Integral-valued polynomials

Darij Grinberg

14 October 2013, Storrs

http://www.cip.ifi.lmu.de/~grinberg/storrs2013.pdf

This talk is about polynomials: $2x^4 + 5x,\ 3x^7 - \sqrt{2}x + 17, \ldots$.

Call a polynomial $P(x)$ **integral-valued** if $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$.

Example: If every coefficient of $P(x)$ is an integer, then $P(x)$ is integral-valued, *e.g.*, $P(x) = 2x^4 + 5x$.

What is an integral-valued polynomial?

This talk is about polynomials: $2x^4 + 5x,\ 3x^7 - \sqrt{2}x + 17, \ldots.$

Call a polynomial $P(x)$ **integral-valued** if $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$.

Example: If every coefficient of $P(x)$ is an integer, then $P(x)$ is integral-valued, *e.g.*, $P(x) = 2x^4 + 5x$.

The converse is *false*: $P(x)$ can be integral-valued without having integral coefficients!

Example: $P(x) = \dfrac{1}{2}x^2 - \dfrac{1}{2}x = \dfrac{x(x-1)}{2}$. For $n \in \mathbb{Z}$, n or $n-1$ is even, so $\dfrac{n(n-1)}{2} \in \mathbb{Z}$.

What is an integral-valued polynomial?

This talk is about polynomials: $2x^4 + 5x,\ 3x^7 - \sqrt{2}x + 17, \ldots$.

Call a polynomial $P(x)$ **integral-valued** if $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$.

Example: If every coefficient of $P(x)$ is an integer, then $P(x)$ is integral-valued, *e.g.*, $P(x) = 2x^4 + 5x$.

The converse is *false*: $P(x)$ can be integral-valued without having integral coefficients!

Example: $P(x) = \frac{1}{2}x^2 - \frac{1}{2}x = \frac{x(x-1)}{2}$. For $n \in \mathbb{Z}$, n or $n-1$ is even, so $\frac{n(n-1)}{2} \in \mathbb{Z}$.

Integral-valued polynomials occur in several areas of math, such as combinatorics, commutative algebra, and algebraic topology.

Our goal: find a nice description of all integral-valued polynomials.

Background: polynomials and their values

A polynomial is determined by "sufficiently many" of its values.

- **If** $P(x)$ and $Q(x)$ are polynomials such that $P(x) = Q(x)$ for infinitely many numbers x, **then** $P(x) = Q(x)$ for **all** x.
  For instance, a polynomial is completely determined by knowing its values at all $x > 0$.
- **If** $P(x)$ and $Q(x)$ are polynomials of degree d such that $P(x) = Q(x)$ for $d + 1$ choices of x, **then** $P(x) = Q(x)$ for **all** x.
  For instance, a quadratic polynomial is completely determined by knowing its values at (any) three choices of x.

Background: polynomials and their values

A polynomial is determined by "sufficiently many" of its values.

- **If** $P(x)$ and $Q(x)$ are polynomials of degree d such that $P(x) = Q(x)$ for $d + 1$ choices of x, **then** $P(x) = Q(x)$ for **all** x.

Example. To verify the identity $x^3 - 1 = (x - 1)(x^2 + x + 1)$ for all x, it is enough to check both sides are equal at 4 numbers: both sides are polynomials of degree 3, so if they agree at 4 numbers then they agree everywhere. At $x = 0, 1, 2, 3$, both sides take the same values ($-1, 0, 7$, and 26).

This method can be used in other cases to prove polynomial identities combinatorially: when x is an integer, the two sides of the identity could count the same thing in two different ways. And equality at enough integers forces equality everywhere.

A polynomial is determined by “sufficiently many” of its values.

- **If** a polynomial $P(x)$ satisfies $P(r) \in \mathbb{Q}$ for all $r \in \mathbb{Q}$, **then** all coefficients of $P(x)$ lie in $\mathbb{Q}$.

Background: polynomials and their values

A polynomial is determined by "sufficiently many" of its values.

- **If** a polynomial $P(x)$ satisfies $P(r) \in \mathbb{Q}$ for all $r \in \mathbb{Q}$, **then** all coefficients of $P(x)$ lie in $\mathbb{Q}$.
- **If** a polynomial $P(x)$ satisfies $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$, **then** the coefficients **need not** all lie in $\mathbb{Z}$.
  1. $P(x) = \dfrac{x^2 - x}{2}$ $\left(\text{since } \dfrac{n(n-1)}{2} \in \mathbb{Z} \text{ for all } n \in \mathbb{Z}\right)$.
  2. $P(x) = \dfrac{x^2 + x}{2}$ $\left(\text{since } \dfrac{n(n+1)}{2} \in \mathbb{Z} \text{ for all } n \in \mathbb{Z}\right)$.
  3. **not** $P(x) = \dfrac{x^4 - x}{4}$ $\left(\text{since } P(2) = \dfrac{7}{2}\right)$.

