

# Polynomial Quotient Rings and Kronecker Substitution for Deriving Combinatorial Identities

Joseph M. Shunia

March 2024

Revised: June 2024, Version 5

## Abstract

We introduce a framework for generating combinatorial identities by applying Kronecker substitution to polynomial expansions within quotient rings. We apply this methodology to derive a general formula for C-recursive integer sequences, as well as explicit formulas for certain combinatorial sequences, including the Pell numbers and central binomial coefficients. We also discover an unusual representation for the real  $n$ -th roots of positive integers  $\sqrt[n]{a}$ , characterized as the limit of a modular expression. The theorems and results presented provide a theoretical basis for future research on the interconnections between Kronecker substitution, polynomial ring expansions, and their applications in combinatorial sequences and beyond.

## 1 Introduction

Kronecker substitution, named after the mathematician Leopold Kronecker, is a technique that allows for the efficient multiplication polynomials by encoding them as integers in a large base [1]. While this technique has been widely used in the design of fast multiplication algorithms [2, 3, 4, 5, 6], its potential applications in combinatorial number theory have remained largely unexplored until recently.

In our previous paper [7], we took some of the first steps in this direction by applying Kronecker substitution to polynomial expansions to derive a novel arithmetic formula for single-variable multinomial coefficients. In this work, we develop a general framework for applying Kronecker substitution to polynomial expansions within quotient rings, which is useful for generating combinatorial identities. Our main theorem establishes a connection between the coefficients of a polynomial remainder and the integers obtained by evaluating the polynomials at specific values. By carefully selecting these values, we can generate new identities for combinatorial sequences and more.

## 1.1 New Formulas

To demonstrate the power and flexibility of our approach, we apply our main result (Theorem 2) to derive several others.

First, we obtain a general formula for the  $n$ -th term of a C-recursive integer sequence (Theorem 4). Let  $n, d, b \in \mathbb{Z}^+$ . Let  $A_n$  be a C-recursive integer sequence of order  $d$  and initial starting conditions  $A_0 = A_1 = \dots = A_{d-1} = 1$ , taking the form

$$A_n = c_{d-1}A_{n-1} + c_{d-2}A_{n-2} + \dots + c_0A_{n-d-1}.$$

where the  $c_j$  are coefficients in  $\mathbb{Z}$ . For  $b > A_n$ , we have

$$A_n = (b^{n-1} \bmod (b^d - c_{d-1}b^{d-1} - \dots - c_1b - c_0)) \bmod (b-1).$$

Second, to illustrate practical specificity, we derive a new formula for the Pell sequence (Theorem 5), which is a fundamental integer sequence. The Pell sequence is [A000129](#) in the OEIS [8]. Valid for  $n > 0$ , our formula expresses the  $n$ -th Pell number  $P_n$  in terms of a double modular expression involving powers of 3:

$$P_n = ((3^n + 1)^{n-1} \bmod (9^n - 2)) \bmod (3^n - 1).$$

Our proof of the formula for the Pell sequence leads us to a general formula for square roots (Corollary 6). Let  $a \in \mathbb{Z}_{>1}$ . Then

$$\sqrt{a} = \lim_{k \rightarrow \infty} \frac{k^k (((k^k + 1)^k \bmod (k^{2k} - a)) \bmod k^k)}{(k^k + 1)^k \bmod (k^{2k} - a)} \in \mathbb{R}.$$

Intrigued by this unusual representation for  $\sqrt{a}$ , we take a slightly different approach to find a general formula for  $n$ -th roots (Theorem 7). Let  $a, n \in \mathbb{Z}_{>1}$ . Then

$$\sqrt[n]{a} = \lim_{k \rightarrow \infty} \frac{(k^{kn} + 1)^{kn+1} \bmod (k^{kn^2} - a)}{(k^{kn} + 1)^{kn} \bmod (k^{kn^2} - a)} - 1 \in \mathbb{R}.$$

Finally, we show one more specific application through creative application of quotient rings, to derive a new formula for the central binomial coefficients (Theorem 8), which are the binomial coefficients of the form  $\binom{2n}{n}$ . These coefficients form sequence [A000984](#) in the OEIS [9] and have numerous applications in combinatorics and number theory. Our formula, which is valid for  $n > 0$ , expresses the  $n$ -th central binomial coefficient in terms of a double modular expression involving powers of 4:

$$\binom{2n}{n} = ((4^n + 1)^{2n} \bmod (4^{n(n+1)} + 1)) \bmod (4^n - 1).$$

## 1.2 Structure of the Paper

The rest of this paper is organized as follows. We begin by briefly restating a relevant result from our previous work [7] on binomial and multinomial coefficient formulas § 2. Our main results, including the quotient ring encoding theorem and its proof, are presented in § 3. In § 4, we apply our quotient ring encoding theorem to derive new formulas. In § 5, we cover our literature review process and a notable blog post, which posed an open question that is resolved by our findings. We also share an update on recent research that followed the initial dissemination of this paper [10]. We conclude with § 6 by detailing some of our plans for future research in this area and related questions.

