arXiv:2304.02946v1 [math.NT] 6 Apr 2023

关于多项式映射的 Bhargava 阶乘

Wataru Takeda

摘要。Bhargava 引入了阶乘函数的一种推广，以将整数中的经典结果推广到 Dedekind 环，并将它们统一起来。我们从解析的角度研究多项式映射像集的 Bhargava 阶乘。首先，我们给出多项式映射像集的 $\mathfrak{p}$-进闭包，这是计算 Bhargava 阶乘的 $\mathfrak{p}$-进部分的关键。然后，作为一个特例，我们给出具有整数系数的二次多项式像集的斯特林公式。

1. 引言

Bhargava 推广了阶乘函数 $l!$，以将 $\mathbb{Z}$ 中的经典结果推广到 Dedekind 环并将它们统一起来 [2, 4]。设 S 是 Dedekind 环R的一个无限子集。首先，对于 R的素理想 $\mathfrak{p}$，我们定义 S 的一个 $\mathfrak{p}$-序列。S 的一个 $\mathfrak{p}$-序列是由 S 中的元素构成的任意序列 $(a_n)_{n=0}^{\infty}$，其构造如下:

- 我们任取一个元素 $a_0 \in S$;
- 对于 $k \geq 1$，我们选取一个元素 $a_n \in S$，使得

$$v_{\mathfrak{p}}^R\left(\prod_{k=0}^{n-1}(a_n - a_k)\right) = \inf_{x\in S} v_{\mathfrak{p}}^R\left(\prod_{k=0}^{n-1}(x - a_k)\right),$$

其中，$v_{\mathfrak{p}}^R$是由 $v_{\mathfrak{p}}^R(a) = \max\{v \geq 0 \mid \mathfrak{p}^v | (a)R\}$ 定义的 $\mathfrak{p}$-进赋值。对于 S 的一个 $\mathfrak{p}$-序，我们构造如下 $\mathfrak{p}$-序列 $(v_{\mathfrak{p}}(n; S))_{n=1}^{\infty}$：

$$v_{\mathfrak{p}}^R(n; S) = v_{\mathfrak{p}}^R\left(\prod_{k=0}^{n-1}(a_n - a_k)\right).$$

已知，S 的相应 $\mathfrak{p}$-序列与 S 的 $\mathfrak{p}$-序的选取无关。在这些设定下，我们定义 Bhargava 阶乘 $l!_S^R$ 为

$$l!_S^R = \prod_{\mathfrak{p}:\text{prime ideal}} \mathfrak{p}^{v_{\mathfrak{p}}^R(l;S)}.$$

设 $R_{\mathfrak{p}}$ 是 R 在 $\mathfrak{p}$ 处的局部化。那么，$R_{\mathfrak{p}}$ 是一个极大理想为 $\mathfrak{m} = \mathfrak{p}R_{\mathfrak{p}}$、赋值为 $v_{\mathfrak{m}}^{R_{\mathfrak{p}}}$ 的离散赋值环。我们用 $\tau\colon R \to R_{\mathfrak{p}}$ 表示将 R 嵌入 $R_{\mathfrak{p}}$ 的标准嵌入。根据定义，可以确认

$$v_{\mathfrak{m}}^{R_{\mathfrak{p}}}(l; \tau(S)) = v_{\mathfrak{p}}^R(l; S). \tag{1.1}$$

在不引起混淆的情况下，本文分别使用缩写 $v_{\mathfrak{p}}(l; S)$ 和 $l!_S$ 来表示$v_{\mathfrak{p}}^R(l;\ S)$ 和 $l!_S^R$。

2020 数学学科分类。 13F20, 11C08,11B83。关键词与短语。 Bhargava 阶乘、离散赋值环、斯特林公式。

现在给出一些 Bhargava 阶乘的例子。当 $S = R = \mathbb{Z}$ 时，对于所有素数 p，我们可以选择自然序 0、1、2、3、.....作为 $l!_S$ 的 p-序，并发现$l!_S$ 就是通常的阶乘 $l!$ 此外，当 $S(a,b) = \{an + b \mid n \in \mathbb{Z}\}$ 对某些 a、$b \in \mathbb{Z}$成立时，则有 $l!_{S(a,b)} = a^l l!$ 。

Bhargava 在 [4] 中提出了多变量的推广，并指出 Bhargava 阶乘的性质的类似结论也适用于这种推广。Evrard[6] 将 Bhargava 阶乘推广到多变量情形，并在 [4]中证明了 Bhargava 所有的断言。几年后，Rajkumar、Reddy 和 Semwal 也提出了这一阶乘的一种推广 [9]。这些论文将 $\mathbb{Z}$ 中的经典代数性质推广到了任意子集 $\underline{S} \subset R^n$。

另一方面，Bhargava 还在 [4]中提出了许多分析方面的问题。例如，问题 31：“广义阶乘的 Stirling 公式有哪些类似形式？”最近，Daiz 获得了素数集合 $\mathbb{P}$ 以及与 www.oeis.org 上编号为 A202367 的数列相关的某个集合 S 的渐近公式。 [5]。更确切地说，证明了

$$\log(l+1)!_{\mathbb{P}} = \log l! + Cl + o(l),$$

其中

$$C = \sum_{p \in \mathbb{P}} \frac{\log p}{(p-1)^2} = 1.2269688\cdots$$

以及 $l!_S$的类似形式公式。本文还研究了多项式映射 $f(R)$ 的像的 Bhargava 阶乘的分析性质，并给出了某个子集 $\mathbb{Z}$的 Bhargava 阶乘的一个分析估计。这对 Bhargava 的问题 [4]给出了部分解答。

