Math 222 Fall 2022, Lecture 7: Introduction

website: `https://www.cip.ifi.lmu.de/~grinberg/t/22fco`

1. Introduction (cont'd)

1.3. Factorials and binomial coefficients (cont'd)

1.3.5. Integrality and arithmetic properties (cont'd)

Last time, we proved the following:

Theorem 1.3.14 (integrality of binomial coefficients)**.** For any $n \in \mathbb{Z}$ and $k \in \mathbb{R}$, the number $\binom{n}{k}$ is an integer.

Proposition 1.3.15. Let p be a prime number, and let $k \in \{1, 2, \ldots, p-1\}$. Then, $p \mid \binom{p}{k}$.

Here are some more arithmetic properties of BCs (= binomial coefficients):

Theorem 1.3.16 (Lucas's congruence)**.** Let p be a prime number. Let $a, b \in \mathbb{Z}$ and $c, d \in \{0, 1, \ldots, p-1\}$. Then,

$$\binom{pa+c}{pb+d} \equiv \binom{a}{b}\binom{c}{d} \bmod p.$$

Theorem 1.3.17 (Babbage's congruence)**.** Let p be a prime number. Let $a, b \in \mathbb{Z}$. Then,

$$\binom{pa}{pb} \equiv \binom{a}{b} \bmod p^2.$$

Elementary proofs of both of these theorems can be found in [Grinbe17].

Remark 1.3.18. Lucas's congruence gives you a quick way of computing the remainder of a binomial coefficient $\binom{n}{k}$ modulo a prime p: Write n and k in base p as follows:

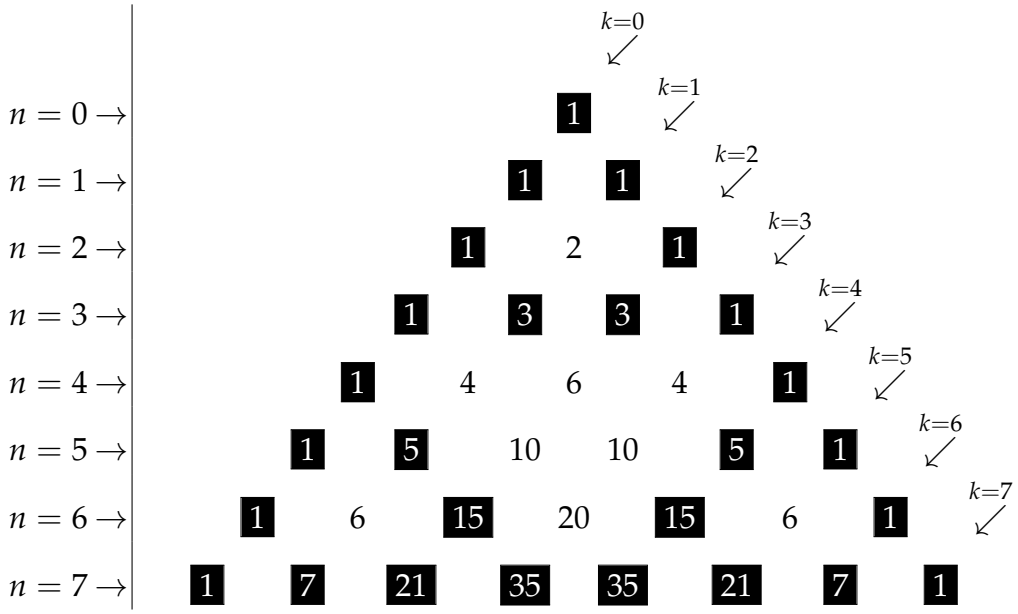
$$n = n_m p^m + n_{m-1} p^{m-1} + \cdots + n_0 p^0 \qquad \text{with } n_m, n_{m-1}, \ldots, n_0 \in \{0, 1, \ldots, p-1\};$$
$$k = k_m p^m + k_{m-1} p^{m-1} + \cdots + k_0 p^0 \qquad \text{with } k_m, k_{m-1}, \ldots, k_0 \in \{0, 1, \ldots, p-1\}.$$

(If n and k have different numbers of base-p digits, then there will be some leading zeroes here – i.e., one of n_m and k_m will be 0.) Then,

$$\binom{n}{k} \equiv \binom{n_m}{k_m}\binom{n_{m-1}}{k_{m-1}}\cdots\binom{n_0}{k_0} \bmod p.$$

This follows by applying Lucas's congruence repeatedly.

