指定迹的本原元 $\epsilon \in \mathbb{F}_{p^t}$ 。随后，Cohen [5]在存在一些例外的情况下推广了这一结果。Chou 和 Cohen [2], 于 2014 年探讨了存在本原元 $\epsilon \in \mathbb{F}_{p^t}$ 的问题，使得$Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon^{-1}) = 0.$。Cao 和 Wang [1], 针对 $t \geq 29$，建立了一个条件，以保证存在本原对 $(\epsilon, f(\epsilon))$，满足 $f(x) = \frac{x^2+1}{x} \in \mathbb{F}_{p^t}(x)$，且对于指定的 a、$b \in \mathbb{F}_p^*$、 $Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = a$和 $Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon^{-1}) = b$。2018 年，Gupta、Sharma 和 Cohen [7], 针对同一有理函数和指定的 $a \in \mathbb{F}_p$，给出了一个条件，保证在 $\mathbb{F}_{p^t}$中存在本原对 $(\epsilon, f(\epsilon))$，满足 $Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = a$，其中 $t \geq 5$。随后在 2019 年，Gupta 和 Sharma [14] 将这一结果推广到了有理函数

$\Gamma_M(x) = \frac{a_{11}x^2+a_{12}x+a_{13}}{a_{22}x+a_{23}}$，其中 $M = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \end{pmatrix} \in \mathbb{M}_{2\times3}(\mathbb{F}_{p^t})$ 是任意秩为 2 的矩阵；若 $\Gamma_M(x) = \lambda x$ 或 λx^2 对某个 $\lambda \in \mathbb{F}_{p^t}$成立，则 $\lambda = 1$。

2021 年，Sharma 和 Sharma [11] 考察了 $\mathbb{F}_{p^t}(x)$ 中的有理函数 $f = f_1/f_2$，其中 f_1 和 f_2 是互素的不可约多项式，并证明：对于指定的 a、$b \in \mathbb{F}_p$，存在本原对 $(\epsilon, f(\epsilon))$，属于 $\mathbb{F}_{p^t}$，且满足 $Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = a$和 $Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon^{-1}) = b$，其中 $t \geq 7$。

在本文之前，对于本原对，所考虑的是 ϵ和ϵ^{-1}的迹。本文将考虑迹到元素 ϵ 上的映射及其在 f下的像，即 $f(\epsilon)$。为便于说明，先介绍一些术语和约定。我们称域 $\mathbb{F}_p[x]$ 上的非零多项式 f 的次数为$k \geq 0$，若 $f(x) = a_kx^k + a_{k-1}x^{k-1} + \cdots + a_1x + a_0$，其中 $a_k \neq 0$，并将 f 的次数记作 $deg(f) = k$。接下来，设有理函数$f(x) = {}^{f_1(x)}\!/_{f_2(x)} \in \mathbb{F}_p(x)$中，$f_1$ 和 f_2 是互素的不~~可约~~多项式，并将次数和定义为 $degsum(f) = deg(f_1) + deg(f_2)$。现在我们将定义若干集合，它们将在本文中发挥关键作用。

1. 我们定义 $R_{p,\ t}(n_1, n_2)$ 表示所有有理函数 $f(x) = {}^{f_1(x)}\!/_{f_2(x)} \in \mathbb{F}_{p^t}(x)$ 的集合，~~其~~中 f_1 和 f_2 是在 $\mathbb{F}_{p^t}$ 上互素的不可约多项式，且满足 $deg(f_1) = n_1$ 和 $deg(f_2) = n_2$。

2. 记 $A_{n_1,\ n_2}$ 为由满足以下条件的有序对 $(p, t) \in \mathbb{N} \times \mathbb{N}$ 构成的集合：对于任意 $f \in R_{p,\ t}(n_1, n_2)$ 以及给定的 a、$b \in \mathbb{F}_p$、$\mathbb{F}_{p^t}$，其中都包含一个元素 ϵ，使得 $(\epsilon, f(\epsilon))$ 是本原对，且 $Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = a$ 和 $Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(f(\epsilon)) = b$。

3. 定义 $R_{p,\ t}(n) = \bigcup_{n_1+n_2=n} R_{p,\ t}(n_1, n_2)$ 以及 $A_n = \bigcap_{n_1+n_2=n} A_{n_1,\ n_2}$。

首先，在本论文中，对于 $n \in \mathbb{N}$，我们考虑 $f(x) \in R_{p,t}(n)$ 和 $a, b \in \mathbb{F}_p$，然后验证存在一个元素 $\epsilon \in \mathbb{F}_{p^t}$，使得 $(\epsilon, f(\epsilon))$ 是 $\mathbb{F}_{p^t}$ 中具有 $Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = a$ 和 $Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(f(\epsilon)) = b$ 的本原对，即我们为 p^t 提供了一个充分条件，使得 $(p, t) \in A_n$。此外，利用这一充分条件的筛法变体，我们证明了以下结果：

定理 1.1. 设 t、q、r、p $\in \mathbb{N}$ 满足 q 是一个素数，t ≥ 7和 $p = q^r$。假设 p 和 t 均不取以下值：

1. $2 \leq p \leq 16$ *or* $p = 19, 23, 25, 27, 31, 37, 43, 49, 61, 67, 79$ *and* $t = 7$*;*

2. $2 \leq p \leq 31$ 或 $p = 32$、37、41、43、47、83 和 $t = 8$；3. $2 \leq p \leq 8$ 或 $p = 11$、16 和 $t = 9$；4. $p = 2$、3、4、5、7 和 $t = 10$、12；5. $p = 2$、3、4 和 $t = 11$；6. $p = 2$ 和 $t = 14$、15、16、18、20、24。

那么 $(p, t) \in A_2$。

注意：上述定理中的例外不一定是真正的例外，它们只是可能的例外。

本文所需的所有非平凡计算均使用 SageMath [16] 完成。

2 预备知识

本节将介绍本文后续各节中会用到的一些基本概念、记号和结果。全文中，t 是一个正整数，p 是任意一个素数幂，$\mathbb{F}_p$ 是一个阶为 p 的有限域。