本文其余部分的概述如下。第 2节回顾Bhargava阶乘的$\mathfrak{p}$-进部分仅取决于 S 的 $\mathfrak{p}$-进闭包 $\overline{S}^{\mathfrak{p}}$ ，并证明亨塞尔引理的一种弱形式，以确定 $f(R)$的 $\mathfrak{p}$-进闭包。随后，在第 3节中，我们在R 是主理想整环的假设下，研究二次多项式 $f(x) \in R[x]$ 。根据 (1.1)，这一假设并不限制所讨论的情形。在本文的主要结果之一——定理3.1 中，我们除一种情形外，给出了$f(R)$的 $\mathfrak{p}$-进闭包。第 4 节处理 $R = \mathbb{Z}$ 的情形。当 f 是二次多项式时，我们可以刻画任意 $\mathfrak{p}$ 下 $f(\mathbb{Z})$ 的 $\mathfrak{p}$-进闭包。作为其推论之一，我们给出了 Bhargava 阶乘的一种斯特林公式。

2. Bhargava 阶乘的 $\mathfrak{p}$-进部分估计

本节中，我们证明计算 $v_{\mathfrak{p}}(l;\ f(R))$ 的关键结果，其中 $f(x) \in R[x]$。以下事实说明，只需考虑 R 中 S 的 $\mathfrak{p}$-进闭包 $\overline{S}^{\mathfrak{p}}$ 。

引理 2.1 ([1])。设 $S \subset T$ 是 Dedekind 环 R 的两个子集，且 R 中的 $\mathfrak{p}$ 是一个素理想。那么，以下断言等价：

(1) 对所有 $l \in \mathbb{Z}_{\geq 0}$，$v_{\mathfrak{p}}(l;\ S) = v_{\mathfrak{p}}(l;\ T)$；(2) R 中 S 和 T 的 $\mathfrak{p}$-进闭包 $\overline{S}^{\mathfrak{p}}$ 和 $\overline{T}^{\mathfrak{p}}$ 相等。

本文聚焦于 $f(R)$ 的 Bhargava 阶乘。为了解决这一问题，我们引入以下引理，利用多项式的优势。该

引理是亨塞尔引理的弱形式。（关于原始亨塞尔引理的详细内容，请参见 [8] 。）

引理 2.2 (亨塞尔引理的弱形式)。 设 R 为一个主理想整环。对于 R的一个固定素理想 $\mathfrak{p} = (\pi)$，我们假设剩余域 $k = R/\mathfrak{p}$ 是有限的。我们记 $C_{\mathfrak{p}}$ 为关于 $R/\mathfrak{p}$的完备的不重复代表系。于是，对于任意多项式 $f(x) \in R[x]$ 和 $a \in C_{\mathfrak{p}}$，以下第一条断言蕴含以下第二条断言。

(1) 存在 $b \in R$ 使得 $f(b) \equiv a$ 模 $\mathfrak{p}$ 且 $f'(b) \notin \mathfrak{p}$。 (2) 对任意正整数 k 以及任意 $c_i \in C_{\mathfrak{p}}$，存在 $b \in R$ 使得$f(b) \equiv a + c_1\pi + \cdots + c_{k-1}\pi^{k-1}$ 模 $\mathfrak{p}^k$。

证明。令 $f(x) = \sum_{i=0}^{n} a_i x^i$。考虑模 $\mathfrak{p}$下带有 $c \equiv a$ 的 $R/\mathfrak{p}^k$ 的代表元 $c \in C_{\mathfrak{p}}$的数量，只需证明：若 $f(b+\beta_1\pi) \equiv f(b+\beta_2\pi)$模 $\mathfrak{p}^k$，则 $\beta_1 \equiv \beta_2$ 模 $\mathfrak{p}^{k-1}$。减去 $f(b+\beta_1\pi) - f(b+\beta_2\pi)$，可得

$$\begin{aligned} f(b+\beta_1\pi) - f(b+\beta_2\pi) &= (\beta_1-\beta_2)\sum_{i=1}^{n} \frac{f^{(i)}(b)}{i!}\frac{\beta_1^i-\beta_2^i}{\beta_1-\beta_2}\pi^i \\ &= (\beta_1-\beta_2)\left(\sum_{i=2}^{n} \frac{f^{(i)}(b)}{i!}\frac{\beta_1^i-\beta_2^i}{\beta_1-\beta_2}\pi^i + f'(b)\pi\right). \end{aligned}$$

根据假设 $f'(b) \notin \mathfrak{p}$，最后一个公式的第二个因子

$$\sum_{i=2}^{n} \frac{f^{(i)}(b)}{i!}\frac{\beta_1^i-\beta_2^i}{\beta_1-\beta_2}\pi^i + f'(b)\pi \not\equiv 0 \mod \mathfrak{p}^2.$$

因此，若 $f(b+\beta_1\pi) \equiv f(b+\beta_2\pi)$mod $\mathfrak{p}^k$，则 $\beta_1 \equiv \beta_2$ mod $\mathfrak{p}^{k-1}$。这就是所需的结论。□

对于固定的模 $R/\mathfrak{p}$ 的一组完全剩余系 $C_{\mathfrak{p}}$，我们将 $C_{\mathfrak{p}}$ 的两个子集定义为

$$S_{f,\mathfrak{p}} = \{a \in C_{\mathfrak{p}} \mid \exists b, f(b) \equiv a \mod \mathfrak{p}, f'(b) \not\equiv 0 \mod \mathfrak{p}\}$$

and

$$S^{-}_{f,\mathfrak{p}} = \{a \in C_{\mathfrak{p}} \mid \exists b, f(b) \equiv a \mod \mathfrak{p}, f'(b) \equiv 0 \mod \mathfrak{p}\}.$$

例如，如果 $f(x) = x^2$ 那么$S_{f,\ \mathfrak{p}}$ 是模 $\mathfrak{p}$ 的二次剩余集合，不包括 0。

推论 2.3. 设 $\mathfrak{p} = (\pi)$ 是主理想整环 R 中的一个素理想，且令$f(x) \in R[x]$。那么

$$\overline{f(R)}^{\mathfrak{p}} = \bigsqcup_{a \in S_{f,\mathfrak{p}}} (a + \mathfrak{p}) \sqcup E,$$

其中 E 由 S_f^- 、$_{\mathfrak{p}} \setminus S_{f、\mathfrak{p}}$ 导致，且满足

$$E \subset \bigsqcup_{a \in S^{-}_{f,\mathfrak{p}} \setminus S_{f,\mathfrak{p}}} \bigcup_{\substack{b \in C_{\mathfrak{p}} \\ f(b) \equiv a \mod \mathfrak{p}}} (f(b) + \mathfrak{p}^2).$$