Integral-valued polynomials

Call a polynomial $P(x)$ **integral-valued** if $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$.

Integral-valued polynomials

Call a polynomial $P(x)$ **integral-valued** if $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$.

Examples.

- A polynomial with integer coefficients, of course. :)

Call a polynomial $P(x)$ **integral-valued** if $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$.

Examples.

- A polynomial with integer coefficients, of course. :)
- $P(x) = \frac{1}{p}(x^p - x)$ for all primes p. (Fermat's little theorem.)

Call a polynomial $P(x)$ **integral-valued** if $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$.

Examples.

- A polynomial with integer coefficients, of course. :)
- $P(x) = \frac{1}{p}(x^p - x)$ for all primes p. (Fermat's little theorem.)
- $P(x) = \frac{1}{6}x(x+1)(2x+1)$, because

Call a polynomial $P(x)$ **integral-valued** if $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$.

Examples.

- A polynomial with integer coefficients, of course. :)
- $P(x) = \frac{1}{p}(x^p - x)$ for all primes p. (Fermat's little theorem.)
- $P(x) = \frac{1}{6}x(x+1)(2x+1)$, because $P(n) = 1^2 + 2^2 + \cdots + n^2 \in \mathbb{Z}$

Call a polynomial $P(x)$ **integral-valued** if $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$.

Examples.

- A polynomial with integer coefficients, of course. :)
- $P(x) = \frac{1}{p}(x^p - x)$ for all primes p. (Fermat's little theorem.)
- $P(x) = \frac{1}{6}x(x+1)(2x+1)$, because
  $P(n) = 1^2 + 2^2 + \cdots + n^2 \in \mathbb{Z}$ for $n \geq 0$,
  $P(n) = -(1^2 + 2^2 + \cdots + (n'-1)^2) \in \mathbb{Z}$ for $n = -n' < 0$.

Call a polynomial $P(x)$ **integral-valued** if $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$.

Further example.

$$P(x) = \binom{x}{m} := \frac{x(x-1)\cdots(x-m+1)}{m!}$$

for integers $m \geq 0$. The first few of these polynomials are

$$\binom{x}{0} = 1,\ \binom{x}{1} = x,\ \binom{x}{2} = \frac{x(x-1)}{2},\ \binom{x}{3} = \frac{x(x-1)(x-2)}{6}.$$

Call a polynomial $P(x)$ **integral-valued** if $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$.

Further example.

$$P(x) = \binom{x}{m} := \frac{x(x-1)\cdots(x-m+1)}{m!}$$

for integers $m \geq 0$. The first few of these polynomials are

$$\binom{x}{0} = 1, \ \binom{x}{1} = x, \ \binom{x}{2} = \frac{x(x-1)}{2}, \ \binom{x}{3} = \frac{x(x-1)(x-2)}{6}.$$

Indeed, for $n \geq 0$, the number $\binom{n}{m}$ **counts** the number of m-element subsets of $\{1, 2, \ldots, n\}$ ("sampling balls from urns").

Integral-valued polynomials

Call a polynomial $P(x)$ **integral-valued** if $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$.

Further example.

$$P(x) = \binom{x}{m} := \frac{x(x-1)\cdots(x-m+1)}{m!}$$

for integers $m \geq 0$. The first few of these polynomials are

$$\binom{x}{0} = 1,\ \binom{x}{1} = x,\ \binom{x}{2} = \frac{x(x-1)}{2},\ \binom{x}{3} = \frac{x(x-1)(x-2)}{6}.$$

Indeed, for $n \geq 0$, the number $\binom{n}{m}$ **counts** the number of m-element subsets of $\{1, 2, \ldots, n\}$ ("sampling balls from urns").

For $n = -N < 0$, we have $\binom{n}{m} = (-1)^m \binom{N+m-1}{m} \in \mathbb{Z}$.

Call a polynomial $P(x)$ **integral-valued** if $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$.

Further example.

$$P(x) = \frac{1}{m} \sum_{d|m} \phi\left(\frac{m}{d}\right) x^d$$

for integers $m \geq 1$, where $\phi(k)$ is the number of integers among $1, 2, \ldots, k$ that are relatively prime to k. The first few are

$$x, \quad \frac{1}{2}(x^2 + x), \quad \frac{1}{3}(x^3 + 2x), \quad \frac{1}{4}(x^4 + x^2 + 2x).$$

Call a polynomial $P(x)$ **integral-valued** if $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$.

