Simple Formulas for Univariate Multinomial Coefficients

Joseph M. Shunia

September 2023
(Revised: July 2024, Version 5)

Abstract

We present novel arithmetic term formulas for univariate multinomial coefficients and their partial sums. Notably, we introduce what appear to be the first closed-form expressions for partial sums of binomial coefficients. These results stem from an underutilized property of polynomials, which allows for their complete determination using only two evaluations under specific conditions. Our findings contribute to the foundation of arithmetic term formulas, an emerging and promising area of research in discrete mathematics.

Keywords: elementary formula; arithmetic term; modular arithmetic; multinomial coefficient; binomial coefficient; partial sums; polynomial interpolation; Kronecker substitution.

2020 Mathematics Subject Classification: 11B65, 11Y55, 11A25.

1 Introduction

This paper marks the beginning of our exploration into the study of explicit arithmetic term formulas for integer sequences and number theoretic functions. We introduce the first known arithmetic term formulas for univariate multinomial coefficients and their partial sums. Remarkably, we also present what are possibly the only closed-form expressions of any kind for the partial sums of binomial coefficients, as detailed in § 4. These foundational results help set the stage for further research into the study of arithmetic term formulas.

To fully appreciate the implications of these contributions, it is essential to understand what constitutes an arithmetic term. An arithmetic term is an integer-valued function that uses only the elementary arithmetic operations:

$$\{a+b, a-b, ab, \lfloor a/b \rfloor, a \bmod b, a^b\},$$

where the modulo operation is implicitly included, as it can be defined by $a \bmod b = a - b \lfloor a/b \rfloor$.

The study of arithmetic terms has its origins in the earliest days of computer science and discrete mathematics, tracing back to the 1950s and the work of Julia Robinson [10]. During that era, research primarily focused on broad theoretical questions about the capabilities of arithmetic terms in computability and their classification within mathematical logic [5, 2, 10]. In particular, a significant question was: What is the class of functions that can be represented using only these elementary arithmetic operations?

Mazzanti's 2002 discovery that arithmetic terms generate the class of Kalmar functions, or elementary functions ($\mathcal{E}^3$), clarified their position in the Grzegorczyk hierarchy, a framework categorizing primitive recursive functions by complexity [20, 2]. Further refinement by Marchenkov in 2006 demonstrated that even a more restricted set of functions could generate $\mathcal{E}^3$ [21]. Collectively, the works of Mazzanti-Marchenkov provide a strong theoretical underpinning for the study of arithmetic terms.

Despite these theoretical milestones, little attention has been given to the explicit construction and study of arithmetic term formulas. Indeed, deriving such formulas for many elementary functions has proven to be exceedingly challenging. Matiyasevich's work [23], for instance, confirms the existence of arithmetic terms for many prominent number theoretic functions that remain elusive, such as: The n-th prime number, the prime counting function, and Euler's totient function.

Interestingly, functions that seem computationally simple, like the logarithm function $\log(n)$, often lack straightforward arithmetic term formulas. Conversely, more complicated functions can sometimes be represented simply. Consider Robinson's elegant formula for the binomial coefficient $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ [10]:

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

This asymmetry is an inversion of our expectations: One reasonably expects that sequences which are hard to compute should necessitate formulas that are sophisticated and hard to find, whereas sequences which are easy to compute should have formulas that are simple and easy to find. This discrepancy is one of the many reasons that compelled us to study arithmetic term formulas. Our hope is that the discovery and study of such formulas can yield new insights in number theory and other branches of mathematics.

2 Structure of the Paper

We begin in § 3 by proving a theorem stating that under certain conditions, a polynomial can be completely determined by only two evaluations (Theorem 3.1). This property allows us to recover the coefficients of a polynomial using an arithmetic term formula.

Subsequently, we revisit an unconventional formula for binomial coefficients, initially given by Julia Robinson (1952) [10]:

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

In § 4, we present elementary formulas for the partial sums of binomial coefficients, for which it has been said that no explicit closed-form expression is known [13, 22]. A formula we prove is

$$\sum_{k=0}^{j} \binom{n}{k} = \left\lfloor \frac{(2^n+1)^n}{2^{n(n-j)}} \right\rfloor \bmod (2^n-1).$$

We proceed in § 5 by generalizing Robinson's binomial coefficient formula, to calculate the coefficients in the expansion of univariate unit polynomials of the form

$$[x^k](1+x+\cdots+x^{r-1})^n.$$

These coefficients are the univariate multinomial coefficients denoted as $\binom{n}{k}_{r-1}$, which are a generalization of the binomial coefficients. Conventional techniques for computing univariate multinomial coefficients involve factorials and summations over specific criteria. In contrast, our formula uses only elementary arithmetic operations and is given by

$$\binom{n}{k}_{r-1} = \left\lfloor \left(\frac{r^{rn} - 1}{r^{n+k} - r^k} \right)^n \right\rfloor \bmod r^n,$$

where $n > 0$ and $0 \leq k \leq n(r-1)$ (Theorem 5.1).