证明。 首先，我们处理满足 $a \in S_{f,\mathfrak{p}}$ 的元素 $\alpha \in a+\mathfrak{p}$。根据引理 2.2，对于所有 $k \in \mathbb{Z}_{\geq 0}$，存在 $b \in R$，使得 $\alpha \equiv f(b) \bmod \mathfrak{p}^k$。因此，$\alpha \in f(R)^{\mathfrak{p}}$。

接下来，我们考虑 $a+\mathfrak{p}$ 中满足 $a \in S_{f,\mathfrak{p}}^{-} \setminus S_{f,\mathfrak{p}}$ 的元素。令 $b \in R$ 使得 $f(b) \equiv a$ 模 $\mathfrak{p}$。由于 $f'(b) \in \mathfrak{p}$，对于所有 $\beta = b + \beta_1 \pi \in b+\mathfrak{p}$，我们有

$$\begin{aligned} f(\beta) - f(b) &= f(b+\beta_1\pi) - f(b) \\ &= \sum_{i=2}^{n} \frac{f^{(i)}(b)}{i!} \beta_1^i \pi^i + f'(b)\beta_1\pi \\ &\equiv 0 \mod \mathfrak{p}^2. \end{aligned}$$

因此，对于所有 $\beta \in b+\mathfrak{p}$，我们有 $f(b) \equiv f(\beta)$ 模 $\mathfrak{p}^2$ 且 $f(\beta) \in f(b) + \mathfrak{p}^2$。将同样的论证应用于其他 $a \in S_{f,\mathfrak{p}}^{-} \setminus S_{f,\mathfrak{p}}$ 和 $b \in C_{\mathfrak{p}}$，其中 $f(b) \equiv a$ 模 $\mathfrak{p}$，我们得到

$$E \subset \bigsqcup_{a \in S_{f,\mathfrak{p}}^{-} \setminus S_{f,\mathfrak{p}}} \bigcup_{\substack{b \in C_{\mathfrak{p}} \\ f(b) \equiv a \bmod \mathfrak{p}}} (f(b) + \mathfrak{p}^2).$$

这就证明了该推论。 □

如果 $S_{f,\mathfrak{p}}^{-} \setminus S_{f,\mathfrak{p}} = \emptyset$，那么我们就可以避免处理不确定集合 E。例如，当我们考虑多项式 $f(x) = x^3 - x^2 \in \mathbb{Z}[x]$ 和 $p = 5$时，发现方程 $f'(x) \equiv 0$ 模 5 的解为 $x \equiv 0$、4 模 5。另一方面，我们确认 $f(0) = f(1)$，且 $f(3) \equiv f(4)$ 模 5。因此，只需计算 $f(5\mathbb{Z}+1)^5$ 和 $f(5\mathbb{Z}+3)^5$，而不必计算 $f(5\mathbb{Z})^5$ 和 $f(5\mathbb{Z}+4)^5$。我们注意到 $f(5\mathbb{Z}+4)^5 \subset f(5\mathbb{Z}+3)^5$ 和 $f(5\mathbb{Z})^5 \subset f(5\mathbb{Z}+1)^5$。更一般地，我们在下文给出一些关于 $S_{f,\mathfrak{p}}^{-} \setminus S_{f,\mathfrak{p}} = \emptyset$ 的例子。

例 2.4. 设 R 是一个特征为 R 的 Dedekind 环，且 $f(x) = x^3 - x^2 \in R[x]$。那么，对于任意素理想 $\mathfrak{p} \subset R$，有：

$$\overline{f(R)}^{\mathfrak{p}} = \bigsqcup_{a \in S_{f,\mathfrak{p}}} (a+\mathfrak{p}).$$

证明。 只需证明，对于任意 $a \in S_{f,\mathfrak{p}}^{-}$，存在元素 $b \in S_{f,\mathfrak{p}}$，使得 $f(a) \equiv f(b) \bmod \mathfrak{p}$。

首先，考虑 $\mathrm{char}(R) = 2$ 的情形。在此情形下，方程 $f'(x) = 0$ 只有解 $x = 0$。由于 $f(0) = f(1)$，对于每个素理想 $\mathfrak{p}$，都有 $S_{f,\mathfrak{p}}^{-} \setminus S_{f,\mathfrak{p}} = \emptyset$。

接下来，讨论 $\mathrm{char}(R) \neq 2, 3$ 的情形。若 $v_{\mathfrak{p}}(6) \geq 1$，则 $x \equiv 0 \bmod \mathfrak{p}$ 是方程 $f'(x) \equiv 0 \bmod \mathfrak{p}$ 的唯一解。如上所述，恒等式 $f(0) = f(1)$ 保证了 $S_{f,\mathfrak{p}}^{-} \setminus S_{f,\mathfrak{p}} = \emptyset$。对于满足 $v_{\mathfrak{p}}(6) = 0$ 的任意素理想 $\mathfrak{p}$，方程 $f'(x) \equiv 0 \bmod \mathfrak{p}$ 在 $\bmod \mathfrak{p}$ 下有两个解 $x \equiv 0$，$2 \cdot 3^{-1}$，其中 3^{-1} 是模 $\mathfrak{p}$ 下 3 的逆元的一个原像。由于 $f(0) \equiv f(1) \bmod \mathfrak{p}$ 且 $f(2 \cdot 3^{-1}) \equiv f(-1 \cdot 3^{-1}) \bmod \mathfrak{p}$，我们还可得到 $S_{f,\mathfrak{p}}^{-} \setminus S_{f,\mathfrak{p}} = \emptyset$。因此，结论成立。 □