Further example.

$$P(x) = \frac{1}{m} \sum_{d|m} \phi\left(\frac{m}{d}\right) x^d$$

for integers $m \geq 1$, where $\phi(k)$ is the number of integers among $1, 2, \ldots, k$ that are relatively prime to k. The first few are

$$x, \quad \frac{1}{2}(x^2 + x), \quad \frac{1}{3}(x^3 + 2x), \quad \frac{1}{4}(x^4 + x^2 + 2x).$$

For $n \geq 1$, $\frac{1}{m} \sum_{d|m} \phi\left(\frac{m}{d}\right) n^d$ **counts** the number of necklaces with m beads of colors $1, 2, \ldots, n$ up to a cyclic rotation (MacMahon 1892). It is **not** clear why it's in $\mathbb{Z}$ for $n < 0$. Will see why later!

Call a polynomial $P(x)$ **integral-valued** if $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$.

Further examples. If $P(x)$ is an integral-valued polynomial, so are

- $P(-x)$,
- $P(x+b)$ for $b \in \mathbb{Z}$,
- $P(Q(x))$ for any other integral-valued polynomial $Q(x)$,

Integral-valued polynomials

Call a polynomial $P(x)$ **integral-valued** if $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$.

Further examples. If $P(x)$ is an integral-valued polynomial, so are

- $P(-x)$,
- $P(x+b)$ for $b \in \mathbb{Z}$,
- $P(Q(x))$ for any other integral-valued polynomial $Q(x)$,
- $aP(x) + bQ(x) + cR(x)$, where $Q(x)$ and $R(x)$ are integral-valued polynomials and $a, b, c \in \mathbb{Z}$.

Integral-valued polynomials

Call a polynomial $P(x)$ **integral-valued** if $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$.

Further examples. If $P(x)$ is an integral-valued polynomial, so are

- $P(-x)$,
- $P(x+b)$ for $b \in \mathbb{Z}$,
- $P(Q(x))$ for any other integral-valued polynomial $Q(x)$,
- $aP(x) + bQ(x) + cR(x)$, where $Q(x)$ and $R(x)$ are integral-valued polynomials and $a, b, c \in \mathbb{Z}$.

What kind of nice description could there be of **all** such polynomials?

Theorem (Polya, 1915)

Let $N \in \mathbb{N}$. The integral-valued polynomials of degree $\leq N$ are exactly the polynomials that can be written as

$$a_0\binom{x}{0} + a_1\binom{x}{1} + \cdots + a_N\binom{x}{N}$$

for some integers $a_0, a_1, \ldots, a_N$. Moreover, an integral-valued polynomial can be written in this form in exactly one way.

We will explain where this formula for integral-valued polynomials comes from (not its uniqueness) using the method of finite differences, which is a discrete analogue of derivatives.

Classification of integral-valued polynomials: Examples

Recall that

$$\binom{x}{0} = 1,\ \binom{x}{1} = x,\ \binom{x}{2} = \frac{x(x-1)}{2},\ \binom{x}{3} = \frac{x(x-1)(x-2)}{6}.$$

In terms of these, integral-valued polynomials seen earlier are

$$\begin{aligned}
\frac{1}{2}(x^2+x) &= \binom{x}{2} + \binom{x}{1}, \\
\frac{1}{6}x(x+1)(2x+1) &= 2\binom{x}{3} + 3\binom{x}{2} + \binom{x}{1}, \\
\frac{1}{3}(x^3+2x) &= 2\binom{x}{3} + 2\binom{x}{2} + \binom{x}{1}, \\
\frac{1}{4}(x^4+x^2+2x) &= 6\binom{x}{4} + 9\binom{x}{3} + 4\binom{x}{2} + \binom{x}{1}.
\end{aligned}$$

[Motivation for proof] Finite differences of x^2

Start with a polynomial P.

- Write the values $P(0), P(1), P(2), \ldots$ in a line.
- Write the successive differences $P(1) - P(0), P(2) - P(1), \ldots$ on the next line.
- Write the successive differences of these successive differences on the next line.
- Etc.

Here is $P(x) = x^2$.

$$
\begin{array}{ccccccccccccc}
0 & & 1 & & 4 & & 9 & & 16 & & 25 & & 36 \\
 & 1 & & 3 & & 5 & & 7 & & 9 & & 11 & \\
 & & 2 & & 2 & & 2 & & 2 & & 2 & & \\
 & & & 0 & & 0 & & 0 & & 0 & & &
\end{array}
$$

[Motivation for proof] Finite differences of $3x^2 - x + 7$

Start with a polynomial P.

- Write the values $P(0), P(1), P(2), \ldots$ in a line.
- Write the successive differences $P(1) - P(0), P(2) - P(1), \ldots$ on the next line.
- Write the successive differences of these successive differences on the next line.
- Etc.