3 Polynomial Interpolation with Two Evaluations

We begin by presenting a theorem which shows how to recover a polynomial in $\mathbb{Z}[x]$ completely using only two carefully chosen evaluation points.

Theorem 3.1. *Let $b, r \in \mathbb{Z}$ such that $b > 0$, $r \geq 0$. Consider a polynomial $f(x) \in \mathbb{Z}[x]$ of degree r, which has the form*

$$f(x) = a_r x^r + a_{r-1} x^{r-1} + \cdots + a_1 x + a_0.$$

Suppose $f(b) \neq 0$ and that all coefficients of $f(x)$ are non-negative. Then, $f(x)$ can be completely determined by the evaluations $f(b)$ and $f(f(b))$. Furthermore, $\forall k \in \mathbb{Z} : 0 \leq k \leq r$, the coefficient a_k can be recovered explicitly from the formula:

$$a_k = \left\lfloor \frac{f(f(b))}{f(b)^k} \right\rfloor \bmod f(b).$$

Proof. By assumption, $\forall k \in \mathbb{Z} : 0 \leq k \leq r$, the coefficient a_k of $f(x)$ can be recovered from the given formula. To prove the validity of the formula, we proceed by examining its arithmetic operations step-by-step.

Suppose we choose some k in the range $0 \leq k \leq r$. Now, let's consider the expansion of $f(f(b))$, which can be written as

$$f(f(b)) = a_r f(b)^r + a_{r-1} f(b)^{r-1} + \cdots + a_k f(b)^k + a_{k-1} f(b)^{k-1} + \cdots + a_1 f(b) + a_0.$$

The first step in the formula is to divide $f(f(b))$ by $f(b)^k$. This results in the quotient

$$\begin{aligned} \frac{f(f(b))}{f(b)^k} &= f(b)^{-k}(a_r f(b)^r + \cdots + a_k f(b)^k + a_{k-1} f(b)^{k-1} + \cdots + a_0) \\ &= a_r f(b)^r f(b)^{-k} + \cdots + a_k f(b)^k f(b)^{-k} + a_{k-1} f(b)^{k-1} f(b)^{-k} + \cdots + a_0 f(b)^{-k} \\ &= a_r f(b)^{r-k} + \cdots + a_k f(b)^{k-k} + a_{k-1} f(b)^{k-k-1} + \cdots + a_0 f(b)^{-k} \\ &= a_r f(b)^{r-k} + \cdots + a_k f(b)^0 + a_{k-1} f(b)^{-1} + \cdots + a_0 f(b)^{-k} \\ &= a_r f(b)^{r-k} + \cdots + a_k + a_{k-1} f(b)^{-1} + \cdots + a_0 f(b)^{-k}. \end{aligned}$$

The next step is to take the floor of the quotient $\frac{f(f(b))}{f(b)^k}$. In doing so, we effectively isolate the terms ranging from $a_k x^k$ up to and including $a_r x^r$. The result is

$$\left\lfloor \frac{f(f(b))}{f(b)^k} \right\rfloor = a_r f(b)^{r-k} + \cdots + a_k.$$

The final step is to take the floored result $\left\lfloor \frac{f(f(b))}{f(b)^k} \right\rfloor$ modulo $f(b)$. Given $r \geq k \geq 0$, we have two possibilities: The first is that $k \geq r$, in which case we have a monomial that is a constant and it is not required to carry out the mod operation, since $a_r f(b)^{r-r} = a_r f(b)^0 = a_r$. Thus, we are done. On the other hand, if $k < r$, we must perform the mod $f(b)$ operation. Carrying it out, noting that the mod operation is distributive over addition, we see

$$\begin{aligned}
\left\lfloor \frac{f(f(b))}{f(b)^k} \right\rfloor \bmod f(b) &= (a_r f(b)^{r-k} \bmod f(b)) + \cdots + (a_k \bmod f(b)) \\
&= (0) + \cdots + (a_k \bmod f(b)) \\
&= 0 + (a_k \bmod f(b)) \\
&= a_k \bmod f(b).
\end{aligned}$$