更一般地，我们可以通过类似的论证证明以下结果。

例 2.5。设 R 是一个特征为 $\neq 3$ 的 Dedekind 环。设 $\alpha, \beta \in R$，并令 $f(x) = x^3 - (2\alpha+\beta)x^2 + (\alpha^2+2\alpha\beta)x \in R[x]$。那么，我们发现，对于 R 中任意满足 $\alpha \not\equiv \beta \bmod \mathfrak{p}$ 的素理想 $\mathfrak{p}$，

$$\overline{f(R)}^{\mathfrak{p}} = \bigsqcup_{a \in S_{f,\mathfrak{p}}} (a + \mathfrak{p}).$$

证明。如例 2.4 的证明所示，只需证明对于任意 $a \in S_{f,\mathfrak{p}}^{-}$ 都存在一个元素 $b \in S_{f,\mathfrak{p}}$，使得 $f(a) \equiv f(b) \bmod \mathfrak{p}$。

由于 $f'(x) = (3x - (\alpha+2\beta))(x-\alpha)$，$S_{f,\mathfrak{p}}^{-}$ 中的候选元素为 $x \equiv \alpha$，$(\alpha+2\beta)\cdot 3^{-1}$ 模 $\mathfrak{p}$，如果 3 在模 $\mathfrak{p}$ 下可逆。我们可以发现 $f(\alpha) = f(\beta)$，并且 $f((\alpha+2\beta)\cdot 3^{-1}) \equiv f((4\alpha-\beta)\cdot 3^{-1})$ 模 $\mathfrak{p}$。假设 $\alpha \not\equiv \beta$ 模 $\mathfrak{p}$ 确保 $f'(\beta) \not\equiv 0$ 模 $\mathfrak{p}$，且 $f'((4\alpha-\beta)\cdot 3^{-1}) \not\equiv 0$ 模 $\mathfrak{p}$。因此，我们可以应用与例 2.4 的证明相同的论证，从而得到所需的断言。□

3. 二次多项式

本节中，我们假设 f 是一个二次多项式。正如我们稍后将指出的，高次情形比二次情形复杂得多。

由 (1.1) 和引理 2.1，只需对环 R 的每个素理想 $\mathfrak{p}$，考虑 $(\tau \circ f)(R_{\mathfrak{p}})$ 在 $R_{\mathfrak{p}}$ 中的 $\mathfrak{p}R_{\mathfrak{p}}$-进闭包。因此，本节中我们假设 R 是一个主理想整环，且 $\mathfrak{p} = (\pi)$。

设 $f(x) = a_2x^2 + a_1x + a_0 \in R[x]$，并设 $v(\mathfrak{p}, f) = \min\{v_{\mathfrak{p}}(a_1), v_{\mathfrak{p}}(a_2)\}$。于是我们定义重要理想：

$$\mathfrak{g}_f = \prod_{\mathfrak{p}} \mathfrak{p}^{v(\mathfrak{p},f)}.$$

根据 Bhargava 阶乘的定义，我们得到

$$l!_{f(R)} = \mathfrak{g}_f^l \times \prod_{\mathfrak{p}} l!_{f(R,\mathfrak{p})},$$

其中 $f(R,\mathfrak{p})$ 是 R 的以下子集：

$$\left\{ \frac{f(x) - a_0}{\pi^{v(\mathfrak{p},f)}} \mid x \in R \right\}.$$

在下文中，我们假设 $\mathfrak{g}_f = (1)$。我们把 $C_{\mathfrak{p}} = \{0, c_2, \ldots, c_N\}$ 称为完备的不重复代表系（对应 $R/\mathfrak{p}$）。然后，我们证明以下定理。

定理 3.1。设 R 是一个主理想整环，且 $\mathfrak{p}$ 是 R 的一个素理想。我们假设剩余类域 $\kappa = R/\mathfrak{p}$ 是有限的。对于理想为 $\mathfrak{g}_f = (1)$ 的二次多项式 $f(x) = a_2x^2 + a_1x + a_0 \in R[x]$，以下结论成立。

1. 如果 $v_{\mathfrak{p}}(2a_2) = 0$，那么

$$\overline{f(R)}^{\mathfrak{p}} = \{a_0 + \alpha\} \sqcup \bigsqcup_{k=0}^{\infty} \bigsqcup_{i=1}^{N} (a_0 + \alpha_{k,i} + \mathfrak{p}^{2k+1}),$$

其中 $\alpha, \alpha_{k,i} \in R$ 和 $N = \frac{\#\kappa - 1}{2}$。特别地，集合 $\{\alpha_{0,1}, \ldots, \alpha_{0,N}\} = S_{f,\mathfrak{p}}$。2. 若 $v_{\mathfrak{p}}(a_2) \geq 1$，则 $f(R)^{\mathfrak{p}} = R$。

3. 若 $v_{\mathfrak{p}}(2) \geq 1$ 且 $v_{\mathfrak{p}}(a_2 a_1) = 0$，则

$$\overline{f(R)}^{\mathfrak{p}} = \bigsqcup_{i=1}^{N} (a_0 + \alpha_i + \mathfrak{p}),$$

其中 $\alpha_i \in R$ 和 $N = \#\frac{\kappa}{2}$。

备注 3.2。如果 $v_{\mathfrak{p}}(2) \geq 1$ 且 $v_{\mathfrak{p}}(a_1) \geq 1$，那么 $f'(x)$ 模 $\mathfrak{p}$ 恒等于 0。这使得这种情况比其他情况困难得多。我们将在定理 3.1 的证明之后讨论这一点。

定理*3.1* 的证明。由于常数项 a_0 只会导致加性平移，我们可以不失一般性地假设 $a_0 = 0$。令 $f(x) = a_2 x^2 + a_1 x \in R[x]$。

1. 首先，我们处理 $v_{\mathfrak{p}}(2a_2) = 0$ 的情况。我们注意到 $\mathrm{char}(R) \neq 2$。在这种情况下，$f'(x) \equiv 0 \bmod \mathfrak{p}$ 只有一个解 $x \equiv -\frac{a_1}{2a_2} \bmod \mathfrak{p}$。推论 2.3 导致

$$\overline{f(R)}^{\mathfrak{p}} = \bigsqcup_{a \in S_{f,\mathfrak{p}}} (a + \mathfrak{p}) \sqcup E,$$

