Polynomial Quotient Rings and Kronecker Substitution for Deriving Combinatorial Identities

Joseph M. Shunia

March 2024

Abstract

We establish a new connection between combinatorial number theory and polynomial ring theory by applying Kronecker substitution and related polynomial encoding techniques to polynomial expansions within quotient rings. We prove a new theorem which provides a general framework for generating combinatorial identities using polynomial quotient rings in conjunction with Kronecker substitution. We demonstrate the theorem's utility by deriving an explicit formula for famous integer sequences, such as the Fibonacci sequence, Pell sequence, and the central binomial coefficients. To give an example, we present a formula for the n-th Fibonacci number, valid for $n > 1$, given by: $F_n = (2^{n(n-1)} \bmod (4^n - 2^n - 1)) \bmod (2^n - 1)$. Additionally, we find a new formula for square roots using our approach. This work builds upon our previous results on binomial and multinomial coefficients, extending the application of Kronecker substitution beyond its traditional use in improving the efficiency of integer and polynomial multiplication algorithms.

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], its potential applications in combinatorial number theory have remained largely unexplored.

In an unpublished preprint [4], we took the first steps in this direction by applying Kronecker substitution to binomial expansions, yielding a new formula for binomial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.

1.1 New Formulas

To demonstrate the power of our approach, we apply our main theorem to derive new explicit formulas for several important combinatorial sequences. We also find a result on square roots.

First, we obtain a formula for the Fibonacci sequence, one of the most well-known and widely studied combinatorial sequences. The Fibonacci sequence is A000045 in the OEIS [5]. Valid for $n > 1$, our formula expresses the n-th Fibonacci number F_n in terms of a double modular expression involving powers of 2:

$$F_n = (2^{n(n-1)} \bmod (4^n - 2^n - 1)) \bmod (2^n - 1)$$

Second, we derive a new formula for the Pell sequence, which is another fundamental integer sequence. The Pell sequence is A000129 in the OEIS [6]. Valid for $n > 1$, our formula expresses the n-th Pell number P_n in terms of a double modular expression involving powers of 2:

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

In proving the above formula for the Pell sequence, we uncover a general formula for square roots. Let $n \in \mathbb{Z}^+$ such that $n > 1$. Then

$$\sqrt{n} = \lim_{k\to\infty} \quad \frac{n^k((n^k+1)^k \bmod (n^k - n, n^k))}{(n^k+1)^k \bmod (n^k - n)}$$

Finally, we derive a new formula for the central binomial coefficients, which are the binomial coefficients of the form $\binom{2n}{n}$. These coefficients form sequence A000984 in the OEIS [7] 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. In § 2, we introduce the notations used throughout the paper. § 3 provides a brief primer on Kronecker substitution. Our main results, including the quotient ring encoding theorem and its proof, are presented in § 5. In § 6, we apply our quotient ring encoding theorem to derive the new Fibonacci and central binomial coefficient formulas.

2 Notations

This section provides a brief overview of the notations used throughout this paper.

Notation 1 (Sequential moduli)**.** Let $n \in \mathbb{Z}$ and let $(m_0, m_1, \ldots, m_k)$ be a sequence of moduli. We define the application of mod operations on n by this sequence as follows:

$$n \bmod (m_0, m_1, \ldots, m_k) \Longleftrightarrow (((n \bmod m_0) \bmod m_1) \cdots) \bmod m_k,$$

where the mod operations are performed sequentially from left to right, following the order of the moduli as listed.

Notation 2 (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

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

3 A Brief 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.

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 $f(b)$ [8].

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.

4 Polynomial Encoding Theorem

For completeness, we restate a theorem we first shared in our previous work on a formula for binomial coefficients [4].

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, the coefficient a_k, where $0 \leq k \leq d$, can be recovered explicitly using the formula:

$$a_k = \left\lfloor \frac{f(f(b)) \bmod f(b)^{k+1}}{f(b)^k} \right\rfloor$$

Proof. By assumption, for all coefficients a_k of $f(x)$, where $0 \leq k \leq d$, we can recover a_k using the given formula.

