Divisibility of Central Binomial Coefficients by Falling Factorials: Formal Verification in Lean 4

Naoki Takata

January 11, 2026

Abstract

We study the divisibility condition asking whether, for each non-negative integer k, there exists a positive integer n such that the product $\prod_{i=0}^{k}(n-i)$ divides the central binomial coefficient $\binom{2n}{n}$. We formalize this problem in Lean 4 and provide constructive proofs for $k = 0, 1, 2, 3$ by exhibiting explicit witnesses: $n = 1, 2, 2480, 8178$ respectively. To verify the cases $k = 2$ and $k = 3$, we implement an efficient divisibility check based on p-adic valuations and Legendre's formula, and prove its correctness. All results have been formally verified in the Lean 4 proof assistant using the Mathlib library.

1 Introduction

The central binomial coefficients $\binom{2n}{n}$ possess remarkable divisibility properties that have been studied extensively in combinatorics and number theory. A classical result states that $n + 1$ always divides $\binom{2n}{n}$; indeed, the quotient

$$C_n = \frac{1}{n+1}\binom{2n}{n}$$

is the n-th Catalan number. However, divisibility by n itself is considerably rarer.

Erdős and Graham posed the following natural question:

Conjecture 1.1 (Erdős–Graham)**.** For every non-negative integer k, there exists a positive integer $n > k$ such that

$$\prod_{i=0}^{k}(n-i) \mid \binom{2n}{n}.$$

Pomerance [1] made significant progress on related problems. He showed that for any fixed $k \geq 0$, there are infinitely many n such that $(n-k) \mid \binom{2n}{n}$, although the set of such n has upper density less than 1/3. Pomerance also proved that the set of n for which $\prod_{i=1}^{k}(n+i) \mid \binom{2n}{n}$ has density 1.

The smallest values of n satisfying the divisibility condition for each k are recorded in the OEIS as sequence A375077 [2].

In this paper, we provide a formal verification of the existence of witnesses for small values of k, using the Lean 4 proof assistant and the Mathlib library.

2 The Divisibility Condition

Definition 2.1 (Divisibility Condition)**.** For non-negative integers k and n with $n > k$, we define the predicate

$$\text{divides\_prod}(k, n) \iff \prod_{i=0}^{k}(n-i) \mid \binom{2n}{n}.$$

Remark 2.2. The product $\prod_{i=0}^{k}(n-i) = n(n-1)(n-2)\cdots(n-k)$ is the falling factorial $(n)_{k+1}$, which counts the number of ways to arrange $k+1$ distinct objects chosen from n objects.

Remark 2.3. For $n > k$, all factors in the product are positive, so $\prod_{i=0}^{k}(n-i) > 0$.

3 Witnesses for Small Values of k

We now present the witnesses that satisfy the divisibility condition for $k = 0, 1, 2, 3$.

3.1 The Case $k = 0$

Theorem 3.1. *We have* divides_prod$(0, 1)$*, i.e.,* $1 \mid \binom{2}{1}$.

Proof. The product $\prod_{i=0}^{0}(1-i) = 1$, and 1 divides any integer. This is verified by the `one_dvd` lemma in Lean. □

3.2 The Case $k = 1$

Theorem 3.2. *We have* divides_prod$(1, 2)$*, i.e.,* $2 \cdot 1 \mid \binom{4}{2}$.

Proof. The product is $\prod_{i=0}^{1}(2-i) = 2 \cdot 1 = 2$. The central binomial coefficient is $\binom{4}{2} = 6$. Since $6 = 2 \cdot 3$, we have $2 \mid 6$. Verified by `decide` in Lean. □

3.3 The Case $k = 2$

Theorem 3.3. *We have* divides_prod$(2, 2480)$*, i.e.,*

$$2480 \cdot 2479 \cdot 2478 \mid \binom{4960}{2480}.$$

Proof. The product is

$$\prod_{i=0}^{2}(2480-i) = 2480 \times 2479 \times 2478 = 15\,235\,735\,680.$$

The verification that this divides $\binom{4960}{2480}$ is computationally intensive. We use `native_decide` in Lean, which compiles the divisibility check to native code. □

3.4 The Case $k = 3$

Theorem 3.4. *We have* divides_prod$(3, 8178)$*, i.e.,*

$$8178 \cdot 8177 \cdot 8176 \cdot 8175 \mid \binom{16356}{8178}.$$

Proof. The product is

$$\prod_{i=0}^{3}(8178-i) = 8178 \times 8177 \times 8176 \times 8175 = 4\,468\,421\,684\,680\,320.$$

Verified by `native_decide` in Lean using the efficient computable check described in Section 4. □

k	Witness n	Product $\prod_{i=0}^{k}(n-i)$
0	1	1
1	2	2
2	2480	15 235 735 680
3	8178	4 468 421 684 680 320

Table 1: Witnesses for the divisibility condition for $k = 0, 1, 2, 3$, consistent with OEIS A375077.

4 Efficient Divisibility Check via p-adic Valuations

Direct computation of $\binom{2n}{n}$ for large n is impractical due to the exponential growth of the binomial coefficient. Instead, we employ a criterion based on p-adic valuations.

