Bhargava factorials and irreducibility of integer-valued polynomials

Conference on Rings and Factorizations 2023
July 10–14, 2023
University of Graz, Graz, Austria.

Presented by - Devendra Prasad
Chennai, India

SHIV NADAR
UNIVERSITY

Outline

Introduction

In his celebrated work, Bhargava [1] (see also Bhargava [2]) generalized the notion of factorials to an arbitrary subset S of $\mathbb{Z}$. These factorials are intrinsic to the given subset. He obtained these factorials by the notion of p-orderings.

Introduction

In his celebrated work, Bhargava [1] (see also Bhargava [2]) generalized the notion of factorials to an arbitrary subset S of $\mathbb{Z}$. These factorials are intrinsic to the given subset. He obtained these factorials by the notion of p-orderings.

p-orderings

Let S be an arbitrary subset of $\mathbb{Z}$ and p be a fixed prime. A p-ordering of S is a sequence $a_0, a_1, a_2, \cdots$ of elements of S that is formed as follows:

[1] Manjul Bhargava. P-orderings and polynomial functions on arbitrary subsets of Dedekind rings. J. Reine Angew. Math., 490:101–127, 1997.

[2] Manjul Bhargava. The factorial function and generalizations. Amer. Math. Monthly, 107(9):783–799, 2000.

SHIV NADAR UNIVERSITY CHENNAI

Step 0

Choose any element $a_0 \in S$;

Step 0

Choose any element $a_0 \in S$;

Step 1

Choose an element $a_1 \in S$ that minimizes the highest power of p dividing $a_1 - a_0$;

Step 0

Choose any element $a_0 \in S$;

Step 1

Choose an element $a_1 \in S$ that minimizes the highest power of p dividing $a_1 - a_0$;

Step 2

Choose an element $a_2 \in S$ that minimizes the highest power of p dividing $(a_2 - a_0)(a_2 - a_1)$;

Step 0

Choose any element $a_0 \in S$;

Step 1

Choose an element $a_1 \in S$ that minimizes the highest power of p dividing $a_1 - a_0$;

Step 2

Choose an element $a_2 \in S$ that minimizes the highest power of p dividing $(a_2 - a_0)(a_2 - a_1)$;

Step k

In a similar way,

Choose an element $a_k \in S$ that minimizes the highest power of p dividing $\prod_{i=0}^{k-1}(a_k - a_i)$

Generalized factorials

Fact

A p-ordering of any set need not be unique but the highest power of p dividing $\prod_{i=0}^{k-1}(a_k - a_i)$ is always unique.

SHIV NADAR UNIVERSITY CHENNAI

Fact

A p-ordering of any set need not be unique but the highest power of p dividing $\prod_{i=0}^{k-1}(a_k - a_i)$ is always unique.

generalized factorials

the generalized factorial of index $k \; \forall \; k \geq 0$ is defined as

$$k!_S = \prod_p w_p((a_k - a_0)(a_k - a_1)\dots(a_k - a_{k-1})).$$

where $w_p(d)$ denotes the highest power of p dividing d for a given integer d. For instance, $w_2(12) = 2^2$.

SHIV NADAR UNIVERSITY CHENNAI

Examples

Ex . 1

Let $S = \mathbb{Z}$, then for all positive integers k, we have $k!_{\mathbb{Z}} = k!$.

Examples

Ex . 1

Let $S = \mathbb{Z}$, then for all positive integers k, we have $k!_{\mathbb{Z}} = k!$.

Ex . 2

Let $S = 2\mathbb{Z}$, then for all positive integers k, we have $k!_S = 2^k k!$.

SHIV NADAR UNIVERSITY CHENNAI

Examples

Ex . 1

Let $S = \mathbb{Z}$, then for all positive integers k, we have $k!_{\mathbb{Z}} = k!$.

Ex . 2

Let $S = 2\mathbb{Z}$, then for all positive integers k, we have $k!_S = 2^k k!$.

