On the Divisibility of Binomial Coefficients

Sílvia Casacuberta Puig

Abstract

We analyze an open problem in number theory regarding the divisibility of binomial coefficients. It is conjectured that for every integer n there exist primes p and r such that if $1 \leq k \leq n-1$ then the binomial coefficient $\binom{n}{k}$ is divisible by at least one of p or r. We prove the validity of the conjecture in several cases and obtain inequalities under which the conjecture is satisfied. We relate the problem to Cramér's, Oppermann's and Riemann's conjectures on prime gaps and study cases in which the conjecture is true using three primes instead of two. We also establish four upper bounds on the minimum number of primes needed for the conjecture to be true.

1 Introduction

Apart from their many uses in various fields of mathematics, binomial coefficients display interesting divisibility properties. Kummer's [8] and Lucas' [10] Theorems are two remarkable results relating binomial coefficients and prime numbers. Kummer's Theorem provides an easy way to determine the highest power of a prime that divides a binomial coefficient, and Lucas' Theorem yields the remainder of the division of a binomial coefficient by a prime number. Davis and Webb [4] found a generalization of Lucas' Theorem for prime powers. Legendre [9] found two expressions for the largest power of a prime p that divides the factorial $n!$ of a given integer n.

However, some conjectures about binomial coefficients still remain unproven. We focus on the following condition considered by Shareshian and Woodroofe in a recent paper [13]:

Condition 1. *For a positive integer n, there exist primes p and r such that, for all integers k with $1 \leq k \leq n-1$, the binomial coefficient $\binom{n}{k}$ is divisible by at least one of p or r.*

This condition leads to the following question:

Question 1.1. *Does Condition 1 hold for every positive integer n?*

In [13] it is conjectured that Condition 1 is true for all positive integers, yet there is no known proof. Shareshian and Woodroofe construct a chain of implications in group theory that lead to Condition 1. We tackle this problem using mainly number theory, although some links with group theory are made.

We also introduce the following variation of Condition 1, which we study later in this paper:

Definition 1.2. A positive integer n satisfies the *N-variation* of Condition 1 if there exists a set consisting of N different primes such that if $1 \leq k \leq n-1$ then the binomial coefficient $\binom{n}{k}$ is divisible by at least one of the N primes.

This paper is organized as follows. After providing background information in Section 2, we prove that n satisfies Condition 1 if it is a product of two prime powers and also if it satisfies a certain inequality regarding the largest prime smaller than n. Next we provide bounds related to the prime power divisors of n and discuss several cases in which n satisfies Condition 1 depending on the largest prime smaller than $n/2$. In Section 6 and Section 7 we use prime gap conjectures in order to settle some cases in which a sufficiently large integer n satisfies Condition 1, and discuss cases in which n satisfies the 3-variation of Condition 1. Finally, in Section 8 we provide upper bounds for a number N so that all integers n satisfy the N-variation of Condition 1, followed by computational results and a generalization of Condition 1 to multinomials.

2 Background

Three theorems about divisibility of binomial coefficients and factorials are relevant for the proofs given in this paper.

Theorem 2.1. (Kummer [8]) *Let k and n be integers with $0 \leq k \leq n$. If α is a positive integer and p a prime, then p^α divides $\binom{n}{k}$ if and only if α carries are needed when adding k and $n-k$ in base p.*

Theorem 2.2. (Lucas [10]) *Let m and n be positive integers, let p be a prime, and let $m = m_k p^k + m_{k-1}p^{k-1} + \cdots + m_1 p + m_0$ and $n = n_k p^k + n_{k-1}p^{k-1} + \cdots + n_1 p + n_0$ be the base p expansions of m and n respectively. Then $\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \pmod{p}$.*

It is important to notice that by convention $\binom{m}{n} = 0$ if $m < n$. Hence, if any of the digits of the base p representation of m is 0 whereas the corresponding digit of the base p representation of k is not 0, then $\binom{m}{k}$ is divisible by p because everything is multiplied by zero and by Lucas' Theorem we have that $\binom{m}{k} \equiv 0 \pmod{p}$.