Lucas's congruence can also be used to explain the fractal structure that emerges in Pascal's triangle if we color each odd entry white (more precisely, we are printing it white-on-black):



The white parts resemble (a finite stage in the construction of) the Sierpiński triangle, and this is no accident, as the replication rule that is used to define the latter is also satisfied for the modulo-2 remainders of the BCs in Pascal's triangle: Namely, for any $n \in \mathbb{N}$ and any $a, b \in \{0, 1, \ldots, 2^n - 1\}$, we have

$$\binom{2^n + a}{b} \equiv \binom{a}{b} \bmod 2 \qquad \text{and} \qquad \binom{2^n + a}{2^n + b} \equiv \binom{a}{b} \bmod 2.$$

These two congruences can be proved easily using Lucas's congruence (see `http://larryriddle.agnesscott.org/ifs/siertri/Pascalmath.htm` for the details of this proof). Alternatively, they can also be proved by induction (see [18s-hw1s, Exercise 4] for this proof).

Binomial coefficients satisfy many more arithmetic properties (divisibilities and congruences, particularly modulo primes). See [Mestro14] and [Granvi05] for some of them.

1.3.6. The binomial formula

You have likely seen the **binomial formula** (aka the **binomial theorem**):

Theorem 1.3.19 (the binomial formula)**.** Let $x, y \in \mathbb{R}$ and $n \in \mathbb{N}$. Then,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

This formula is the reason why $\binom{n}{k}$ is called a "binomial coefficient": it is a literal coefficient in expanding the binomial $(x+y)^n$.

Of course, $\mathbb{R}$ can be replaced by $\mathbb{C}$ (or, for algebraists, by any commutative ring) in Theorem 1.3.19.

Example 1.3.20. For $n = 3$, the binomial formula becomes

$$\begin{aligned}
(x+y)^3 &= \sum_{k=0}^{3} \binom{3}{k} x^k y^{3-k} \\
&= \binom{3}{0} x^0 y^{3-0} + \binom{3}{1} x^1 y^{3-1} + \binom{3}{2} x^2 y^{3-2} + \binom{3}{3} x^3 y^{3-3} \\
&= 1x^0 y^{3-0} + 3x^1 y^{3-1} + 3x^2 y^{3-2} + 1x^3 y^{3-3} \\
&= y^3 + 3xy^2 + 3x^2 y + x^3.
\end{aligned}$$

Proof of Theorem 1.3.19. Let me first "simplify" the claim by replacing the finite sum $\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$ by the **infinite** sum $\sum_{k \in \mathbb{Z}} \binom{n}{k} x^k y^{n-k}$.

In order to do so, I need to explain two things:

- Why is the infinite sum $\sum_{k \in \mathbb{Z}} \binom{n}{k} x^k y^{n-k}$ well-defined?
- Why does it equal the finite sum $\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$?

Let me begin with the well-definedness. First of all, it isn't even clear that the addends $\binom{n}{k} x^k y^{n-k}$ are well-defined. For example, if $k = n+1$, then $y^{n-k} = y^{-1}$, which is undefined when $y = 0$. So the sum is undefined on-the-nose.

However, we solve this problem by **declaring** that a product of the form ab should always be understood to be 0 if $a = 0$, even if b is undefined. So,

for example, $0y^{-1} = 0$ even if y is 0. We recall that $\binom{n}{k} = 0$ whenever $k \notin \{0, 1, \ldots, n\}$ (because $\binom{n}{k} = 0$ by definition when $k \notin \mathbb{N}$, and because we showed in Lecture 5 that $\binom{n}{k} = 0$ when $k > n$). So, in the infinite sum $\sum_{k \in \mathbb{Z}} \binom{n}{k} x^k y^{n-k}$, all the addends except for the addends for $k \in \{0, 1, \ldots, n\}$ are 0 due to having the $\binom{n}{k} = 0$ factor at the front. In particular, this infinite sum has only finitely many addends. We furthermore decree that an infinite sum that has only finitely many nonzero addends is defined to be the sum of its nonzero addends[1]. Thus, the infinite sum $\sum_{k \in \mathbb{Z}} \binom{n}{k} x^k y^{n-k}$ is well-defined (since it has only finitely many nonzero addends), and equals the finite sum $\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$ (since all its nonzero addends also appear in the latter sum).

