arXiv:2305.01856v1 [math.NT] 3 May 2023

关于 $\mathbb{F}_q$ 上向量空间的素数幂剩余与线性覆盖

Bhawesh Mishra[a]

[a]俄亥俄州立大学数学系，231W 18^{th}大道，美国俄亥俄州哥伦布市，邮编 43210

摘要

设 q 为一个奇素数， $B=\{b_j\}_{j=1}^{l}$ 为一个不含完全 q^{th} 次幂的非零整数有限集。我们证明，对于每个不整除 $\prod_{b\in B} b$ 的素数 $p\neq q$ ， B 模 $p\neq q$ 有一个 q^{th} 次幂，当且仅当 B 对应于 $\mathbb{F}_q^k$ 的线性超平面覆盖。这里， k 是 B 中各元素的 q- 自由部分所含不同素因子的个数。因此：（i）基数小于 $q+1$ 的集合 $B\subset\mathbb{Z}\setminus\{0\}$，若不含完全 q^{th} 次幂，则不可能模几乎所有素数都有一个 q^{th} 次幂；（ii）对于每个集合 $B=\{b_j\}_{j=1}^{l}\subset\mathbb{Z}\setminus\{0\}$ 和每个 $\left(c_j\right)_{j=1}^{l}\in\left(\mathbb{F}_q\setminus\{0\}\right)^l$，集合 B 模每个不整除 $\prod_{j=1}^{l}$ 的素数 $p\neq q$ 都有一个 q^{th} 次幂，当且仅当集合 $\{b_j^{c_j}\}_{j=1}^{l}$ 也如此。

关键词：模几乎所有素数的素数幂，素数幂剩余。2020 MSC：11A15, 11A07

1. 引言

1.1. 历史与动机。

我们的出发点是以下关于模几乎所有素数含有二次剩余的集合的经典结果，该结果最初由 Friedin [3], 得出，后来由 Filaseta 和 Richman 在 [2] 中重新发现。

命题1. 设 a_1、a_2、.....、a_l 是有限个互不相同的非零整数。则以下三个条件等价：

1. 集合 $\{a_1,a_2,\ldots,a_l\}$ 中的元素模几乎所有素数都是平方数。

2. 对于每个奇素数 $p \nmid \prod_{j=1}^{l} a_j$，集合 $\{a_1, a_2, \ldots, a_l\}$ 中都含有模 p 的平方数。

3. 存在一个 $T \subseteq \{1, 2, \ldots, l\}$ 基数为奇数的集合，使得$\prod_{j\in T} a_j$是一个完全平方数。

A. Schinzel 和 M. Skalba 通过获得数域 K 的有限子集模几乎所有素数 [6, 包含 n^{th} 次幂（$n \geq 2$）的必要且充分条件，对命题 1 作了实质性的推广，见定理 1, 2]。然而，对于一般的 n^{th} 次幂而言，这些条件相当复杂。在后续论文中，M. Skalba 进一步简化了 $n = q$ 为素数 [7] 时的条件。当 $K = \mathbb{Q}$ 时，Skalba 的结果如下。

命题 2. 设 q 为素数， $B = \{b_1, b_2, \ldots, b_l\}$ 为一个由有限个互不相同的非零整数构成的集合。则以下条件等价:

1. 对几乎所有素数 p，集合 B 模 p 包含一个 q^{th} 次幂。

2. 对于每个素数 $p \neq q$ 和 $p \nmid \prod_{j=1}^{l} b_j$，集合 B 在几乎每个素数模下都包含一个 q^{th} 次幂。

3. 对于每个整数序列 $\{c_j\}_{j=1}^{l}$，都存在一个整数序列 $\{f_j\}_{j=1}^{l}$，使得

$$\sum_{j=1}^{l} f_j \not\equiv 0(\bmod q) \text{ and } \prod_{j=1}^{l} b_j^{c_j f_j} = d^q \text{ for some integer } d. \tag{1.1}$$

