A Novel Formula for Binomial Coefficients

Joseph M. Shunia

August 2023

Abstract

Computing binomial coefficients is a fundamental problem in combinatorics and number theory, with applications across mathematics. The typical approach relies on factorials, Gamma functions, or Pascal's triangle. 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 $0 \le k \le n$. We generalize the formula to multinomials, and discuss how it follows from a key property of polynomial interpolation rarely highlighted in textbooks. The simplicity of our arithmetic approach provides opportunities to develop more efficient algorithms and analyze computational complexity. Further, our formula establishes a new connection between binomial coefficients and modular arithmetic that may yield theoretical insights into their underlying mathematical foundations.

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:

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

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:

$$P(x) = 1 + x \tag{2}$$

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

$$P(x)^n = (1+x)^n$$
$$= a_n x^n + a_{n-1} x^{n-1} + \ldots + a_k x^k + \ldots + a_1 x + a_0$$

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:

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

2.2 Polynomial Expansion and Binomial Coefficients

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

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

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:

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

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:

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

2.3 Polynomial Interpolation

Polynomial interpolation is the problem of constructing a polynomial $P(x)$ that passes through a given set of data points $(x0, y0), (x1, y1), \ldots, (xn, yn)$. That is, finding a polynomial $P(x)$ such that $P(xi) = yi$ for $i = 0, 1, \ldots, n$ [4, 5].

There are various methods to interpolate polynomials, including Lagrange interpolation, Newton polynomial interpolation, and methods using divided differences [4, 5]. A fundamental result is that there exists a unique polynomial of degree n or less that interpolates $n+1$ data points [4]. The key fact we require is that a polynomial is uniquely determined if we know its value at enough points. Specifically, if we know the value of $P(x)$ at $n + 1$ distinct inputs, then we can recover its terms, and therefore the coefficients [6].

We will utilize a less known variant of this idea: that a polynomial can be unambiguously determined by evaluating just two carefully selected inputs [7, 8]. This forms the basis for our subsequent derivations of formula for binomial coefficients and its generalization to multinomials.

3 Derivation of the Formula

3.1 A Key Property of Polynomials

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 [7]. $\square$

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 [8]. The proof given above was first proposed by user ARupinski in a MathOverflow post [7] 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:

Theorem 2. *If $P(x)$ is a polynomial with non-negative integer coefficients, and $Q(x)$ is any non-zero polynomial with integer coefficients, 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. $\qquad\square$

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:

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

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

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

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:*

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

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 [9]:

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

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

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

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

Hence, the theorem is proven. $\qquad\square$

3.4 Main Theorem and Its Proof

Theorem 4.

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

Proof. **Step 1: Proof that the equation is valid:**
We begin with the identity we established in Theorem 3:

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

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

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

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

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

To simplify the expression, we can utilize the following well-known identity for the mod operation [10]:

$$a \bmod b = a - b \left\lfloor \frac{a}{b} \right\rfloor \tag{18}$$

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

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

$$= \left\lfloor \frac{X - Y \left\lfloor \frac{X}{Y} \right\rfloor}{Z} \right\rfloor \tag{20}$$

$$= \left\lfloor \frac{X}{Z} - \frac{Y}{Z} \left\lfloor \frac{X}{Y} \right\rfloor \right\rfloor \tag{21}$$

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

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

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

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

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

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

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

We have arrived at our formula.

Step 2: Proof that the equation holds only for $n > 0$ and $0 \le k \le n$:
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 $0 \le k \le n$, we consider the following cases:

1. $n \le 0$: In this case, the modulus becomes 2^{-n} and the original equation 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 $0 \le k \le n$. Hence, the theorem is proven. $\qquad\square$

4 Generalization to Coefficients in the Multinomial Expansion of Univariate Polynomials

4.1 Notation for Coefficients

We introduce a simplified notation to represent coefficients in the multinomial expansion of univariate polynomials. To denote the coefficient of the term with degree k in the polynomial expansion of $(1 + x + \ldots + x^D)^n$, we write:

$$\underline{D}\binom{n}{k}$$

Examples

1. For the binomial expansion $(1+x)^n$, the coefficient of the term x^k can be denoted as $\underline{1}\binom{n}{k}$. This is equivalent to the conventional binomial coefficient $\binom{n}{k}$.

2. For the trinomial expansion $(1 + x + x^2)^n$, the coefficient of the term x^k can be represented as $\underline{2}\binom{n}{k}$.

4.2 Generalized Formula and Its Proof

Theorem 5.

$$\underline{D}\binom{n}{k} = \left\lfloor \left(\frac{(D+1)^{nD+n} - 1}{(D+1)^n - 1} \right)^n \cdot (D+1)^{-nk} \right\rfloor \bmod (D+1)^n, \tag{27}$$

$$\text{for } n > 0 \text{ and } 0 \leq k \leq nD \tag{28}$$

Proof. **Step 1: Proof that the equation is valid:**
We define the polynomial function:

$$P(x, D)^n = (1 + x + \ldots + x^D)^n \tag{29}$$

In this case, it is clear that:

$$P(1, D)^n = (D+1)^n \tag{30}$$

Therefore, we have:

$$P(P(1, D)^n)^n = (1 + (D+1)^n + \ldots + (D+1)^{nD})^n \tag{31}$$

Observe that the inner sum is equivalent to the summation of the powers of $(D+1)^n$ from 0 to D. We note the following identity [11]:

$$\sum_{k=0}^{n-1} n^k = \frac{n^n - 1}{n - 1} \tag{32}$$

By substitution, we have:

$$P(P(1, D)^n)^n = \left(\sum_{k=0}^{D} (D+1)^{nk} \right)^n = \left(\frac{(D+1)^{nD+n} - 1}{(D+1)^n - 1} \right)^n \tag{33}$$

