Integral-valued polynomials

Darij Grinberg

14 October 2013, Storrs
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**: \(P(x) = \frac{1}{2}x^2 - \frac{1}{2}x = \frac{x(x-1)}{2}\). For \(n \in \mathbb{Z}\), \(n\) or \(n-1\) is even, so \(\frac{n(n-1)}{2} \in \mathbb{Z}\).
What is an integral-valued polynomial?

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

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.
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 $x$. 
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 \((-1, 0, 7, \text{and } 26)\).

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 $\mathbb{Q}$. 

\[P(x) = x^2 - x^2 \text{ (since } n(n-1) \in \mathbb{Z} \text{ for all } n \in \mathbb{Z})\]

\[P(x) = x^2 + x^2 \text{ (since } n(n+1) \in \mathbb{Z} \text{ for all } n \in \mathbb{Z})\]

\[\not P(x) = x^4 - x^4 \text{ (since } P(2) = 7 \notin \mathbb{Z})\]
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. $P(x) = \frac{x^2 - x}{2}$ (since $\frac{n(n-1)}{2} \in \mathbb{Z}$ for all $n \in \mathbb{Z}$).

2. $P(x) = \frac{x^2 + x}{2}$ (since $\frac{n(n+1)}{2} \in \mathbb{Z}$ for all $n \in \mathbb{Z}$).

3. **not** $P(x) = \frac{x^4 - x}{4}$ (since $P(2) = \frac{7}{2}$).
Call a polynomial $P(x)$ **integral-valued** if $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$. 
Call a polynomial $P(x)$ \textbf{integral-valued} if $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$.

Examples.

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

---

**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. :)  
- $P(x) = \frac{1}{p}(x^p - x)$ 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
  
  $$P(n) = 1^2 + 2^2 + \cdots + n^2 \in \mathbb{Z}$$
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. :) 
- $P(x) = \frac{1}{p}(x^p - x)$ for all primes $p$. (Fermat’s little theorem.)
- $P(x) = \frac{1}{6}x(x + 1)(2x + 1)$, because 
  \[ P(n) = 1^2 + 2^2 + \cdots + n^2 \in \mathbb{Z} \text{ for } n \geq 0, \]
  \[ P(n) = -(1^2 + 2^2 + \cdots + (n' - 1)^2) \in \mathbb{Z} \text{ for } n = -n' < 0. \]
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

\[
\begin{align*}
\binom{x}{0} &= 1, & \binom{x}{1} &= x, & \binom{x}{2} &= \frac{x(x - 1)}{2}, & \binom{x}{3} &= \frac{x(x - 1)(x - 2)}{6}.
\end{align*}
\]
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

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

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

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

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 $Q(x)$,
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 \( a, b, c \in \mathbb{Z} \).
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

$$a_0 \begin{pmatrix} x \\ 0 \end{pmatrix} + a_1 \begin{pmatrix} x \\ 1 \end{pmatrix} + \cdots + a_N \begin{pmatrix} x \\ N \end{pmatrix}$$

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.
Recall that
\[
\binom{x}{0} = 1, \quad \binom{x}{1} = x, \quad \binom{x}{2} = \frac{x(x-1)}{2}, \quad \binom{x}{3} = \frac{x(x-1)(x-2)}{6}.
\]

In terms of these, integral-valued polynomials seen earlier are
\[
\frac{1}{2}(x^2 + x) = \binom{x}{2} + \binom{x}{1},
\]
\[
\frac{1}{6}x(x + 1)(2x + 1) = 2\binom{x}{3} + 3\binom{x}{2} + \binom{x}{1},
\]
\[
\frac{1}{3}(x^3 + 2x) = 2\binom{x}{3} + 2\binom{x}{2} + \binom{x}{1},
\]
\[
\frac{1}{4}(x^4 + x^2 + 2x) = 6\binom{x}{4} + 9\binom{x}{3} + 4\binom{x}{2} + \binom{x}{1}.
\]
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 $P(x) = x^2$.

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>4</th>
<th>9</th>
<th>16</th>
<th>25</th>
<th>36</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>7</td>
<td>9</td>
<td>11</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 $P(x) = 3x^2 - x + 7$.

