

A Novel Formula for Binomial Coefficients

Joseph M. Shunia

August 2023

Abstract

In this paper, we introduce a novel formula for binomial coefficients: $\binom{n}{k} = \left\lfloor \frac{(1+2^n)^n}{2^{nk}} \right\rfloor \bmod 2^n$ for $n > 0$ and $0 \leq k \leq n$. This formula utilizes only basic arithmetic operations and represents a significant departure from traditional methods, which typically involve factorials or the Gamma function. It also establishes an intriguing connection between modular arithmetic and binomial coefficients. The derivation of our formula is rooted in a rarely explored property of polynomials, specifically, that any polynomial with non-negative integer coefficients can be completely determined by the values $P(1)$ and $P(P(1))$. We demonstrate how this property is used to derive our formula and extend it to polynomials over a field. This novel approach not only offers a simple method to compute binomial coefficients, but also opens the door to new insights and formulas pertaining to binomial coefficients and related topics, such as multinomial coefficients and factorials.

1 Introduction

Binomial coefficients, denoted as $\binom{n}{k}$, are a cornerstone of mathematical theory. They quantify the number of distinct ways to select k elements from a set of n elements, irrespective of the order of selection. These coefficients permeate various branches of mathematics, from the coefficients in the expansion of a binomial equation to the calculation of probabilities in statistical theory. Traditional methods to compute binomial coefficients include the use of Pascal's triangle, factorials, or the Gamma function [1]. Despite the prevalence of these methods, there is always room for fresh perspectives that can lead to novel insights and applications. In this paper, we introduce such a perspective.

We present a new formula to compute binomial coefficients, given by:

$$\binom{n}{k} = \left\lfloor \frac{(1+2^n)^n}{2^{nk}} \right\rfloor \bmod 2^n, \quad \text{for } n > 0 \text{ and } 0 \leq k \leq n \quad (1)$$

This formula stems from a fascinating property of polynomials that has been rarely explored in mathematical literature. By connecting the computation of

binomial coefficients with this polynomial property, we establish a formula that depends only on basic arithmetic operations. Our contribution is not just in offering an alternative computation method but in unveiling a connection that may lead to further explorations and insights in both combinatorics and number theory.

2 Preliminaries and Definitions

2.1 Definition of Polynomial Function

We define $P(x)$ as the polynomial function:

$$P(x) = 1 + x \quad (2)$$

To denote $P(x)$ raised to the power of n , we write:

$$\begin{aligned} P(x)^n &= (1 + x)^n \\ &= a_n x^n + a_{n-1} x^{n-1} + \dots + a_k x^k + \dots + a_1 x + a_0 \end{aligned}$$

We define $P(x)_k^n$ to represent the coefficient of the k -th degree term in the polynomial expansion of $P(x)^n$, that is the value of a_k in $a_k x^k$. Using this definition, we can write the polynomial expansion of $P(x)^n$ as the sum:

$$P(x)^n = \sum_{k=0}^n P(x)_k^n \cdot x^k \quad (3)$$

2.2 Polynomial Expansion and Binomial Coefficients

If n is a non-negative integer, then by the Binomial Theorem [2] we have:

$$P(x)^n = (1 + x)^n = \sum_{k=0}^n \binom{n}{k} x^k \quad (4)$$

Since we have defined $P(x)_k^n$ to represent the coefficient of the k -th degree term in the polynomial expansion of $P(x)^n$, it follows that:

$$P(x)^n = \sum_{k=0}^n P(x)_k^n \cdot x^k = \sum_{k=0}^n \binom{n}{k} x^k \quad (5)$$

As the coefficients of the terms in $P(x)$ are precisely the binomial coefficients for the n -th row of Pascal's Triangle [3], it is apparent:

$$P(x)_k^n = \binom{n}{k} \quad (6)$$

3 Derivation of the Formula

3.1 A Key Property of Polynomials

We explore a key property of polynomials that plays a pivotal role in our subsequent proofs. The property in question is that a polynomial's coefficients and terms can be completely determined by judiciously selecting two inputs.

Theorem 1. *If $P(x)$ is a polynomial with non-negative integer coefficients, it can be completely determined by the values $P(1)$ and $P(P(1))$.*

Proof. Let $q = P(1)$, which gives the sum of the coefficients. Consider $P(P(1)) = P(q)$ expressed in base q ; the digits correspond exactly to the coefficients of P . The only possible ambiguity arises if $P(q) = q \cdot n$ for some n , but since the coefficients sum to q , we deduce that $P = q \cdot x^{n-1}$ in this case [4]. \square

Remark. This property appears to be underexplored in the literature; we were unable to find any papers explicitly describing it. However, it has been the subject of some online discussion and at least one blog post [5]. The proof given above was first proposed by user ARupinski in a MathOverflow post [4] and has been slightly modified for the purposes of this paper.