Thus, we are allowed to "simplify" the finite sum $\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$ to the infinite sum $\sum_{k \in \mathbb{Z}} \binom{n}{k} x^k y^{n-k}$ (although you have every right to wonder why this should count as "simplifying"). It remains to prove that

$$(x+y)^n = \sum_{k \in \mathbb{Z}} \binom{n}{k} x^k y^{n-k}. \tag{1}$$

We shall now prove (1) by induction on n:

Base case: For $n = 0$, our original binomial formula (as stated in Theorem 1.3.19) says that

$$(x+y)^0 = \sum_{k=0}^{0} \binom{0}{k} x^k y^{0-k} = \binom{0}{0} x^0 y^{0-0} = 1,$$

which is clearly true. Thus, (1) is also true for $n = 0$ (since $\sum_{k \in \mathbb{Z}} \binom{n}{k} x^k y^{n-k} = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$). This completes the base case.

Induction step: Fix $m \in \mathbb{N}$. Assume that (1) holds for $n = m$. We must show that (1) holds for $n = m + 1$. In other words, we must show that

$$(x+y)^{m+1} \stackrel{?}{=} \sum_{k \in \mathbb{Z}} \binom{m+1}{k} x^k y^{m+1-k}.$$

[1] For example, the sum $1 + 3 + 0 + 0 + 0 + \cdots$ (with infinitely many zeroes after the 3) thus equals $1 + 3 = 4$.

Our induction hypothesis says that (1) holds for $n = m$. In other words,

$$(x+y)^m = \sum_{k\in\mathbb{Z}} \binom{m}{k} x^k y^{m-k}. \tag{2}$$

Now,

$$\begin{aligned}
(x+y)^{m+1} &= (x+y)\cdot(x+y)^m \\
&= (x+y)\cdot \sum_{k\in\mathbb{Z}} \binom{m}{k} x^k y^{m-k} \qquad \text{(by (2))} \\
&= x\cdot \sum_{k\in\mathbb{Z}} \binom{m}{k} x^k y^{m-k} + y\cdot \sum_{k\in\mathbb{Z}} \binom{m}{k} x^k y^{m-k} \qquad \text{(by distributivity)} \\
&= \underbrace{\sum_{k\in\mathbb{Z}} \binom{m}{k} x x^k y^{m-k}}_{= \sum_{k\in\mathbb{Z}} \binom{m}{k-1} x x^{k-1} y^{m-(k-1)}} + \sum_{k\in\mathbb{Z}} \binom{m}{k} x^k y y^{m-k} \\
&\qquad \begin{array}{l}\text{(here, we substituted } k-1 \text{ for } k \text{ in this sum,}\\ \text{since the map } \mathbb{Z}\to\mathbb{Z},\ k\mapsto k-1 \text{ is a bijection)}\end{array} \\
&\qquad \left(\begin{array}{c}\text{here, we have moved the } x \text{ factor into the first sum,}\\ \text{and moved the } y \text{ factor into the second sum}\end{array}\right) \\
&= \sum_{k\in\mathbb{Z}} \binom{m}{k-1} \underbrace{x x^{k-1}}_{=x^k} \underbrace{y^{m-(k-1)}}_{=y^{m+1-k}} + \sum_{k\in\mathbb{Z}} \binom{m}{k} x^k \underbrace{y y^{m-k}}_{=y^{m-k+1}=y^{m+1-k}} \\
&= \sum_{k\in\mathbb{Z}} \binom{m}{k-1} x^k y^{m+1-k} + \sum_{k\in\mathbb{Z}} \binom{m}{k} x^k y^{m+1-k} \\
&= \sum_{k\in\mathbb{Z}} \left(\binom{m}{k-1} x^k y^{m+1-k} + \binom{m}{k} x^k y^{m+1-k} \right) \\
&= \sum_{k\in\mathbb{Z}} \underbrace{\left(\binom{m}{k-1} + \binom{m}{k} \right)}_{= \binom{m+1}{k}} x^k y^{m+1-k} = \sum_{k\in\mathbb{Z}} \binom{m+1}{k} x^k y^{m+1-k}. \\
&\qquad \text{(by Pascal's recurrence)}
\end{aligned}$$

But this is precisely our goal. Hence, (1) holds for $n = m+1$. This completes the induction step, so (1) is proved. And as we explained, this proves Theorem 1.3.19.