<table>
<thead>
<tr>
<th>7</th>
<th>9</th>
<th>17</th>
<th>31</th>
<th>51</th>
<th>77</th>
<th>109</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>8</td>
<td>14</td>
<td>20</td>
<td>26</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
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 $P(x) = x^3$.

\[
\begin{array}{cccccccc}
0 & 1 & 8 & 27 & 64 & 125 & 216 \\
1 & 7 & 19 & 37 & 61 & 91 \\
6 & 12 & 18 & 24 & 30 \\
6 & 6 & 6 & 6 \\
0 & 0 & 0 & 0 \\
\end{array}
\]
Why does it always boil down to zeroes?
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 \( \binom{N}{1}x^{N-1} = Nx^{N-1} \) has 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 \( N - 1 \).
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 \( P(x) = a_0 + a_1x^1 + \cdots + a_Nx^N, a_N \neq 0 \). Then

\[
P(x + 1) - P(x) = (a_0 + a_1(x + 1)^1 + \cdots + a_N(x + 1)^N) - (a_0 + a_1x^1 + \cdots + a_Nx^N)
\]

\[
= a_0 (1 - 1) + a_1 ((x + 1)^1 - x^1) + \cdots + a_N ((x + 1)^N - x^N).
\]

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

For polynomials of degree $\leq 0$, $P(x) = a_0 = a_0 \begin{pmatrix} x \\ 0 \end{pmatrix}$, 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,

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

for some integers $b_0, b_1, \ldots, b_{N-1}$.
We are now ready to prove the theorem (minus the “exactly one way” claim) by induction on $N$.

For polynomials of degree $\leq 0$, $P(x) = a_0 = a_0\left(\begin{array}{c}x \\ 0 \end{array}\right)$, 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,

$$P(x + 1) - P(x) = b_0\left(\begin{array}{c}x \\ 0 \end{array}\right) + b_1\left(\begin{array}{c}x \\ 1 \end{array}\right) + \cdots + b_{N-1}\left(\begin{array}{c}x \\ N - 1 \end{array}\right)$$

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

$$\sum_{k=0}^{n-1} (P(k+1) - P(k)) = P(n) - P(0) = P(n).$$
Classification of integral-valued polynomials: proof

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

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

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

\[
\sum_{k=0}^{n-1} (P(k+1) - P(k)) = P(n) - P(0) = P(n).
\]

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 \( n \geq 1 \)

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

\[
= b_0 \sum_{k=0}^{n-1} \binom{k}{0} + b_1 \sum_{k=0}^{n-1} \binom{k}{1} + \cdots + b_{N-1} \sum_{k=0}^{n-1} \binom{k}{N-1}.
\]

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 \( n \geq 1 \)

\[
P(n) = \sum_{k=0}^{n-1} \binom{k}{0} b_0 + \binom{k}{1} b_1 + \cdots + \binom{k}{N-1} b_{N-1}
\]

\[
= b_0 \sum_{k=0}^{n-1} \binom{k}{0} + b_1 \sum_{k=0}^{n-1} \binom{k}{1} + \cdots + b_{N-1} \sum_{k=0}^{n-1} \binom{k}{N-1}
\]

\[
= b_0 \binom{n}{1} + b_1 \binom{n}{2} + \cdots + b_{N-1} \binom{n}{N},
\]

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

\[ P(x) = b_0 \binom{x}{1} + b_1 \binom{x}{2} + \cdots + b_{N-1} \binom{x}{N}. \]
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 \( n \in \mathbb{Z} \).
If $P(x)$ is integral-valued, how can we find $a_0, a_1, \ldots, a_N$ such that

$$P(x) = a_0 \binom{x}{0} + a_1 \binom{x}{1} + \cdots + a_N \binom{x}{N}?$$
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 $j$th derivative $P^{(j)}(x)$.

(Compare $P(x + 1) - P(x)$ to $P'(x) = \lim_{h \to 0} \frac{P(x + h) - P(x)}{h}$.)
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 $(\Delta^{j+1}P)(x) = (\Delta^jP)(x + 1) - (\Delta^jP)(x)$. Think of $(\Delta^jP)(x)$ as discrete analogue of $j$th derivative $P^{(j)}(x)$.