其中，E 由唯一解 $x \equiv -\frac{a_1}{2a_2}$ 模 $\mathfrak{p}$ 导致。令 $\alpha_{\mathfrak{p}}$ 为 R 中的一个元素，使得 $2a_2 \mid (\alpha_{\mathfrak{p}}\pi - a_1)$且 $\alpha_{\mathfrak{p}} \notin \mathfrak{p}$。那么 $f'(\frac{\alpha_{\mathfrak{p}}\pi - a_1}{2a_2}) \equiv 0$ 模 $\mathfrak{p}$，并且

$$f\left(\frac{\alpha_{\mathfrak{p}}\pi - a_1}{2a_2}\right) = \frac{(\alpha_{\mathfrak{p}}\pi - a_1)^2}{4a_2} + \frac{\alpha_{\mathfrak{p}}\pi a_1 - a_1^2}{2a_2} = \frac{\alpha_{\mathfrak{p}}^2\pi^2 - a_1^2}{4a_2}.$$

可以确认，

$$f(x) \equiv \frac{\alpha_{\mathfrak{p}}^2\pi^2 - a_1^2}{4a_2} \mod \mathfrak{p} \Longleftrightarrow x \equiv \left(\frac{\alpha_{\mathfrak{p}}\pi - a_1}{2a_2}\right) \mod \mathfrak{p}.$$

令 $s = \pi^2\beta_1 + \frac{\alpha_{\mathfrak{p}}^2\pi^2 - a_1^2}{4a_2} \in \overline{f(R)}^{\mathfrak{p}}$。则

$$f\left(\pi\beta_2 + \frac{\alpha_{\mathfrak{p}}\pi - a_1}{2a_2}\right) = \pi^2\beta_1 + \frac{\alpha_{\mathfrak{p}}^2\pi^2 - a_1^2}{4a_2}$$
$$a_2\beta_2^2 + \alpha_{\mathfrak{p}}\beta_2 = \beta_1.$$

为了刻画 β_1，我们考虑多项式 $f_1(x) = a_2 x^2 + \alpha_{\mathfrak{p}} x \in R[x]$ 和$f_1(R)^{\mathfrak{p}}$。由于 $v_{\mathfrak{p}}(2a_2) = 0$，我们可以用上述相同的论证，并将 $f_1(R)^{\mathfrak{p}} = \bigsqcup_{a \in S_{f_1},\mathfrak{p}} (a + \mathfrak{p}) \sqcup E_1$ 和表达为

$$E = \pi^2 \left(\bigsqcup_{a \in S_{f_1,\mathfrak{p}}} (a + \mathfrak{p}) \sqcup E_1 \right) + \frac{\alpha_{\mathfrak{p}}^2\pi^2 - a_1^2}{4a_2}.$$

令 $\alpha'_{\mathfrak{p}} \in R$ 使得 $2a_2 \mid (\alpha'_{\mathfrak{p}}\pi - \alpha_{\mathfrak{p}})$且 $\alpha'_p \notin \mathfrak{p}$。应用上述相同的论证，我们选择 $f_2(x) = a_2 x^2 + \alpha'_{\mathfrak{p}} x \in R[x]$ 作为 f_1 在 f 中的角色，并在 E中得到其他元素。因此，我们可以归纳地刻画 E。在此过程中，存在唯一的元素 $x \in R$使得 $f'(x) \equiv f_i'(x) \equiv 0$模 $\mathfrak{p}$for

全部 i。因此，我们将此元素添加到 E。此外，$\#S_{f,\mathfrak{p}} = \#S_{f_1,\mathfrak{p}} = \cdots = \frac{}{\#\kappa-1}$ 并得到第一条陈述。

2. 接下来，我们假设 $v_{\mathfrak{p}}(a_2) \geq 1$。在这种情况下，$f'(x) \equiv 0 \bmod \mathfrak{p}$ 无解；并且如果 $f(x) \equiv f(y) \bmod \mathfrak{p}$，那么 $(a_2(x+y)+a_1)(x-y) \equiv 0 \bmod \mathfrak{p}$。因此，$f(x) \equiv f(y) \bmod \mathfrak{p}$ 当且仅当 $x \equiv y \bmod \mathfrak{p}$，并且对于任意 $b \in \{0, c_2, \ldots, c_N\}$，都存在 a 使得 $f(a) \equiv b \bmod \mathfrak{p}$。根据推论 2.3，有 $f(R)^{\mathfrak{p}} = R$。

3. 我们假设 $v_{\mathfrak{p}}(2) \geq 1$ 且 $v_{\mathfrak{p}}(a_1 a_2) = 0$。在这种情况下，我们也可以确认 $f'(x) \equiv 0 \bmod \mathfrak{p}$ 无解。因此，根据推论 2.3 以及 $\#S_{f,\ \mathfrak{p}} = {}_{\#}{}_{2}^{\kappa} = N$这一事实，我们得到

$$\overline{f(R)}^{\mathfrak{p}} = \bigsqcup_{i=1}^{N} (\alpha_{k,i} + \mathfrak{p}).$$

这完成了该定理的证明。 □

以下我们考虑左侧情形下的 $\mathfrak{p}$-闭包 $f(R)^{\mathfrak{p}}$，其中 $v_{\mathfrak{p}}(2) \geq 1$ 和$v_{\mathfrak{p}}(a_1) \geq 1$。平移 x 后，我们可以假设 $v_{\mathfrak{p}}(a_1) = v_{\mathfrak{p}}(2)$。由于 $v_{\mathfrak{p}}(a_1) = v_{\mathfrak{p}}(2) \geq 1$，所以 $f'(x) \bmod \mathfrak{p}$ 恒等于 0。我们考虑形如 $\pi^{2v_{\mathfrak{p}}(a_1)}\beta_1$ 的元素，它们由 $f(0) \equiv 0 \bmod \mathfrak{p}^{2v_{\mathfrak{p}}(a_1)}$ 所导致。对于 $k \geq 2v_{\mathfrak{p}}(a_1)+1$

$$\begin{aligned} f(\pi^{v_{\mathfrak{p}}(a_1)}\beta_2) &\equiv \pi^{2v_{\mathfrak{p}}(a_1)}\beta_1 \mod \mathfrak{p}^k \\ \pi^{2v_{\mathfrak{p}}(a_1)}a_2\beta_2^2 + \pi^{v_{\mathfrak{p}}(a_1)}a_1\beta_2 &\equiv \pi^{2v_{\mathfrak{p}}(a_1)}\beta_1 \mod \mathfrak{p}^k \\ a_2\beta_2^2 + \frac{a_1}{\pi^{v_{\mathfrak{p}}(a_1)}}\beta_2 &\equiv \beta_1 \mod \mathfrak{p}^{k-2v_{\mathfrak{p}}(a_1)}. \end{aligned}$$