### 1.2.1 Appendices

For those unfamiliar with Kronecker substitution, § 7 provides a brief overview and an example.

## 2 Polynomial Encoding Theorem

For completeness, we restate a theorem proved in our previous work, regarding a novel arithmetic formula for single-variable multinomial coefficients [7].

**Theorem 1.** *Let  $b, d \in \mathbb{Z}$  such that  $b > 0$ ,  $d \geq 0$ . Consider a polynomial  $f(x) \in \mathbb{Z}[x]$  of degree  $d$ , which has the form*

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

*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,  $\forall k \in \mathbb{Z} : 0 \leq k \leq d$ , 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.* We proved this theorem in our previous work [7]. □

## 3 Main Result

For our main result, we apply Theorem 1 to polynomial quotient rings to devise a theorem which serves a framework for translating polynomial quotient rings to combinatorial identities.

**Notation 1** (Polynomial normalized form). Given a polynomial of the form

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0.$$

We use the notation  $\tilde{f}(x)$  to represent its normalized form, where the leading coefficient is scaled to 1. Formally, we can write this as

$$\tilde{f}(x) = \frac{f(x)}{a_d} = x^d + \frac{a_{d-1}}{a_d} x^{d-1} + \cdots + \frac{a_0}{a_d}.$$

**Theorem 2.** Let  $k, d \in \mathbb{Z}^+$  such that  $k \geq d$ . Consider a polynomial

$$g(x) := a_d x^d - a_{d-1} x^{d-1} - \cdots - a_0 \in \mathbb{Z}[x],$$

and the remainder

$$r(x) := f(x)^k \bmod \tilde{g}(x),$$

where  $f(x)$  is any non-constant polynomial in  $\mathbb{Z}[x]$ . Let  $c, \gamma \in \mathbb{Z}^+$  and suppose  $\gamma^k > |r(b)|$ . Then,

$$r(b) = (f(\gamma^k)^k \bmod \tilde{g}(\gamma^k)) \bmod (\gamma^k - b) \quad \text{or} \quad r(b) \equiv 0 \pmod{\gamma^k - b}.$$

*Proof.* First, consider the evaluation

$$r(x)|_{x=b} = r(b).$$

In modular arithmetic, evaluating a polynomial  $h(x) \in \mathbb{Z}[x]$  at  $x = b$  is the same as taking  $h(x)$  modulo  $(x - b)$ . In our case, since we are working modulo  $\tilde{g}(x)$ , we have the relation

$$r(b) = (f(x)^k \bmod \tilde{g}(x)) \bmod (x - b).$$

Applying Kronecker substitution to all polynomials in the above equation, using the substitution  $x = \gamma^k$ , yields

$$r(b) = (f(\gamma^k)^k \bmod \tilde{g}(\gamma^k)) \bmod (\gamma^k - b).$$

Which is the formula we aimed to prove. Furthermore, recall that we are given  $\gamma$  such that

$$\gamma^k > |r(b)|.$$

This implies that, when applying Kronecker substitution, the base  $\gamma^k$  is sufficient to losslessly encode all of the coefficients of  $r(x)$  (Theorem 1). Moreover, since  $k \geq d$ , the same is true of  $f(x)$  and  $g(x)$ . Thus, the only way to have

$$r(b) \neq (f(\gamma^k)^k \bmod \tilde{g}(\gamma^k)) \bmod (\gamma^k - b),$$

is if

$$\begin{aligned} &(\gamma^k - b) \mid (f(\gamma^k)^k \bmod \tilde{g}(\gamma^k)) \\ &\iff (\gamma^k - b) \mid r(b) \\ &\iff r(b) \equiv 0 \pmod{\gamma^k - b}. \end{aligned}$$

This completes the proof. □

## 4 Applications

### 4.1 C-Recursive Integer Sequences

The proceeding lemma is likely well-known. However, we prove it here for completeness.

**Lemma 3.** *Let  $n, d \in \mathbb{Z}^+$ . Let  $A_n$  be a C-recursive integer sequence of order  $d$  and initial starting conditions  $A_0 = A_1 = \dots = A_{d-1} = 1$ , taking the form*

$$A_n = c_{d-1}A_{n-1} + c_{d-2}A_{n-2} + \dots + c_0A_{n-d},$$

where the  $c_j$  are coefficients in  $\mathbb{Z}$ . Consider a polynomial

$$g(x) := c_{d-1}x^{d-1} + \dots + c_1x + c_0 \in \mathbb{Z}[x].$$

Fix a ring

$$R = \mathbb{Z}[x]/(x^d - g(x)).$$

Then,  $\forall n \in \mathbb{Z}$ , the sequence term  $A_n$  can be calculated by expanding the polynomial

$$f(x) := x^{n-1} \in R.$$

and then evaluating the result at  $x = 1$ .