Here is $P(x) = 3x^2 - x + 7$.

$$
\begin{array}{ccccccccccccc}
7 & & 9 & & 17 & & 31 & & 51 & & 77 & & 109 \\
& 2 & & 8 & & 14 & & 20 & & 26 & & 32 & \\
& & 6 & & 6 & & 6 & & 6 & & 6 & & \\
& & & 0 & & 0 & & 0 & & 0 & & &
\end{array}
$$

[Motivation for proof] Finite differences of x^3

Start with a polynomial P.

- Write the values $P(0), P(1), P(2), \ldots$ in a line.
- Write the successive differences $P(1) - P(0), P(2) - P(1), \ldots$ on the next line.
- Write the successive differences of these successive differences on the next line.
- Etc.

Here is $P(x) = x^3$.

$$
\begin{array}{ccccccccccccc}
0 & & 1 & & 8 & & 27 & & 64 & & 125 & & 216 \\
& 1 & & 7 & & 19 & & 37 & & 61 & & 91 & \\
& & 6 & & 12 & & 18 & & 24 & & 30 & & \\
& & & 6 & & 6 & & 6 & & 6 & & & \\
& & & & 0 & & 0 & & 0 & & & &
\end{array}
$$

Classification of integral-valued polynomials: proof

Why does it always boil down to zeroes?

Classification of integral-valued polynomials: proof

Why does it always boil down to zeroes?

Main lemma: *If* $P(x)$ *is a polynomial of degree* $N \geq 1$ *then* $P(x+1) - P(x)$ *is a polynomial of degree* $N - 1$.

Why does it always boil down to zeroes?

Main lemma: *If $P(x)$ is a polynomial of degree $N \geq 1$ then $P(x+1) - P(x)$ is a polynomial of degree $N-1$.*

Special case: $P(x) = x^N$.
To show $(x+1)^N - x^N$ is a polynomial of degree $N-1$, the binomial theorem says

$$(x+1)^N = x^N + \binom{N}{1} x^{N-1} + \binom{N}{2} x^{N-2} + \cdots + 1.$$

Subtracting the x^N term leaves only terms of degree $\leq N-1$ on the right hand side, and the term $\binom{N}{1} x^{N-1} = N x^{N-1}$ has degree $N-1$.

Classification of integral-valued polynomials: proof

Why does it always boil down to zeroes?

Main lemma: *If $P(x)$ is a polynomial of degree $N \geq 1$ then $P(x+1) - P(x)$ is a polynomial of degree $N-1$.*

Classification of integral-valued polynomials: proof

Why does it always boil down to zeroes?

Main lemma: *If $P(x)$ is a polynomial of degree $N \geq 1$ then $P(x+1) - P(x)$ is a polynomial of degree $N-1$.*

General case: Set $P(x) = a_0 + a_1 x^1 + \cdots + a_N x^N$, $a_N \neq 0$. Then

$$\begin{aligned}
&P(x+1) - P(x) \\
&= \left(a_0 + a_1(x+1)^1 + \cdots + a_N(x+1)^N\right) \\
&- \left(a_0 + a_1 x^1 + \cdots + a_N x^N\right) \\
&= a_0 \underbrace{(1-1)}_{\text{vanishes}} + a_1 \underbrace{\left((x+1)^1 - x^1\right)}_{\substack{\text{degree } 0 \\ \text{(by special case)}}} + \cdots + a_N \underbrace{\left((x+1)^N - x^N\right)}_{\substack{\text{degree } N-1 \\ \text{(by special case)}}}.
\end{aligned}$$

Since $a_N \neq 0$, $P(x+1) - P(x)$ has degree $N-1$. After enough successive differences the polynomial becomes constant, and at the next step all successive differences are 0.

Classification of integral-valued polynomials: proof

We are now ready to prove the theorem (minus the "exactly one way" claim) by induction on N.

For polynomials of degree ≤ 0, $P(x) = a_0 = a_0 \binom{x}{0}$, where $a_0 = P(0) \in \mathbb{Z}$. So we can take $N \geq 1$.

Let $P(x)$ be an integral-valued polynomial of degree $\leq N$.

By main lemma, $P(x+1) - P(x)$ is a polynomial of degree $\leq N - 1$, and is integral-valued of course. Hence by induction hypothesis,

$$P(x+1) - P(x) = b_0 \binom{x}{0} + b_1 \binom{x}{1} + \cdots + b_{N-1} \binom{x}{N-1}$$

for some integers $b_0, b_1, \ldots, b_{N-1}$.

Classification of integral-valued polynomials: proof

We are now ready to prove the theorem (minus the "exactly one way" claim) by induction on N.

For polynomials of degree ≤ 0, $P(x) = a_0 = a_0 \binom{x}{0}$, where $a_0 = P(0) \in \mathbb{Z}$. So we can take $N \geq 1$.

Let $P(x)$ be an integral-valued polynomial of degree $\leq N$.