[6] 中的主要结果讨论了一个比模几乎所有素数都包含某些幂的集合更一般的问题，因此只陈述条件（1）与（3）等价。然而，由 [6] 中的结果可知，条件（1）和（3）实际上都等价于命题 2 中的条件（2）。回想一下，如果数域 K 包含复q^{th} 单位根 ζ_q，那么对于每个与 q 互素的 K 素理想 $\mathfrak{p}$ 以及每个$\mathfrak{p}$-进单位 $\alpha \in K$，我们将 q^{th} 幂剩余符号 $\left(\alpha|\mathfrak{p}\right)_q$ 定义为满足下述条件的唯一 q^{th} 单位根 ζ_q^j：

$$\alpha^{\frac{\mathrm{Norm}(\mathfrak{p})-1}{q}} \equiv \zeta_q^j \,(\bmod\, \mathfrak{p}).$$

在 [6] 中推导这些条件时，使用了幂剩余符号。因此，我们需要在上文命题 2 的条件 2 中排除 $p \neq q$ 和 $p \nmid \prod_{j=1}^{l} b_j$。这是为了确保 p 与 q 互素，并且整数 b_1、b_2、.....、b_l 是模 p的 p-进单位，从而所有幂剩余符号 $\left(b_j|p\right)_q$（例如 $1 \leq j \leq l$）都有定义。

容易看出，当 $q = 2$ 时，1 中的条件 (3) 实际上等价于 2 中的条件 (3)。这是因为，对于满足 $\sum_{j=1}^{l} f_j \neq 0$ 的整数序列 $\{f_j\}_{j=1}^{l}$，当项数 f_j 为奇数时，(mod 2) 与 $f_j \equiv 1$ (mod 2) 等价。

我们通过一个例子来讨论主要结果。考虑集合

$$B = \{p_1, p_2, p_1p_2, p_1p_2^2\} \tag{1.2}$$

其中 p_1 和 p_2 是两个不同于 3 的互异素数。容易看出，对任意素数 $p \notin \{3, p_1, p_2\}$，集合 B 都包含一个模 p 的三次剩余。例如，如果 p_1 和 p_2 都不是模 p 的立方数，则会出现两种情况。第一种情况是，p_1 和 p_2 位于模 $\left(\mathbb{F}_p^{\times}\right)^3$ 的 $\left(\mathbb{F}_p^{\times}\right)$ 的不同陪集中。在这种情况下，p_1p_2 是模 p 的立方数。另一种情况下，$p_1p_2^2$ 是模 p 的立方数。

我们将证明，上述例子中的集合 B 对应于 $\mathbb{F}_3^2$ 的一个线性覆盖（定义见第 1.3 小节）。更一般地，本文旨在证明，对于奇素数 q，有限集 $B \subset \mathbb{Z} \setminus \{0\}$ 中几乎对每个素数都包含一个模素数意义下的 q^{th} 次幂这一性质，等价于 B 对应于 $\mathbb{F}_q^k$ 的一个线性覆盖。这里，k 是整除 B 中各元素的 q 无因子部分的互异素数个数。我们还将在第 3 节中展示，这种方法能够为理解那些模除有限多个素数外均包含 q^{th} 次幂剩余的子集结构带来有趣的新见解。在陈述并证明主要结果之前，我们先介绍所需的一些记号和初等结果。

1.2. 正 q^{th} 次幂等价类内的调整。

除非另有说明，本文从此处起用 q 表示一个奇素数。我们假设集合 $B = \{b_j\}_{j=1}^{l} \subset \left(\mathbb{Z} \setminus \{0\}\right)$ 不包含完全的 q^{th} 次幂。否则，对于几乎所有素数，集合 B 都显然包含一个模 q^{th}次幂。由于当 q 是奇素数时，-1 是一个 q^{th} 次幂，因此负整数 b 是模 p 的 q^{th} 次幂，当且仅当 $-b$ 是模 p 的 q^{th}次幂。因此，不失一般性，我们可以假设集合 $B = \{b_j\}_{j=1}^{l}$ 只包含正整数。