*Proof.* In the ring  $R$ , any power of  $x^k$  with  $k \geq d$  can be reduced using the relation  $x^d = g(x)$ . For a general  $k$ , the power  $x^k$  can be expressed recursively by repeatedly applying the relation

$$x^k = x^{k-1}x = (x^{k-1-d}x^d)x = (x^{k-1-d}g(x))x = \dots$$

This continues until all terms are in terms of  $x^{d-1}$  or lower. That is, we express  $x^k$  as a linear combination of  $\{1, x, x^2, \dots, x^{d-1}\}$ . In particular, when expanding  $f(x) = x^{n-1} \in R$ , we recursively replace each occurrence of  $x^d$  using  $x^d = g(x)$  until the exponent of  $x$  in each term is less than  $d$ .

Now, the polynomial  $g(x) = c_{d-1}x^{d-1} + \dots + c_1x + c_0$  represents the characteristic polynomial of the recurrence relation. Here, it's used to define the quotient ring  $R = \mathbb{Z}[x]/(x^d - g(x))$ . Since the expanded polynomial  $f(x)$  represents  $x^{n-1}$  in the ring  $R$  and is expressed as a linear combination of lower powers of  $x$  due to the quotient relation  $x^d = g(x)$ , it is equivalent to reducing  $x^{n-1}$  by repeatedly applying the recurrence relation defined by the characteristic polynomial.

We assume  $f(x) = x^{n-1} \in R$  has been reduced to

$$f(x) = x^{n-1} = a_{d-1}x^{d-1} + a_{d-2}x^{d-2} + \dots + a_0,$$

where each  $a_j$  is an integer coefficient determined by the reduction process in  $R$ .

Evaluating the expanded polynomial at  $x = 1$  in  $R$  gives

$$\begin{aligned} f(1) &= a_{d-1}1^{d-1} + a_{d-2}1^{d-2} + \cdots + a_0 \\ &= a_{d-1} + a_{d-2} + \cdots + a_0. \end{aligned}$$

We observe that the sequence  $A_n$  is governed by the recurrence

$$A_n = c_{d-1}A_{n-1} + c_{d-2}A_{n-2} + \cdots + c_0A_{n-d}.$$

with initial conditions  $A_0 = A_1 = \cdots = A_{d-1} = 1$ . The corresponding characteristic polynomial  $g(x)$  represents these relations

$$g(x) = c_0 + c_1x + \cdots + c_{d-1}x^{d-1}.$$

Under this setup,  $x^d = g(x)$  implies that the recurrence relations used in the definition of  $R$  match those used to calculate  $A_n$ . The process of reducing  $f(x) = x^{n-1} \in R$  mimics the process of determining  $A_n$  using the recurrence relation.

Specifically, the coefficients  $a_0, a_1, \dots, a_{d-1}$  in the expansion of  $f(x) = x^{n-1} \in R$  directly correspond to the coefficients in the linear combination that expresses  $A_n$  in terms of the base cases  $A_0, A_1, \dots, A_{d-1}$ . The evaluation at  $x = 1$  yields the same combination that one would compute directly using the recurrence relation on  $A_n$ .

Hence, the result of evaluating the polynomial expansion of  $f(x) = x^{n-1} \in R$  at  $x = 1$  yields  $A_n$ .  $\square$

To demonstrate the practical applications of Theorem 2, we apply it to derive a new formula for the  $n$ -th term of a C-recursive integer sequence of order  $d$ .

**Theorem 4.** *Let  $n, d \in \mathbb{Z}^+$ . Let  $A_n$  be a C-recursive integer sequence of order  $d$  and initial starting conditions  $A_0 = A_1 = \cdots = A_{d-1} = 1$ , taking the form*

$$A_n = c_{d-1}A_{n-1} + c_{d-2}A_{n-2} + \cdots + c_0A_{n-d}.$$

*where the  $c_j$  are coefficients in  $\mathbb{Z}$ . Consider a polynomial*

$$g(x) := c_{d-1}x^{d-1} + \cdots + c_1x + c_0 \in \mathbb{Z}[x].$$

*Let  $b \in \mathbb{Z}^+$ . Suppose  $b > A_n$ . Then*

$$A_n = (b^{n-1} \bmod (b^d - g(b))) \bmod (b - 1).$$

*Proof.* Consider the ring

$$R = \mathbb{Z}[x]/(x^d - g(x)).$$

By Lemma 3, we have that  $\forall n \in \mathbb{Z}$ , the sequence term  $A_n$  can be calculated by expanding the polynomial  $f(x) := x^{n-1} \in R$  and then evaluating the result at  $x = 1$ .