To prove the validity of the formula, we proceed by examining its arithmetic operations step-by-step. Let's consider the expansion of $f(f(b))$, which is

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

The first step in the formula is to take $f(f(b)) \bmod f(b)^{k+1}$. In doing so, we effectively isolate the terms up to x^k. The result is

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

The next step is to divide by $f(b)^k$, which gives

$$\begin{aligned} \frac{f(f(b)) \bmod f(b)^{k+1}}{f(b)^k} &= f(b)^{-k}(a_k f(b)^k + \cdots + a_1 f(b) + a_0) \\ &= a_k f(b)^{k-k} + a_k f(b)^{k-(k-1)} + \cdots + a_1 f(b)^{1-k} + a_0 b^{-k} \\ &= a_k + \cdots + a_1 f(b)^{1-k} + a_0 b^{-k} \end{aligned}$$

Finally, since $b > |a_j|$ for all j in $0 \leq j \leq (k-1)$, the floor operation isolates the coefficient we want

$$\begin{aligned} \left\lfloor \frac{f(f(b)) \bmod f(b)^{k+1}}{f(b)^k} \right\rfloor &= \left\lfloor a_k + \cdots + a_1 f(b)^{1-k} + a_0 b^{-k} \right\rfloor \\ &= a_k \end{aligned}$$

The floor operation ensures that the result is in $\mathbb{Z}$, and since the coefficients are non-negative, the floor operation does not affect the result.

Thus, we can recover all the coefficients $a_0, a_1, \ldots, a_d$ using only the values $f(b)$ and $f(f(b))$. Furthermore, since we can recover a_k given k, we can determine the degree of the term corresponding to the coefficient recovered.

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. $\square$

5 Main Results

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.

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 $\gamma \in \mathbb{Z}^+$ and suppose $\gamma^k \geq |r(r(1))|$. Then,

$$r(b) = f(\gamma^k)^k \bmod (\tilde{g}(\gamma^k), \gamma^k - b) \quad \text{or} \quad r(b) \equiv 0 \pmod{\gamma^k - b}, \quad \forall b \in \mathbb{Z}$$

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

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

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

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

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

$$\gamma^k \geq r(r(1))$$

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

$$r(b) \neq f(\gamma^k)^k \bmod (\tilde{g}(\gamma^k), \gamma^k - b), \tag{1}$$

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. □

6 Applications

6.1 Fibonacci Formula

To demonstrate the practical applications of Theorem 2, we apply it to derive a new formula for the n-th Fibonacci number, which is sequence A000045 in the OEIS [5]. Starting from $n = 1$, the sequence F_n begins as

$$F_n = 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, 6765, \ldots$$

Theorem 3. *Let F_n denote the n-th term of the Fibonacci sequence, such that $F_0 = 0, F_1 = 1$, and for $n > 1$:*

$$F_n = F_{n-1} + F_{n-2}$$

Then, for $n > 1$

$$F_n = 2^{n(n-1)} \bmod (4^n - 2^n - 1, 2^n - 1)$$

Proof. Fix a ring $R = \mathbb{Z}[x]/(x^2 - x - 1)$. In the ring R, the elements obey the relation $x^2 = x + 1$. Solving for x using the quadratic equation gives the solutions

$$x = \frac{1+\sqrt{5}}{2}, \quad x = \frac{1-\sqrt{5}}{2}$$

Since F_n is always non-negative for $n \geq 0$, we choose $x = \frac{1+\sqrt{5}}{2} = \varphi$, where φ denotes the so-called "golden ratio". From the OEIS [5], we have the following formula:

$$\varphi^{n-1} = F_{n-1}\varphi + F_{n-2}$$

Substituting $\varphi = x \in R$, we can see

$$x^{n-1} \bmod (x^2 - x - 1, x - 1) = (F_{n-1}x + F_{n-2}) \bmod (x - 1)$$

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

$$\begin{aligned}(2^n)^{n-1} \bmod ((2^n)^2 - 2^n - 1, 2^n - 1) &= (F_{n-1}x + F_{n-2}) \bmod (x - 1)\\ 2^{n(n-1)} \bmod (4^n - 2^n - 1, 2^n - 1) &= F_n\end{aligned}$$