给定一个不是完全 q^{th} 次幂的正整数 b，其唯一的素因数分解为 $\prod_{i=1}^{m} p_i^{a_i}$，则 b 的 q-自由部分可定义为

$$\mathrm{rad}_q(b) := \prod_{i=1}^{m} p_i^{a_i (\mathrm{mod}\ q)}.$$

因此，只要我们关注模素数 p 的幂剩余，对于 $p \neq q$ 和 $p \nmid \prod_{j=1}^{l} b_j$，在 $B = \{b_j\}_{j=1}^{l} \subset \mathbb{Z} \setminus \{0\}$ 中就可以用集合 B 替换集合

$$\left\{\mathrm{rad}_q\big(|b_j|\big)\right\}_{j=1}^{l}.$$

例如，当 $q = 3$ 时，可以用 $\{3, 13, 2\}$ 替换集合 $\{24, -104, 54\}$，因为 $24 = 2^3 \cdot 3$、$104 = 2^3 \cdot 13$ 和 $54 = 3^3 \cdot 2$。

1.3. 向量空间的线性覆盖。

设 V 是域 K 上维数为 $k \geq 2$ 的向量空间。V 的线性覆盖是由真子空间 $\{W_i\}_{i \in I}$ 组成的集合，满足 $V = \bigcup_{i \in I} W_i$。向量空间 V 的线性覆盖数记为 # LC(V)，它是 V 的线性覆盖的最小基数。我们将使用关于 # LC(V) 的以下事实，这是在 [1] 中证明的主要结果的一部分。

命题 3. 对于每个维数为 ≥ 2 的 $\mathbb{F}_q$ 向量空间 V，我们有 #LC(V) =q + 1。

我们还将用到一个著名结果，该结果通过零空间的包含关系刻画向量空间上线性泛函的线性相关性。更具体地说，我们将采用 [5, pp. 110, Theorem20] 中给出的以下结果。

命题 4. 设 $g, f_1, f_2, \ldots, f_r$ 是向量空间 V 上的线性泛函，其对应的零空间分别为 $N, N_1, N_2, \ldots, N_r$。那么，g 是 $f_1, f_2, \ldots, f_r$ 的线性组合，当且仅当 $\bigcap_{j=1}^{r} N_j \subseteq N$。

陈述结果所需的最后一个要素，是将整数的有限子集与 $\mathbb{F}_q$ 向量空间中的某个超平面集合对应起来。

1.4. 整数的有限子集与向量空间中的超平面。

设 $p_1, p_2, \ldots, p_k$ 为有限多个素数，它们整除集合 $\{\mathrm{rad}_q(|b_j|) : 1 \le j \le l\}$ 中的某个元素。设 $\nu_{ij} \ge 0$ 满足：对每个 $1 \le i \le k$ 和每个 $1 \le j \le l$，都有 $p_i^{\nu_{ij}} \mid\mid \mathrm{rad}_q(|b_j|)$。考虑在 $\mathbb{F}_q^k$ 中定义的超平面方程

$$\sum_{i=1}^{k} \nu_{ij} x_i = 0 \text{ for } 1 \le j \le l,$$

其中变量为 $x_1, x_2, \ldots, x_k$。我们称集合

$$\Big\{ \sum_{i=1}^{k} \nu_{ij} x_i = 0 : 1 \le j \le l \Big\},$$

为与 $B = \{b_1, b_2, \ldots, b_l\}$ 相关联的 $\mathbb{F}_q^k$ 中超平面的集合。

在上述定理中，我们假设 $k \ge 2$，因为容易证明，对于任意素数 p_1，都存在无穷多个素数 p，使得集合 $B = \{p_1, p_1^2, \ldots, p_1^{q-1}\}$ 不含模 p 的 q^{th} 次幂。例如，我们注意到，伽罗瓦扩张 $\mathbb{Q}\big(p_1^{1/q}, \zeta_q\big)/\mathbb{Q}$ 是不可约多项式 $f(x) = x^q - p_1$ 的分裂域。这里 ζ_q 是一个本原 q^{th} 单位根。该扩张的伽罗瓦群 G 是 $\big(\mathbb{Z}/q\mathbb{Z}\big)$ 与 $\big(\mathbb{Z}/q\mathbb{Z}\big)^{\times}$ 的半直积。中间扩张 $\mathbb{Q}\big(p_1^{1/q}, \zeta_q\big)/\mathbb{Q}\big(p_1^{1/q}\big)$ 的自同构群 H 同构于 $\big(\mathbb{Z}/q\mathbb{Z}\big)^{\times}$，并在 G 中构成一个共轭类 $\mathcal{C}$。因此，应用切博塔廖夫密度定理（例如参见 [4, 第 58 页，定理 5.6]），可得使多项式 f 仍然不可约的模素数集合的密度为 $\frac{|\mathcal{C}|}{|G|} = \frac{q-1}{q\ q-1}() = \frac{1}{q}$。换言之，使 p_1 不是模素数的 q^{th} 次幂的素数集合密度为 $\frac{1}{q}$。我们的主要结果如下定理所示。