2.1 定义

1. 有限阿贝尔群 G 的特征标是从集合 G 到复数域 $\mathbb{C}$ 中绝对值为 1 的所有元素组成的集合 Z^1 的同态 χ。G 的平凡特征标记作 χ_0，定义为对所有 $g \in G$，$\chi_0(g) = 1$。此外，G的所有特征标构成的集合记作 G，在乘法运算下构成一个群，该群与 G同构。特征标 χ的阶是满足 $\chi^d = \chi_0$的最小正整数 d。对于有限域 $\mathbb{F}_{p^t}$，加法群 $\mathbb{F}_{p^t}$ 的特征标称为加法特征，乘法群 $\mathbb{F}_{p^t}^*$ 的特征标称为乘性特征。

2. 对于 p^t-1 的因子 u，如果在 $\zeta = \xi^s$ 时，$\xi \in \mathbb{F}_{p^t}$ 和 $s|u$ 蕴含 $s = 1$，则称元素 $\zeta \in \mathbb{F}_{p^t}^*$ 为 u-$free$。我们看到，当且仅当元素 $\zeta \in \mathbb{F}_{p^t}^*$ 是 $\mathbb{F}_{p^t}$ 的本原元时，它是 $(p^t - 1)$-$free$。

关于特征、本原元和有限域的更多信息，请参阅 [9]。

以下结论是 [15, 引理 10]的一个特例 :

引理 2.1. 设 u 是 p^t-1 的因子， $\zeta \in \mathbb{F}_{p^t}^*$，则有:

$$\sum_{s|u} \frac{\mu(s)}{\phi(s)} \sum_{\chi_s} \chi_s(\zeta) = \begin{cases} \frac{u}{\phi(u)} & if\ \zeta\ is\ u-free, \\ 0 & otherwise \end{cases}$$

其中， μ(.) 是莫比乌斯函数， ϕ(.) 是欧拉函数， χ_s 遍历 $\mathbb{F}_{p^t}^*$ 上阶为 s的所有 ϕ(s)乘性特征。

因此，对于 u，它是 p^t-1 的因子

$$\rho_u : \epsilon \mapsto \theta(u) \sum_{s|u} \frac{\mu(s)}{\phi(s)} \sum_{\chi_s} \chi_s(\epsilon) \tag{1}$$

给出了 $\mathbb{F}_{p^t}^*$ 中 u-$free$ 个元素所成子集的示性函数，其中θ(u) = ϕ(u)/u。

此外，对于 $a \in \mathbb{F}_p$,

$$\tau_a : \epsilon \mapsto \frac{1}{p} \sum_{\psi \in \hat{\mathbb{F}_p}} \psi(Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) - a) \tag{2}$$

是子集 $\mathbb{F}_{p^t}$ 的示性函数，其中的元素满足 $Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}$($\epsilon$) = a。根据 [9, 定理 5.7], , $\mathbb{F}_p$ 的任意加法特征 ψ 均可由 ψ(a) = ψ_0(ua) 导出，其中 ψ_0 是 $\mathbb{F}_p$ 的典范加法特征，而 u 是 $\mathbb{F}_p$ 中与 ψ 对应的元素。因此

$$\begin{aligned} \tau_a &= \frac{1}{p} \sum_{\psi \in \hat{\mathbb{F}_p}} \psi_0(Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(u\epsilon) - ua) \\ &= \frac{1}{p} \sum_{u \in \mathbb{F}_p} \hat{\psi_0}(u\epsilon)\psi_0(-ua) \end{aligned} \tag{3}$$

ˆ ˆ 其中 ψ_0 是由 ψ_0(ϵ) = ψ_0($Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}$($\epsilon$))定义的 $\mathbb{F}_{p^t}$ 的加法特征。在下一个定理中，我们将大量运用 Wang 和 Fu 于 2014 年给出的以下结果 [6] 。

引理 2.2。 *[6, 定理 5。5]* 设 $F(x) \in \mathbb{F}_{p^d}(x)$ 是一个有理函数。记 $F(x) = \prod_{j=1}^{k} f_j(x)^{r_j}$，其中 $f_j(x) \in \mathbb{F}_{p^d}[x]$ 是不可约多项式，r_j 是非零整数。设 χ 是 $\mathbb{F}_{p^d}$的一个乘性特征。假设有理函数 $\prod_{i=1}^{d-1} f(x^{p^i})$ 不能写成 $h(x)^{ord(\chi)} \in \mathbb{F}_{p^d}(x)$ 的形式，其中 $ord(\chi)$ 是 χ的阶，则有

$$\left| \sum_{\epsilon \in \mathbb{F}_p, f(\epsilon) \neq 0, \infty} \chi(F(\epsilon)) \right| \leq \left(d \sum_{j=1}^{k} deg(f_j) - 1 \right) p^{\frac{1}{2}}.$$

引理 2.3. *[6, 定理 5.6]* 设 f(x), g(x) $\in \mathbb{F}_{p^t}(x)$ 为有理函数。将 f(x) $= \prod_{j=1}^{k} f_j(x)^{r_j}$ 写成如下形式：$f_j(x) \in \mathbb{F}_{p^t}[x]$ 为不可约多项式，r_j 为非零整数。设 $D_1 = \sum_{j=1}^{k} deg(f_j)$，$D_2 = max\{deg(g)\ 0\}$，$D_3$ 是 g(x) 的分母的次数，D_4 是整除 g 的分母、但不同于 $f_j(x)$（j=1,2,...,k）的不可约多项式的次数之和。设 χ 是 $\mathbb{F}_{p^t}$ 上的乘性特征，ψ 是 $\mathbb{F}_{p^t}$ 上的非平凡加法特征。假设 g(x) 不能写成 $v(x)^{p^t} - v(x)$ 的形式，其中$\mathbb{F}_{p^t}(x)$。那么我们有

$$\left| \sum_{\epsilon \in \mathbb{F}_{p^t}, f(\epsilon) \neq 0, \infty, g(\epsilon) \neq \infty} \chi(f(\epsilon))\psi(g(\epsilon)) \right| \leq (D_1 + D_2 + D_3 + D_4 - 1) p^{\frac{t}{2}}.$$

显然，充分条件（定理 3.1）及其筛法变体（定理 3.4）完全取决于 p^t 以及有理函数的分子和分母多项式的次数。容易看出，[11]中主要结果的迹部分是我们关于 $f(x) = \frac{1}{x}$ 的发现的一个特例。