By main lemma, $P(x+1) - P(x)$ is a polynomial of degree $\leq N - 1$, and is integral-valued of course. Hence by induction hypothesis,

$$P(x+1) - P(x) = b_0 \binom{x}{0} + b_1 \binom{x}{1} + \cdots + b_{N-1} \binom{x}{N-1}$$

for some integers $b_0, b_1, \ldots, b_{N-1}$.

Using $P(x) - P(0)$ in place of $P(x)$, WLOG $P(0) = 0$ (subtracting constant term can't hurt).

Classification of integral-valued polynomials: proof

Using a telescoping sum, for every $n \geq 1$ we have

$$\sum_{k=0}^{n-1} (P(k+1) - P(k)) = P(n) - \underbrace{P(0)}_{=0} = P(n).$$

Classification of integral-valued polynomials: proof

Using a telescoping sum, for every $n \geq 1$ we have

$$\sum_{k=0}^{n-1} (P(k+1) - P(k)) = P(n) - \underbrace{P(0)}_{=0} = P(n).$$

Since

$$P(x+1) - P(x) = b_0 \binom{x}{0} + b_1 \binom{x}{1} + \cdots + b_{N-1} \binom{x}{N-1}$$

we set $x = k$ and get

$$P(k+1) - P(k) = b_0 \binom{k}{0} + b_1 \binom{k}{1} + \cdots + b_{N-1} \binom{k}{N-1}.$$

Substituting this above,

Classification of integral-valued polynomials: proof

Using a telescoping sum, for every $n \geq 1$ we have

$$\sum_{k=0}^{n-1}(P(k+1) - P(k)) = P(n) - \underbrace{P(0)}_{=0} = P(n).$$

Since

$$P(x+1) - P(x) = b_0\binom{x}{0} + b_1\binom{x}{1} + \cdots + b_{N-1}\binom{x}{N-1}$$

we set $x = k$ and get

$$P(k+1) - P(k) = b_0\binom{k}{0} + b_1\binom{k}{1} + \cdots + b_{N-1}\binom{k}{N-1}.$$

Substituting this above,

$$\sum_{k=0}^{n-1}\left(b_0\binom{k}{0} + b_1\binom{k}{1} + \cdots + b_{N-1}\binom{k}{N-1}\right) = P(n).$$

So for $n \geq 1$

$$
\begin{aligned}
P(n) &= \sum_{k=0}^{n-1} \left(b_0 \binom{k}{0} + b_1 \binom{k}{1} + \cdots + b_{N-1} \binom{k}{N-1} \right) \\
&= b_0 \sum_{k=0}^{n-1} \binom{k}{0} + b_1 \sum_{k=0}^{n-1} \binom{k}{1} + \cdots + b_{N-1} \sum_{k=0}^{n-1} \binom{k}{N-1}.
\end{aligned}
$$

But the hockey-stick identity says for every $j \geq 0$ that

$$
\sum_{k=0}^{n-1} \binom{k}{j} = \binom{n}{j+1}
$$

So for $n \geq 1$

$$
\begin{aligned}
P(n) &= \sum_{k=0}^{n-1} \left(b_0 \binom{k}{0} + b_1 \binom{k}{1} + \cdots + b_{N-1} \binom{k}{N-1} \right) \\
&= b_0 \sum_{k=0}^{n-1} \binom{k}{0} + b_1 \sum_{k=0}^{n-1} \binom{k}{1} + \cdots + b_{N-1} \sum_{k=0}^{n-1} \binom{k}{N-1} \\
&= b_0 \binom{n}{1} + b_1 \binom{n}{2} + \cdots + b_{N-1} \binom{n}{N},
\end{aligned}
$$

since the hockey-stick identity says for all $j \geq 0$ that

$$
\sum_{k=0}^{n-1} \binom{k}{j} = \binom{n}{j+1}.
$$

So

$$P(n) = b_0 \binom{n}{1} + b_1 \binom{n}{2} + \cdots + b_{N-1} \binom{n}{N}$$

for all $n \geq 1$.

So

$$P(n) = b_0\binom{n}{1} + b_1\binom{n}{2} + \cdots + b_{N-1}\binom{n}{N}$$

for all $n \geq 1$. Setting

$$Q(x) = b_0\binom{x}{1} + b_1\binom{x}{2} + \cdots + b_{N-1}\binom{x}{N},$$

the polynomials $P(x)$ and $Q(x)$ have $P(n) = Q(n)$ for all $n \geq 1$. Since a polynomial is determined by its values at infinitely many numbers, $P(x) = Q(x)$ for all x, so