In the ring  $R$ , the elements obey the relation  $x^d = g(x)$ . This means that in the ring  $R$ , all elements are implicitly reduced modulo  $(x^d - g(x))$ . For  $f(x)$ , this results in

$$f(x) = x^{n-1} \bmod (x^d - g(x)).$$

In modular arithmetic, evaluating at  $x = 1$  is the same as reducing modulo  $(x - 1)$ . Hence, the evaluation of  $f(1) \in R$  is equal to

$$f(1) = (x^{n-1} \bmod (x^d - g(x))) \bmod (x - 1) \in R.$$

Applying Theorem 2 by substituting with  $x = b$ , we arrive at the given formula

$$A_n = (b^{n-1} \bmod (b^d - g(b))) \bmod (b - 1).$$

By Theorem 2, this substitution is valid since  $b > A_n$ . This completes the proof.  $\square$

## 4.2 Pell Sequence Formula

We apply Theorem 2 to derive a new formula for the  $n$ -th Pell number, which is sequence [A000129](#) in the OEIS [8]. Starting from  $n = 0$ , the sequence  $P$  begins as

$$P_n = 0, 1, 2, 5, 12, 29, 70, 169, 408, 985, 2378, 5741, 13860, 33461, 80782, 195025, \dots$$

**Theorem 5.** *Let  $n \in \mathbb{Z}^+$ . Let  $P_n$  denote the  $n$ -th term of the Pell sequence, such that  $P_0 = 0, P_1 = 1$ , and for  $n > 1$ :*

$$P_n = 2P_{n-1} + P_{n-2}.$$

*Then*

$$P_n = ((3^n + 1)^{n-1} \bmod (9^n - 2)) \bmod (3^n - 1).$$

*Proof.* Fix a ring  $R = \mathbb{Z}[x]/(x^2 - 2)$ . Consider  $f(x) = x + 1 \in R$ . Expanding  $f(x)^n$  using the binomial theorem gives

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

In the ring  $R$ , the elements obey the relation  $x^2 = 2$ . This means that in the ring  $R$ , all elements are implicitly reduced modulo  $(x^2 - 2)$ . Factoring out  $x^2$  from  $x^k$  in our previous expansion (to apply the modular reduction), and then simplifying, yields

$$f(x)^n \bmod (x^2 - 2) = \sum_{k=0}^n \binom{n}{k} 2^{\lfloor \frac{1}{2}k \rfloor} x = \sum_{k=0}^n \binom{n}{k} 2^{\lfloor \frac{k}{2} \rfloor} x.$$

Recall that evaluating at  $x = 1$  is the same as reducing modulo  $(x - 1)$ . Thus, we have

$$(f(x)^n \bmod (x^2 - 2)) \bmod (x - 1) = \sum_{k=0}^n \binom{n}{k} 2^{\lfloor \frac{k}{2} \rfloor}.$$

From the OEIS [8], we have the formula

$$P_{n+1} = \sum_{k=0}^n \binom{n}{k} 2^{\lfloor \frac{k}{2} \rfloor}.$$

Hence,

$$\begin{aligned} P_{n+1} &= (f(x)^n \bmod (x^2 - 2)) \bmod (x - 1) \\ &= ((x + 1)^n \bmod (x^2 - 2)) \bmod (x - 1). \end{aligned}$$

Replacing  $n$  with  $n - 1$  yields

$$P_n = ((x + 1)^{n-1} \bmod (x^2 - 2)) \bmod (x - 1).$$

To arrive at our stated formula, we apply Theorem 2 by substituting with  $x = 3^n$ , followed by simplifying

$$\begin{aligned} P_n &= ((3^n + 1)^{n-1} \bmod ((3^n)^2 - 2)) \bmod (3^n - 1) \\ &= ((3^n + 1)^{n-1} \bmod (9^n - 2)) \bmod (3^n - 1). \end{aligned}$$

By Theorem 2, this substitution is valid since  $3^n > P_n$ .

Considering  $n = 0$ , since the final modulus  $(3^0 - 1) = 1 - 1 = 0$  results in an undefined remainder (due to division by zero). Thus, the formula is valid for  $n > 0$ .  $\square$

### 4.3 Roots

The previous result on Pell numbers (Theorem 5) leads us to an interesting result on square roots.

**Corollary 6.** *Let  $a \in \mathbb{Z}_{>1}$ . Then*

$$\sqrt{a} = \lim_{k \rightarrow \infty} \frac{k^k \left( ((k^k + 1)^k \bmod (k^{2k} - a)) \bmod k^k \right)}{(k^k + 1)^k \bmod (k^{2k} - a)} \in \mathbb{R}.$$

*Proof.* Fix a ring  $S = \mathbb{Z}[x]/(x^2 - a)$ . In the ring  $S$ , the elements obey the relation  $x^2 = a$ . This means that in the ring  $S$ , all elements are implicitly reduced modulo  $(x^2 - a)$ .



Consider  $f(x) = x + 1 \in S$ . Let  $u, v \in \mathbb{Z}$ . Expanding  $f(x)^k \in S$  for some  $k \in \mathbb{Z}^+$  yields a polynomial of the form

$$f(x)^n \equiv u + vx \pmod{x^2 - a}.$$

Let  $g(x) = f(x) \pmod{x^2 - a}$ . To find  $\sqrt{a}$ , it suffices to solve for  $x \in S$ . But first, we must solve for the two unknowns  $u, v$ .

