Polynomial Quotient Rings and Kronecker Substitution for Deriving Combinatorial Identities

Joseph M. Shunia

March 2024
Revised: April 2024

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 linear recurrences, as well as explicit formulas for certain combinatorial sequences, including the Pell numbers and central binomial coefficients. For example, we present the formula: $\binom{2n}{n} = \left((4^n+1)^{2n} \mod (4^{n(n+1)}+1)\right) \mod (4^n-1)$. We also discover an unusual representation for the real rth roots of positive integers, characterized as the limit of a modular congruence. 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 of integers and polynomials by encoding them as integers in a larger 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.

In an unpublished preprint [7], we took some of the first steps in this direction by applying Kronecker substitution to binomial expansions, yielding a new formula for binomial coefficients:

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

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 3) to derive several others.

First, we obtain a general formula for the nth term of a linear recurrence with constant coefficients (Theorem 5). Let $n, d, b \in \mathbb{Z}^+$. Let A_n be a linear recurrence relation with constant coefficients of order d and initial starting conditions $A_0 = A_1 = \cdots = A_{d-1} = 1$, taking the form

$$A_n = c_{d-1}A_{n-1} + c_{d-2}A_{n-2} + \cdots + c_0 A_{n-d-1}$$

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

$$A_n = \left(b^{n-1} \bmod (b^d - c_{d-1}b^{d-1} - \cdots - c_1 b - c_0)\right) \bmod (b-1)$$

Second, to illustrate practical specificity, we derive a new formula for the Pell sequence (Theorem 6), which is a fundamental integer sequence. The Pell sequence is A000129 in the OEIS [8]. Valid for $n > 0$, our formula expresses the nth Pell number P_n in terms of a double modular expression involving powers of 3:

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

Our proof of the formula for the Pell sequence leads us to a general formula for square roots (Corollary 7). Let $n \in \mathbb{Z}^+$ such that $n > 1$. Then

$$\sqrt{n} = \lim_{k\to\infty} \frac{k^k \left(((k^k+1)^k \bmod (k^{2k} - n)) \bmod k^k\right)}{(k^k+1)^k \bmod (k^{2k} - n)} \quad \in \mathbb{R}$$

Intrigued by this unusual representation for $\sqrt{n}$, we take a slightly different approach to find a general formula for the rth roots of n (Corollary 8). Let $n, r \in \mathbb{Z}^+$ such that $n > 1$. Then

$$\sqrt[r]{n} = \lim_{k\to\infty} \frac{(k^{kr}+1)^{kr+1} \bmod (k^{kr^2} - n)}{(k^{kr}+1)^{kr} \bmod (k^{kr^2} - n)} - 1 \quad \in \mathbb{R}$$

Finally, we show one more specific application through creative application of quotient rings, to derive a new formula for the central binomial coefficients (Theorem 9), 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 nth central binomial coefficient in terms of a double modular expression involving powers of 4:

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

1.2 Structure of the Paper

The rest of this paper is organized as follows. We begin by briefly restating relevant results from our previous work 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 prior work of note, which posed an open question that is resolved by our findings. We conclude with § 6 by detailing some of our plans for future research in this area, as well as stating some related questions and an open problem that is equivalent to integer factorization.

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 we first proved in our previous work regarding a novel formula for binomial and 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. By assumption, $\forall k \in \mathbb{Z} : 0 \leq k \leq d$, 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 $0 \leq k \leq d$. Now, let's consider the expansion of $f(f(b))$, which can be written as

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

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

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

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 $a_d x^d$. The result is

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

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

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

By assumption, all coefficients of $f(x)$ are positive. Hence, it follows that $\forall k \in \mathbb{Z} : 0 \leq k \leq d$. 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 $a_0, a_1, \ldots, a_d$ 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 1. *The polynomial property described in Theorem 1 appears to be underexplored in the literature. While writing our unpublished preprint [7] in 2023, we conducted a preliminary literature review and were unable to find any papers explicitly describing it. However, it has been the subject of some online discussions [10, 11] and at least one blog post [12]. Despite these mentions, the property has been treated mostly as a novelty or curiosity, and its applications have not been thoroughly examined. We believe this property warrants further investigation, as it may have potential applications in areas such as combinatorics, number theory, p-adic analysis, computational algebra, and cryptography.*

To show how Theorem 1 can be used, we reprove another result from our previous paper [7] as a corollary.