Ex . 3

Let $S = 2\mathbb{Z} + 1$, then for all positive integers k, we have $k!_S = 2^k k!$.

SHIV NADAR UNIVERSITY CHENNAI

Examples

Ex . 1

Let $S = \mathbb{Z}$, then for all positive integers k, we have $k!_{\mathbb{Z}} = k!$.

Ex . 2

Let $S = 2\mathbb{Z}$, then for all positive integers k, we have $k!_S = 2^k k!$.

Ex . 3

Let $S = 2\mathbb{Z} + 1$, then for all positive integers k, we have $k!_S = 2^k k!$.

Ex . 4

Let $S = \{2^n : n \in \mathbb{Z}\}$, then for all positive integers k, we have
$k!_S = (2^n - 2^0)(2^n - 2^1) \ldots (2^k - 2^{k-1})$.

Integer-valued polynomials

Definition

the ring of integer-valued polynomials over a subset $S \subseteq \mathbb{Z}$ is defined as

$$\mathrm{Int}(S, \mathbb{Z}) = \{f \in \mathbb{Q}[x] : f(S) \subset \mathbb{Z}\}.$$

SHIV NADAR UNIVERSITY CHENNAI

Integer-valued polynomials

Definition

the ring of integer-valued polynomials over a subset $S \subseteq \mathbb{Z}$ is defined as

$$\mathrm{Int}(S, \mathbb{Z}) = \{f \in \mathbb{Q}[x] : f(S) \subset \mathbb{Z}\}.$$

Denote the set of polynomials of $\mathrm{Int}(S, \mathbb{Z})$ of degree k by $\mathrm{Int}_k(S, \mathbb{Z})$. It turns out that

$$k!_S = \gcd\{a : a\mathrm{Int}_k(S, \mathbb{Z}) \subseteq \mathbb{Z}[x]\}.$$

SHIV NADAR UNIVERSITY CHENNAI

Integer-valued polynomials

Definition

the ring of integer-valued polynomials over a subset $S \subseteq \mathbb{Z}$ is defined as

$$\mathrm{Int}(S, \mathbb{Z}) = \{f \in \mathbb{Q}[x] : f(S) \subset \mathbb{Z}\}.$$

Denote the set of polynomials of $\mathrm{Int}(S, \mathbb{Z})$ of degree k by $\mathrm{Int}_k(S, \mathbb{Z})$. It turns out that

$$k!_S = \gcd\{a : a\mathrm{Int}_k(S, \mathbb{Z}) \subseteq \mathbb{Z}[x].$$

d_k-orderings

For given integers d and k, let $p_1, p_2, \ldots, p_r$ be all the prime divisors of d. For $1 \leq j \leq r$, let $\{u_{ij}\}_{i \geq 0}$ be a p_j-ordering of $S \subset \mathbb{Z}$. Then a d_k-ordering $\{x_i\}_{0 \leq i \leq k}$ of S is a solution to the following congruences

$$x_i \equiv u_{ij} \mod \pi_j^{e_{kj}+1} \; \forall \; 1 \leq j \leq r, \tag{1}$$

where $p_j^{e_{kj}} = w_{p_j}(k!_S)$.

SHIV NADAR UNIVERSITY CHENNAI

Examples

Ex . 1

Let $S = \mathbb{Z}$, then $0, 1, \ldots, k$ is a d_k - ordering for all positive integers d and k.

Examples

Ex . 1

Let $S = \mathbb{Z}$, then $0, 1, \dots, k$ is a d_k - ordering for all positive integers d and k.

Ex . 2

Let $S = 2\mathbb{Z}$, then $0, 2, 4, \dots, 2k$ is a d_k - ordering for all positive integers d and k.

SHIV NADAR UNIVERSITY CHENNAI

Examples

Ex . 1

Let $S = \mathbb{Z}$, then $0, 1, \ldots, k$ is a d_k - ordering for all positive integers d and k.