To solve for  $u$ , we simply need to find the constant term in  $g(x)$ . To do so, we can simply consider  $g(x)$  modulo  $x$ , which gives

$$u = g(x) \pmod{x}.$$

Solving for  $v$  is also simple. We need to find the coefficient  $[x]g(x)$ . To do so, we divide  $g(x)$  by  $x$  to get

$$v = x^{-1}g(x).$$

Now, solving for  $x$  in  $u + vx$  yields

$$x = -uv^{-1}.$$

Here, the root of  $x$  is likely to be irrational. Hence, the solution to  $x \in S$  will not be exact, and will grow more precise as  $k$  goes to infinity. Taking the limit, and substituting for all variables in  $x = -uv^{-1}$ , gives

$$x = \lim_{k \rightarrow \infty} \frac{-x \left( ((x+1)^k \pmod{x^2 - n}) \pmod{x} \right)}{(x+1)^k \pmod{x^2 - a}}.$$

Next, we apply Kronecker substitution on the right-hand side with  $x = k^k$ , to get

$$x = \lim_{k \rightarrow \infty} \frac{-k^k \left( ((k^k + 1)^k \pmod{k^{2k} - a}) \pmod{k^k} \right)}{(k^k + 1)^k \pmod{k^{2k} - a}}.$$

By Theorem 2, this Kronecker substitution is valid as  $k \rightarrow \infty$ , since  $k^k$  is greater than the coefficient sum of  $f(x)^k \pmod{x^2 - a}$ . It is important to note that, by the nature of Kronecker substitution, substituting  $x = k^k$  does not change the value of  $x$  on the left-hand side. This is because the substitution is injective and only used temporarily. The value of  $x$  is restored to  $\sqrt{a}$  upon decoding from the base  $k^k$ , which is carried out by the mod operations.

Typically,  $\sqrt{a}$  is defined as positive. Making this adjustment, and substituting with  $x = \sqrt{a} \in \mathbb{R}$  on the left-hand side, gives

$$\sqrt{a} = \lim_{k \rightarrow \infty} \frac{k^k \left( ((k^k + 1)^k \pmod{k^{2k} - a}) \pmod{k^k} \right)}{(k^k + 1)^k \pmod{k^{2k} - a}} \in \mathbb{R}.$$

Which is the formula we wanted to prove. This completes the proof. □

**Remark 1.** The square root formula derived in Corollary 6 is quite intriguing. It is unusual to see an irrational number, such as  $\sqrt{a}$ , represented as the limit of a modular expression. Fascinated by this, we proceed by generalizing our approach to calculate the  $n$ -th roots of  $a$ .

**Theorem 7.** Let  $a, n \in \mathbb{Z}^+$  such that  $a > 1$ . Then

$$\sqrt[n]{a} = \lim_{k \rightarrow \infty} \frac{(k^{kn} + 1)^{kn+1} \bmod (k^{kn^2} - a)}{(k^{kn} + 1)^{kn} \bmod (k^{kn^2} - a)} - 1 \in \mathbb{R}.$$

*Proof.* Fix a ring  $S = \mathbb{Z}[x]/(x^n - a)$ . In the ring  $S$ , the elements obey the relation  $x^n = a$ . This means that in the ring  $S$ , all elements are implicitly reduced modulo  $(x^n - a)$ . Furthermore,  $x$  is an algebraic integer in the ring  $S$ , representing the  $n$ -th root of  $a$ . Formally, this means  $S = \mathbb{Z}[x]/(x^n - a) \cong \mathbb{Z}[\sqrt[n]{a}]$ .

Consider  $f(x) = x + 1 \in S$ . To solve for  $x \in S$ , we can use the identity

$$\frac{f(x)^{k+1}}{f(x)^k} = \frac{(x+1)^{k+1}}{(x+1)^k} = x + 1.$$

In this case, we have

$$x + 1 = \frac{(x+1)^{kn+1} \bmod (x^n - a)}{(x+1)^{kn} \bmod (x^n - a)} \implies x = \frac{(x+1)^{kn+1} \bmod (x^n - a)}{(x+1)^{kn} \bmod (x^n - a)} - 1.$$

While seemingly trivial, in the context of  $f(x)^k = x^k \bmod (x^n - a)$ , its application is reminiscent of applying the Newton-Raphson method to approximate roots [11]. Particularly, as  $k \rightarrow \infty$ , solving for  $x$  gives us a closer and closer approximation to  $x = \sqrt[n]{a}$  in  $\mathbb{R}$ . Applying this substitution and taking the limit as  $k \rightarrow \infty$  gives

$$\sqrt[n]{a} = \lim_{k \rightarrow \infty} \frac{(x+1)^{kn+1} \bmod (x^n - a)}{(x+1)^{kn} \bmod (x^n - a)} - 1 \in \mathbb{R}.$$

Next, using Theorem 2, we apply Kronecker substitution to the right-hand side with  $x = k^{kn}$ , to get

$$\sqrt[n]{a} = \lim_{k \rightarrow \infty} \frac{(k^{kn} + 1)^{kn+1} \bmod (k^{kn^2} - a)}{(k^{kn} + 1)^{kn} \bmod (k^{kn^2} - a)} - 1 \in \mathbb{R}.$$