Corollary 2. *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 nth row of Pascal's triangle. This sum is well-known to be equal to 2^n [13]. 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 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 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 3. *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,

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

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

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

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

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

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

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

This implies that, when applying Kronecker substitution, the base γ^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

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

is if

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

This completes the proof. □

4 Applications

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

Lemma 4. *Let $n, d \in \mathbb{Z}^+$. Let A_n be a linear recurrence relation with constant coefficients of order d and initial starting conditions $A_0 = A_1 = \cdots = A_{d-1} = 1$, taking the form*

$$A_n = c_{d-1}A_{n-1} + c_{d-2}A_{n-2} + \cdots + c_0 A_{n-d-1}$$

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

$$g(x) := c_{d-1}x^{d-1} + \cdots + c_1 x + c_0 \in \mathbb{Z}[x]$$

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

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

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 $\{1, x, x^2, \ldots, x^{d-1}\}$. 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 $g(x) = c_{d-1}x^{d-1} + \cdots + c_1 x + c_0$ 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

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

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

$$A_n = c_{d-1}A_{n-1} + c_{d-2}A_{n-2} + \cdots + c_0 A_{n-d-1}$$

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

$$g(x) = c_0 + c_1 x + \cdots + c_{d-1} x^{d-1}$$

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 $a_0, a_1, \ldots, a_{d-1}$ 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 $A_0, A_1, \ldots, A_{d-1}$. 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. □

4.1 Linear Recurrences Formula

To demonstrate the practical applications of Theorem 3, we apply it to derive a new formula for the nth term of a linear recurrence with constant coefficients.

Theorem 5. *Let $n, d \in \mathbb{Z}^+$. Let A_n be a linear recurrence relation with constant coefficients of order d and initial starting conditions $A_0 = A_1 = \cdots = A_{d-1} = 1$, taking the form*

$$A_n = c_{d-1} A_{n-1} + c_{d-2} A_{n-2} + \cdots + c_0 A_{n-d-1}$$

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

$$g(x) := c_{d-1} x^{d-1} + \cdots + c_1 x + c_0 \in \mathbb{Z}[x]$$

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

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

Proof. Consider the ring

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

By Lemma 4, 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

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

Applying Theorem 3 by substituting with $x = b$, we arrive at the given formula

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

By Theorem 3, this substitution is valid since $b > A_n$. This completes the proof. □

4.2 Pell Formula

We apply Theorem 3 to derive a new formula for the nth Pell number, which is sequence A000129 in the OEIS [8]. Starting from $n = 0$, the sequence P begins as

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

Theorem 6. *Let P_n denote the nth 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, for $n > 0$

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

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

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

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

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

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

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

Replacing n with $n-1$ yields

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

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

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

By Theorem 3, 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 $n > 0$. □

4.3 Roots

The previous result on Pell numbers (Theorem 6) leads us to an interesting result on square roots.

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

$$\sqrt{n} = \lim_{k\to\infty} \frac{k^k\Big(\big((k^k+1)^k \bmod (k^{2k}-n)\big) \bmod k^k\Big)}{(k^k+1)^k \bmod (k^{2k}-n)} \quad \in \mathbb{R}$$

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

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

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

Let $g(x) = f(x) \bmod (x^2-n)$. To find $\sqrt{n}$, 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

$$u = g(x) \bmod x$$

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 n goes to infinity. Taking the limit, and substituting for all variables in $x = -uv^{-1}$, gives

$$x = \lim_{k\to\infty} \frac{-x\Big(\big((x+1)^k \bmod (x^2-n)\big) \bmod x\Big)}{(x+1)^k \bmod (x^2-n)}$$

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

$$x = \lim_{k\to\infty} \frac{-k^k\Big(\big((k^k+1)^k \bmod (k^{2k}-n)\big) \bmod k^k\Big)}{(k^k+1)^k \bmod (k^{2k}-n)}$$

By Theorem 3, this Kronecker substitution is valid as $k \to \infty$, since k^k is greater than the coefficient sum of $f(x)^k \bmod (x^2-n)$. 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 $\sqrt{n}$ upon decoding from the base k^k, which is carried out by the mod operations.