By assumption, all coefficients of $f(x)$ are positive. Therefore, the modular reduction by $f(b)$ leaves the coefficient a_k unchanged. Thus, we arrive at

$$a_k = \left\lfloor \frac{f(f(b))}{f(b)^k} \right\rfloor \bmod f(b).$$

Which is the formula we wanted to prove. In proving the formula, we have shown that it is possible to recover all the coefficients $a_0, a_1, \ldots, a_r$ using only the values $f(b)$ and $f(f(b))$ under the given conditions. Since we can recover the coefficient a_k given its degree k, we can determine the degree of the term corresponding to the coefficient recovered. Hence, we can reconstruct the polynomial $f(x)$, with the correct degrees and coefficients, using only the evaluations $f(b)$ and $f(f(b))$. Thus, we can reconstruct the polynomial one-to-one.

In conclusion, under the given conditions, $f(x)$ can be completely determined by the evaluations $f(b)$ and $f(f(b))$ using the provided formula. □

Remark 3.1. *The polynomial property described in Theorem 3.1 appears to be underexplored in the literature. However, it has been the subject of some online discussions [16, 19] and at least one blog post [9]. Despite these mentions, the property has been treated mostly as a novelty or curiosity, and its applications have not been thoroughly examined.*

3.1 Binomial Coefficients

To provide an intuitive example of how Theorem 3.1 can be used, we provide a new proof of Robinson's binomial coefficient formula [10] as a corollary.

Corollary 3.1. *Let $n, k \in \mathbb{Z} : 0 \leq k \leq n$. Then*

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

Proof. Consider the polynomial $f(x) := (x+1)^n \in \mathbb{Z}[x]$. The binomial theorem gives the polynomial expansion

$$f(x) = (x+1)^n = \sum_{j=0}^{n} \binom{n}{j} x^j 1^{n-j} = \sum_{j=0}^{n} \binom{n}{j} x^j.$$

By expanding out the inner terms of sum, we can see

$$f(x) = \binom{n}{0}x^0 + \binom{n}{1}x^1 + \cdots + \binom{n}{n-1}x^{n-1} + \binom{n}{n}x^n.$$

Hence, $f(x)$ is a polynomial with terms whose coefficients are the binomial coefficients for row n of Pascal's triangle.

If we evaluate at $x = 1$, we get the coefficient sum. Applying this to $f(x)$, the evaluation $f(1)$ is equal to the sum of the coefficients of the n-th row of Pascal's triangle. This sum is well-known to be equal to 2^n [6]. Carrying out the evaluation, we get

$$\begin{aligned} f(1) &= \binom{n}{0}1^0 + \binom{n}{1}1^1 + \cdots + \binom{n}{n-1}1^{n-1} + \binom{n}{n}1^n \\ &= \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n} \\ &= 2^n. \end{aligned}$$

Let $b = 1$, so that $f(b) = f(1) = 2^n$. By Theorem 3.1, for all $0 \leq k \leq n$, we can recover the coefficient $\binom{n}{k}$ using only the evaluations $f(b)$ and $f(f(b))$ by way of the formula

$$a_k = \left\lfloor \frac{f(f(b))}{f(b)^k} \right\rfloor \bmod f(b).$$

In this case, $a_k = \binom{n}{k}$. Substituting $f(b) = 2^n$ and $a_k = \binom{n}{k}$ into the formula, we get

$$\binom{n}{k} = \left\lfloor \frac{f(2^n)}{(2^n)^k} \right\rfloor \bmod 2^n.$$

Finally, by expanding $f(2^n) = (2^n + 1)^n$ and simplifying, we arrive at

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

Proving the formula. □

3.2 Kronecker Substitution

The polynomial interpolation procedure described by Theorem 3.1 is closely related to the process of Kronecker substitution, which is a technique for converting a polynomial to an integer representation [11].