Which is the formula we wanted to prove. By Theorem 2, the Kronecker substitution is valid as  $k \rightarrow \infty$ , since  $k^{kn}$  is greater than the coefficient sum of  $f(x)^{kn} \bmod (x^n - a)$ . As in our proof of Corollary 6, applying Kronecker substitution using  $x = k^{kn}$  does not change the value of  $x$  on the left-hand side. This is because the substitution is injective and only used temporarily. The value of  $x$  is restored to  $\sqrt[n]{a}$  upon decoding from the base  $k^{kn}$ , which is being carried out by the mod operations. This complete the proof.  $\square$

An interesting aspect of the formula for  $\sqrt[n]{a}$ , as provided in Theorem 7, is the applicability of a second modular reduction when evaluating the polynomial  $f(x)$ . Although it appears that both the original and modified formulas theoretically converge to the same value, our cursory analysis suggests that the convergence rates and the actual values in  $\mathbb{R}$  differ. Let  $c \in \mathbb{Z}_{\geq -1}$ . Then, we observe

$$\sqrt[n]{a} = \lim_{k \rightarrow \infty} \frac{\left( (k^{kn} + 1)^{kn+1} \bmod (k^{kn^2} - a) \right) \bmod (k^{kn} - c)}{\left( (k^{kn} + 1)^{kn} \bmod (k^{kn^2} - a) \right) \bmod (k^{kn} - c)} - 1 \in \mathbb{R},$$

contrasted with

$$\sqrt[n]{a} = \lim_{k \rightarrow \infty} \frac{(k^{kn} + 1)^{kn+1} \bmod (k^{kn^2} - a)}{(k^{kn} + 1)^{kn} \bmod (k^{kn^2} - a)} - 1 \in \mathbb{R}.$$

It is important to note that both formulas are convergent, but not monotone. A deeper examination into the differences between these expressions and their numerical stabilities could yield further simplifications or conclusions.

**Remark 2.** *Additionally, the overall structure of our root formula and the machinery we employed to derive it, share notable conceptual similarities to root calculations in the field of  $p$ -adic analysis, as detailed by Kecić and Tahar [12]. In particular, both approaches leverage integer bases, modular arithmetic, convergence, and utilize adaptations of the Newton-Raphson method to perform iterative refinement of calculations. Despite fundamental differences, the potential for results from  $p$ -adic analysis to inform or enhance our understanding, or vice versa, is compelling.*

## 4.4 Central Binomial Coefficients Formula

We apply Theorem 2 to derive a new formula for the  $n$ -th central binomial coefficient  $\binom{2n}{n}$ , which is sequence [A000984](#) in the OEIS [9]. Starting from  $n = 0$ , the sequence of central binomial coefficients begins as

$$\binom{2n}{n} = 1, 2, 6, 20, 70, 252, 924, 3432, 12870, 48620, 184756, 705432, 2704156, 10400600, \dots$$

**Theorem 8.** *Let  $n \in \mathbb{Z}^+$  such that  $n > 0$ . Then*

$$\binom{2n}{n} = ((4^n + 1)^{2n} \bmod (4^{n(n+1)} + 1)) \bmod (4^n - 1).$$

*Proof.* Fix a ring  $R = \mathbb{Z}[x]/(x^{n+1} + 1)$ . In the ring  $R$ , the elements obey the relation  $x^{n+1} = -1$ .

Let  $f(x) = (x + 1)^{2n} \in R$ . Expanding  $f(x)$  and taking the result modulo  $(x - 1)$  gives

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

Thus, we have

$$\binom{2n}{n} = ((x + 1)^{2n} \bmod (x^{n+1} + 1)) \bmod (x - 1).$$

Applying Theorem 2 by substituting with  $x = 4^n$  and simplifying, yields

$$\binom{2n}{n} = ((4^n + 1)^{2n} \bmod (4^{n(n+1)} + 1)) \bmod (4^n - 1).$$

By Theorem 2, this substitution is valid since  $4^n > \binom{2n}{n}$ .

Considering  $n = 0$ , the final modulus  $(4^n - 1) = 4^0 - 1 = 0$  results in an undefined remainder (due to division by zero). Thus, the formula is valid for  $n > 0$ .  $\square$

## 5 Literature Review and the Resolution of an Open Question

Our literature review revealed no formal studies closely aligned with the methodologies and results discussed in this paper. However, an informal reference of note is a blog post by Paul Hankin [13] (2018). Hankin and a contributor, Faré Rideau, explored modular expressions for Fibonacci numbers, initially discovered by examining the decimal expansion of the generating function:

$$F(x) = \frac{x}{1 - x - x^2}.$$

From this generating function, Hankin proposed a formula

$$F_n = \left\lfloor \frac{2^{(n+1)(n+2)}}{2^{2n+2} - 2^{n+1} - 1} \right\rfloor \bmod 2^{n+1},$$

which was experimentally simplified by Rideau to

$$F_n = (2^{(n+1)(n+2)} \bmod (2^{2n+2} - 2^{n+1} - 1)) \bmod 2^{n+1}.$$

Our research developed independently as a natural extension of our previous works on quotient rings [14] and binomial coefficient formulas [7]. Coincidentally, our work addresses an important open question posed by Hankin at the conclusion of his 2018 blog post [13]. In particular, Hankin asks whether the approach can be generalized to compute terms of other recurrence sequences. Not only does our research provide an affirmative answer to this question (Theorem 4), but it also extends the methodology to real numbers via roots (Corollary 6), thereby expanding the scope and potential applications of these techniques.