对于每个 $\kappa \in \mathbb{N}$，我们用 $\omega(\kappa)$ 表示 κ 的不同素因子个数，用 $W(\kappa)$ 表示 κ 的无平方因子约数个数。显然，$W(\kappa) = 2^{\omega(\kappa)}$。

3 充分条件

设 $k_1, k_2, p, t \in \mathbb{N}$ 满足：p 是素数幂，且 k_1, k_2 是整除 $p^t - 1$. 的正整数。令 a, $b \in \mathbb{F}_p$, $f(x) \in R_{p,t}(n)$。令 $A_{f,a,b}(k_1, k_2)$ 表示由所有满足以下条件的元素 $\epsilon \in \mathbb{F}_{p^t}$ 构成的集合：ϵ 是无 k_1 因子的，$f(\epsilon)$ 是无 k_2 因子的，$Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = a$，且 $Tr_{\mathbb{F}_{p^t}/\mathbb{F}_t}(f(\epsilon)) = b$。

现在我们按如下方式验证充分条件：

定理 3.1. 设 t、n、p $\in \mathbb{N}$ 和 p 是一个素数幂。设

$$p^{\frac{t}{2}-2} > (2n+1)W(p^t-1)^2.$$

那么 $(p,t) \in A_n$.

证明。为了证明这一结果，只需证明对于每个 $f(x) \in R_{p,t}(n)$ 以及任意给定的 $a,b \in \mathbb{F}_p$，$b(k_1,k_2) > 0$，其中 $A_{f,a,}$。设 $f(x) \in R_{p,t}(n)$ 是一个有理函数，且 $a,b \in \mathbb{F}_p$。令 P 表示 $f(x) \in \mathbb{F}_{p^t}$ 和 $P' = P \cup \{0\}$ 的零点与极点集合。设 k_1, k_2是 p^t-1的因子。根据定义，$A_{f,a,b}(k_1,k_2)$ 可表示为

$$A_{f,a,b}(k_1,k_2) = \sum_{\epsilon \in \mathbb{F}_{p^t}-P'} \rho_{k_1}(\epsilon)\rho_{k_2}(f(\epsilon))\tau_a(\epsilon)\tau_b(f(\epsilon)).$$

利用上一节定义的特征函数 (1) 和 (3)，我们得到

$$A_{f,a,b}(k_1,k_2) = \frac{\theta(k_1)\theta(k_2)}{p^2} \sum_{s_1|k_1,s_2|k_2} \frac{\mu(s_1)\mu(s_2)}{\phi(s_1)\phi(s_2)} \sum_{s_1,s_2} \chi_{f,a,b}(s_1,s_2)$$

其中 $\theta(k_i) = \underline{\phi(k_i)}\, k_i$；$i = 1, 2$
和

$$\chi_{f,a,b}(s_1,s_2) = \sum_{u,v \in \mathbb{F}_p} \psi_0(-au-bv) \sum_{\epsilon \in \mathbb{F}_{p^t}-P'} \chi_{s_1}(\epsilon)\chi_{s_2}(\epsilon_0)\hat{\psi}_0(u\epsilon + v\epsilon_0)$$

其中 $\epsilon_0 = f(\epsilon)$。由 [9, 例 5.1] 可知，对于 p^t-1的任意因子 s_1, s_2，存在整数 m_1, m_2，使得 $0 < m_1, m_2 < p^t-1$，且$\chi_{s_1}(x) = \chi_{p^t-1}(x^{m_1})$，以及 $\chi_{s_2}(x) = \chi_{p^t-1}($ $x^{m_2})$。因此

$$\chi_{f,a,b}(s_1,s_2) = \sum_{u,v \in \mathbb{F}_p} \psi_0(-au-bv) \sum_{\epsilon \in \mathbb{F}_{p^t}-P'} \chi_{p^t-1}(\epsilon^{m_1} f(\epsilon)^{m_2})\hat{\psi}_0(u\epsilon + v\epsilon_0) \tag{4}$$

$$= \sum_{u,v \in \mathbb{F}_p} \psi_0(-au-bv) \sum_{\epsilon \in \mathbb{F}_{p^t}-P'} \chi_{p^t-1}(F_1(\epsilon))\hat{\psi}_0(F_2(\epsilon)), \tag{5}$$

其中 $F_1(x) = x^{m_1} f(x)^{m_2} \in \mathbb{F}_{p^t}(x)$，且 $F_2(x) = ux + vf(x) \in \mathbb{F}_{p^t}(x)$。

首先，我们考虑这样的情形：对于某个 $l(x) \in \mathbb{F}_{p^t}(x)$，有 $F_2(x) = l(x)^{p^t} - l(x)$，其中 $l(x) = \frac{l_1(x)}{l_2(x)}$，且 $(l_1, l_2) = 1$。我们有，$\frac{ux+v}{f_1(x)} \frac{f_1(x)}{f_2(x)} = \frac{l_1(x)}{l_2(x)}^{p^t} - \frac{l_1(x)}{l_2(x)}$，即

$$f_2(x)(l_1(x)^{p^t} - l_1(x)l_2(x)^{p^t-1}) = l_2(x)^{p^t}(uxf_2(x) + vf_1(x)).$$

由于 $(l_1(x)^{p^t} - l_1(x)l_2(x)^{p^t-1}, l_2(x)^{p^t}) = 1$，因此可得，$l_2(x)^{p^t}$ 整除 $f_2(x)$，而这只有在 $l_2(x)$ 为常数时才可能发生。也就是说，我们有

$$c^{-(p^t)} f_2(x)(l_1(x)^{p^t} - l_1(x)c^{p^t-1}) = uxf_2(x) + vf_1(x)$$

其中 $c = l_2$。现在，上述方程仅在 $v = 0$ 时成立。将其代入上式可得，$c^{-(p^t)}(l_1(x)^{p^t} - l_1(x)c^{p^t-1}) = ux$，这只有在 l_1 为常数且 $u = 0$ 时才可能发生。此外，若对任意 $r(x) \in \mathbb{F}_{p^t}(x)$，都有 $F_1(x) \neq r(x)^{p^t-1}$，则由引理 2.2 可得

$$|\chi_{f,a,b}(s_1, s_2)| \leq np^{\frac{t}{2}+2}. \tag{6}$$

并且，当对某个 $r(x) \in \mathbb{F}_{p^t}(x)$ 有 $F_1(x) = r(x)^{p^t-1}$ 时，其中 $r(x) = \frac{r_1(x)}{r_2(x)}$ 满足 $(r_1, r_2) = 1$。根据 [11], ，只有在 $m_1 = m_2 = 0$ 时才会出现这种情况，这就产生了矛盾。