Ex . 2

Let $S = 2\mathbb{Z}$, then $0, 2, 4, \ldots, 2k$ is a d_k - ordering for all positive integers d and k.

Ex . 3

Let $S = 2\mathbb{Z} + 1$, then $1, 3, 5, \ldots, 2k + 1$ is a d_k - ordering for all positive integers d and k.

Examples

Ex . 1

Let $S = \mathbb{Z}$, then $0, 1, \ldots, k$ is a d_k - ordering for all positive integers d and k.

Ex . 2

Let $S = 2\mathbb{Z}$, then $0, 2, 4, \ldots, 2k$ is a d_k - ordering for all positive integers d and k.

Ex . 3

Let $S = 2\mathbb{Z} + 1$, then $1, 3, 5, \ldots, 2k + 1$ is a d_k - ordering for all positive integers d and k.

Ex . 4

Let $S = \{2^n : n \in \mathbb{Z}\}$, then $2^0, 2^1, 2^2, \ldots, 2^k$ is a d_k - ordering for all positive integers d and k.

SHIV NADAR UNIVERSITY CHENNAI

the μ-function

Definition

For a given polynomial $f = \frac{g}{d} \in \mathbb{Q}[x]$, define $\mu_i(d, p)$ by

$$\mu_i(d, p) w_p(i!_S) = w_p(d).$$

SHIV NADAR UNIVERSITY CHENNAI

Definition

For a given polynomial $f = \frac{g}{d} \in \mathbb{Q}[x]$, define $\mu_i(d,p)$ by

$$\mu_i(d,p)w_p(i!_S) = w_p(d).$$

The function $\mu_i(d,p)$ also depends on the set since $i!_S$ depends. Therefore, we assume that in the notation $\mu_i(d,p)$, the subset and the underlying ring automatically come from the context (see Prasad [3]).

the μ-function

Definition

For a given polynomial $f = \frac{g}{d} \in \mathbb{Q}[x]$, define $\mu_i(d, p)$ by

$$\mu_i(d, p) w_p(i!_S) = w_p(d).$$

The function $\mu_i(d, p)$ also depends on the set since $i!_S$ depends. Therefore, we assume that in the notation $\mu_i(d, p)$, the subset and the underlying ring automatically come from the context (see Prasad [3]).

A Z-module basis

Let $a_0, a_1, \ldots, a_k$ is a d_k-ordering of $S \subseteq \mathbb{Z}$, then $S_i(x) = (x - a_0)(x - a_1)\ldots(x - a_k)$ where $0 \leq i \leq k$ is a Z-module basis for $\mathrm{Int}_k(S, \mathbb{Z})$.

[3] Devendra Prasad. Bhargava factorials and irreducibility of integer-valued polynomials. Rocky Mountain J. Math. 52 (3) 1031 - 1038, June 2022.

Some results

Lemma

For every polynomial $f = \frac{g}{d} \in \mathbb{Q}[x]$ of degree k, the following holds

$$f \in \mathrm{Int}(S, \mathbb{Z}) \Leftrightarrow f(\underline{a}_i) \in \mathbb{Z} \ \forall \ 0 \leq i \leq k,$$

where $a_0, a_1, \ldots, a_k$ is a d_k-ordering of $S \subseteq \mathbb{Z}$.

Some results

Lemma

For every polynomial $f = \frac{g}{d} \in \mathbb{Q}[x]$ of degree k, the following holds

$$f \in \mathrm{Int}(S, \mathbb{Z}) \Leftrightarrow f(\underline{a}_i) \in \mathbb{Z} \; \forall \; 0 \leq i \leq k,$$

where $a_0, a_1, \ldots, a_k$ is a d_k-ordering of $S \subseteq \mathbb{Z}$.

Lemma

A polynomial $f = \frac{\sum_{i=0}^{k} b_i S_i(x)}{d} \in \mathbb{Q}[x]$ is integer-valued iff $\forall \; p \mid d, w_p(d) \leq w_p(b_i i!_S) \; \forall \; 0 \leq i \leq k$.