Hankin and Rideau’s explorations were innovative, however they lacked a formal theoretical framework and rigorous proofs. Our contributions advance the theoretical understanding of these processes by providing detailed proofs and establishing a comprehensive mathematical framework. This framework lays a solid foundation for future applications and extensions of these methods, enabling researchers to build upon our work and explore new avenues for investigation.

## 5.1 An Update on Subsequent Related Research

Shortly following the initial dissemination of this paper on arXiv in March 2024, Prunescu and Sauras-Altuzarra independently explored related ideas in their research on integer representations of C-recursive integer sequences [10]. While our work employs Kronecker substitution in conjunction with quotient rings to derive formulas for C-recursive integer sequences, their approach utilizes Kronecker substitution with generating functions to achieve the same outcome. Despite the differences in the intermediate machinery used, both works share the fundamental principle of leveraging Kronecker substitution to study C-recursive integer sequences. The connections between our approaches highlight the potential for collaboration and the development of new insights in this emerging area of research.

## 6 Future Research

Harvey (2009) [2] proposed a method for improving the efficiency of polynomial multiplication by performing Kronecker substitution via multiple evaluations, termed “multi-point Kronecker substitution”. Harvey described how to compute his method up to  $r = 4$  points. Bos et al. (2020) [5] generalized Harvey’s result using an approach which they have called “Kronecker+”. A brief description of the process is as follows:

First, a base  $b$  is selected along with a fixed constant  $r$ , which corresponds to the number of evaluation points. Next, the polynomial  $f(x)$  is evaluated at  $r$  points, which are the products of  $b$  and the  $n$ -th roots of unity. The results of all evaluations are then combined using a modified version of the Inverse Discrete Fourier Transform (IDFT) to recover the polynomial coefficients. The use of multiple evaluation points allows for a more efficient encoding and decoding process, as it reduces the size of the integers involved in the arithmetic operations.

The aforementioned techniques both present promising avenues for future research, specifically as pertains to the efficient computation of integer sequence terms using our approach.

Furthermore, research into efficient computation modulo  $n$  using our formulas could lead to new and improved methods. For instance, Dumas et al. (2011) [15] give a method for computing remainders of polynomials encoded as integers via Kronecker substitution, termed “simultaneous modular reduction”. Applying their technique to our results, or finding new methods to achieve modular reduction in Kronecker substitution form, is of great interest.

## 6.1 Research Questions

1. Can computations be optimized?

For instance, by way of multipoint Kronecker substitution or Kronecker+ [2, 5].

2. Can computations modulo  $n$  be optimized?

For instance, using simultaneous modular reduction [15].

3. Can our root formulas inform new methods for root finding in finite fields like  $\mathbb{F}_p$ ?

See in particular Theorem 7 and its proceeding remarks.

4. Can our results be extended to multivariate polynomial quotient rings?

For instance, by applying techniques from Wang et al [16].

## 7 Appendix: Kronecker Substitution

Kronecker substitution, named after the mathematician Leopold Kronecker, is a technique for converting a polynomial to an integer representation [1]. The technique is named for Kronecker, as he used it to derive a method for polynomial factorization [17]. The technique works as follows:

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  $f(x)$  in its digits.

More formally, let  $f(x) \in \mathbb{Z}[x]$  be a polynomial of degree  $d$ , represented as

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0,$$

where  $a_i \in \mathbb{Z}$  for  $0 \leq i \leq d$ . Performing Kronecker substitution with  $x = b$  yields the integer

$$f(b) = a_d b^d + a_{d-1} b^{d-1} + \cdots + a_1 b + a_0.$$

When  $b$  is sufficiently large, the base- $b$  representation of  $f(b)$  directly corresponds to the coefficients of  $f(x)$ . In other words, the digits of  $f(b)$  in base  $b$  are precisely the coefficients  $a_d, a_{d-1}, \dots, a_1, a_0$ , in order from most significant to least significant.

To ensure a one-to-one correspondence between the coefficients and the digits, the base  $b$  must be chosen such that

$$b > \max_{0 \leq i \leq d} |a_i|.$$

This guarantees that there is no “carry over” between digits when performing arithmetic operations on the integer representation.

**Remark 3.** *Traditionally, the base  $b$  is selected to be the smallest power of 2 which is greater than any of the coefficients of the encoded polynomial. Though, this is typically not the optimally smallest base. As we demonstrated in [7], the base  $b = f(1)$  is optimal for any polynomial in  $\mathbb{Z}[x]$  with non-negative coefficients.*

The process of Kronecker substitution can be reversed to recover the original polynomial  $f(x)$  from its integer representation  $f(b)$ . Given  $f(b)$  and the base  $b$ , one can extract the coefficients by successively dividing  $f(b)$  by powers of  $b$  and taking the remainders. This allows for the reconstruction of  $f(x)$  from  $f(b)$  [18].