Given a polynomial $f(x) \in \mathbb{Z}[x]$ and a suitable integer $b \in \mathbb{Z}$, Kronecker substitution evaluates $f(x)$ at $x = b$. By choosing an appropriate base b, the resulting integer $f(b)$ encodes the coefficients of f in its digits. An integer base b is said to be "suitable" for a polynomial f if b is greater than the sum of the absolute values of the coefficients of the polynomial, ensuring that the coefficients can be uniquely determined from the digits of $f(b)$. This technique is commonly used for fast polynomial multiplication [3, 4, 15, 12, 1]. However, its potential applications in number theory remain largely unexplored. The aim of this paper, along with our ongoing research, is to investigate and broaden the traditional applications of Kronecker substitution and related methods.

4 Partial Sums of Binomial Coefficients

Boardman (2004) asserted that “it is well-known that there is no closed form (that is, direct formula) for the partial sum of binomial coefficients” [13]. This statement has been cited in the Wikipedia article on binomial coefficients to suggest the impossibility of a closed-form expression for these partial sums [22]. However, this interpretation appears to misconstrue Boardman’s intended meaning. In his paper, Boardman references a theorem by Petkovšek et al. which proves the non-existence of a closed-form expression for the partial sums of binomial coefficients specifically as a hypergeometric function [14]. In our opinion, it is more likely that Boardman was citing this result to indicate the absence of a known formula, rather than asserting the impossibility of any such formula. If indeed no closed-form expression has been previously established, then the formulas we present here may constitute the first of their kind.

Theorem 4.1. *Let $n, j \in \mathbb{Z}_{>-1}$ such that $j \leq n$. Then*

$$\sum_{k=0}^{j} \binom{n}{k} = \left\lfloor \frac{(2^n+1)^n}{2^{n(n-j)}} \right\rfloor \bmod (2^n - 1)$$

and

$$\sum_{k=0}^{j} \binom{n}{k} = \left((2^n+1)^n \bmod 2^{nj+1}\right) \bmod (2^n - 1).$$

Proof. First, we note that $(2^n-1)^n = \sum_{k=0}^{n} \binom{n}{k} 2^{nk}$. Next, we divide the sum by 2^{nj} to get

$$\left\lfloor \frac{(2^n+1)^n}{2^{n(n-j)}} \right\rfloor = \sum_{k=0}^{j} \binom{n}{k} 2^{nk}.$$

Taking this sum mod $(2^n - 1)$ is the same as replacing all instances of 2^n with 1. Thus

$$\sum_{k=0}^{j} \binom{n}{k} 2^{nk} \bmod (2^n-1) = \sum_{k=0}^{j} \binom{n}{k} (1)^k = \sum_{k=0}^{j} \binom{n}{k}.$$

Due to the symmetry of the binomial coefficients in row n, we see that taking $(2^n + 1)^n \bmod 2^{nj+1}$, then mod $(2^n - 1)$, yields the same result. Consider

$$\left((2^n+1)^n \bmod 2^{nj+1}\right) = \sum_{k=0}^{j} \binom{n}{n-k} 2^{n(n-k)} = \sum_{k=0}^{j} \binom{n}{k} 2^{nk}$$

By taking this sum mod $(2^n - 1)$, we once again obtain $\sum_{k=0}^{j} \binom{n}{k}$. □

Corollary 4.1. *Let $n, a, b \in \mathbb{Z}_{>-1}$ such that $n > 0$ and $a < b \leq n$. Then*

$$\sum_{k=a}^{b} \binom{n}{k} = \left(\left((2^n+1)^n \bmod 2^{nb+1}\right) - \left((2^n+1)^n \bmod 2^{na}\right)\right) \bmod (2^n - 1)$$

Proof. The proof follows trivially from Theorem 4.1, since

$$\begin{aligned}
&\left(\left((2^n+1)^n \bmod 2^{nb+1}\right) \bmod (2^n-1)\right) - \left(\left((2^n+1)^n \bmod 2^{na}\right) \bmod (2^n-1)\right)\\
&= \left(\left((2^n+1)^n \bmod 2^{nb+1}\right) - \left((2^n+1)^n \bmod 2^{na}\right)\right) \bmod (2^n-1)\\
&= \sum_{k=0}^{b}\binom{n}{k} - \sum_{k=0}^{a-1}\binom{n}{k}\\
&= \sum_{k=a}^{b}\binom{n}{k}.
\end{aligned}$$

□

We now provide an alternative formula for the partial sums of binomial coefficients, using results from Boardman [13].