4.1 Legendre's Formula

Definition 4.1 (p-adic Valuation of Factorials)**.** For a prime p and a positive integer n, the p-adic valuation of $n!$, denoted $\nu_p(n!)$, is given by Legendre's formula:

$$\nu_p(n!) = \sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor = \frac{n - s_p(n)}{p-1},$$

where $s_p(n)$ is the sum of the digits of n in base p.

Lemma 4.2. *The function* `valuation_factorial` *defined by*

```
def valuation_factorial_aux (p : ) (hp : 2  p) (m : ) (acc : ) :  :=
  if h : m < p then acc
  else valuation_factorial_aux p hp (m / p) (acc + m / p)
```

correctly computes $\nu_p(m!)$ *when initialized with* $\text{acc} = 0$.

Proof. By strong induction on m. The recursion terminates since $m/p < m$ for $m \geq p$ and $p \geq 2$. The correctness follows from the identity

$$\nu_p(m!) = \left\lfloor \frac{m}{p} \right\rfloor + \nu_p\left(\left\lfloor \frac{m}{p} \right\rfloor !\right).$$

Formally verified in Lean as `valuation_factorial_eq`. ☐

4.2 Valuation of Central Binomial Coefficients

Definition 4.3 (p-adic Valuation of Central Binomial Coefficients)**.** For a prime p and a positive integer n, the p-adic valuation of $\binom{2n}{n}$ is

$$\nu_p\left(\binom{2n}{n}\right) = \nu_p((2n)!) - 2\nu_p(n!).$$

Lemma 4.4. *The function* `valuation_centralBinom` *correctly computes* $\nu_p\left(\binom{2n}{n}\right)$.

Proof. By the formula $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$ and the properties of p-adic valuations. Formally verified in Lean as `valuation_centralBinom_eq`. ☐

4.3 The Efficient Check

Theorem 4.5 (Divisibility Criterion). *Let a, b be positive integers. Then $a \mid b$ if and only if $\nu_p(a) \leq \nu_p(b)$ for all primes p.*

Proof. This follows from the fundamental theorem of arithmetic: $a \mid b$ if and only if the factorization of a is "contained" in that of b, which is equivalent to the stated inequality for all primes. □

Corollary 4.6. *To check whether $\prod_{i=0}^{k}(n-i) \mid \binom{2n}{n}$, it suffices to verify that for each prime p dividing the product,*

$$\nu_p\left(\prod_{i=0}^{k}(n-i)\right) \leq \nu_p\left(\binom{2n}{n}\right).$$

Definition 4.7 (Computable Divisibility Check). The function `check_divides_computable` is defined as:

```
def check_divides_computable (k n : ) : Bool :=
  let prod := (List.range (k + 1)).foldl (fun acc i => acc * (n - i)) 1
  if prod == 0 then false else
  let factors := prod.primeFactorsList
  factors.all (fun p =>
    factors.count p  valuation_centralBinom_exec p n)
```

Theorem 4.8. *For all $k, n \in \mathbb{N}$, if `check_divides_computable k n = true`, then* divides_prod(k, n) *holds.*

Proof. The function computes the prime factorization of the product and checks that each prime's multiplicity in the product does not exceed its multiplicity in $\binom{2n}{n}$. By Theorem 4.5, this implies divisibility. Formally verified in Lean as `check_divides_computable_correct`. □

5 Formal Verification

All theorems in this paper have been formally verified in the Lean 4 proof assistant (version 4.24.0) using the Mathlib library (commit `f897ebcf`). The formalization includes:

- Definition of the divisibility condition: `divides_prod`.
- Naive search functions: `find_n`, `find_witness`.
- Efficient valuation computations: `valuation_factorial`, `valuation_centralBinom`.
- Correctness proofs: `valuation_factorial_eq`, `valuation_centralBinom_eq`.
- The computable divisibility check: `check_divides_computable`.
- Correctness of the check: `check_divides_computable_correct`.
- Witness theorems: `witness_0`, `witness_1`, `witness_2`, `witness_3`.

The verification of `witness_2` and `witness_3` uses `native_decide`, which compiles the Boolean check to native code for efficient execution.

6 Conclusion

We have formally verified the existence of witnesses for the Erdős–Graham divisibility condition for $k = 0, 1, 2, 3$. The witnesses are $n = 1, 2, 2480, 8178$ respectively, consistent with the OEIS sequence A375077.

The key technical contribution is the implementation and correctness proof of an efficient divisibility check based on p-adic valuations. This approach avoids the computation of astronomically large binomial coefficients by reducing the problem to comparing prime factorization exponents.

The general conjecture—that for every k there exists such an n—remains open. Our formalization provides a verified computational framework that could be extended to search for witnesses for larger values of k.

Acknowledgments

The formalization was developed using the Mathlib library maintained by the Lean community.

References

[1] C. Pomerance, *Divisors of the middle binomial coefficient*, American Mathematical Monthly, 122(7):636–644, 2015.

[2] OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*, Sequence A375077, `https://oeis.org/A375077`, 2024.

[3] The Mathlib Community, *Mathlib: The Lean mathematical library*, `https://github.com/leanprover-community/mathlib4`, 2024.

[4] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in Automated Deduction – CADE 28, pp. 625–635, Springer, 2021.