In of our proof of Theorem 4, we established that:

$$\binom{n}{k} = \left\lfloor \frac{P(P(1)^n)^n}{P(1)^{nk}} \right\rfloor \bmod P(1)^n \tag{34}$$

By equivalence, we have:

$$\underline{D}\binom{n}{k} = \left\lfloor \frac{P(P(1, D)^n)^n}{P(1, D)^{nk}} \right\rfloor \bmod P(1, D)^n \tag{35}$$

Finally, we replace the values of $P(1, D)^n$ and $P(P(1, D)^n, D)^n$ to arrive at our original equation:

$$\underline{D}\binom{n}{k} = \left\lfloor \left(\frac{(D+1)^{nD+n} - 1}{(D+1)^n - 1} \right)^n \cdot (D+1)^{-nk} \right\rfloor \bmod (D+1)^n \tag{36}$$

Step 2: Proof that the equation holds only for $n > 0$ and $0 \leq k \leq nD$:
To prove why the equation holds only for $n > 0$ and $0 \leq k \leq nD$, we consider the following cases:

7

1. $n \leq 0$: In this case, the modulus becomes $(D+1)^{-n}$ and the original equation does not make sense.

2. $k < 0$: In this case, we have $(D+1)^{-(-nk)} = (D+1)^{nk}$ and thus the original expression is always equal to 0, since $(D+1)^n \mid (D+1)^{nk}$.

3. $k > nD$: In this case, $(D+1)^{nk} > \left(\frac{(D+1)^{nD+n}-1}{(D+1)^n-1} \right)^n > (D+1)^{nn}$, so the value of the expression is always equal to 0.

Conclusion:

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

5 Summary

In this paper, we have made two key contributions. First, we derived and proved a novel formula for computing binomial coefficients:

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

This formula depends only on basic arithmetic operations and establishes an interesting connection between binomial coefficients and modular arithmetic. Second, we generalized this formula to find closed form expressions for the coefficients of terms in the multinomial expansion of arbitrary degree univariate polynomials. Specifically, we showed:

$$\underline{D}\binom{n}{k} = \left\lfloor \left(\frac{(D+1)^{nD+n}-1}{(D+1)^n-1} \right)^n \cdot (D+1)^{-nk} \right\rfloor \mod (D+1)^n,$$
$$\text{for } n > 0 \text{ and } 0 \leq k \leq nD$$

Where $\underline{D}\binom{n}{k}$ denotes the coefficient of the term with degree k in the expansion of $(1 + x + \ldots + x^D)^n$.

Our novel approach stems from connecting binomial coefficients to a key, but rarely explored, property of polynomials: that they can be unambiguously determined by two judiciously chosen inputs. This insight allowed us to derive simple arithmetic formulas for computing these coefficients. In doing so, our work strengthens the connection between binomial coefficients and polynomial functions, while also establishing an elegant new link to modular arithmetic. This link is not only mathematically appealing, but also ripe with potential for further exploration. Our formula serves not merely as an alternative means to compute binomial coefficients, but more profoundly, as a gateway to discover new mathematical identities and relations between these fundamental concepts.

8

Discoveries such as ours underscore the idea that profound insights can often emerge from concepts that, once discovered, seem simple and obvious, yet have remained overlooked. We hope that this reminds others of the vast potential for innovation that still lies latent even within well-studied fields of mathematics. By revisiting old problems with fresh perspectives, there is always the possibility of unearthing powerful new insights.

6   Future Directions

Future research could explore the computational efficiency of the formulas and their behavior for large values of n, k, and D with a view to potential optimizations. This may be of particular importance, as applying our formulas 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. 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] Richard L Burden, J Douglas Faires, and Annette M Burden. *Numerical Analysis*. Brooks/Cole, Cengage Learning, Boston, MA, 9th edition, 2011.

[5] David R Kincaid and E Ward Cheney. *Numerical Analysis: Mathematics of Scientific Computing*. American Mathematical Soc., 2012.

[6] Elliott Ward Cheney and William Allan Light. *A Course in Approximation Theory*. American Mathematical Soc., 2013.

[7] Rupinski A. Mathoverflow: Application of polynomials with non-negative coefficients. `https://mathoverflow.net/questions/91827/`, 2012. Accessed: 2023-08-05.

[8] Cook J. Polynomial determined by two inputs. `https://www.johndcook.com/blog/2012/03/27/polynomial-trick/`, 2012. Accessed: 2023-08-05.

[9] Thomas H Cormen, Charles E Leiserson, Ronald L Rivest, and Clifford Stein. *Introduction to Algorithms*. MIT press, 2009.

[10] Ivan Niven, Herbert S Zuckerman, and Hugh L Montgomery. *An Introduction to the Theory of Numbers*. John Wiley & Sons, 2008.

[11] David W. Wilson. Entry a023037 in the on-line encyclopedia of integer sequences. `https://oeis.org/A023037`, 2023. Accessed: 2023-08-07.