设 $h(x) = a_2x^2 + \frac{a_1}{\pi^{v_{\mathfrak{p}}(a_1)}}x$。根据假设，$v_{\mathfrak{p}}(\frac{a_1}{\pi^{v_{\mathfrak{p}}(a_1)}}) = 0$。因此，我们得到

$$\overline{h(R)}^{\mathfrak{p}} = \pi^{2v_{\mathfrak{p}}(a_1)}R$$

根据定理 3.1。当我们处理由 $f(c_i)$ 引起的其他形如 $\pi^{2v_{\mathfrak{p}}(a_1)}\beta_1 + a_2c_i^2 + a_1c_i$ 的元素时，需要对每个 $c_i (2 \leq i \leq N)$ 估计 $v_{\mathfrak{p}}(2a_2c_i + a_1)$，并采用前面的讨论。因此，我们有

$$\overline{f(R)}^{\mathfrak{p}} = \pi^{2v_{\mathfrak{p}}(a_1)}R \cup E,$$

其中，E 是由形如 $\pi^{2v_{\mathfrak{p}}(a_1)}\beta_1 + a_2c_i^2 + a_1c_i$的元素引起的。$f'(x)$ 模 $\mathfrak{p}$ 恒等于 0 这一事实使得处理 E 极其困难。

4. 整数系数二次多项式的 Bhargava 阶乘

在定理3.1中，我们考察了 $\mathfrak{p}$-进闭包 $f(R)^{\mathfrak{p}}$。然而，很难刻画所有 $\mathfrak{p}$ 的 $f(R)^{\mathfrak{p}}$。因此，我们专注于 $R = \mathbb{Z}$的情形。在这种情况下，我们将素理想 $p\mathbb{Z}$ 替换为素数 p，并使用缩写 $l!_{f(\mathbb{Z})}$ 表示 $l!_{f(\mathbb{Z})}^{\mathbb{Z}}$。首先，我们给出 $f(\mathbb{Z})^p$ 的例子。

例 4.1. 设 $s(x) = x^2$。对于任意奇素数 p,

$$\overline{s(\mathbb{Z})}^p = \{0\} \sqcup \bigsqcup_{k=0}^{\infty} \bigsqcup_{\substack{\left(\frac{r}{p}\right)=1 \\ 1\le r\le p-1}} (rp^{2k} + p^{2k+1}\mathbb{Z}),$$

其中，$\left(\frac{r}{p}\right)$ 是模 p 的勒让德符号，定义为。

$$\left(\frac{r}{p}\right) = \begin{cases} 1 & \text{if there exists } p \nmid a \text{ with } a^2 \equiv r \mod p, \\ -1 & \text{if for any } a \in \mathbb{Z},\ a^2 \not\equiv r \mod p, \\ 0 & \text{if } r \equiv 0 \mod p. \end{cases}$$

此外，如果 $p = 2$，则有

$$\overline{s(\mathbb{Z})}^2 = \{0\} \sqcup \bigsqcup_{k=0}^{\infty} (2^{2k} + 2^{2k+3}\mathbb{Z}).$$

我们首先利用定理 3.1 展示上一个例子中的前一种情况。 .

例 *4.1*的第一个断言的证明。 对于固定的奇素数 p，同余式 $2x \equiv 0$ 模 p 的解为 $x \equiv 0$ 模 p，并且

$$S_{s,p} = \left\{ r \mod p \;\middle|\; \left(\frac{r}{p}\right) = 1 \right\}.$$

根据定理 3.1，我们有

$$\overline{s(\mathbb{Z})}^p = \bigsqcup_{\substack{\left(\frac{r}{p}\right)=1 \\ 1\le r\le p-1}} (r + p\mathbb{Z}) \sqcup E.$$

接下来我们考虑 $p|s(x)$的情形，这对应于 E，也就是说， $x \equiv 0$ 模 p。令 $x = pk$，我们发现 $p^2|s(pk) = p^2k^2$。只需刻画当 $s_1(x) = {}^{s_{(pk)}}{}_{p^2}$ 时$s_1(\mathbb{Z})$的 p进闭包。由于 $s(x) = s_1(x)$，通过与上面相同的论证，我们发现

$$E = \overline{s_1(\mathbb{Z})}^p = \bigsqcup_{\substack{\left(\frac{r}{p}\right)=1 \\ 1\le r\le p-1}} (r + p\mathbb{Z}) \sqcup E_1,$$

and

$$\overline{s(\mathbb{Z})}^p = \bigsqcup_{k=0}^{1} \bigsqcup_{\substack{\left(\frac{r}{p}\right)=1 \\ 1\le r\le p-1}} (rp^{2k} + p^{2k+1}\mathbb{Z}) \sqcup p^2E_1.$$

我们可以反复应用相同的论证，取 $p^2s_{i+1}(x) = s_i(px)$，并注意到$s(0) = s_i(0) = 0$ 对任意 $i \ge 1$ 都成立。因此，我们有

$$\overline{s(\mathbb{Z})}^p = \{0\} \sqcup \bigsqcup_{k=0}^{\infty} \bigsqcup_{\substack{\left(\frac{r}{p}\right)=1 \\ 1\le r\le p-1}} (rp^{2k} + p^{2k+1}\mathbb{Z}).$$