Theorem 4.2. *Let $n, j \in \mathbb{Z}_{>-1}$ such that $n > 0$ and $j \leq n$. Then*

$$\sum_{k=0}^{j}\binom{n}{k} = 1 + \left(\left\lfloor \frac{(2^n+1)^n-1}{2^{nj}(1-2^n)} \right\rfloor \bmod 2^n\right)$$

Proof. From Boardman (2004) [13], we have

$$\frac{(x+1)^n-1}{1-x} = \binom{n}{1}x + \left(\binom{n}{1}+\binom{n}{2}\right)x^2 + \cdots + \left(\binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{n}\right)x^n.$$

By substituting $x = 2^n$, we get

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

This substitution is valid, since the coefficients are at most $(2^n - 1)$.

Now, to recover the partial sum of binomial coefficients from $\binom{n}{1}$ up to $\binom{n}{j}$, we must isolate the j-th term in the sum. To do this, we can divide by 2^{nj} and then mod by 2^n (Theorem 3.1). This yields

$$\left\lfloor \frac{(2^n+1)^n-1}{2^{nj}(1-2^n)} \right\rfloor \bmod 2^n = \binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{n}.$$

Finally, we add $\binom{n}{0} = 1$ to get the desired sum, which is

$$1 + \left(\left\lfloor \frac{(2^n+1)^n-1}{2^{nj}(1-2^n)} \right\rfloor \bmod 2^n\right) = \binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{n} = \sum_{k=0}^{j}\binom{n}{j}.$$

□

5 Univariate Multinomial Coefficients

Applying Theorem 3.1, we derive a generalized formula for calculating coefficients within the multinomial expansion of arbitrary degree univariate unit polynomials. These are polynomials of the form

$$\left(\frac{x^r-1}{x-1}\right)^n = (1+x+\cdots+x^{r-1})^n.$$

The conventional approach to determine these coefficients utilizes conditional summations of multivariate multinomial coefficients, which represent the number of ways specific choices can be made to yield the term x^k [18]. The standard formula for multivariate multinomial coefficients is

$$\binom{n}{k_0, k_1, \cdots, k_{r-1}} = \frac{n!}{k_0!k_1!\cdots k_{r-1}!}.$$

In the context of our univariate polynomial, for each power of x in the expansion, the coefficient will come from all the combinations of powers that sum up to that specific power. Specifically, the coefficient of x^k in the expansion of our polynomial is [17]

$$\binom{n}{k}_{r-1} = [x^k](1 + x + \cdots + x^{r-1})^n = \sum \binom{n}{k_0, k_1, \cdots, k_{r-1}},$$

where the summation criteria are

$$\begin{aligned} k_0 + k_1 + \cdots + k_{r-1} &= n, \\ 0k_0 + 1k_1 + \cdots + (r-1)k_{r-1} &= k. \end{aligned}$$

Theorem 5.1. *Let $n, k, r \in \mathbb{Z}$ such that $n > 0$ and $0 \leq k \leq n(r-1)$. Then*

$$\binom{n}{k}_{r-1} = \left\lfloor \left(\frac{r^{rn} - 1}{r^{n+k} - r^k} \right)^n \right\rfloor \bmod r^n.$$

Proof. Consider the polynomial function

$$f_r(x)^n = \left(\frac{x^r - 1}{x - 1} \right)^n = (1 + x + \cdots + x^{r-1})^n.$$

In this case, it is clear that

$$f_r(1)^n = r^n.$$

Therefore, we have

$$f_r(f_r(1)^n)^n = (1 + r^n + \cdots + r^{n(r-1)})^n.$$

Observe that the inner sum is equivalent to the summation of the powers of r^n from 0 to $(r-1)$. We note the following identity from the OEIS [8]:

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

By substitution, we have

$$f_r(f_r(1)^n)^n = \left(\sum_{k=0}^{r-1} r^{nk} \right)^n = \left(\frac{r^{rn} - 1}{r^n - 1} \right)^n.$$

In Theorem 3.1, we showed that

$$[x^k]f(x)^n = \left\lfloor \frac{f(f(1)^n)^n}{f(1)^{nk}} \right\rfloor \bmod f(1)^n.$$

By equivalence, we have

$$\binom{n}{k}_{r-1} = [x^k] f_r(x)^n = \left\lfloor \frac{f_r(f_r(1)^n)^n}{f_r(1)^{nk}} \right\rfloor \bmod f_r(1)^n.$$