Theorem 2.3. (Legendre [9]) *If $v_p(n)$ denotes the maximum power α of p such that p^α divides n, then $v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$.*

Here $\lfloor x \rfloor$ denotes the integer part of x. Moreover, Legendre also showed that

$$v_p(n!) = \frac{n - S_p(n)}{p-1},$$

where $S_p(n)$ denotes the sum of all the digits in the base p expansion of n.

3 Some cases of n satisfying Condition 1

3.1 When n is a prime power

Proposition 3.1. *A positive integer n satisfies the 1-variation of Condition 1 with p if and only if $n = p^\alpha$ for some $\alpha > 0$, for $\alpha \in \mathbb{N}$.*

Proof. If $n = p^\alpha$, then the base p representation of n is equal to $1\overbrace{0\ldots0}^{\alpha \text{ zeroes}}$. Any k such that $1 \leq k \leq n-1$ has at most $\alpha - 1$ zeroes in base p. Therefore, at least one of the digits of the base p representation of k is bigger than the corresponding digit of n in base p (at least the leading one). It then follows from Lucas' Theorem that $\binom{n}{k}$ is divisible by p. Otherwise, if n is not a prime power, then the i^{th} digit of n in base p is not 0 for some value of i. Thus, we can find at least one k such that the i^{th} digit of k in base p is larger than 0. Hence, by Lucas' Theorem $\binom{n}{k}$ is not divisible by p. □

Corollary 3.2. *If $n = p^\alpha + 1$, then n satisfies Condition 1 with p and any prime factor of n.*

Proof. The proof relies on the fact that $\binom{m}{k} + \binom{m}{k+1} = \binom{m+1}{k+1}$ for all positive integers m and k. If m is a power of a prime p, then it follows from Proposition 3.1 that $\binom{m}{k}$ and $\binom{m}{k+1}$ are divisible by p if $1 \leq k \leq m-1$. In these cases, because $\binom{m+1}{k+1}$ is the result of the sum of two multiples of p, it also is a multiple of p. When $k = 1$ or $k = m$, we have that $\binom{m+1}{k} = m + 1$, so any prime factor of $m + 1$ divides it. □

Corollary 3.3. *If H is a proper subgroup of the alternating group A_n and n is a power of a prime p then the index $[A_n : H]$ is divisible by p.*

Proof. As observed in [13], it is enough to prove this claim when the subgroup H is maximal, and in this case, the index is either $\binom{n}{k}$ for some k or a multiple of it, as shown in [13]. □

3.2 When n is a product of two prime powers

Proposition 3.4. *If a positive integer n is equal to the product of two prime powers p_1^α and p_2^β, then n satisfies Condition 1 with p_1 and p_2.*

Proof. Observe that $\text{lcm}(p_1^\alpha, p_2^\beta) = n$. The base p_1 representation of n ends in α zeroes and the base p_2 representation of n ends in β zeroes. Because any positive k smaller than n cannot be divisible by both p_1^α and p_2^β, it is not possible that k finishes with α zeroes in base p_1 and β zeroes in base p_2. Thus, we can apply Lucas' Theorem modulo the prime p_1 if $p_1^\alpha \nmid k$ or modulo the prime p_2 if $p_2^\beta \nmid k$. □

Corollary 3.5. *Let $n = p_1^\alpha p_2^\beta$ and H be a proper subgroup of A_n. Then the index $[An : H]$ is divisible by at least one of p_1 or p_2.*

3.3 Considering the closest prime to n

Theorem 3.6. *Let q be the largest prime smaller than n and let $p_i^{a_i}$ be any prime factor divisor of n. If $n - q < p_i^{a_i}$, then n satisfies Condition 1 with p_i and q.*

For the proofs of Theorem 3.4 and Corollary 3.6 we use the Bertrand-Chebyshev Theorem:

Theorem 3.7. (Bertrand-Chebyshev [1]) *For every integer $n > 3$ there exists a prime p such that $n/2 < p < n$.*