$$P(x) = b_0\binom{x}{1} + b_1\binom{x}{2} + \cdots + b_{N-1}\binom{x}{N}.$$

So

$$P(n) = b_0\binom{n}{1} + b_1\binom{n}{2} + \cdots + b_{N-1}\binom{n}{N}$$

for all $n \geq 1$. Setting

$$Q(x) = b_0\binom{x}{1} + b_1\binom{x}{2} + \cdots + b_{N-1}\binom{x}{N},$$

the polynomials $P(x)$ and $Q(x)$ have $P(n) = Q(n)$ for all $n \geq 1$. Since a polynomial is determined by its values at infinitely many numbers, $P(x) = Q(x)$ for all x, so

$$P(x) = b_0\binom{x}{1} + b_1\binom{x}{2} + \cdots + b_{N-1}\binom{x}{N}.$$

$\square$

Summary

We have now proven the existence part of

Theorem

Let $N \in \mathbb{N}$. The integral-valued polynomials of degree $\leq N$ are exactly the polynomials that can be written as

$$a_0 \binom{x}{0} + a_1 \binom{x}{1} + \cdots + a_N \binom{x}{N}$$

for some integers $a_0, a_1, \ldots, a_N$. Moreover, an integral-valued polynomial can be written in this form in exactly one way.

Summary

We have now proven the existence part of

Theorem

Let $N \in \mathbb{N}$. The integral-valued polynomials of degree $\leq N$ are exactly the polynomials that can be written as

$$a_0\binom{x}{0} + a_1\binom{x}{1} + \cdots + a_N\binom{x}{N}$$

for some integers $a_0, a_1, \ldots, a_N$. Moreover, an integral-valued polynomial can be written in this form in exactly one way.

A polynomial of degree $\leq N$ is determined by its values at 0, 1, $\ldots, N$, and our proof only needed such values, so we proved

Corollary

If a polynomial $P(x)$ of degree $\leq N$ satisfies $P(n) \in \mathbb{Z}$ for $n = 0, 1, \ldots, N$ then $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$.

Therefore if $P(n) \in \mathbb{Z}$ for $n \geq 0$, $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$.

Coefficients

If $P(x)$ is integral-valued, how can we find $a_0, a_1, \ldots, a_N$ such that

$$P(x) = a_0 \binom{x}{0} + a_1 \binom{x}{1} + \cdots + a_N \binom{x}{N}?$$

Coefficients

If $P(x)$ is integral-valued, how can we find $a_0, a_1, \ldots, a_N$ such that

$$P(x) = a_0\binom{x}{0} + a_1\binom{x}{1} + \cdots + a_N\binom{x}{N}?$$

Ans: Use higher-order differences. Set $(\Delta P)(x) = P(x+1) - P(x)$, and for $j \geq 1$ set $(\Delta^{j+1} P)(x) = (\Delta^j P)(x+1) - (\Delta^j P)(x)$. Think of $(\Delta^j P)(x)$ as discrete analogue of jth derivative $P^{(j)}(x)$.

(Compare $P(x+1) - P(x)$ to $P'(x) = \lim_{h\to 0} \dfrac{P(x+h) - P(x)}{h}$.)

Coefficients

If $P(x)$ is integral-valued, how can we find $a_0, a_1, \ldots, a_N$ such that

$$P(x) = a_0 \binom{x}{0} + a_1 \binom{x}{1} + \cdots + a_N \binom{x}{N}?$$

Ans: Use higher-order differences. Set $(\Delta P)(x) = P(x+1) - P(x)$, and for $j \geq 1$ set $(\Delta^{j+1} P)(x) = (\Delta^j P)(x+1) - (\Delta^j P)(x)$. Think of $(\Delta^j P)(x)$ as discrete analogue of jth derivative $P^{(j)}(x)$.
(Compare $P(x+1) - P(x)$ to $P'(x) = \lim_{h \to 0} \dfrac{P(x+h) - P(x)}{h}$.)

Example. If $P(x) = 3x^2 - x + 7$ then

$$\begin{aligned} (\Delta P)(x) &= P(x+1) - P(x) \\ &= 6x + 2, \\ (\Delta^2 P)(x) &= (\Delta P)(x+1) - (\Delta P)(x) \\ &= 6, \end{aligned}$$

and $(\Delta^j P)(x) = 0$ for $j > 2$.

