An Introduction to P-orderings

Lori Watson

University of Georgia

Mock AMS 2015

Outline

- Motivation
- How P-ordering Works
- Properties of P-orderings
- Applications

Question: For which polynomials $f(x) \in \mathbb{Q}[x]$ will $f(\mathbb{Z}) \subseteq \mathbb{Z}$?

Question: For which polynomials $f(x) \in \mathbb{Q}[x]$ will $f(\mathbb{Z}) \subseteq \mathbb{Z}$?

Every polynomial in $\mathbb{Z}[x]$ will map $\mathbb{Z}$ to $\mathbb{Z}$. But there are polynomials with non-integer coefficients that work as well, e.g. $g(x) = \frac{1}{2}x(x+1)$

Question: For which polynomials $f(x) \in \mathbb{Q}[x]$ will $f(\mathbb{Z}) \subseteq \mathbb{Z}$?

Every polynomial in $\mathbb{Z}[x]$ will map $\mathbb{Z}$ to $\mathbb{Z}$. But there are polynomials with non-integer coefficients that work as well, e.g. $g(x) = \frac{1}{2}x(x+1)$

Theorem (Pólya, 1915)

A polynomial $f \in \mathbb{Q}[x]$ of degree n maps $\mathbb{Z}$ to $\mathbb{Z}$ if and only if

$$f(x) = \sum_{k=0}^{n} a_k h_k(x),$$

where

$$a_k, \in \mathbb{Z}, \quad h_0(x) = 1, \quad \textit{and} \quad h_k(x) = \frac{x(x-1)\cdots(x-(k-1))}{k!}$$

Question: For which polynomials $f(x) \in \mathbb{Q}[x]$ will $f(\mathbb{Z}) \subseteq \mathbb{Z}$?

Every polynomial in $\mathbb{Z}[x]$ will map $\mathbb{Z}$ to $\mathbb{Z}$. But there are polynomials with non-integer coefficients that work as well, e.g. $g(x) = \frac{1}{2}x(x+1)$

Theorem (Pólya, 1915)

A polynomial $f \in \mathbb{Q}[x]$ of degree n maps $\mathbb{Z}$ to $\mathbb{Z}$ if and only if

$$f(x) = \sum_{k=0}^{n} a_k h_k(x),$$

where

$$a_k, \in \mathbb{Z}, \quad h_0(x) = 1, \quad \textit{and} \quad h_k(x) = \frac{x(x-1)\cdots(x-(k-1))}{k!}$$

In otherwords, the ring of integer-valued polynomials has a *regular basis* (i.e., a $\mathbb{Z}$-basis that has exactly one polynomial of degree n for every $n \geq 0$)

Given Pólya's result, it's natural to ask: Can the result be generalized, and if so, how?

For example, if D is a Dedekind domain with field of fractions K and an A is an arbitrary subset of D, does

$$\operatorname{Int}(A, D) := \{f \in K[x] : f(A) \subseteq D\}$$

have a regular basis?

Given Pólya's result, it's natural to ask: Can the result be generalized, and if so, how?

For example, if D is a Dedekind domain with field of fractions K and an A is an arbitrary subset of D, does

$$\mathrm{Int}(A, D) := \{f \in K[x] : f(A) \subseteq D\}$$

have a regular basis?

Manjul Bhargava answered this question by giving necessary and sufficient conditions for a regular basis for the ring $\mathrm{Int}(A, D)$ to exist. To do so, he used the concept of *P-ordering*

How P-ordering works

- Start with a *Dedekind ring* R (a Noetherian, locally principal ring in which all nonzero prime ideals are maximal), and a non-empty subset $S \subseteq R$.
- Fix a nonzero prime ideal P.
- Choose any $a_0 \in S$.
- For $k \geq 1$, choose an element $a_k \in S$ that minimizes the highest power of P in which $\displaystyle\prod_{j=0}^{k}(a_k - a_j)$ appears.