若对于任意 $d(x) \in \mathbb{F}_{p^t}(x)$，均有 $F_2(x) \neq d(x)^{p^t} - d(x)$，则，

情况 1：当 $n_1 \leq n_2$ 时。根据引理 2.3，我们有 $D_2 = 1$，并且

$$|\chi_{f,a,b}(s_1, s_2)| \leq (2n+1)p^{\frac{t}{2}+2}. \tag{7}$$

情况 2：当 $n_1 > n_2$ 时。我们有 $D_2 = n_1 - n_2$，并且

$$|\chi_{f,a,b}(s_1, s_2)| \leq 2np^{\frac{t}{2}+2}. \tag{8}$$

因此，若 $(\chi_{s_1}, \chi_{s_2}, u, v) \neq (\chi_1, \chi_1, 0, 0)$，那么根据上述讨论，并利用 (6)、(7) 和 (8)，可得 $|\chi_{f,a,b}(s_1, s_2)| \leq (2n+1)p^{\frac{t}{2}+2}$. 由此以及 $A_{f,a,b}(k_1, k_2)$ 的定义，可得

$$A_{f,a,b}(k_1, k_2) \geq \frac{\theta(k_1)\theta(k_2)}{p^2}((p^t - |P'|) - (2n+1)p^{\frac{t}{2}+2}(W(k_1)W(k_2) - 1)) \tag{9}$$

$$\geq \frac{\theta(k_1)\theta(k_2)}{p^2}((p^t - (n+1)) - (2n+1)p^{\frac{t}{2}+2}(W(k_1)W(k_2) - 1)) \tag{10}$$

因此，若 $p^{\frac{t}{2}-2} > (2n+1)W(k_1)W(k_2)$，则对每个 $f(x)$，$A_{f,a,b}(k_1,k_2) > 0$ $\in R_{p,t}(n)$，且迹 $a,b \in \mathbb{F}_p$ 已指定。考虑 $k_1 = k_2 = p^t - 1$，结论即得。

□

现在，我们给出 $A_{f,a,b}(mk,k) - \theta(m)A_{f,a,b}(k,k)$ 和 $A_{f,a,b}(k,mk) - \theta(m)A_{f,a,b}(k,k)$ 的绝对值的界。证明从 [7] 的思想即可推出，故略去。

引理 3.2。设 k 是一个整除 p^t-1 的正整数，且 m 是一个整除 p^t-1 但不整除 k 的素数。则

$$|A_{f,a,b}(mk,k) - \theta(m)A_{f,a,b}(k,k)| \leq \frac{\theta(k)^2\theta(m)}{p^2}(2n+1)W(k)^2 p^{\frac{t}{2}+2}$$

and

$$|A_{f,a,b}(k,mk) - \theta(m)A_{f,a,b}(k,k)| \leq \frac{\theta(k)^2\theta(m)}{p^2}(2n+1)W(k)^2 p^{\frac{t}{2}+2}.$$

引理 3.3。设 k 是一个整除 p^t-1 的正整数，且 $\{q_1,q_2,\ldots,q_m\}$ 是所有整除 p^t-1 但不整除 k 的素数所组成的集合。则

$$A_{f,a,b}(p^t-1,p^t-1) \geq \sum_{i=1}^{m} A_{f,a,b}(k,q_ik) + \sum_{i=1}^{m} A_{f,a,b}(q_ik,k) - (2m-1)A_{f,a,b,}(k,k).$$

充分条件（定理 3.1）的筛法变体如下所示，其证明不再给出，因为它可由引理 3.2、引理 3.3 以及 [7] 中的思想推出。

定理 3.4。设 t、n、p、$k \in \mathbb{N}$ 满足 k 整除 p^t-1，其中 p 是一个素数幂。假设 $\{q_1,q_2,\ldots,q_m\}$ 是所有整除 p^t-1 但不整除 k 的素数组成的集合。设 $\delta = 1 - 2\sum_{i=1}^{m}\frac{1}{q_i}$ 且 $\Delta = \frac{2m-1}{\delta} + 2$。若 $\delta > 0$ 且

$$p^{\frac{t}{2}-2} > (2n+1)\Delta W(k)^2$$

那么 $(p,t) \in A_n$.

引理 3.5. 假设 $\kappa \in \mathbb{N}$ 满足 $\omega(\kappa) \geq 1547$，则 $W(\kappa) \leq \kappa^{1/12}$。

证明. 令 $V = \{2, 3, 5, \ldots, 12983\}$ 为前1547个素数构成的集合。我们看到， V 中所有元素的乘积大于 $K = 6.57 \times 10^{5588}$。令 $\kappa = \kappa_1\kappa_2$，其中 κ_1 和 κ_2 是互素整数，并且 κ_1 的所有素因子均来自 κ 最小的1547个素因子，其余素因子都是 κ_2 的因子。因此， $\kappa_1^{1/12} > K^{1/12} > 5.42 \times 10^{465}$，而 $W(\kappa_1) < 4.93 \times 10^{465}$。由于对所有素数 $\rho > 12983$，均有 $\rho^{1/12} > 2$，故结论成立。

□

在下一节进行计算时，我们需要用到定理 3.4 和引理 3.5。

4 定理 1.1 的证明

我们将对情形 $t \geq 7$ 给出证明，因为根据 [2]，不存在本原元 ϵ，使得对于 $t \leq 4$， $Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = 0$ 且$Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon^{-1}) = 0$。情形 $t = 5$ 和 6 需要大量计算，而且似乎需要采用不同的方法。因此，我们将这些情形留待进一步研究。