SHIV NADAR UNIVERSITY CHENNAI

Some results

Lemma

For every polynomial $f = \frac{g}{d} \in \mathbb{Q}[x]$ of degree k, the following holds

$$f \in \mathrm{Int}(S, \mathbb{Z}) \Leftrightarrow f(\underline{a}_i) \in \mathbb{Z} \ \forall\ 0 \leq i \leq k,$$

where $a_0, a_1, \ldots, a_k$ is a d_k-ordering of $S \subseteq \mathbb{Z}$.

Lemma

A polynomial $f = \frac{\sum_{i=0}^{k} b_i S_i(x)}{d} \in \mathbb{Q}[x]$ is integer-valued iff $\forall\ p \mid d, w_p(d) \leq w_p(b_i i!_S)\ \forall\ 0 \leq i \leq k$.

Definition

A polynomial $f \in \mathrm{Int}(S, \mathbb{Z})$ is said to be “image primitive " iff the ideal $\{f(s) : s \in \mathbb{Z}\}$ is the whole ring $\mathbb{Z}$.

Lemma

A polynomial $f = \frac{\sum_{i=0}^{k} b_i S_i(x)}{d} \in \mathrm{Int}(S, \mathbb{Z})$ is image primitive iff $\forall\ p \mid d,\ \exists\ 0 \leq i \leq k$ such that $w_p(d) = w_p(b_i i!_S)$.

SHIV NADAR UNIVERSITY CHENNAI

Irreducibility condition

Let $f = \frac{g}{d} \in \mathrm{Int}(S, \mathbb{Z})$ be a polynomial of degree k and $a_0, a_1, \ldots, a_k$ be a d_k-ordering. Then f is irreducible iff for any factorization $g = (\sum_{i=0}^{k_1} b_i S_i(x))(\sum_{j=0}^{k_2} c_i S_i(x))$ there exist a prime $p \mid d$ and non-zero positive integers $r \leq k_1$ and $s \leq k_2$ such that $\frac{\mu_r(d,p)\mu_s(d,p)}{w_p(d)} \nmid w_p(b_r c_s)$.

SHIV NADAR UNIVERSITY CHENNAI

Irreducibility condition

Let $f = \frac{g}{d} \in \mathrm{Int}(S, \mathbb{Z})$ be a polynomial of degree k and $a_0, a_1, \ldots, a_k$ be a d_k-ordering. Then f is irreducible iff for any factorization $g = (\sum_{i=0}^{k_1} b_i S_i(x))(\sum_{j=0}^{k_2} c_i S_i(x))$ there exist a prime $p \mid d$ and non-zero positive integers $r \leq k_1$ and $s \leq k_2$ such that $\frac{\mu_r(d,p)\mu_s(d,p)}{w_p(d)} \nmid w_p(b_r c_s)$.

Example

Let us check the irreducibility of the polynomial

$$f = \frac{18x^6 - 48x^5 + 47x^4 - 29x^2 + 41x + 6}{6}$$

in $\mathrm{Int}(\mathbb{Z})$. We have only the following way of factoring f

$$f = \frac{f_1 f_2}{6},$$

where $f_1 = 2 + 3x + 6x(x-1) + 2x(x-1)(x-2)$ and $f_2 = 3 + 4x + 3x(x-1) + 9x(x-1)(x-2)$. Since $b_0 = 2$ and $c_1 = 4$ are not multiple of three, it follows that $w_3(b_0 c_1) = w_3(2 \times 4) = 3^0$. However, $\frac{\mu_0(6,3)\mu_1(6,3)}{w_3(6)} = \frac{3^1 3^1}{3^1} > w_p(b_r c_s)$, which implies that the polynomial is irreducible.

SHIV NADAR UNIVERSITY CHENNAI

Thank You