定理 1. 设 q 是一个奇素数，且 $B = \{b_1, b_2, \ldots, b_l\} \subset \mathbb{Z} \setminus \{0\}$ 不含完全的 q^{th} 次幂。设 $p_1, p_2, \ldots, p_k (k \ge 2)$ 是所有整除 $\{\mathrm{rad}_q(|b_j|)$ 中元素的素数：$1 \le j \le l\}$，使得对每个 $1 \le i \le k$ 和每个 $1 \le j \le l$，均有 $p_i^{\nu_{ij}} \mid\mid \mathrm{rad}_q(|b_j|)$。那么，以下三个条件等价：

1. 集合 B 中的元素模几乎所有素数都是一个 q^{th} 次幂。

2. 对于每个素数 $p \ne q$ 且不整除 $\prod_{j=1}^{l} b_j$，集合 B 模 p 含有一个 q^{th} 次幂。

3. 超平面的集合

$$\Big\{\sum_{i=1}^{k}\nu_{ij}x_i=0:1\le j\le l\Big\}$$

与 B 相关，包含 $\mathbb{F}_q^k$ 的一个线性覆盖。

2. 定理 1 的证明

如第 1.2 小节所述，不失一般性，我们可以假设 B 的元素为正且 q-free。因此，从现在起，我们将在定理 1 的表述中用 b_j 替换 $\mathrm{rad}_q(|b_j|)$。由于对于每个 $1\le i\le k$ 和每个 $1\le j\le l$，$p_i^{\nu_{ij}}\ ||\ b_j$，我们对每个 $1\le j\le l$ 都有 $b_j=\prod_{i=1}^{k}p_i^{\nu_{ij}}$。因此，条件

$$\prod_{j=1}^{l}b_j^{c_jf_j}=d^q$$

在等式 1.1 中可以改写为

$$\prod_{j=1}^{l}\Big(\prod_{i=1}^{k}p_i^{\nu_{ij}}\Big)^{c_jf_j}=d^q\Leftrightarrow\prod_{j=1}^{l}\Big(\prod_{i=1}^{k}p_i^{\nu_{ij}c_jf_j}\Big)=d^q$$

$$\Leftrightarrow\sum_{j=1}^{l}\nu_{ij}c_jf_j\equiv0\ (\mathrm{mod}\ q)\ \text{for every}\ 1\le i\le k.\quad(2.1)$$

因此，只需考虑命题 2 的条件（2）中的 c_j、$f_j\in\mathbb{F}_q$。我们还注意到，如果对于某个 $1\le j_0\le l$ 有 $c_{j_0}=0$，那么取 $f_j=\begin{cases}0,&j=j_0\\1,&j\ne j_0\end{cases}$，即可直接解出方程（2.1），从而满足命题 2 中的条件（2）。因此，我们只需考虑 $(c_j)_{j=1}^{l}\in\big(\mathbb{F}_q\setminus\{0\}\big)^l$。

同余方程组

$$\sum_{j=1}^{l}\nu_{ij}c_jf_j\equiv0\ (\mathrm{mod}\ q),\ 1\le i\le k$$

可写为

$$M\left((c_j)_{j=1}^{l}\right) \times F = 0 \tag{2.2}$$

在域 $\mathbb{F}_q$ 上，其中 $M\left((c_j)_{j=1}^{l}\right)$ 是一个 $(k \times l)$ 矩阵，其第 ij 个元素由 M_{ij}给出：$= \nu_{ij} c_j$且 $F = \begin{bmatrix} f_1 \\ f_2 \\ \ldots\ldots \\ f_l \end{bmatrix}$。现在，我们证明一个引理，用另