我们首先假设 $\omega(p^t - 1) \geq 1547$。利用定理 3.1 和引理 3.5，若 $p^{\frac{t}{2}-2} > 5p^{\frac{t}{6}}$，即若 $p^t > 5^{\frac{3t}{t-6}}$，则 $(p, t) \in A_2$。但是$t \geq 7$ 给出 $\frac{3t}{t-6} \leq 21$。因此，若 $p^t > 5^{21}$，则 $(p, t) \in A_2$，且这对 $\omega(p^t - 1) \geq 1547$ 同样成立。因此，我们可以假设 $\omega(p^t - 1) \leq 1546$。为继续进行计算工作，我们将使用筛法变体。设 $62 \leq \omega(p^t - 1) \leq 1546$。为应用定理 3.4，假设 k 是整除 $p^t - 1$ 的最小 62 个素数的乘积，即 $W(k) = 2^{62}$，那么$m \leq 1485$，且当 $\{q_1, q_2, \ldots, q_{1485}\} = \{307, 311, 313, \ldots, 12979\}$ 时， δ 取其最小正值。由此得到 $\delta > 0.004174$ 和 $\Delta < 710770.7395$。因此 $5\Delta W(k)^2 < 7.558211 \times 10^{43}$。设 $Z = 7.558211 \times 10^{43}$。根据筛法变体，若 $q^{\frac{t}{2}-2} > Z$，即若 $p^t > Z^{\frac{2t}{t-4}}$，则 $(p, t) \in A_2$。由于 $t \geq 7$，可得$\frac{2t}{t-4} \leq \frac{14}{3}$。因此，在 $p^t > 5.834 \times 10^{204}$ 的条件下，$(p, t) \in A_2$。由此， $\omega(p^t - 1) \geq 95$ 蕴含 $(p, t) \in A_2$。类似地，若 $\omega(p^t - 1) \geq 95$，则 $(p, t) \in A_3$,A_4；若 $\omega(p^t - 1) \geq 96$，则 $(p, t) \in A_5$。

表1。

$Sr.No.$	$a \leq \omega\ (p^t-1)\ \leq b$	$W\ (k)$	$\delta >$	$\Delta <$	$5\Delta W\ (k)^{\ 2} <$
1	$a=13,\ b=94$	2^{13}	0.04481712	3594.3767988	1,206,072,718,756
2	$a=7,\ b=34$	2^7	0.04609692	1151.7513186	94,351,469
3	$a=6,\ b=25$	2^6	0.08241088	450.9698124	9,235,862
4	$a=6,\ b=23$	2^6	0.12550135	264.9453729	5,426,082
5	$a=6,\ b=22$	2^6	0.14959773	209.2223842	4,284,875
6	$a=5,\ b=19$	2^5	0.07663431	354.3225878	1,814,132
7	$a=5,\ b=17$	2^5	0.13927194	167.1445296	855,780
8	$a=5,\ b=16$	2^5	0.17317025	123.2679422	631,132
9	$a=5,\ b=15$	2^5	0.21090610	92.0874844	471,488

利用上文表1中的数值并重复筛法变体的过程，我们确定，若 $p^t > (4284875)^{\frac{14}{3}}$ 或 $p^t > 8.8929 \times 10^{30}$（其中 $t \geq 7$），则 $(p,t) \in A_2$；而由于 $t \geq 8$ 蕴含 $\frac{2t}{t-4} \leq 4$，因此若 $p^t > 3.371 \times 10^{26}$（其中 $t \geq 8$），则 $(p,t) \in A_2$。

因此，对于 $t \geq 8$，只需满足 $\omega\ (p^t-1)\ \geq 20$。我们反复利用前表第二部分中各值的筛法变体，推得：若 $p^t > 1.084 \times 10^{25}$，则（$p,\ t$）$\in A_2$。

类似地，$\omega\ (p^t-1)\ \geq 18$ 足以保证（$p,\ t$）属于 A_2；根据上表，对于 $t \geq 9$，若 $p^t > 2.2725 \times 10^{21}$，则（$p,\ t$）$\in A_2$；对于 $t \geq 10$，若 $p^t > 8.158 \times 10^{18}$，则（$p,\ t$）$\in A_2$。

因此，$(p,t) \in A_2$ 除非 $t=7$ 和 $p < 26382$、$t=8$ 和 $p < 1347$、$t=9$和 $p < 237$、$t=10$ 和 $p < 78$、$t=11$ 和 $p < 53$、$t=12$ 和 $p < 38$、$t=13$ 和 $p < 29$、$t=14$ 和 $p < 23$、$t=15$ 和 $p < 19$、$t=16$ 和 $p < 16$、$t=17$ 和 $p < 13$、$t=18$ 和 $p < 12$、$t=19$ 和 $p < 10$、$t=20$ 和 $p < 9$、$t=21$、22和 $p < 8$、$t=23$、24和 $p < 7$、$t=25$、26、27和 $p=2$、3、4、5。$28 \leq t \leq 31$ 和 $p=2$、3、4。$32 \leq t \leq 39$ 并且对于 $p=2$、3。$40 \leq t \leq 62$ 和$p=2$。

根据前文讨论，对于每个 (p,t)，我们验证了定理 3.1，并整理出 570 个可能的例外情形（见附录）。

接着，对于这些可能的例外情形，我们发现，除定理 1.1 中提到的情况外，筛法变体对绝大多数素数幂都成立（见附录）。定理 1.1 由此得出。运用类似的推理，可以为任意 $n \in \mathbb{N}$ 找到 A_n 的一个子集。特别是，对于 A_3，我们有以下结果。

定理 4.1。假设 t q、r、p $\in \mathbb{N}$ 满足 q 为素数，t≥ 7 且 $p = q^r$。令 p 和 t 不取以下任何值：

1. $2 \leq p \leq 31$ 或 $p = 37$、41、43、49、61、67、71、79、103、121 和 $t = 7$；2. $2 \leq p \leq 47$ 或 $p = 53$、83 和 $t = 8$；3. $2 \leq p \leq 7$ 或 $p = 9$、11、16 和 $t = 9$；4. $2 \leq p \leq 8$ 和 $t = 10$；5. $p = 2$、3、4 和 $t = 11$；6. $2 \leq p \leq 7$ 和 $t = 12$；7. $p = 2$ 和 $t = 14$、15、16、18、20、24。

那么（p，t）$\in A_3$。

参考文献

[1] Cao, X., Wang, P. (2014). 具有给定迹的本原元. AAECC 25(5):339–345.[2] Chou, W. S., Cohen, S. D. (2001). 零迹本原元. Finite Fields Appl. 7(1):125–141.[3] Cohen, S. D. (1985). 有限域中的连续本原根. Proc. Amer. Math. Soc. 93(2):189–197.[4] Cohen, S .D., Sharma, H., Sharma, R. K. (2021). 有限域本原元处有理函数的本原值. J. Number Theory 219:237–246.[5] Cohen, S. D., Presern, M. (2005). 具有指定迹的本原有限域元. Southeast Asian Bull. Math. 29(2):283–300.