The choice of 1 as an input for $P(x)$ is not particularly special; if we replace 1 with any non-zero integer, the proof will hold. This revelation enables us to observe that the theorem and its proof can be generalized to work with polynomials over a field:

Theorem 2. *Let F be a field. If $P(x)$ is a polynomial with coefficients in F , and $Q(x)$ is any non-zero polynomial with coefficients in F , then $P(x)$ can be completely determined by the values $P(Q(1))$ and $P(P(Q(1)))$.*

Proof. Let $q = P(Q(1))$, which gives the sum of the coefficients of P evaluated at $Q(1)$. Consider $P(P(Q(1))) = P(q)$ expressed in base q ; the digits correspond exactly to the coefficients of P . The only possible ambiguity arises if $P(q) = q \cdot n$ for some n , but since the coefficients evaluated at $Q(1)$ sum to q , we deduce that $P = q \cdot x^{n-1}$ in this case. \square

3.2 Application of the Polynomial Property

The value of $P(1)^n$ is simply the summation of the coefficients of $P(x)^n$. It is easy to see that:

$$P(1)^n = \sum_{k=0}^n \binom{n}{k} 1^k = (1+1)^n = 2^n \quad (7)$$

$$P(P(1)^n)^n = \sum_{k=0}^n \binom{n}{k} (P(1)^n)^k = (1 + P(1)^n)^n \quad (8)$$

$$= \sum_{k=0}^n \binom{n}{k} (2^n)^k = (1 + 2^n)^n \quad (9)$$

We can now use Theorem 1 to recover the coefficients of $P(x)^n$. We will achieve this by first encoding $P(P(1)^n)^n$ in base $P(1)^n$, and then recovering the coefficients of $P(x)^n$ from the encoded value.

3.3 Reconstruction of Polynomial Coefficients

Theorem 3. *The formula to recover the k -th coefficient of $P(x)^n$ is given by:*

$$P(x)_k^n = \left\lfloor \frac{(1 + P(1)^n)^n \bmod P(1)^{nk+n}}{P(1)^{nk}} \right\rfloor \quad (10)$$

Proof. Given an integer n and a base $b > 1$. Let $L = \lfloor \log_b n \rfloor$. Then the encoded representation of n in base b is the unique representation of n , such that [6]:

$$n = \sum_{k=0}^L b^k \left\lfloor \frac{n \bmod b^{k+1}}{b^k} \right\rfloor \quad (11)$$

By inserting $P(1)$ into the equation, we can see:

$$P(x)_k^n = \left\lfloor \frac{P(P(1)^n)^n \bmod (P(1)^n)^{k+1}}{(P(1)^n)^k} \right\rfloor \quad (12)$$

$$= \left\lfloor \frac{(1 + P(1)^n)^n \bmod P(1)^{nk+n}}{P(1)^{nk}} \right\rfloor \quad (13)$$

Hence, the theorem is proven. \square

3.4 Main Theorem and Its Proof

Theorem 4.

$$\binom{n}{k} = \left\lfloor \frac{(1 + 2^n)^n}{2^{nk}} \right\rfloor \bmod 2^n, \quad \text{for } n > 0 \text{ and } 0 \leq k \leq n \quad (14)$$

Proof. Step 1: Proof that the equation is valid:

We begin with the identity we established in Theorem 3:

$$P(x)_k^n = \left\lfloor \frac{(1 + P(1)^n)^n \bmod P(1)^{nk+n}}{P(1)^{nk}} \right\rfloor \quad (15)$$

By substituting $P(x)_k^n = \binom{n}{k}$ and $P(1) = 2$, we have:

$$\binom{n}{k} = \left\lfloor \frac{(1 + 2^n)^n \bmod 2^{nk+n}}{2^{nk}} \right\rfloor \quad (16)$$

Next, we define $X = (1 + 2^n)^n$, $Y = 2^{nk+n}$, $Z = 2^{nk}$. By replacement:

$$\binom{n}{k} = \left\lfloor \frac{X \bmod Y}{Z} \right\rfloor \quad (17)$$

To simplify the expression, we can utilize the following well-known identity for the mod operation [7]:

$$a \bmod b = a - b \left\lfloor \frac{a}{b} \right\rfloor \quad (18)$$

By application of the identity, the expression simplifies as follows:

$$\binom{n}{k} = \left\lfloor \frac{X \bmod Y}{Z} \right\rfloor \quad (19)$$

$$= \left\lfloor \frac{X - Y \left\lfloor \frac{X}{Y} \right\rfloor}{Z} \right\rfloor \quad (20)$$

$$= \left\lfloor \frac{X}{Z} - \frac{Y}{Z} \left\lfloor \frac{X}{Y} \right\rfloor \right\rfloor \quad (21)$$