一个等价命题替代命题 2 中的条件 3。

引理 2。使用第 2 节中定义的记号，以下三个陈述等价。

A. 命题 2 中的条件 3。B. 对每个 $(c_j)_{j=1}^{l} \in \left(\mathbb{F}_q \setminus \{0\}\right)^l$，都存在 $(f_j)_{j=1}^{l} \in \left(\mathbb{F}_q \setminus \{0\}\right)^l$，使得对于每个 $1 \leq i \leq k$，$\sum_{j=1}^{l} \nu_{ij} c_j f_j \equiv 0$（模 q），且 $\sum_{j=1}^{l} f_j \not\equiv 0$（模 q）。C. 对每个 $(c_j)_{j=1}^{l} \in \left(\mathbb{F}_q \setminus \{0\}\right)^l$，矩阵 $M\left((c_j)_{j=1}^{l}\right)$的行空间不包含 $\begin{bmatrix} 1 & 1 & \ldots & 1 \end{bmatrix}$。

证明。设 $(c_j)_{j=1}^{l} \in \left(\mathbb{F}_q \setminus \{0\}\right)^l$。根据第 2 节，条件 A与B的等价性成立，因为 $\sum_{j=1}^{l} \nu_j c_j f_j \equiv 0$(模 q)等价于如下事实：$F = \begin{bmatrix} f_1 \\ f_2 \\ \ldots\ldots \\ f_l \end{bmatrix}$ 属于 $M\left((c_j)_{j=1}^{l}\right)$的零空间，正如(2.2)中所述。现在我们证明条件 B 与 C的等价性。

由于任意一个大小为 $1 \times l$ 的行 R 都会在 $\mathbb{F}_q^l$ 上诱导一个线性泛函 $v \longmapsto R \times v$，根据命题 4，条件 C 等价于

$$\mathrm{Null}\left(M\left((c_j)_{j=1}^{l}\right)\right) = \bigcap_{i=1}^{k} \mathrm{Null}(R_i) \not\subseteq \mathrm{Null}(\begin{bmatrix} 1 & 1 & \ldots & 1 \end{bmatrix}).$$

这里， R_i 是矩阵 $M\Big((c_j)_{j=1}^{l}\Big)$ 的第 i^{th} 行，其中 $1 \le i \le k$。换言之，条件 C 等价于存在

$$F = \begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_l \end{bmatrix} \in \bigcap_{i=1}^{k} \mathrm{Null}(R_i) = \mathrm{Null}\left(M\Big((c_j)_{j=1}^{l}\Big) \right)$$

使得 $\sum_{j=1}^{l} f_j \not\equiv 0$ （模 q）。 □

因此，由命题 2 可知，为了证明定理 1，我们需要证明以下两个命题等价。

(I) For every $(c_j)_{j=1}^{l} \in \Big((\mathbb{F}_q) \setminus \{0\}\Big)^l$ the linear span of rows of $M\Big((c_j)_{j=1}^{l}\Big)$ does not contain the vector $\begin{bmatrix} 1 & 1 & \dots & 1 \end{bmatrix}$.

(II) 超平面集合

$$\Big\{ \sum_{i=1}^{k} \nu_{ij} x_i = 0 : 1 \le j \le l \Big\}$$

与 B 相关联，且包含 $\mathbb{F}_q^k$ 的一个线性覆盖。

2.1. (II) 推出 (I) 的证明

假设超平面集合

$$\Big\{ \sum_{i=1}^{k} \nu_{ij} x_i = 0 : 1 \le j \le l \Big\}$$

与 B 相关联，包含 $\mathbb{F}_q^k$ 的一个线性覆盖。剩下需要证明的是，不存在 $\big(\mathbb{F}_q \setminus \{0\}\big)$ 的线性组合，使 $M\Big((c_j)_{j=1}^{l}\Big)$ 的行组合等于 $\begin{bmatrix} 1 & 1 & \dots & 1 \end{bmatrix}$。