Kronecker substitution has found numerous applications in computer algebra and symbolic computation, particularly in the design of efficient algorithms for polynomial multiplication [2, 3]. By reducing polynomial operations to integer arithmetic, Kronecker substitution enables the use of fast integer multiplication algorithms, resulting in improved performance for polynomial computations.

## 7.1 Kronecker Substitution in Action

To demonstrate Kronecker substitution, we proceed with a simple example in base-10.

**Example 1.** Fix  $b = 10$ . Consider the polynomial

$$f(x) = 4x^3 + 3x^2 + 2x + 1 \in \mathbb{Z}[x].$$

### Step 1. Encoding:

We encode the coefficients of  $f(x)$  using base  $b = 10$ , chosen because it exceeds the absolute

values of all coefficients in  $f(x)$ , thereby ensuring no overlap or “carry over” in the encoding process.

Substituting  $x = 10$  into  $f(x)$ , we calculate

$$\begin{aligned} f(10) &= 4(10)^3 + 3(10)^2 + 2(10) + 1 \\ &= 4000 + 300 + 20 + 1 \\ &= 4321. \end{aligned}$$

## Step 2. Decoding:

To decode  $f(x)$  from its integer representation,  $f(10) = 4321$ , one can extract each digit according to its positional value in base-10:

- The thousands digit, 4, is the coefficient of  $x^3$ .
- The hundreds digit, 3, is the coefficient of  $x^2$ .
- The tens digit, 2, is the coefficient of  $x$ .
- The units digit, 1, is the constant term.

Thus, we can reconstruct  $f(x) = 4x^3 + 3x^2 + 2x + 1$  from the integer 4321 by interpreting each digit according to its position in the base-10 representation.

## References

- [1] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 3rd edition, 2013. ISBN 978-1107039032.
- [2] D. Harvey. Faster Polynomial Multiplication via Multipoint Kronecker Substitution. *Journal of Symbolic Computation*, 44, 2009. doi: 10.1016/j.jsc.2009.05.004.
- [3] D. Harvey, J. van der Hoeven, and G. Lecerf. Faster Polynomial Multiplication Over Finite Fields, 2014.
- [4] 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>.
- [5] J. W. Bos, J. Renes, 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>.



- [6] 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>.
- [7] J. M. Shunia. A Simple Formula for Single-Variable Multinomial Coefficients, 2023. URL <https://arxiv.org/abs/2312.00301>. arXiv Preprint.
- [8] OEIS Foundation Inc. Pell Numbers - Entry A000129 in The On-Line Encyclopedia of Integer Sequences. <https://oeis.org/A000129>, 2024.
- [9] OEIS Foundation Inc. Central Binomial Coefficients - Entry A000984 in The On-Line Encyclopedia of Integer Sequences. <https://oeis.org/A000984>, 2024.
- [10] M. Prunescu and L. Sauras-Altuzarra. On the Representation of C-recursive Integer Sequences by Arithmetic Terms, May 2024. URL <https://arxiv.org/abs/2405.04083>.
- [11] J. Hubbard, D. Schleicher, S. Sutherland. How to Find All Roots of Complex Polynomials by Newton’s Method. *Inventiones mathematicae*, 146:1–33, 2001. doi: 10.1007/s002220100149.
- [12] M. Kecies and Z. Tahar. General Approach of the Root of a P-Adic Number. *Filomat*, 27(3):429–434, 2013. ISSN 03545180, 24060933. URL <https://www.jstor.org/stable/24896372>.
- [13] P. Hankin, F. Rideau. A Novel and Efficient Way to Compute Fibonacci Numbers, 2018. URL <https://blog.paulhankin.net/fibonacci2>. Blog Post.
- [14] J. M. Shunia. A Polynomial Ring Connecting Central Binomial Coefficients and Gould’s Sequence, 2023. URL <https://arxiv.org/abs/2312.00302>. arXiv Preprint.
- [15] J. Dumas, L. Fousse, and B. Salvy. Simultaneous Modular Reduction and Kronecker Substitution for Small Finite Fields. *Journal of Symbolic Computation*, 46(7):823–840, 2011. ISSN 0747-7171. doi: <https://doi.org/10.1016/j.jsc.2010.08.015>. URL <https://www.sciencedirect.com/science/article/pii/S0747717110001458>.
- [16] C. Wang, M. Su, G. Wang, and Q. Zhang. A New Reduction Method from Multivariate Polynomials to Univariate Polynomials, 2024. URL <https://arxiv.org/abs/2403.12716>. arXiv Preprint.
- [17] L. Kronecker. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. (Abdruck einer Festschrift zu Herrn E. E. Kummer’s Doctor-Jubiläum, 10. September 1881.). *Journal für die reine und angewandte Mathematik*, 92:1–122, 1882. URL <http://eudml.org/doc/148487>.
- [18] R. P. Grimaldi. *Discrete and Combinatorial Mathematics*. Pearson Education India, 2004. ISBN 978-0321385024.