[You might well wonder what the point of our "simplification" was: Couldn't we have made the same argument using the original finite sum, without artificially making it infinite? Yes, we could, but this would have required a somewhat more complicated computation in our induction step, because substituting $k-1$ for k in a sum of the form $\sum_{k=0}^{m}$ turns it into a $\sum_{k=1}^{m+1}$ sum, but two

sums with different ranges cannot be immediately combined. Here is the computation we would need to do if we stuck with finite sums:

$$
\begin{aligned}
(x+y)^{m+1} &= (x+y)\cdot(x+y)^m \\
&= (x+y)\cdot\sum_{k=0}^{m}\binom{m}{k}x^k y^{m-k} \qquad \text{(by the induction hypothesis)} \\
&= x\cdot\sum_{k=0}^{m}\binom{m}{k}x^k y^{m-k} + y\cdot\sum_{k=0}^{m}\binom{m}{k}x^k y^{m-k} \\
&= \underbrace{\sum_{k=0}^{m}\binom{m}{k}x x^k y^{m-k}}_{=\sum_{k=1}^{m+1}\binom{m}{k-1}x x^{k-1}y^{m-(k-1)}} + \sum_{k=0}^{m}\binom{m}{k}x^k \underbrace{y y^{m-k}}_{\substack{=y^{m-k+1}\\=y^{m+1-k}}} \\
&\qquad \text{(here, we substituted } k-1 \text{ for } k \text{ in this sum,} \\
&\qquad \text{since the map } \{1,2,\ldots,m+1\}\to\{0,1,\ldots,m\},\ k\mapsto k-1 \\
&\qquad \text{is a bijection)} \\
&= \sum_{k=1}^{m+1}\binom{m}{k-1}\underbrace{x x^{k-1}}_{=x^k}\underbrace{y^{m-(k-1)}}_{=y^{m+1-k}} + \sum_{k=0}^{m}\binom{m}{k}x^k y^{m+1-k} \\
&= \sum_{k=1}^{m+1}\binom{m}{k-1}x^k y^{m+1-k} + \sum_{k=0}^{m}\binom{m}{k}x^k y^{m+1-k} \\
&= \sum_{k=0}^{m+1}\binom{m}{k-1}x^k y^{m+1-k} + \sum_{k=0}^{m+1}\binom{m}{k}x^k y^{m+1-k} \\
&\qquad \left(\begin{array}{c}\text{here, we have extended the first sum by an extra}\\ \text{addend for } k=0, \text{ and the second sum by}\\ \text{an extra addend for } k=m+1; \text{ this is allowed}\\ \text{because both of these extra addends are } 0\\ \left(\text{since } \binom{m}{-1}=0 \text{ and } \binom{m}{m+1}=0\right)\end{array}\right) \\
&= \sum_{k=0}^{m+1}\left(\binom{m}{k-1}x^k y^{m+1-k} + \binom{m}{k}x^k y^{m+1-k}\right) \\
&= \sum_{k=0}^{m+1}\underbrace{\left(\binom{m}{k-1}+\binom{m}{k}\right)}_{=\binom{m+1}{k}} x^k y^{m+1-k} = \sum_{k=0}^{m+1}\binom{m+1}{k}x^k y^{m+1-k}. \\
&\qquad \text{(by Pascal's recurrence)}
\end{aligned}
$$

Note what we gained and what we lost: We gained by not having to worry about the well-definedness of infinite sums, but we lost in that we now had to pay attention to the bounds of our sums. This is a tradeoff that sometimes is

worth making and sometimes is not. In more complicated situations, paying attention to the bounds is often harder (and certainly more distracting), so the clarity of infinite sums is preferrable.] □

One takeaway from this proof is that infinite sums often are easier to work with than finite sums. The infinite sums we are talking about are not "properly infinite sums" like $\sum_{i=0}^{\infty} \frac{1}{2^i}$, but actually just "finite sums in disguise", i.e., infinite sums with only finitely many nonzero addends. As we said in our above proof:

Definition 1.3.21. An infinite sum with only finitely many nonzero addends is defined to be the sum of these nonzero addends. That is, if S is an infinite set, and if a_s is a number for each $s \in S$, and if we know that only finitely many $s \in S$ satisfy $a_s \neq 0$, then the sum $\sum_{s \in S} a_s$ is understood to mean $\sum_{\substack{s \in S; \\ a_s \neq 0}} a_s$.

Infinite sums like this behave almost as nicely as finite sums; in particular, all the summation rules still apply, except for the interchange of summations (which we haven't properly discussed yet). See [Grinbe15, §2.14.15] for a rigorous treatment of such sums.