Proof of Theorem 3.4. We distinguish between two intervals: the interval $(1, n-q]$ and the interval $(n-q, n]$. Due to the symmetry of binomial coefficients, we only consider $k \leq n/2$. By the Bertrand-Chebyshev Theorem, we know that there is at least one prime between $n/2$ and n, hence $n/2 < q < n$. Then, for all k, $k < n/2 < q$. The base q representation of n is $1 \cdot q + (n-q)$. Therefore, we do not need to consider the interval $(n-q, n)$ because the last digit of the base q representation of any $k > n - q$ is larger than the last digit of the base q representation of n. Thus, by Lucas' Theorem, the binomial coefficient $\binom{n}{k}$ is divisible by q. If there is no multiple of $p_i^{a_i}$ in the interval $(1, n-q)$, then by Lucas' Theorem all the binomial coefficients $\binom{n}{k}$ with $1 \leq k \leq n/2$ are divisible by at least p_i or q. Moreover, equality in Theorem 3.4 cannot hold because $p_i^{a_i}$ divides both $p_i^{a_i}$ and n, and hence q would not be a prime. □

Corollary 3.8. *Let $p_j^{a_j}$ denote the largest prime power divisor of an integer n and q the closest prime to n. If $n - q < p_j^{a_j}$, then n satisfies Condition 1 with p_j and q.*

Note that if n satisfies Condition 1 then at least one of these two primes has to be a prime factor of n, because otherwise $\binom{n}{1} = n$ is not divisible by either one of the two primes.

The only remaining cases are those in which $n - q > p_i^{a_i}$ and n is neither a prime nor a prime power. Let q_2 denote the largest prime smaller than $n/2$. By analyzing the integers that are part of these remaining cases, we notice that n usually satisfies Condition 1 with the pair formed by a prime factor of n and q_2. If we analyze the six numbers smaller than 2,000 such that $n - q > p_i^{a_i}$, we see that the inequality $p_i^{a_i} > n - 2q_2$ holds and q_2 and p_i satisfy Condition 1. Table 1 provides evidence with the only four numbers until 1,000 that do not satisfy Condition 1 with q and p_i. However, the sequence of all such integers is infinite. The On-Line Encyclopedia of Integer Sequences (OEIS) has accepted our submission of this sequence [2] with the reference A290203.

Number	126	210	330	630
Prime factorization	$2 \cdot 3^2 \cdot 7$	$2 \cdot 3 \cdot 5 \cdot 7$	$2 \cdot 3 \cdot 5 \cdot 11$	$2 \cdot 3^2 \cdot 5 \cdot 7$
q	113	199	317	619
q_2	61	103	163	313
$n - q$	13	11	13	11
$n - 2q_2$	4	4	4	4
$(1, n - q]$	2, 3, 4	2, 3, 4	2, 3, 4	2, 3, 4
$(n - q, n]$	62, 63	104, 105	164, 165	314, 315
Pairs that satisfy 1	3-61	5-103	5-163	3-313, 5-313, 7-313

Table 1: Information about the four numbers below 1,000 that do not satisfy Condition 1 with q and p_i.

4 Bounds for $p_i^{a_i}$

Before analyzing q and q_2 further, we establish some bounds for $p_i^{a_i}$ assuming that $n - q > p_i^{a_i}$.

Lemma 4.1. *If n is not a prime and $n - q > p_i^{a_i}$, then $p_i^{a_i} < n/2$.*

Proof. Using the Bertrand-Chebyshev Theorem we see that $n/2 > n - q > 0$. Also, $n - q > p_i^{a_i}$. Therefore, $n/2 > p_i^{a_i}$. □

We can find an even lower bound for $p_i^{a_i}$. In 1952, Nagura [11] showed that if $n \geq 25$ then there is always a prime between n and $(1 + 1/5)n$. Therefore, we find that $5n/6 < q < n$ when $n \geq 30$.

Lemma 4.2. *If $n \geq 30$ is not a prime and $n - q > p_i^{a_i}$, then $p_i^{a_i} < n/6$.*

The proof is the same as the one for Lemma 4.1. In 1976 Schoenfeld [14] showed that for $n \geq$ 2,010,760 there is always a prime between n and $(1 + 1/16{,}597)n$. Therefore, we know that if $n >$ 2,010,882 then

$$\frac{16{,}597n}{16{,}598} < q_2 < n.$$

Shareshian and Woodroofe [13] checked computationally that all integers smaller than 10 million satisfy Condition 1, which means that we can apply Schoenfeld's bound.

Lemma 4.3. *If n is not a prime, $n >$ 2,010,882 and $n - q > p_i^{a_i}$, then $p_i^{a_i} < n/16{,}598$.*

The proof follows the same steps as the previous two lemmas.