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

$$\sqrt{n} = \lim_{k\to\infty} \frac{k^k\Big(\big((k^k+1)^k \bmod (k^{2k}-n)\big) \bmod k^k\Big)}{(k^k+1)^k \bmod (k^{2k}-n)} \quad \in \mathbb{R}$$

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

Remark 2. *The square root formula derived in Corollary 7 is quite intriguing. It is unusual to see an irrational number, such as $\sqrt{n}$, represented as the limit of a modular expression. Fascinated by this, we proceed by generalizing our approach to calculate the rth roots of n.*

Corollary 8. *Let $n, r \in \mathbb{Z}^+$ such that $n > 1$. Then*

$$\sqrt[r]{n} = \lim_{k\to\infty} \frac{(k^{kr}+1)^{kr+1} \bmod (k^{kr^2}-n)}{(k^{kr}+1)^{kr} \bmod (k^{kr^2}-n)} - 1 \quad \in \mathbb{R}$$

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

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

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

Hence

$$x + 1 = \frac{(x+1)^{kr+1}}{(x+1)^{kr}} \quad \Longrightarrow \quad x = \frac{(x+1)^{kr+1}}{(x+1)^{kr}} - 1$$

While seemingly trivial, in the context of $f(x)^k = x^k \in S$, its application is reminiscent of applying the Newton-Raphson method to approximate roots [14]. Particularly, as $k \to \infty$, solving for x gives us a closer and closer approximation to $x = \sqrt[r]{n} \in \mathbb{R}$. Applying this substitution and taking the limit as $k \to \infty$ gives

$$\sqrt[r]{n} = \lim_{k\to\infty} \frac{(x+1)^{kr+1}}{(x+1)^{kr}} - 1 \quad \in \mathbb{R}$$

Next, using Theorem 3, we apply Kronecker substitution to the right-hand side with $x = k^{kr}$, to get

$$\sqrt[r]{n} = \lim_{k\to\infty} \frac{(k^{kr}+1)^{kr+1} \bmod (k^{kr^2} - n)}{(k^{kr}+1)^{kr} \bmod (k^{kr^2} - n)} - 1 \quad \in \mathbb{R}$$

Which is the formula we wanted to prove. By Theorem 3, the Kronecker substitution is valid as $k \to \infty$, since k^{kr} is greater than the coefficient sum of $f(x)^{kr} \bmod (x^r - n)$. As in our proof of Corollary 7, applying Kronecker substitution using $x = k^{kr}$ 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 $\sqrt[r]{n}$ upon decoding from the base k^{kr}, which is being carried out by the mod operations. This complete the proof. □

Remark 3. *An interesting aspect of the formula for $\sqrt[r]{n}$, as provided in Corollary 8, 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*

$$\sqrt[r]{n} = \lim_{k\to\infty} \frac{\Big((k^{kr}+1)^{kr+1} \bmod (k^{kr^2} - n)\Big) \bmod (k^{kr} - c)}{\big((k^{kr}+1)^{kr} \bmod (k^{kr^2} - n)\big) \bmod (k^{kr} - c)} - 1 \quad \in \mathbb{R},$$

contrasted with

$$\sqrt[r]{n} = \lim_{k\to\infty} \frac{(k^{kr}+1)^{kr+1} \bmod (k^{kr^2} - n)}{(k^{kr}+1)^{kr} \bmod (k^{kr^2} - n)} - 1 \quad \in \mathbb{R}.$$

A deeper examination into the differences between these expressions and their numerical stabilities could yield further simplifications or conclusions.

Remark 4. *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 Kecies and Tahar [15]. 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 3 to derive a new formula for the nth 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

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

Theorem 9. *Let $n \in \mathbb{Z}^+$ such that $n > 0$. Then*

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

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

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

Thus, we have

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

Applying Theorem 3 by substituting with $x = 4^n$ and simplifying, yields

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

By Theorem 3, 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 $n > 0$. □

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

[16] (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:

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

Our research developed independently as a natural extension of our previous works on quotient rings [17] and binomial coefficient formulas [7]. Coincidentally, our work addresses an important open question posed by Hankin at the conclusion of his 2018 blog post [16]. 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 5), but it also extends the methodology to real numbers via roots (Corollary 7), 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 significantly 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. Furthermore, the formalization of these techniques enables applications across various fields, from theoretical mathematics to practical algorithms in computer science and engineering.

Remark 5. *An early version of this paper included a Fibonacci formula similar to Hankin and Rideau's. We removed the formula after finding Hankin's blog post in a subsequent literature review.*

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 rth 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) [18] 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 [18].

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

   See in particular Corollary 8 and its proceeding remarks.