Next, we replace X , Y , and Z with their respective values and simplify further:

$$\binom{n}{k} = \left\lfloor \frac{X}{Z} - \frac{Y}{Z} \left\lfloor \frac{X}{Y} \right\rfloor \right\rfloor \quad (22)$$

$$= \left\lfloor \frac{(1 + 2^n)^n}{2^{nk}} - \frac{2^{nk+n}}{2^{nk}} \left\lfloor \frac{(1 + 2^n)^n}{2^{nk+n}} \right\rfloor \right\rfloor \quad (23)$$

$$= \left\lfloor \frac{(1 + 2^n)^n}{2^{nk}} - 2^n \left\lfloor \frac{(1 + 2^n)^n}{2^{nk+n}} \right\rfloor \right\rfloor \quad (24)$$

$$= \left\lfloor \frac{(1 + 2^n)^n}{2^{nk}} \right\rfloor - 2^n \left\lfloor \frac{(1 + 2^n)^n}{2^{nk+n}} \right\rfloor \quad (25)$$

Finally, we again make use of the mod operation identity (18) to simplify:

$$\binom{n}{k} = \left\lfloor \frac{(1 + 2^n)^n}{2^{nk}} \right\rfloor \bmod 2^n \quad (26)$$

We have arrived at our formula.

Step 2: Proof that the equation holds only for $n > 0$ and $0 \leq k \leq n$:

To prove why the equation $\binom{n}{k} = \left\lfloor \frac{(1+2^n)^n}{2^{nk}} \right\rfloor \bmod 2^n$ holds only for $n > 0$ and $0 \leq k \leq n$, we consider the following cases:

1. $n \leq 0$: In this case, the modulus becomes 2^{-n} and the original expression does not make sense.
2. $k < 0$: In this case, we have $2^{-nk} = \frac{1}{2^{nk}}$ and the original expression becomes $2^{nk}(1 + 2^n)^n \bmod 2^n$, which is always equal to 0 since $2^n \mid 2^{nk}$.

3. $k > n$: In this case, $2^{nk} > (1 + 2^n)^n > 2^{nn}$, hence $\left\lfloor \frac{(1+2^n)^n}{2^{nk}} \right\rfloor = 0$. We note that $\binom{n}{k} = \binom{k}{n}$ here, which cannot equal 0.

Conclusion:

We have shown that our formula is valid and that it holds only for $n > 0$ and $0 \leq k \leq n$. Hence, the theorem is proven. \square

4 Summary

We have introduced and proven a novel formula for computing binomial coefficients, leveraging a seldom-explored property of polynomials. This formula facilitates the calculation of $\binom{n}{k}$ through a sequence of straightforward arithmetic operations.

Our work strengthens the connection between binomial coefficients and polynomial functions, while also establishing a new link to modular arithmetic; a link that is not only mathematically elegant, but also ripe with potential for further exploration. The formula itself serves not merely as an alternative means to compute binomial coefficients, but as a gateway to new mathematical identities and relations.

This work underscores the idea that profound insights can often emerge from concepts that, once discovered, seem simple and obvious, yet have remained overlooked. We hope that our findings inspire others to revisit well-explored problems, with the potential of uncovering similarly simple yet powerful insights. Such discoveries serve as a reminder of the vast potential for innovation that lies within the realm of seemingly well-explored mathematical domains.

5 Future Directions

Future research could explore the computational efficiency of the formula and its behavior for large values of n and k , with a view to potential optimizations. This may be of particular importance, as applying our formula to the computation of factorials may unearth new and more efficient methods that can be applied to important problems in computer science and number theory, such as primality testing and integer factorization. Further investigation into the polynomial property and its generalization could potentially reveal applications in computing values of other sequences, like multinomial coefficients. An examination of the relationship between modular arithmetic and binomial coefficients also presents a promising avenue for exploration.

References

- [1] Richard A Brualdi. *Introductory Combinatorics*. Prentice Hall, 1992.

- [2] James Stewart. *Calculus: Early Transcendentals*. Cengage Learning, 2007.
- [3] Kenneth H Rosen. *Discrete Mathematics and Its Applications*. McGraw-Hill Science/Engineering/Math, 2011.
- [4] Rupinski A. Mathoverflow: Application of polynomials with non-negative coefficients. <https://mathoverflow.net/questions/91827/>, 2012. Accessed: 2023-08-05.
- [5] Cook J. Polynomial determined by two inputs. <https://www.johndcook.com/blog/2012/03/27/polynomial-trick/>, 2012. Accessed: 2023-08-05.
- [6] Thomas H Cormen, Charles E Leiserson, Ronald L Rivest, and Clifford Stein. *Introduction to Algorithms*. MIT press, 2009.
- [7] Ivan Niven, Herbert S Zuckerman, and Hugh L Montgomery. *An Introduction to the Theory of Numbers*. John Wiley & Sons, 2008.