设 $(c_j)_{j=1}^{l} \in \big(\mathbb{F}_q \setminus \{0\}\big)^l$，并令 $R_1, R_2, \dots, R_k$ 为矩阵$M\big((c_j)_{j=1}^{l}\big)$的行。换句话说，

$$R_i := \begin{bmatrix} c_1\nu_{i1} & c_2\nu_{i2} & \dots & c_l\nu_{il} \end{bmatrix} \text{ for every } 1 \le i \le k.$$

设 d_1、d_2、.....、$d_k \in \mathbb{F}_q$，并考虑行的线性组合 $d_1R_1 + d_2R_2 + \ldots + d_kR_k$，其等于

$$\begin{bmatrix} c_1\big(\sum_{i=1}^k d_i\nu_{i1}\big) & c_2\big(\sum_{i=1}^k d_i\nu_{i2}\big) & \ldots & c_1\big(\sum_{i=1}^k d_i\nu_{il}\big) \end{bmatrix}.$$

由于超平面集合 $\left\{\sum_{i=1}^k \nu_{ij}x_i = 0\colon\ 1 \le j \le l\right\}$ 包含 $\mathbb{F}_q^k$ 和 $(d_i)_{i=1}^k \in \mathbb{F}_q^k$的一个线性覆盖，因此存在 $1 \le j_0 \le l$ 使得$\sum_{i=1}^k \nu_{ij_0}d_i = 0$。换言之，$d_1R_1 + d_2R_2 + \ldots + d_kR_k$的某个元素等于零，因此不可能等于行矩阵 $\begin{bmatrix}1 & 1 & \ldots & 1\end{bmatrix}$。由于 $(c_j)_{j=1}^l \in \big(\mathbb{F}_q \setminus \{0\}\big)^l$ 和 $d_1, d_2, \ldots, d_k \in \mathbb{F}_q$ 均为任意选取，故这一方向的证明完成。 □

2.2. 证明 (I) 推出 (II)

设超平面集合

$$\left\{\sum_{i=1}^k \nu_{ij}x_i = 0 : 1 \le j \le l\right\}$$

不包含 $\mathbb{F}_q^k$ 的线性覆盖。我们将证明，对于某个 $(c_j)_{j=1}^l \in \big(\mathbb{F}_q \setminus \{0\}\big)^l$，矩阵 $M\big((c_j)_{j=1}^l\big)$ 的某个行线性组合等于 $\begin{bmatrix}1 & 1 & 1 \ldots & 1\end{bmatrix}$。

由于集合 $\left\{\sum_{i=1}^k \nu_{ij}x_i = 0\colon\ 1 \le j \le l\right\}$ 不包含 $\mathbb{F}_q^k$ 的线性覆盖，因此存在 $(d_1, d_2, \ldots, d_k) \in \mathbb{F}_q^k$ 使得

$$\sum_{i=1}^k \nu_{ij}d_i \ne 0 \text{ for any } 1 \le j \le l.$$

定义

$$c_j := \big(\sum_{i=1}^k \nu_{ij}d_i\big)^{-1} \in \mathbb{F}_q \setminus \{0\} \text{ for every } 1 \le j \le l.$$

考虑与 $(c_j)_{j=1}^l$ 相关联的矩阵 $M\big((c_j)_{j=1}^l\big)$，并令 $R_1, R_2, \ldots, R_k$ 为其各行，即

$$R_i := \begin{bmatrix} c_1\nu_{i1} & c_2\nu_{i2} & \ldots & c_l\nu_{il}\end{bmatrix} \text{ for every } 1 \le i \le k.$$

如上一小节所示，$d_1R_1 + d_2R_2 + \ldots + d_kR_k$ 个行的线性组合等于

$$\begin{bmatrix} c_1\big(\sum_{i=1}^k d_i\nu_{i1}\big) & c_2\big(\sum_{i=1}^k d_i\nu_{i2}\big) & \ldots & c_1\big(\sum_{i=1}^k d_i\nu_{il}\big)\end{bmatrix} = \begin{bmatrix}1 & 1 & \ldots & 1\end{bmatrix}.$$