6.2 An Open Problem

6.2.1 Problem Statement

Let $n, b \in \mathbb{Z}^+$. Let $f(x), g(x) \in \mathbb{Z}[x]$ such that $g(x)$ is a monomial, and

$$\deg(f(x)), \deg(g(x)) = O(n)$$

Find an efficient algorithm or method to compute the remainder $\alpha \in \mathbb{Z}/n\mathbb{Z}$, given by:

$$\alpha \equiv \big(f(b) \bmod g(b)\big) \pmod{n}$$

Solutions should avoid direct computations of $f(b), g(b) \in \mathbb{Z}$ in calculating the intermediate remainder term $f(b) \bmod g(b)$, as their values can be exponential in n.

6.2.2 A Non-Trivial Example

Let $f(x) := (x+1)^{2n}$, $g(x) := x^n$, and $b = 4^n$. Hence, we have

$$f(b) = f(4^n) = (4^n + 1)^{2n}$$
$$g(b) = g(4^n) = (4^n)^n = 4^{n^2}$$

A solution to this problem would be able to efficiently calculate the remainder

$$\alpha \equiv \big(f(b) \bmod g(b)\big) \pmod{n}$$
$$\iff \alpha \equiv \big((4^n + 1)^{2n} \bmod 4^{n^2}\big) \pmod{n}$$

The stated problem is equivalent to integer factorization by way of our binomial coefficient formulas (Corollary 2, Theorem 9) [7]. This equivalence is due to existence of a polynomial time algorithm for calculating $k!$ given $\binom{2k}{k}$ [9], where $k \in \mathbb{Z}^+ : k < n$.

To elaborate: Given a polynomial time algorithm for calculating $\binom{2k}{k} \pmod{n}$, one can calculate $k! \pmod{n}$. Then, $\gcd(n, k! \bmod n)$ computations can be performed in $O(n \log n)$ time to find a nontrivial factor of n. Thus, an efficient solution to our problem would enable an efficient solution to the problem of integer factorization.

6.2.3 On Difficulty

While our problem is an interesting framing of the integer factorization problem, this variant is seemingly quite difficult. Indeed, the naive approach to solving it exhibits an exponential complexity of $O(2^n)$ [7]. In contrast, several randomized subexponential time algorithms on the order of $O(2^{\log n})$ are known for integer factorization [19].

In the given example, the bottleneck is in the calculation of the intermediate term

$$(4^n + 1)^{2n} \bmod 4^{n^2}$$

Finding an efficient way to calculate remainders such as these modulo n, is the key to solving the problem. Any improvement over the naive approach would be of interest.

7 Appendix: A Primer on Kronecker Substitution

Kronecker substitution, named after the mathematician Leopold Kronecker who first described it in 1882 [1], is a technique for converting a polynomial to an integer representation. 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 $a_d, a_{d-1}, \ldots, a_1, a_0$, 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 6. *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. In Theorem 1, we show that $b = f(1)$ 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 $f(b)$ [20].

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

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

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] L. Kronecker. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. (Abdruck einer Festschrift zu Herrn E. E. Kummers Doctor-Jubiläum, 10. September 1881.). *Journal für die reine und angewandte Mathematik*, 92:1–122, 1882. URL http://eudml.org/doc/148487.

[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] Joseph M. Shunia. A Simple Formula for Binomial Coefficients Revealed Through Polynomial Encoding, 2023. URL https://arxiv.org/abs/2312.00301. Unpublished 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] Mathoverflow Users. Application of Polynomials with Non-Negative Coefficients, 2012. URL https://mathoverflow.net/questions/91827. MathOverflow Discussion.

[11] 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.

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

[13] OEIS Foundation Inc. Powers of 2 - Entry A000079 in The On-Line Encyclopedia of Integer Sequences. https://oeis.org/A000045, 2024.

[14] 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.

[15] 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.

[16] P. Hankin, F. Rideau. A Novel and Efficient Way to Compute Fibonacci Numbers, 2018. URL https://blog.paulhankin.net/fibonacci2. Blog Post.

[17] J. M. Shunia. A Polynomial Ring Connecting Central Binomial Coefficients and Gould's Sequence, 2023. URL https://arxiv.org/abs/2312.00302. Unpublished Preprint.

[18] 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.

[19] C. Pomerance. A Tale of Two Sieves. *Notices of the American Mathematical Society*, 43(12): 1473–1484, 1996. URL https://www.ams.org/notices/199612/pomerance.pdf.

[20] R. P. Grimaldi. *Discrete and Combinatorial Mathematics*. Pearson Education India, 2004. ISBN 978-0321385024.