Example: Let $R = \mathbb{Z}$ and $S = \{0, ..., n\}$, the natural ordering $0, 1, 2, ..., n$ works for any nonzero prime ideal (p) of $\mathbb{Z}$.

Example: Let $R = \mathbb{Z}$ and $S = \{0, ..., n\}$, the natural ordering $0, 1, 2, ..., n$ works for any nonzero prime ideal (p) of $\mathbb{Z}$.

Example: The natural ordering of the nonnegative integers forms a (p)-ordering of $\mathbb{Z}$ for all primes p.

Example: Let $R = \mathbb{Z}$ and $S = \{0, ..., n\}$, the natural ordering $0, 1, 2, ..., n$ works for any nonzero prime ideal (p) of $\mathbb{Z}$.

Example: The natural ordering of the nonnegative integers forms a (p)-ordering of $\mathbb{Z}$ for all primes p.

This follows by induction: Assume $0, ..., k-1$ is a (p)-ordering for the first $k-1$ steps. For any a_k we choose,

$$(a_k - 0)(a_k - 1) \cdots (a_k - (k-1))$$

is divisible by $k!$. The choice $a_k = k$ minimizes the highest power of p that divides this product for every prime p.

It is important to note that a P-ordering is not, in general, unique (we could take a_0 to be any element of S). But if we let $v_k(S, P)$ denote the highest power of P containing the product $(a_k - a_0) \cdots (a_k - a_{k-1})$ then the P-sequence of X,

$$\{v_k(S, P)\}_{k=0}^{\infty}$$

is unique.

By convention, $v_0(S, P)$ is taken be the unit ideal. If $(a_k - a_0) \cdots (a_k - a_{k-1}) = 0$, then $v_k(S, P)$ is the zero ideal.

Example: Let $R = \mathbb{Z}$ and let $p > 2$ be a prime number. Let $S = \{1, p, 2p, p^2, p^2 + 1\}$.

Example: Let $R = \mathbb{Z}$ and let $p > 2$ be a prime number. Let $S = \{1, p, 2p, p^2, p^2 + 1\}$.

The orderings $1, p, 2p, p^2, p^2 + 1$ and $1, p, p^2, p^2 + 1, 2p$ are both (p)-orderings of S, and they yield the same (p)-sequence:

$$(1), (1), (p), (p^2), (p^2), (0), (0), ...$$

A generalized factorial function

Earlier we noted that $0, 1, 2, \ldots$ is a (p)-ordering of $\mathbb{Z}$ for all primes p. That is, to construct a (p)-ordering on $\mathbb{Z}$, we can choose the sequence $a_k = k$ for $k \geq 0$. Then for this (p)-ordering, we have

$$(a_k - a_0)(a_k - a_1) \cdots (a_k - a_{k-1}) = k(k-1) \cdots (1) = k!$$

This tells us that, for a given prime p, $v_k(\mathbb{Z}, (p))$ is keeping track of the highest power of p that divides $k!$. If we fix k, it's easy to see that

$$\textstyle\prod_p v_k(\mathbb{Z}, (p)) = (k!)$$

This example inspires the following definition:

Definition (The k-th factorial of S)

$$k!_S = \prod_{P_{prime}} v_k(S, P)$$

This very useful generalization of the factorial turns out to be what was needed to answer the question Pólya posed.

Leveraging P-orderings and this generalized factorial, Bhargava was able to show

Theorem (Bhargava, 1997)

For a Dedekind domain D and a subset S of D, $Int(S, D)$ has a regular basis if and only if $k!_S$ is a principal ideal for all $k \geq 0$

In addition, he gave an explicit construction for such bases, thereby resolving Pólya's question completely and giving us a useful new tool in the study of integer-valued polynomials.

Thank You

References:

- M. Bhargava, *P*-orderings and polynomial functions on arbitrary subsets of Dedekind Rings, J. reine Angew. Math. **490** (1997), 101-127
- M. Bhargava, The factorial function and generalizations, Amer. Math. Monthly **107** (2000), 783-799.
- W. Narkiewicz, Polynomial Mappings, Springer-Verlag, Berlin 1995