最后一个等式由 c_j 的定义得出。 □

3. 推论与示例。

3.1. 推论。

我们的第一个推论为这样的整数子集的基数给出了下界：它们模几乎所有素数都包含一个 q^{th} 次幂，但不包含一个完全 q^{th} 次幂。

推论 1。若集合 $B \subset \mathbb{Z}$ 满足 $|B| < q+1$，且符合定理 1 中的条件，则 B 包含一个完全 q^{th} 次幂。更具体地说，基数小于 $q+1$ 的非零整数集合，几乎对每个素数都包含一个模 q^{th} 次幂，当且仅当 B 包含一个完全 q^{th} 次幂。

证明。假设 $|B| = l$，且 B 不包含完全 q^{th} 次幂，则定理 1 表明，与 B 相关联的 l 个超平面集合必定包含 $\mathbb{F}_q^k$ 的一个线性覆盖。然而，命题 3 表明，任何此类线性覆盖至少包含 $q+1$ 个元素，因此 $|B| = l \geq q+1$。

□

定理 1 还表明，给定的有限整数集 B 是否几乎对每个素数都包含一个模 q^{th} 次幂这一性质，在以下意义下对 $\mathbb{F}_q \setminus \{0\}$ 中元素的乘方运算保持不变。

推论 2. 设 $B = \{b_1, b_2, \ldots, b_l\} \subset \mathbb{Z}$、$(a_j)_{j=1}^l \in \big(\mathbb{F}_q \setminus \{0\}\big)^l$ 和

$$B' := \big\{b_j^{a_j} : 1 \leq j \leq l\big\}.$$

那么，B 满足定理 1 中的条件，当且仅当 B' 满足定理 1 中的条件。

证明。不失一般性，我们可以假设 B 不包含一个完全的 q^{th} 次幂。否则，B' 也包含一个完全的 q^{th} 次幂，并且B 和 B' 模几乎所有素数都包含一个 q^{th} 次幂。

设 $p_1, p_2, \ldots, p_k$ 为所有整除 $\big\{\mathrm{rad}_q(|b_j|)\big\}_{1\leq j\leq l}$ 中某个元素的素数。对于每个 $1 \leq j \leq l$ 和每个 $1 \leq i \leq k$，令 $\nu_{ij} \geq 0$ 满足 $p_i^{\nu_{ij}} \mid\mid b_j$。那么，与集合 B 相关联的 $\mathbb{F}_q^k$ 中超平面的集合等于

$$H := \Big\{ \sum_{i=1}^{k} \nu_{ij} x_i = 0 \text{ for } 1 \leq j \leq l. \Big\}$$

由于 $p_i^{\nu_{ij}} \mid\mid b_j$，我们有 $p_i^{a_j\nu_{ij}} \mid\mid b_j^{a_j}$。因此，与集合 B' 相关联的 $\mathbb{F}_q^k$ 中超平面的集合等于

$$H' := \Big\{ \sum_{i=1}^{k} a_j \nu_{ij} x_i = 0 \text{ for } 1 \le j \le l \Big\} = \Big\{ \sum_{i=1}^{k} \nu_{ij} x_i = 0 \text{ for } 1 \le j \le l \Big\} = H.$$

由于与 $\mathbb{F}_q^k$ 相关联的超平面集合等于与 $\mathbb{F}_q^k$ 相关联的超平面集合，定理 1 蕴含该推论。

□

3.2. 例子。

作为定理 1 的一个应用，我们现在给出一些说明性例子，这些例子中的集合对 $q = 3$ 而言在几乎每个素数模 q^{th} 次幂都包含一个 $q = 5$。

1. 现在我们将使用定理 1 来证明集合

$$B = \{p_1, p_2, p_1p_2, p_1p_2^2\}$$

如例 (1.2) 中所示，对每个满足 $p \nmid 3p_1p_2$ 的素数 p，该集合模该素数都包含一个立方数。这里，令 p_1、p_2 为两个不同于 3 的互异素数。
注意，超平面集合

$$H := \big\{x_1 = 0, x_2 = 0, x_1 + x_2 = 0, x_1 + 2x_2 = 0\big\}$$

构成了 $\mathbb{F}_3^2$ 的一个线性覆盖，因为每个 $(c_1, c_2) \in \mathbb{F}_3^2$ 都满足 H 中至少一个方程。因此，定理 1 表明集合