Considering $n = 1$, since $2^1 - 1 = F_1 = 1$, we have $F_1 \equiv 0 \pmod{2^n - 1}$. Thus, the formula is valid for $n > 1$. □

6.2 Pell Formula

We apply Theorem 2 to derive a new formula for the n-th Pell number, which is sequence A000129 in the OEIS [6]. Starting from $n = 1$, 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 4. *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, for $n > 1$

$$P_n = (2^n + 1)^{n-1} \bmod (4^n - 2, 2^n - 1)$$

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 mean 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

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

From the OEIS [6], we have the formula

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

Hence

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

Replacing n with $n - 1$ yields

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

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

$$\begin{aligned} P_n &= (2^n + 1)^{n-1} \bmod ((2^n)^2 - 2, 2^n - 1) \\ &= (2^n + 1)^{n-1} \bmod (4^n - 2, 2^n - 1) \end{aligned}$$

Considering $n = 1$, we have $P_1 = 1$. However, in applying our derived formula, we arrive at a contradiction

$$\begin{aligned} & P_1 = (2^1 + 1)^{1-1} \bmod (4^1 - 2, 2^1 - 1) \\ & P_1 = 3^0 \bmod (2, 1) \\ & P_1 = 1 \bmod (2, 1) \\ & P_1 = 0 \\ \Rightarrow\ & 1 = 0 & \text{(contradiction)} \end{aligned}$$

Hence, the formula is invalid for $n = 1$. On the other hand, considering $n > 1$, we see that

$$(x+1)^n \not\equiv 0 \pmod{x^2-2, x-1}, \quad \forall n > 1,$$

leading to

$$(2^n+1)^n \not\equiv 0 \pmod{4^n-2, 2^n-1}, \quad \forall n > 1.$$

Thus, the given formula is valid for $n > 1$. $\square$

6.3 Square Roots

The previous result on Pell numbers (Theorem 4) leads us to an interesting result on square roots.

Theorem 5. *Let $n \in \mathbb{Z}^+$ such that $n > 1$. Then*

$$\sqrt{n} = \lim_{k\to\infty} \quad \frac{n^k((n^k+1)^k \bmod (n^k-n, n^k))}{(n^k+1)^k \bmod (n^k-n)}$$

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

Consider $f(x) = x + 1 \in R$. Let $a, b \in \mathbb{Z}$. Expanding $f(x)^n$ in R yields a polynomial of the form

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

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

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

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

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

$$b = x^{-1}g(x)$$

Now, solving for x in $a + bx$ yields

$$x = -ab^{-1}$$

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

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

Typically, $\sqrt{n}$ is defined as positive. Making this adjustment, and substituting with $x = \sqrt{n}$, gives

$$\sqrt{n} = \lim_{k\to\infty} \frac{n^k((n^k+1)^k \bmod (n^k-n, n^k))}{(n^k+1)^k \bmod (n^k-n)}$$

Which is the formula we wanted prove. □

6.4 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 [7]. Starting from $n = 1$, 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 6. *Let $n \in \mathbb{Z}^+$ such that $n > 0$. Then*

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

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

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

Thus, we have

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

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

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

Considering $n = 0$, since $4^0 - 1 = 0$, the final modulus in the sequence $(4^{n(n+1)}+1, 4^n-1)$ is undefined. Thus, the formula is valid for $n > 0$. $\square$

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] Joseph M. Shunia. A Simple Formula for Binomial Coefficients Revealed Through Polynomial Encoding, 2023.

[5] OEIS Foundation Inc. Fibonacci Numbers - Entry A000045 in The On-Line Encyclopedia of Integer Sequences. https://oeis.org/A000045, 2024.

[6] OEIS Foundation Inc. Pell Numbers - Entry A000129 in The On-Line Encyclopedia of Integer Sequences. https://oeis.org/A000129, 2024.

[7] OEIS Foundation Inc. Central Binomial Coefficients - Entry A000984 in The On-Line Encyclopedia of Integer Sequences. https://oeis.org/A000984, 2024.

[8] R. P. Grimaldi. *Discrete and Combinatorial Mathematics*. Pearson Education India, 2004.