Coefficients

Theorem. *For any polynomial* $P(x)$ *of degree* $\leq N$,

$$P(x) = a_0 \binom{x}{0} + a_1 \binom{x}{1} + \cdots + a_N \binom{x}{N}$$

where $a_j = (\Delta^j P)(0) = \sum_{i=0}^{j} (-1)^{j-i} \binom{j}{i} P(i)$. *That is,*

$$P(x) = \sum_{j=0}^{\deg P} (\Delta^j P)(0) \binom{x}{j}.$$

Coefficients

Theorem. *For any polynomial $P(x)$ of degree $\leq N$,*

$$P(x) = a_0\binom{x}{0} + a_1\binom{x}{1} + \cdots + a_N\binom{x}{N}$$

where $a_j = (\Delta^j P)(0) = \sum_{i=0}^{j}(-1)^{j-i}\binom{j}{i}P(i)$. *That is,*

$$P(x) = \sum_{j=0}^{\deg P}(\Delta^j P)(0)\binom{x}{j}.$$

This is a discrete analogue of Taylor's formula

$$P(x) = \sum_{j=0}^{\deg P} P^{(j)}(0)\frac{x^j}{j!}.$$

Coefficients

We have seen several integral-valued polynomials $P(x)$ earlier, and how they are written as $a_0\binom{x}{0} + a_1\binom{x}{1} + \cdots + a_N\binom{x}{N}$:

$$\begin{aligned}
\frac{1}{2}(x^2+x) &= \binom{x}{2} + \binom{x}{1}, \\
\frac{1}{6}x(x+1)(2x+1) &= 2\binom{x}{3} + 3\binom{x}{2} + \binom{x}{1}, \\
\frac{1}{3}(x^3+2x) &= 2\binom{x}{3} + 2\binom{x}{2} + \binom{x}{1}, \\
\frac{1}{4}(x^4+x^2+2x) &= 6\binom{x}{4} + 9\binom{x}{3} + 4\binom{x}{2} + \binom{x}{1}.
\end{aligned}$$

All coefficients on the right can be found using the higher-order difference formula $(\Delta^j P)(0) = \sum_{i=0}^{j}(-1)^{j-i}\binom{j}{i}P(i)$ for the coefficient of $\binom{x}{j}$. Let's look at other examples.

Coefficients of $(x^p - x)/p$.

For prime p, $\frac{1}{p}(x^p - x)$ is integral-valued. How does it look in Polya's theorem?

- $\frac{1}{2}(x^2 - x) = \binom{x}{2}$.

Coefficients of $(x^p - x)/p$.

For prime p, $\frac{1}{p}(x^p - x)$ is integral-valued. How does it look in Polya's theorem?

- $\frac{1}{2}(x^2 - x) = \binom{x}{2}$.
- $\frac{1}{3}(x^3 - x) = 2\binom{x}{3} + 2\binom{x}{2}$.

Coefficients of $(x^p - x)/p$.

For prime p, $\frac{1}{p}(x^p - x)$ is integral-valued. How does it look in Polya's theorem?

- $\frac{1}{2}(x^2 - x) = \binom{x}{2}$.
- $\frac{1}{3}(x^3 - x) = 2\binom{x}{3} + 2\binom{x}{2}$.
- $\frac{1}{5}(x^5 - x) = 24\binom{x}{5} + 48\binom{x}{4} + 30\binom{x}{3} + 6\binom{x}{2}$.

For prime p, $\dfrac{1}{p}(x^p - x)$ is integral-valued. How does it look in Polya's theorem?

- $\dfrac{1}{2}(x^2 - x) = \dbinom{x}{2}$.
- $\dfrac{1}{3}(x^3 - x) = 2\dbinom{x}{3} + 2\dbinom{x}{2}$.
- $\dfrac{1}{5}(x^5 - x) = 24\dbinom{x}{5} + 48\dbinom{x}{4} + 30\dbinom{x}{3} + 6\dbinom{x}{2}$.
- $\dfrac{1}{p}(x^p - x) = \sum_{j=2}^{p} \dfrac{j!}{p} \left\{ {p \atop j} \right\} \dbinom{x}{j}$, where the curly braces denote Stirling numbers of the second kind.

Famous identities: for any integer $n \geq 1$,

$$\begin{aligned} 1 + 2 + \cdots + n &= \frac{1}{2} n(n+1), \\ 1^2 + 2^2 + \cdots + n^2 &= \frac{1}{6} n(n+1)(2n+1). \end{aligned}$$

For any $k \geq 1$, $1^k + 2^k + \cdots + n^k = S_k(n)$ for a polynomial $S_k(x)$ of degree $k+1$.

- $\frac{1}{2}x(x+1) = \binom{x}{2} + \binom{x}{1}$.
- $\frac{1}{6}x(x+1)(2x+1) = 2\binom{x}{3} + 3\binom{x}{2} + \binom{x}{1}$.
- $S_k(x) = \sum_{j=1}^{k+1} (j-1)! \left\{ {k+1 \atop j} \right\} \binom{x}{j}$, where the curly braces denote Stirling numbers of the second kind.

Coefficients: binomial coefficients I

- $\binom{x}{m} = \binom{x}{m}$, duh.