[6] Fu, L., Wan, D. (2014). 一类不完全特征和. Q. J. Math. 65(4):1195–1211.[7] Gupta, A., Sharma, R. K., Cohen, S. D. (2018). 有限域上具有一个指定迹的本原元对. Finite Fields Appl. 54:1–14.[8] Jungnickel, D., Vanstone, S. A. (1989). 关于有限域上的本原多项式. J. Algebra 124(2):337–353.[9] Lidl, R., Niederreiter, H. (1997). 有限域, 第20卷. 剑桥（英国）：剑桥大学出版社.[10] Paar, C., Pelzl, J. (2010). 基于离散对数问题的公钥密码系统，第205–238页. 柏林、海德堡：施普林格.[11] Sharma, H., Sharma, R.K. (2021). 有限域上具有指定迹的本原元对的存在性.《代数通讯》49(4):1773-1780.[12] Sharma, R.K., Awasthi, A., Gupta, A. (2018). 特征2有限域上本原元对的存在性. J. Number Theory 193:386–394.[13] Sharma, R. K., Gupta, A. (2017). 有限域上某些特殊本原正规元的存在性. Finite Fields Appl. 46:280–303.[14] Sharma, R. K., Gupta, A. (2019). 有限域上具有指定迹的本原元对.《代数通讯》47(3):1278–1286.[15] Shuqin, F., Wenbao, H. (2004). 伽罗瓦环上的特征和与有限域上的本原多项式. Finite Fields Appl. 10(1):36–52.[16] Sage 开发团队，SageMath，Sage 数学软件系统（9.0 版），https://www.sagemath.org，2020.

附录

使本文定理 3.1 中的条件不成立的 570 个 (p, t) 值列表:

当 t=7 时:

$p=$ 2, 4, 8, 16, 32, 64, 256, 512, 1024, 4096, 3, 9, 27, 81, 243, 729, 6561, 5, 25, 125, 625, 3125, 15625, 7, 49, 343, 2401, 11, 121, 1331, 14641, 13, 169, 2197, 17, 19, 361, 23, 529, 29, 31, 37, 41, 1681, 43, 1849, 47, 53, 59, 3481, 61, 67, 4489, 71, 79, 6241, 83, 6889, 97, 9409, 101, 103, 10609, 107, 109, 11881, 113, 127, 131, 17161, 139, 19321, 151, 22801, 157, 181, 191, 197, 199, 211, 223, 227, 229, 233, 239, 241, 263, 269, 271, 277, 281, 283, 293, 311, 331, 359, 367, 389, 397, 401, 409, 431, 439, 463, 491, 499, 509, 547, 571, 593, 601, 607, 613, 619, 631, 643, 659, 661, 683, 691, 709, 727, 733, 739, 743, 877, 919, 953, 967, 1021, 1051, 1063, 1093, 1123, 1151, 1171, 1181, 1231, 1283, 1301, 1303, 1321, 1381, 1399, 1453, 1481, 1483, 1499, 1523, 1531, 1597, 1607, 1693, 1723, 1741, 1759, 1789, 1801, 1823, 1877, 1879, 1951, 2003, 2141, 2161, 2281, 2311, 2381, 2591, 2713, 2731, 2791, 2887, 2971, 3041, 3083, 3191, 3221, 3229, 3271, 3301, 3307, 3313, 3499, 3547, 3571, 3739, 3851, 3911, 4013, 4159, 4219, 4241, 4243, 4261, 4327, 4421, 4423, 4567, 4621, 4663, 4691, 4751, 4957, 5419, 5923, 5981, 6067, 6211, 6491, 6577, 7159, 7759, 8009, 8053, 8191, 8807, 9103, 9403, 9421, 9463, 9719, 9767, 9871, 9901, 9967, 10427, 10949, 10957, 10979, 11311, 11593, 11621, 12959, 14323, 15313, 15511, 16381, 17431,17491, 19483, 19687, 19891, 20011, 20441, 21391, 22543, 23143, 23671, 24181,24683, 25171, 25411.

当 t=8 时:

$p=$ 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 3, 9, 27, 81, 243, 729, 5, 25, 125, 7, 49, 343, 11, 121, 1331, 13, 169, 17, 19, 361, 23, 529, 29, 841, 31, 961, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149,151,157, 163,167,173,179, 181,191,193, 197, 211, 223, 227, 229, 233, 239,241,251, 257,263,269,271, 277,281,283, 293, 307, 311, 313, 317, 331, 337,347,349, 353,359,367,373, 379,383,389, 397, 401, 409, 419, 421, 433, 439,443,457, 461,463,467,491, 499,509,521, 523, 541, 547, 557, 563, 569, 571,587,593, 599,601,617,619, 631,647,653, 659, 661, 683, 691, 701, 709, 727,733,739, 743,757,773,787, 797,809,811, 823, 827, 829, 839, 853, 857, 859,863,881, 887,911,919,929, 937,941,947, 953, 967, 971, 977, 983, 991, 1009, 1013, 1021, 1033, 1039, 1061, 1063, 1069, 1087, 1091,

1093, 1097, 1103, 1109, 1117, 1123, 1201, 1213, 1217, 1223, 1231, 1277,1279, 1283, 1289, 1291, 1301, 1303, 1319, 1321.

当 t=9 时：

$p = 2$, 4,8, 16, 32, 3,9, 27, 81, 5, 25, 125, 7, 49, 11, 121, 13, 169, 17, 19, 23, 29, 31, 37, 43, 47, 53, 61, 79, 83, 137, 139, 149, 157, 211.

当 t=10 时：

$p = 2$, 4, 8,16, 32, 64, 3, 9, 27, 5, 25, 7, 49, 11, 13, 17, 19, 23, 29, 31, 37, 41, 53, 59, 61, 67.

当 t=11 时：

$p = 2$, 4, 16, 3, 9, 7, 13.