Replacing the values of $f_r(1)^n$ and $f_r(f_r(1)^n)^n$ and simplifying, we arrive at our original formula

$$\binom{n}{k}_{r-1} = [x^k] \left(\frac{x^r-1}{x-1}\right)^n = \left\lfloor \left(\frac{r^{rn}-1}{r^n-1}\right)^n r^{-nk} \right\rfloor \bmod r^n = \left\lfloor \left(\frac{r^{rn}-1}{r^{n+k}-r^k}\right)^n \right\rfloor \bmod r^n.$$

To prove why the equation holds only for $n > 0$ and $0 \leq k \leq n(r-1)$, we consider the possible cases in relation to

$$\binom{n}{k}_{r-1} = \left\lfloor \left(\frac{r^{rn}-1}{r^{n+k}-r^k}\right)^n \right\rfloor \bmod r^n = \left\lfloor \left(\frac{r^{rn}-1}{r^n-1}\right)^n r^{-nk} \right\rfloor \bmod r^n.$$

Cases:

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

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

(iii) $k > n(r-1)$: In this case, $r^{nk} > \left(\frac{r^{rn}-1}{r^n-1}\right)^n > r^{n^2}$, so the value of the expression is always equal to 0.

In conclusion, we have shown that the formula is valid and that it holds only for $n > 0$ and $0 \leq k \leq n(r-1)$. This completes the proof. □

5.1 Central Trinomial Coefficients

To illustrate how our univariate multinomial coefficient formula (Theorem 5.1) can be applied, we consider the central trinomial coefficients.

The coefficients of the term x^n in the polynomial expansion of $(1+x+x^2)^n$, denoted as $\binom{n}{n}_2$, are known as the central trinomial coefficients. These form the sequence A002426 in the OEIS [7]. Applying our univariate multinomial coefficient formula from Theorem 5.1, we see that

$$\binom{n}{n}_2 = \left\lfloor \left(\frac{3^{3n}-1}{3^{2n}-3^n}\right)^n \right\rfloor \bmod 3^n = \left\lfloor \left(\frac{27^n-1}{9^n-3^n}\right)^n \right\rfloor \bmod 3^n = \left\lfloor \frac{(27^n-1)^n}{(9^n-3^n)^n} \right\rfloor \bmod 3^n.$$

Starting from $n = 1$, our formula yields the correct sequence terms, which are:

$$1, 3, 7, 19, 51, 141, 393, 1107, 3139, 8953, 25653, 73789, 212941, 616227, 1787607, 5196627, \ldots.$$

It is intriguing to note that, as is the case with the partial sums of binomial coefficients (See § 4), it was proved by Petkovšek et al. that there is no closed form for the central trinomial coefficients as a hypergeometric function [14]. Graham et al. have posed a related research problem asking for a proof that no closed form exists in some other large class of simple closed forms [18].

6 Partial Sums of Univariate Multinomial Coefficients

We conclude with a formula for the partial sums of univariate multinomial coefficients, taking a similar approach as in § 4.

Corollary 6.1. *Let $n, j, r \in \mathbb{Z}^+$ such that $n > 0$ and $0 \leq j \leq n(r-1)$. Then*

$$\sum_{k=0}^{j} \binom{n}{k}_{r-1} = \left(\left(\frac{r^{rn}-1}{r^n-1} \right)^n \bmod r^{n(j+1)} \right) \bmod (r^n - 1).$$

Proof. First, we note that $\left(\frac{r^{nr}-1}{r^n}\right)^n = \sum_{k=0}^{n} \binom{n}{k}_{r-1} r^{nk}$. Reducing the sum mod $r^{n(j+1)}$, we get

$$\sum_{k=0}^{j} \binom{n}{k}_{r-1} r^{nk}.$$

Finally, reducing this sum mod $(r^n - 1)$ is the same as replacing all instances of r^n with 1. Thus

$$\sum_{k=0}^{j} \binom{n}{k}_{r-1} r^{nk} \bmod (r^n - 1) = \sum_{k=0}^{j} \binom{n}{k}_{r-1} (1)^k = \sum_{k=0}^{j} \binom{n}{k}_{r-1}.$$

□

References

[1] A. Greuet, S. Montoya, and C. Vermeersch. Modular Polynomial Multiplication Using RSA/ECC coprocessor. Cryptology ePrint Archive, Paper 2022/879, 2022. URL https://eprint.iacr.org/2022/879.