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

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

$$(\Delta P)(x) = P(x + 1) - P(x)$$

$$= 6x + 2,$$

$$(\Delta^2 P)(x) = (\Delta P)(x + 1) - (\Delta P)(x)$$

$$= 6,$$

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

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

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

\[
\frac{1}{2}(x^2 + x) = \binom{x}{2} + \binom{x}{1},
\]

\[
\frac{1}{6}x(x + 1)(2x + 1) = 2 \binom{x}{3} + 3 \binom{x}{2} + \binom{x}{1},
\]

\[
\frac{1}{3}(x^3 + 2x) = 2 \binom{x}{3} + 2 \binom{x}{2} + \binom{x}{1},
\]

\[
\frac{1}{4}(x^4 + x^2 + 2x) = 6 \binom{x}{4} + 9 \binom{x}{3} + 4 \binom{x}{2} + \binom{x}{1}.
\]

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?

\[
\frac{1}{2}(x^2 - x) = \binom{x}{2}.
\]
For prime \( p \), \( \frac{1}{p} (x^p - x) \) is integral-valued. How does it look in Pólya’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?

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

- \( \frac{1}{2}(x^2 - x) = \binom{x}{2} \).
- \( \frac{1}{3}(x^3 - x) = 2 \binom{x}{3} + 2 \binom{x}{2} \).
- \( \frac{1}{5}(x^5 - x) = 24 \binom{x}{5} + 48 \binom{x}{4} + 30 \binom{x}{3} + 6 \binom{x}{2} \).
- \( \frac{1}{p}(x^p - x) = \sum_{j=2}^{p} \frac{j!}{p} \left\{ \begin{array}{c} p \\ j \end{array} \right\} \binom{x}{j} \), where the curly braces denote Stirling numbers of the second kind.
Coefficients for sums of powers

Famous identities: for any integer \( n \geq 1 \),

\[
1 + 2 + \cdots + n = \frac{1}{2}n(n + 1),
\]

\[
1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}n(n + 1)(2n + 1).
\]

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

- \( \frac{1}{2}x(x + 1) = \binom{x}{2} + \binom{x}{1} \).
- \( \frac{1}{6}x(x + 1)(2x + 1) = 2\binom{x}{3} + 3\binom{x}{2} + \binom{x}{1} \).
- \( S_k(x) = \sum_{j=1}^{k+1} \frac{(j - 1)!}{j!} \left\{ k + 1 \atop j \right\} \binom{x}{j} \), where the curly braces denote Stirling numbers of the second kind.
\[
\binom{x}{m} = \binom{x}{m}, \text{ duh.}
\]
\[
\binom{x}{m} = \binom{x}{m}, \text{ duh.}
\]
\[
\binom{x+1}{m} = \binom{x}{m-1} + \binom{x}{m}.
\]
\[
\binom{x+2}{m} = \binom{x}{m-2} + 2\binom{x}{m-1} + \binom{x}{m}.
\]
\[
\binom{x+\ell}{m} = \sum_{k=0}^{m} \binom{\ell}{m-k} \binom{x}{k} \text{ for } \ell \geq 0.
\]
Coefficients: binomial coefficients I

\[
\binom{x}{m} = \binom{x}{m}, \text{ duh.}
\]

\[
\binom{x + 1}{m} = \binom{x}{m-1} + \binom{x}{m}.
\]

\[
\binom{x + 2}{m} = \binom{x}{m-2} + 2\binom{x}{m-1} + \binom{x}{m}.
\]

\[
\binom{x + \ell}{m} = \sum_{k=0}^{m} \binom{\ell}{m-k} \binom{x}{k} \text{ for } \ell \geq 0.
\]

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.
\( \binom{kx}{m} = \sum_{j=0}^{m} a_{j,k,m} \binom{x}{j} \) 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.)
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?
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 $\text{GL}_m(\mathbb{Z}/p\mathbb{Z})$.) 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.)
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 $GL_m(\mathbb{Z}/p\mathbb{Z})$.) 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!


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