□

例 4.1 的后一种情况由以下引理得到。

引理 4.2。 设 $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$，且 $\gcd(a_1, a_2) = 1$ 并且 $2|a_1$。那么

$$\overline{f(\mathbb{Z})}^2 = \{a_0 + \alpha\} \sqcup \bigsqcup_{k=0}^{\infty} (a_0 + \alpha_k + 2^{2k+3}\mathbb{Z})$$

其中 α、$\alpha_k \in \mathbb{Z}$。

证明。如定理 3.1 的证明中一样，我们可以假设 $a_0 = 0$。此外，根据假设，我们得到 $2a_2 + a_1 \not\equiv a_1$ 模4，并且不失一般性，我们可以假设 a_1 是 4 的倍数。对于任意整数 k，

$$f(2k+1) = 4\left(a_2k^2 + \left(a_2 + \frac{a_1}{2}\right)k\right) + a_2 + a_1.$$

根据该假设，可以确认 a_2 和 $a_2 + \frac{a_1}{2}$是奇《整数》。由定理 3.1，我们有 $f(2\mathbb{Z}+1)^2 = 8\mathbb{Z} + \overline{(a_2 + a_1)}$。

接下来，我们处理 $f(2\mathbb{Z})$。取一个整数 α_1，使得 $2a_2\alpha_1 \equiv a_1$ 模 8，接着

$$f(2k + \alpha_1) = 4\left(a_2k^2 + \left(a_2\alpha_1 + \frac{a_1}{2}\right)k\right) + a_2\alpha_1^2 + a_1\alpha_1.$$

由于 a_2 是奇数且 $a_2\alpha_1 + \frac{a_1}{2}$ 是 4 的倍数，我们可以应用与上面相同的论证并得到该断言，

$$\overline{f(\mathbb{Z})}^2 = \{\alpha\} \sqcup (8\mathbb{Z} + a_2 + a_1) \sqcup \bigsqcup_{k=1}^{\infty} (\alpha_k + 2^{2k+3}\mathbb{Z})$$

对 α、$\alpha_k \in \mathbb{Z}$ 进行归纳。这证明了该引理。 □

定理 4.3. 设 $f(x) = g(a_2x^2 + a_1x) + a_0 \in \mathbb{Z}[x]$，其中 $g \geq 1$ 且 $\gcd(a_1, a_2) = 1$。那么

$$l!_{f(\mathbb{Z})} = g^l \prod_{p|a_2} p^{k(p,l)} \prod_{p\nmid a_2} p^{k(p,2l)} 2^{-\delta_{\{2|a_1, 2\nmid a_2\}}},$$

其中

$$k(p,l) = \sum_{k=1}^{\infty} \left\lfloor \frac{l}{p^k} \right\rfloor$$

且 δ_P 表示，如果 P 为真，则 $\delta_P = 1$；否则为 $\delta_P = 0$。

证明。只需证明 $g = 1$ 的情形。首先，对于素数 $p \mid a_2$，我们考虑 $v_p(l!_{f(\mathbb{Z})})$。由定理3.1，我们得到 $f(\mathbb{Z})^p = \mathbb{Z}$。因此，有 $v_p(\overline{l!_{f(\mathbb{Z})}}) = v_p(l!) = k(p,l)$。接下来，我们处理奇素数 $p \nmid a_2$。众所周知，$l!_{s(\mathbb{Z})} = (2l)!_2$ 对于 $s(x) = x^2$[4]。由定理 3.1，我们可以计算 $f(\mathbb{Z})$ 的 ~~p-~~进闭包，如下

$$\overline{f(\mathbb{Z})}^p = \{\alpha\} \sqcup \bigsqcup_{k=0}^{\infty} \bigsqcup_{i=1}^{\frac{p-1}{2}} (\alpha_{k,i} + p^{2k+1}\mathbb{Z})$$

对于奇素数 p。由于 $\#\{f(a) \bmod p \mid f'(a) \not\equiv 0 \bmod p\} = \#\{s(a) \bmod p \mid s'(a) \not\equiv 0 \bmod p\} = \frac{p-1}{2}$，存在一个双射 $\phi: f(\mathbb{Z})^p \longrightarrow \overline{s(\mathbb{Z})^p}$，使得 $\alpha \longmapsto 0$ 且[9]

$\alpha_{k,\ i} \longmapsto r_i p^{2k}$，其中 $\{r_1, \ldots, r_{\frac{p-1}{2}}\}$ 是模 p的所有二次剩余的集合。因此，对于任意奇素数 $p \nmid a_2$，$v_p(l!_{f(\mathbb{Z})}) = v_p(l!_{s(\mathbb{Z})})$，且 $v_p(l!_{f(\mathbb{Z})}) = v_p((2l)!)$。

最后，在假设 a_2 为奇数的情况下，我们考察 $v_2(l!_{f(\mathbb{Z})})$。当 a_1 为偶数时，引理 4.2 给出

$$\overline{f(\mathbb{Z})}^2 = \{\alpha\} \sqcup \bigsqcup_{k=0}^{\infty} (\alpha_k + 2^{2k+3}\mathbb{Z})$$

其中 α、$\alpha_k \in \mathbb{Z}$。于是，通过双射 $\phi: f(\mathbb{Z})^2 \longrightarrow s(\mathbb{Z})^2$，使得 $\alpha \longmapsto 0$ 和 $\alpha_k \longmapsto 2^{2k}$，我们得到 $v_2(l!_{f(\mathbb{Z})}) = v_2(l!_{s(\mathbb{Z})}) = v_2((2l)!) - 1$。接下来，我们假设 a_1 为奇数，即 $2 \nmid a_2 a_1$。定理 3.1 给出 $f(\mathbb{Z})^2 = 2\mathbb{Z}$。众所周知，自然序 0、2、4、6、.....构成 $2\mathbb{Z}$ 的一个 2-序（见 [4]）。因此，$v_2(l!_{f(\mathbb{Z})}) = v_2((2l)!)$。我们得到所需结论。□

如果 $|a_2| \leq 2$，那么我们可以直接计算 $l!_{f(\mathbb{Z})}$，并得到以下显式公式。当 $|a_1| = 1$ 时，那么

$$l!_{f(\mathbb{Z})} = \begin{cases} g^l(2l)! & 2 \nmid a_1, \\ \frac{g^l(2l)!}{2} & 2 | a_1, \end{cases}$$