[2] A. Grzegorczyk. Some Classes of Recursive Functions. *Rozprawy Matematyczne*, 4, 1953. URL http://matwbn.icm.edu.pl/ksiazki/rm/rm04/rm0401.pdf.

[3] D. Harvey. Faster Polynomial Multiplication via Multipoint Kronecker Substitution. *Journal of Symbolic Computation*, 44, 2009. doi: 10.1016/j.jsc.2009.05.004.

[4] D. Harvey and J. van der Hoeven. Faster Polynomial Multiplication Over Finite Fields Using Cyclotomic Coefficient Rings. *Journal of Complexity*, 54, 2019. ISSN 0885-064X. URL https://www.sciencedirect.com/science/article/pii/S0885064X19300378.

[5] G. T. Herman. A New Hierarchy of Elementary Functions. *Proceedings of the American Mathematical Society*, 20(2): 557–562, 1969. ISSN 0002-9939.

[6] OEIS Foundation Inc. Powers of 2 - Entry A000079 in The On-Line Encyclopedia of Integer Sequences, 2024. URL https://oeis.org/A000079.

[7] OEIS Foundation Inc. Central Trinomial Coefficients - Entry A002426 in The On-Line Encyclopedia of Integer Sequences, 2024. URL https://oeis.org/A002426.

[8] OEIS Foundation Inc. Entry A023037 in The On-Line Encyclopedia of Integer Sequences. https://oeis.org/A023037, 2024.

[9] J. D. Cook. Polynomial Determined by Two Inputs, 2012. URL https://johndcook.com/blog/2012/03/27/polynomial-trick. Blog Post.

[10] J. Robinson. Existential Definability in Arithmetic. *Transactions of the American Mathematical Society*, 72(3):437–449, 1952. ISSN 0002-9947.

[11] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra.* Cambridge University Press, 3rd edition, 2013. ISBN 978-1107039032.

[12] J. W. Bos, J. Renes, and C. van Vredendaal. Post-Quantum Cryptography with Contemporary Co-Processors: Beyond Kronecker, Schönhage-Strassen and Nussbaumer. Cryptology ePrint Archive, Paper 2020/1303, 2020. URL https://eprint.iacr.org/2020/1303.

[13] M. Boardman. The Egg-Drop Numbers. *Mathematics Magazine*, 77(5):368–372, 2004. URL https://doi.org/10.1080/0025570X.2004.11953281.

[14] M. Petkovšek, H. S. Wilf, and D. Zeilberger. *A=B*. A K Peters/CRC Press, 1996. ISBN 978-1568810638.

[15] M. R. Albrecht, C. Hanser, A. Hoeller, T. Pöppelmann, F. Virdia, and A. Wallner. Implementing RLWE-based Schemes Using an RSA Co-Processor. Cryptology ePrint Archive, Paper 2018/425, 2018. URL https://eprint.iacr.org/2018/425.

[16] MathOverflow Users. Application of Polynomials with Non-Negative Coefficients, 2012. URL https://mathoverflow.net/questions/91827. MathOverflow Discussion.

[17] R. A. Brualdi. *Introductory Combinatorics*. Pearson, 5th edition, 2017. ISBN 978-0134689616.

[18] R. L. Graham, D. E. Knuth, and O. Patashnik. *Concrete Mathematics: A Foundation For Computer Science*. Addison-Wesley Professional, 2nd edition, 1994. ISBN 978-0201558029.

[19] Reddit Users. Determine a Polynomial from Just Two Inputs, 2023. URL https://www.reddit.com/r/math/comments/yx0i7r/determine_a_polynomial_from_just_two_inputs. Reddit Discussion.

[20] S. Mazzanti. Plain Bases for Classes of Primitive Recursive Functions. *Mathematical Logic Quarterly*, 48(1):93–104, 2002. ISSN 0942-5616.

[21] S. S. Marchenkov. Superpositions of Elementary Arithmetic Functions. *Journal of Applied and Industrial Mathematics*, 1(3):351–360, 2007. ISSN 1990-4789.

[22] Wikipedia Contributors. Binomial Coefficient, 2024. URL https://en.wikipedia.org/wiki/Binomial_coefficient. Wikipedia Article.

[23] Y. Matiyasevich. A New Proof of the Theorem on Exponential Diophantine Representation of Enumerable Sets. *Journal of Soviet Mathematics*, 14(5):1475–1486, 1980. ISSN 0090-4104.