Coefficients: binomial coefficients I

- $\binom{x}{m} = \binom{x}{m}$, duh.
- $\binom{x+1}{m} = \binom{x}{m-1} + \binom{x}{m}$.
- $\binom{x+2}{m} = \binom{x}{m-2} + 2\binom{x}{m-1} + \binom{x}{m}$.
- $\binom{x+\ell}{m} = \sum_{k=0}^{m} \binom{\ell}{m-k}\binom{x}{k}$ for $\ell \geq 0$.

- $\binom{x}{m} = \binom{x}{m}$, duh.
- $\binom{x+1}{m} = \binom{x}{m-1} + \binom{x}{m}$.
- $\binom{x+2}{m} = \binom{x}{m-2} + 2\binom{x}{m-1} + \binom{x}{m}$.
- $\binom{x+\ell}{m} = \sum_{k=0}^{m} \binom{\ell}{m-k}\binom{x}{k}$ for $\ell \geq 0$.

  This is the Chu-Vandermonde convolution identity. To prove it, it suffices to show that $\binom{n+\ell}{m} = \sum_{k=0}^{m} \binom{\ell}{m-k}\binom{n}{k}$ for $n \in \mathbb{N}$, or even just for $0 \leq n \leq m$. There is a balls-and-urns argument.

Coefficients: binomial coefficients II

- $\binom{kx}{m} = \sum_{j=0}^{m} a_{j,k,m} \binom{x}{j}$ for $k \geq 1$,
  where $a_{j,k,m}$ is the number of $0,1$-matrices of size $k \times j$ with entry sum m without zero columns. (Thanks to Gjergji Zaimi.)

Bonus: a question

For each $m \geq 1$, let

$$\begin{aligned} P_m(x) &= \frac{1}{m!} \prod_{i=0}^{m-1} (x^m - x^i) \\ &= \frac{1}{m!}(x^m - 1)(x^m - x)(x^m - x^2) \cdots (x^m - x^{m-1}). \end{aligned}$$

Why is $P_m(x)$ integral-valued?

Bonus: a question

For each $m \geq 1$, let

$$P_m(x) = \frac{1}{m!} \prod_{i=0}^{m-1} (x^m - x^i)$$
$$= \frac{1}{m!} (x^m - 1)(x^m - x)(x^m - x^2) \cdots (x^m - x^{m-1}).$$

Why is $P_m(x)$ integral-valued?

There is a slick proof that $P_m(p) \in \mathbb{Z}$ for **prime** p. (Namely: The symmetric group S_m embeds into $\mathrm{GL}_m(\mathbb{Z}/p\mathbb{Z})$.) This generalizes to $P_m(p^r) \in \mathbb{Z}$ for **prime powers** p^r. But this is not enough to ensure $P_m(n) \in \mathbb{Z}$ for all integers n! (Yet, this holds.)

Bonus: a question

For each $m \geq 1$, let

$$P_m(x) = \frac{1}{m!} \prod_{i=0}^{m-1} (x^m - x^i)$$
$$= \frac{1}{m!} (x^m - 1)(x^m - x)(x^m - x^2) \cdots (x^m - x^{m-1}).$$

Why is $P_m(x)$ integral-valued?

There is a slick proof that $P_m(p) \in \mathbb{Z}$ for **prime** p. (Namely: The symmetric group S_m embeds into $\mathrm{GL}_m(\mathbb{Z}/p\mathbb{Z})$.) This generalizes to $P_m(p^r) \in \mathbb{Z}$ for **prime powers** p^r. But this is not enough to ensure $P_m(n) \in \mathbb{Z}$ for all integers n! (Yet, this holds.)

Thanks to Keith Conrad and Tom Roby for help.
Thank you for listening!

References

- Wikipedia, *Integer-valued polynomial*. http://en.wikipedia.org/wiki/Integer-valued_polynomial and references therein.
- Manjul Bhargava, *The Factorial Function and Generalizations*, American Mathematical Monthly, vol. 107, Nov. 2000, pp. 783-799. http://www.maa.org/sites/default/files/pdf/upload_library/22/Hasse/00029890.di021346.02p0064l.pdf
- Ronald L. Graham, Donald E. Knuth, and Oren Patashnik, *Concrete Mathematics*, 2nd edition, 1994.
- http://mathlinks.ro/viewtopic.php?t=421474, http://mathlinks.ro/viewtopic.php?t=299793

- Qimh Ritchey Xantcha, *Binomial rings: axiomatisation, transfer, and classification*, arXiv:1104.1931v3. http://arxiv.org/abs/1104.1931v3
- Manjul Bhargava, *On P-orderings, rings of integer-valued polynomials, and ultrametric analysis*, Journal of the AMS, vol. 22, no. 4, Oct. 2009, pp. 963-993. http://www.ams.org/journals/jams/2009-22-04/S0894-0347-09-00638-9/S0894-0347-09-00638-9.pdf

and many others ("binomial rings", λ-rings, etc.).