当 t=12 时：

$p = 2$、4、8、16、32、3、9、27、5、7、11、13、17、19、23、29、31、37。

当 t=14 时：$p = 2$、
4、3、5、7。

当 t=15 时：

$p = 2$、4、16、3、9、5。

当 t=16 时：$p = 2$、
4、8、3、5。

当 t=18:$p = 2$、
3、4、5 时。

对于 t=20:
$p = 2$，4、8。

对于 t=24:
$p = 2$, 3、4。

对于 t=22、28、30、
36：$p = 2$。

本文中，列出了与 (p,t) 对应的 k、m 的取值；对于这些取值，定理 3.1 的条件不成立，但对某些 k，筛法变分条件成立。

当 t=7 时:

$Sr.No.$	p	k	m
1	32	1	4
2	64	3	5
3	256	3	7
4	512	1	6
5	1024	3	8
6	4096	3	11
7	81	2	5
8	243	2	4
9	729	2	7
10	6561	2	8
11	125	2	4
12	625	6	5
13	3125	2	7
14	15625	6	10
15	343	6	4
16	2401	6	6
17	121	6	4
18	1331	2	8
19	14641	6	8
20	169	6	4
21	2197	6	6
22	17	2	1
23	361	6	5
24	529	6	6
25	29	2	2
26	41	2	3
27	1681	6	6
28	1849	6	5
29	47	2	3
30	53	2	3
31	59	2	5
32	3481	6	8
33	4489	6	8
34	71	2	4
35	6241	6	8
36	83	2	3
37	6889	6	7
38	97	6	3
39	9409	6	7
40	101	2	3
41	103	6	4
42	10609	6	7
43	107	2	4
44	109	6	3
45	11881	6	7
46	113	2	3
47	127	6	4
48	131	2	5
49	17161	6	9
50	139	6	4
51	19321	6	9
52	151	6	3
53	22801	6	9
54	157	6	3
55	181	6	4
56	191	2	6
57	197	2	4
58	199	6	5
59	211	6	4
60	223	6	5
61	227	2	4
62	229	6	3
63	233	2	4
64	239	2	5
65	241	6	3
66	263	2	4

$Sr.No.$	q	l	s
67	269	2	6
68	271	6	3
69	277	6	4
70	281	2	5
71	283	6	3
72	293	2	4
73	311	2	5
74	331	6	4
75	359	2	6
76	367	6	4
77	389	2	6
78	397	6	5
79	401	2	5
80	409	6	4
81	431	2	7
82	439	6	4
83	463	6	4
84	491	2	5
85	499	6	4
86	509	2	5
87	547	6	4
88	571	6	4
89	593	2	5
90	601	6	4
91	607	6	4
92	613	6	5
93	619	6	4
94	631	6	4
95	643	6	4
96	659	2	5
97	661	6	5
98	683	2	5
99	691	6	6
100	709	6	4
101	727	6	5
102	733	6	4
103	739	6	4
104	743	2	5
105	877	6	5
106	919	6	6

$Sr.No.$	q	l	s
107	953	2	8
108	967	6	5
109	1021	6	5
110	1051	6	5
111	1063	6	5
112	1093	6	5
113	1123	6	6
114	1151	2	6
115	1171	6	5
116	1181	2	6
117	1231	6	6
118	1283	2	6
119	1301	2	6
120	1303	6	5
121	1321	6	5
122	1381	6	5
123	1399	6	5
124	1453	6	5
125	1481	2	6
126	1483	6	6
127	1499	2	6
128	1523	2	6
129	1531	6	6
130	1597	6	5
131	1607	2	6
132	1693	6	6
133	1723	6	5
134	1741	6	6
135	1759	6	5
136	1789	6	5
137	1801	6	6
138	1823	2	6
139	1877	2	6
140	1879	6	5
141	1951	6	7
142	2003	2	7
143	2141	2	7
144	2161	6	7
145	2281	6	6
146	2311	6	6

$Sr.No.$	p	k	m
147	2381	2	8
148	2591	2	7
149	2713	6	6
150	2731	6	7
151	2791	6	7
152	2887	6	6
153	2971	6	6
154	3041	2	7
155	3083	2	7
156	3191	2	7
157	3221	2	7
158	3229	6	6
159	3271	6	6
160	3301	6	7
161	3307	6	6
162	3313	6	6
163	3499	6	8
164	3547	6	8
165	3571	6	6
166	3739	6	6
167	3851	2	7
168	3911	2	7
169	4013	27	7
170	4159	6	6
171	4219	6	7
172	4241	2	7
173	4243	6	7
174	4261	6	6
175	4327	6	7
176	4421	2	7
177	4423	6	6
178	4567	6	6
179	4621	6	6
180	4663	6	6
181	4691	2	7
182	4751	2	7
183	4957	6	7
184	5419	6	7
185	5923	6	7
186	5981	2	8
187	6067	6	7
188	6211	6	7
189	6491	2	8

$Sr.No.$	p	k	m
190	6577	6	7
191	7159	6	7
192	7759	6	8
193	8009	2	9
194	8053	6	9
195	8191	6	7
196	8807	2	8
197	9103	6	7
198	9403	6	7
199	9421	6	7
200	9463	6	7
201	9719	2	8
202	9767	2	8
203	9871	6	7
204	9901	6	7
205	9967	6	7
206	10427	2	8
207	10949	2	10
208	10957	6	8
209	10979	2	8
210	11311	6	7
211	11593	6	7
212	11621	2	8
213	12959	2	9
214	14232	6	8
215	15313	6	8
216	15511	6	8
217	16381	6	8
218	17431	6	9
219	17491	6	9
220	19483	6	8
221	19687	6	8
222	19891	6	8
223	20011	6	8
224	20441	2	10
225	21391	6	8
226	22543	6	8
227	23143	6	8
228	23671	6	9
229	24181	6	8
230	24683	2	9
231	25171	6	9
232	25411	6	8

当 t=8 时:

$Sr.No.$	p	k	m
1	64	6	7
2	128	3	6
3	256	3	6
4	512	6	10
5	1024	3	8
6	81	2	5
7	243	2	6
8	125	6	6
9	49	6	4
10	343	6	9
11	121	6	5
12	169	6	5
13	361	6	6
14	529	6	7
15	841	6	7
16	961	6	7
17	53	6	5
18	59	6	6
19	61	6	4
20	67	6	6
21	71	6	4
22	73	6	5
23	79	6	6
24	89	6	6
25	97	6	5
26	101	6	5
27	103	6	5
28	107	6	5
29	109	6	6
30	113	6	5
31	127	6	6
32	131	6	6
33	137	6	7
34	139	6	6
35	149	6	6
36	151	6	6
37	157	6	7
38	163	6	5