且若 $|a_2| = 2$ 则 $l!_{f(\mathbb{Z})} = g^l(2l)!2^{-l}$。下文中，我们给出商 $l!_{f(\mathbb{Z})}$ 除以 $g^l(2l!)$的估计。

命题 4.4。对于任意二次多项式 $f(x) = g(a_2x^2 + a_1x) + a_0$ 满足 $g \geq 1$且 $\gcd(a_1, a_2) = 1$，均有此结论。

$$\frac{1}{2}\prod_{p|a_2} p^{-\frac{2l}{p}} \leq \frac{l!_{f(\mathbb{Z})}}{g^l(2l)!} \leq \prod_{p|a_2} p^{-\frac{l}{p}+1}.$$

此外，我们利用经典斯特林公式得到 $\log\ l!_{f(\mathbb{Z})} \sim 2l \log 2l$。

证明。根据定理 4.3，我们得到

$$\frac{l!_{f(\mathbb{Z})}}{g^l(2l)!} = \prod_{p|a_2} p^{k(p,l)-k(p,2l)} 2^{-\delta_{\{2|a_1, 2\nmid a_2\}}}.$$

由于 $\frac{l}{p} - 1 \leq k(p, 2l) - k(p, l) \leq \frac{2l}{p}$ 以及 $-\delta_{\{2|a_1, 2\nmid a_2\}} \in \{0, 1\}$，有

$$\frac{1}{2}\prod_{p|a_2} p^{-\frac{2l}{p}} \leq \frac{l!_{f(\mathbb{Z})}}{g^l(2l)!} \leq \prod_{p|a_2} p^{-\frac{l}{p}+1}.$$

□

当 $\deg f \geq 3$ 时，这个问题会变得困难得多。举例来说，我们考虑 $f(x) = x^n$ and $n \geq 3$ 条件下 $S(n) = f(\mathbb{Z})$ 的 Bhargava 阶乘。对于任意素数 $p \nmid n$，我们发现 $f'(x) \equiv 0 \bmod p$ 当且仅当 $p|x$。由于 $f(x) = x^n$ 是 $(\mathbb{Z}/p\mathbb{Z})^\times$ 的自同态，我们有 $\#\operatorname{Im} f = \#S_{f,\ p} = \frac{p-1}{g}$，其中 $g = \gcd(p-1, n)$。由推论 2.3，我们发现

$$\overline{S(n)}^p \supset \bigsqcup_{a \in S_{f,p}} a + p\mathbb{Z}.$$

通过直接计算 Bhargava 阶乘的 p 因子，我们得到以下估计

$$v_p(l!_{S(n)}) < \sum_{k=1}^{\infty} \frac{gl}{p^{k-1}(p-1)}. \tag{4.5}$$

此外，Fares 和 Johnson [7] 证明了对于满足 $n|(p-1)$ 的素数 p，

$$v_p(l!_{S(n)}) = v_p((nl)!). \tag{4.6}$$

设 P_n为所有满足 $n|(p-1)$的素数 p的集合，并设 Q_n为所有满足$\gcd(p-1,n) \leq 2$的素数 p的集合。由不等式(4.5)和恒等式(4.6)，我们可以观察到 $v_p(l!^{S(n)})$在 P_n 中的素数与 Q_n中的素数之间的行为差异。由于 P_n 和 Q_n都是无限集，因此很难给出 $l!^{S(n)}$的解析估计。例如，恒等式 (4.6) 表明，对于任意素数 $p \in P_3$，$v_p(l!^{S(3)}) = v_p((3l)!)$。另一方面，对于任意奇素数 $p \in Q_3$，我们计算

$$v_p(l!_{S(3)}) < \sum_{k=1}^{\infty} \frac{l}{p^{k-1}(p-1)} \leq \sum_{k=1}^{\infty} \frac{2l}{p^k} = v_p((2l)!).$$

$v_p(l!^{S(3)}) = v_p((3l)!)$和 $v_p(l!^{S(3)}) < v_p((2l)!)$都在无穷多个素数处成立。我们注意到，多项式 $f(x)$一般而言不是 $(\mathbb{Z}/p\mathbb{Z})^\times$ 的自同态。因此，当$\deg f \geq 3$时，与前一种情形相比，对 $l!^{f(\mathbb{Z})}$ 给出解析估计要困难得多。

Acknowledgement

本研究得到 JSPS 研究员特别研究员奖励金（项目编号：JP19J10705）资助。

参考文献

[1] Adam, D., Chabert, J. L.（2015）。关于 $\mathbb{Z}$ 和$\mathbb{F}_q[T]$中孪生素数集的 Bhargava 阶乘。《国际数论杂志》**11**，第 6 期，1941–1959。[2] Bhargava, M.（1997）。Dedekind 环任意子集上的 P-序列与多项式函数。《纯粹与应用数学杂志》**490**，101–127。[3] Bhargava，M.（1998）。Dedekind 整环子集上的广义阶乘与固定因子。《数论杂志》**72**，67–75。[4] Bhargava, M.（2000）。阶乘函数及其推广。《美国数学月刊》107，第**9**期，783–799。[5] Diaz, B.（2020）。一类勒让德公式的渐近性质。预印本，arXiv:2010.13645。[6] Evrard, S.（2012）。多变量中的 Bhargava 阶乘。《代数杂志》372，134–148。[7] Fares, Y., Johnson, K.（2012）。整数 d 次幂集合的特征序列与 p-序列。《整数》**12**，第 5 期，865–876。[8] H. Matsumura.（1989）。交换环论（第 8 卷）。剑桥大学出版社。[9] Rajkumar, K., Reddy, A. S., Semwal, D. P.（2018）。多元多项式的固定因子与多变量广义阶乘。《韩国数学会杂志》55，第 6 期，1305–1320。

应用数学系，东京理科大学，日本东京都新宿区神乐坂1-3，邮编162-8601。

电子邮件地址: w.takeda@rs.tus.ac.jp