Let us draw some easy conclusions from the binomial formula:

Corollary 1.3.22. Let $n \in \mathbb{N}$. Then, $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

Proof. Set $x = 1$ and $y = 1$ in the binomial formula. □

Proposition 1.3.23. Let $n \in \mathbb{N}$. Then, $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = [n = 0]$. (Here, we are again using truth values: $[n = 0] = \begin{cases} 1, & \text{if } n = 0; \\ 0, & \text{if } n \neq 0. \end{cases}$)

Proof. Set $x = -1$ and $y = 1$ in the binomial formula to obtain

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = (-1+1)^n = 0^n = \begin{cases} 1, & \text{if } n = 0; \\ 0, & \text{if } n \neq 0 \end{cases} = [n = 0].$$

□

1.3.7. Other properties of binomial coefficients

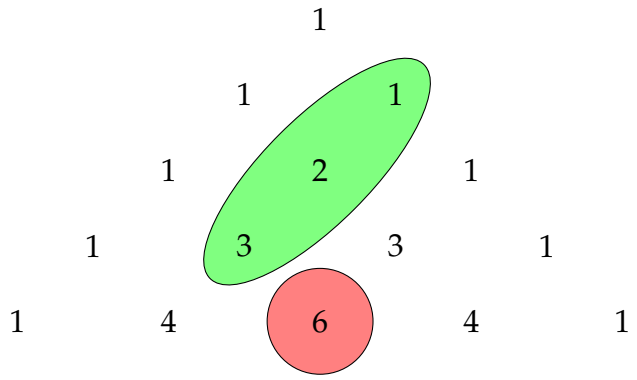
Here is an assortment of other properties of BCs:

Theorem 1.3.24 ("hockey-stick identity"). Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$. Then,

$$\begin{aligned}
&\binom{0}{k} + \binom{1}{k} + \binom{2}{k} + \cdots + \binom{n}{k} \\
&= \binom{k}{k} + \binom{k+1}{k} + \binom{k+2}{k} + \cdots + \binom{n}{k} \\
&= \binom{n+1}{k+1}.
\end{aligned}$$

Proof. Not now, but you can actually easily prove this on your own. □

The "hockey-stick identity" owes its name to the following visual representation on Pascal's triangle:



(this represents the case when $n = 3$ and $k = 1$; the addends on the left hand side are the numbers in the oblong green ellipse, while the right hand side is the number in the red circle). Note that the $k = 1$ case of the hockey-stick identity is the Little Gauss formula $1 + 2 + \cdots + n = \binom{n+1}{2} = \dfrac{n(n+1)}{2}$.

The Fibonacci numbers can be read off from Pascal's triangle by summing the entries along certain "slanted diagonals":

Proposition 1.3.25. Let $n \in \mathbb{N}$. Then, the Fibonacci number f_{n+1} is

$$f_{n+1} = \sum_{k=0}^{n} \binom{n-k}{k} = \binom{n-0}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \cdots + \binom{n-n}{n}.$$

Proof. We will prove this next time combinatorially, but this is also easy to prove by induction on n. □

Note that about half the addends in the sum $\sum_{k=0}^{n} \binom{n-k}{k}$ are 0 (because $\binom{n-k}{k} = 0$ when $0 \leq n-k < k$). However, you cannot extend this sum further past $k = n$ (without changing its value), because as k grows past n, the BCs $\binom{n-k}{k}$ again become nonzero and therefore the sum changes. So beware of writing it as $\sum_{k \in \mathbb{N}} \binom{n-k}{k}$.

Here is a "hidden symmetry" of BCs that you will not see from Pascal's triangle, because it involves fractional inputs:

Proposition 1.3.26. Let $n \in \mathbb{N}$. Then,

$$\binom{-1/2}{n} = \left(\frac{-1}{4}\right)^n \binom{2n}{n}.$$

Proof. Nice exercise. (Exercise 1.3.5 in the 2019 notes.) □

References

[Granvi05] Andrew Granville, *Binomial coefficients modulo prime powers*, preprint.
`https://web.archive.org/web/20181024055320/http://ebooks.bharathuniv.ac.in/gdlc1/gdlc1/EngineeringMergedLibraryv3.0/AndrewGranville/BinomialCoefficientsModuloPrimePowers(5579)/BinomialCoefficientsModuloPrimePowers-AndrewGranville.pdf`

[Grinbe15] Darij Grinberg, *Notes on the combinatorial fundamentals of algebra*, 15 September 2022.
`http://www.cip.ifi.lmu.de/~grinberg/primes2015/sols.pdf`

[Grinbe17] Darij Grinberg, *The Lucas and Babbage congruences*, 10 January 2019.
`https://www.cip.ifi.lmu.de/~grinberg/lucascong.pdf`

[18s-hw1s] Darij Grinberg, *UMN Spring 2018 Math 4707 homework set #1 with solutions*, `http://www.cip.ifi.lmu.de/~grinberg/t/18s/hw1s.pdf`

[Mestro14] Romeo Meštrović, *Lucas' theorem: its generalizations, extensions and applications (1878–2014)*, arXiv:1409.3820v1.