$$B = \{p_1, p_2, p_1p_2, p_1p_2^2\}$$

模几乎所有素数都包含一个立方数。

2. 利用 (1) 和推论 2，可以得到 $|\big(\mathbb{F}_3 \setminus \{0\}\big)^4| - 1 = 15$ 更多满足以下条件的集合例子：

$$\Big\{\{p_1^{a_1}, p_2^{a_2}, p_1^{a_3}p_2^{a_3}, p_1^{a_4}p_2^{2a_4}\} : (a_j)_{j=1}^4 \in \big(\mathbb{F}_3 \setminus \{0\}\big)^4\Big\}$$

满足以下条件：

- 这些集合中的每一个在模几乎所有素数时都包含一个立方数。

- 这些集合中元素的素因子只有 p_1 和 p_2。
- 这些集合都对应于 1 中相同的 $\mathbb{F}_3^2$ 线性超平面覆盖。

3. 设 p_1、p_2、p_3 是三个不同于 5 的互异素数，并设

$$B = \{p_1, p_2p_3, p_1p_2p_3, p_1^2p_2p_3, p_1^3p_2p_3, p_1^4p_2p_3\}.$$

注意，

$$\begin{aligned}
&\nu_{11} = 1, \nu_{12} = 0, \nu_{13} = 1, \nu_{14} = 2, \nu_{15} = 3, \nu_{16} = 4\\
&\nu_{21} = 0, \nu_{22} = 1, \nu_{23} = 1, \nu_{24} = 1, \nu_{25} = 1, \nu_{26} = 1\\
&\nu_{31} = 0, \nu_{32} = 1, \nu_{33} = 1, \nu_{34} = 1, \nu_{35} = 1, \nu_{36} = 1,
\end{aligned}$$

因此，与 B 相关联的超平面集合为

$$\Big\{x_1 = 0, x_2 + x_3 = 0, x_1 + x_2 + x_3 = 0, 2x_1 + x_2 + x_3 = 0,\\ 3x_1 + x_2 + x_3 = 0, 4x_1 + x_2 + x_3 = 0\Big\},$$

不难看出，这构成了 $\mathbb{F}_5^3$的线性覆盖。这是因为每个 $(x_j)_{j=1}^3 \in \mathbb{F}_5^3$ 都满足上述超平面方程之一。因此，集合 B 满足定理 1，并且模几乎所有素数都是一个五次幂。

4. 与 (2) 类似，利用 (3) 和推论 2，可以得到

$$|\big(\mathbb{F}_5 \setminus \{0\}\big)^6| - 1 = 4^6 - 1 = 4095$$

更多满足以下条件的例子：

- 这些集合中各元素的素因子只有 p_1、p_2 和 p_3。
- 这些集合中的每一个在几乎所有素数模下都包含一个五次幂。

- 这些集合中的每一个都对应于式 (3) 中 $\mathbb{F}_5^3$ 的同一个线性超平面覆盖。

致谢

本文当前版本的完善，在很大程度上得益于两位审稿人提出的宝贵意见和建议，这些意见和建议极大地改进了本文的阐述。

参考文献

[1] Clark, L. Pete.（2012）。线性代数中的覆盖数。《美国数学月刊》119:1，65-67。[2] Filaseta, M. A., Richman, D. R.（1989）。几乎对所有 p，都含有模 p 二次剩余的集合。《冈山大学数学杂志》31，1–8。[3] Fried, M.（1969）。多项式值集的算术性质。《算术学报》15，91–115。[4] Fried, M. D. 和 Jarden, M.《域算术》，第2版。数学及其边界领域成果。第3辑。现代数学综述丛书，第11卷。施普林格出版社，柏林，2005年。[5] Hoffman, K. 和 Kunze, R.《线性代数》，第2版。普伦蒂斯-霍尔，新泽西州，1971年。[6] Schinzel, A., Skalba, M.（2003）。关于幂剩余。《算术学报》108(1)，77–94。[7] Skalba, M.（2005）。几乎对所有素数模数都含有 q^{th} 幂剩余的集合。《数学讨论》102(1)，67–71。