$Sr.No.$	p	k	m
39	167	6	6
40	173	6	7
41	179	6	6
42	181	6	6
43	191	6	7
44	197	6	6
45	211	6	7
46	223	6	7
47	227	6	7
48	229	6	8
49	233	6	8
50	239	6	7
51	241	6	7
52	251	6	5
53	257	6	5
54	263	6	7
55	269	6	6
56	271	6	6
57	277	6	6
58	283	6	6
59	293	6	7
60	311	6	7
61	313	6	6
62	317	6	6
63	331	6	8
64	337	6	6
65	347	6	6
66	349	6	6
67	353	6	6
68	359	6	7
69	367	6	6
70	373	6	7
71	379	6	6
72	383	6	7
73	389	6	8
74	397	6	6
75	401	6	8
76	409	6	6

$Sr.No.$	p	k	m
77	433	6	7
78	439	6	7
79	443	6	7
80	457	6	7
81	467	6	7
82	491	6	7
83	499	6	8
84	509	6	7
85	521	6	7
86	523	6	6
87	541	6	6
88	547	6	8
89	557	6	7
90	563	6	9
91	569	6	6
92	571	6	9
93	587	6	7
94	593	6	8
95	599	6	8
96	601	6	7
97	617	6	8
98	619	6	7
99	631	6	7
100	647	6	7
101	653	6	7
102	661	6	7
103	683	6	7
104	691	6	7
105	701	6	7
106	709	6	7
107	733	6	7
108	739	6	7
109	743	6	9
110	757	6	8
111	773	6	8
112	787	6	8
113	797	6	8
114	809	6	8

$Sr.No.$	p	k	m
115	811	6	7
116	823	6	8
117	827	6	8
118	829	6	7
119	839	6	7
120	857	6	7
121	859	6	8
122	863	6	8
123	881	6	7
124	887	6	7
125	919	76	7
126	929	6	7
127	941	6	7
128	947	6	8
129	953	6	7
130	971	6	8
131	977	6	8
132	983	6	7
133	991	6	7
134	1009	6	7
135	1013	6	7
136	1021	6	8
137	1033	6	8
138	1039	6	8
139	1061	6	9
140	1063	6	8
141	1069	6	7
142	1087	6	7
143	1091	6	8
144	1093	6	7
145	1097	6	8
146	1103	6	8
147	1109	6	8
148	1117	6	8
149	1123	6	8
150	1201	6	9
151	1213	6	8
152	1223	6	9

$Sr.No.$	p	k	m
153	1231	6	8
154	1277	6	9
155	1279	6	8
156	1283	6	9
157	1289	6	9
158	1291	6	9
159	1303	6	8
160	1319	6	8
161	1321	6	8
162	191	6	7
163	911	30	9
164	659	30	8
165	1301	30	10

$Sr.No.$	p	k	m
166	281	30	6
167	410	30	6
168	421	30	8
169	937	30	7
170	1331	30	9
171	307	30	7
172	1217	30	7
173	967	30	8
174	461	30	7
175	463	30	7
176	853	30	9
177	727	30	7
178	729	30	9

当 **t=9** 时:

$Sr.No.$	p	k	m
1	8	7	2
2	32	7	5
3	27	2	5
4	81	14	7
5	25	6	5
6	125	2	7
7	49	6	5
8	121	6	6
9	13	6	2

$Sr.No.$	p	k	m
10	169	6	7
11	17	2	3
12	19	6	3
13	23	2	5
14	29	2	5
15	31	6	4
16	37	6	5
17	43	6	6
18	47	2	5

$Sr.No.$	p	k	m
19	53	2	7
20	61	6	5
21	79	6	5
22	83	2	6
23	137	2	7
24	139	6	6
25	149	2	7
26	157	6	6
27	211	6	7

当 **t=10** 时:

$Sr.No.$	p	k	m
1	8	3	5
2	16	3	6
3	32	3	6
4	64	6	9
5	9	2	4
6	27	2	7
7	25	6	6

$Sr.No.$	p	k	m
8	49	6	6
9	11	6	3
10	13	6	4
11	17	6	4
12	19	6	5
13	23	6	5
14	29	6	6

$Sr.No.$	p	k	m
15	31	6	5
16	37	6	5
17	41	6	6
18	53	6	6
19	59	6	7
20	61	6	6
21	67	6	6

当 **t=11** 时:

$Sr.No.$	p	k	m
1	16	3	6
2	9	2	4
3	7	2	3
4	13	2	5

当 **t=12** 时:

$Sr.No.$	p	k	m
1	8	39	6
2	16	39	7
3	32	39	9
4	9	2	6
5	13	6	6

$Sr.No.$	p	k	m
6	17	6	6
7	19	6	6
8	29	6	9
9	27	30	6

$Sr.No.$	p	k	m
10	11	30	6
11	23	30	7
12	31	30	6
13	37	30	8

当 **t=14** 时:

$Sr.No.$	p	k	m
1	4	15	4
2	5	6	3
3	7	6	4
4	3	2	2

当 **t=15** 时:

$Sr.No.$	p	k	m
1	4	3	5
2	3	2	3
3	9	2	7
4	5	2	5
5	16	15	9

对于 **t=16**:

$Sr.No.$	p	k	m
1	4	3	4
2	8	3	8
3	3	2	4
4	5	2	5

对于 t=18:

$Sr.No.$	p	k	m
1	3	2	5
2	4	15	6
3	5	6	5

当 t=20 时:

$Sr.No.$	p	k	m
1	4	3	6
2	8	15	9

当 t=22 时:

$Sr.No.$	p	k	m
1	2	15	2

当 t=24 时:

$Sr.No.$	p	k	m
1	4	3	8
2	3	2	6

当 t=28 时:

$Sr.No.$	p	k	m
1	2	15	4

当 t=30 时:

$Sr.No.$	p	k	m
1	2	3	5

当 t=36 时:

$Sr.No.$	p	k	m
1	2	15	6