Proposition 4.4. *Let $n = p_i^{a_i} m$. If $n \geq$ 2,010,882 and $m <$ 16,598, then n satisfies Condition 1 with p_i and q.*

Proof. By Schoenfeld's bound we know that $n - q < n/16{,}598$. If $m < 16{,}598$, it means that $p_i^{a_i} > n/16{,}598$. Thus, $p_i^{a_i} > n - q$ and, by Theorem 3.4, q and p_i satisfy Condition 1. □

5 When $n - q > p_i^{a_i} > n - 2q_2$

In this section we analyze the integers n that satisfy the inequalities

$$n - q > p_i^{a_i} > n - 2q_2,$$

and we prove some cases in which n satisfies Condition 1 with p_i and q_2. The fact that we are considering $n - 2q_2$ comes from the base q_2 representation of n. We distinguish between two cases: when $k < q_2$ and when $k > q_2$. The base q_2 representation of n is $2 \cdot q_2 + (n - 2q_2)$. The base q_2 representation of k is $0 \cdot q_2 + k$ if $k < q_2$ and $1 \cdot q_2 + (k - q_2)$ if $k > q_2$. Hence, there is no need to analyze the interval $(n - 2q_2, q_2]$ because for all k such that $n - 2q_2 < k \leq q_2$, we can use Lucas' Theorem to see that the binomial coefficient $\binom{n}{k}$ is congruent to 0 modulo q_2. Therefore, we only need to consider the interval $(q_2, n/2]$.

5.1 If n is odd

It is important to remark that if k is not a multiple of $p_i^{a_i}$ then by Lucas' Theorem $\binom{n}{k}$ is divisible by p_i. Therefore, we only have to analyze the integers in $(q_2, n/2]$ that are multiples of $p_i^{a_i}$. We then claim the following:

Theorem 5.1. *If n is odd and $n - q > p_i^{a_i} > n - 2q_2$, then n satisfies Condition 1 with p_i and q_2.*

Proof. Since n is odd, $n/2$ is not an integer. Hence it is enough to prove that there is no multiple of $p_q^{a_q}$ in the interval $(q_r, n/2)$. We will prove this by contradiction. Thus assume that $q_r < \lambda p_q^{a_q} < n/2$ for some integer λ. Then $\lambda \geq (m-1)/2$ if $n = m p_q^{a_q}$, since $((m-1)/2)p_q^{a_q}$ is the largest multiple of $p_q^{a_q}$ that is smaller than $n/2$ (note that m is odd because n is odd). Now from the inequality $((m-1)/2)p_q^{a_q} > q_r$ it follows that $n - p_q^{a_q} > 2q_r$ and this contradicts the assumption that $n - 2q_r < p_q^{a_q}$. □

5.2 If n is even and p_i is not 2

Lemma 5.2. *If n is even and $p_q \neq 2$, then the only multiple of $p_q^{a_q}$ in the interval $(q_r, n/2]$ is $n/2$.*

Proof. Since $p_q \neq 2$, the integer $n/2$ is still a multiple of $p_q^{a_q}$. Hence we may write $n/2 = \lambda p_q^{a_q}$ for some integer λ. If there is another multiple of $p_q^{a_q}$ between q_r and $n/2$, then we have $q_r < (\lambda - 1)p_q^{a_q} < n/2$, and this implies that $n/2 - p_q^{a_q} > q_r$. Hence $n - 2q_r > 2p_q^{a_q} > p_q^{a_q}$, which is incompatible with our assumption which states that $n - 2q_r < p_q^{a_q}$. □

Theorem 5.3. *If 2^α is a prime power divisor of n and 2^α satisfies*

$$n - q > 2^\alpha > n - 2q_2,$$

then n satisfies Condition 1 with 2 and q_2.

Proof. The integer n has the factor 2^α in its prime factorization, which means that $n/2$ has the factor $2^{\alpha-1}$. The base 2 representation of n has one more zero than the base 2 representation of $n/2$, which means that by Lucas' Theorem $\binom{n}{n/2}$ is congruent to 0 modulo 2^α. By Lemma 5.2, $n/2$ is the only multiple of 2^α in the interval $(q_2, n/2]$; hence the proof is complete. □

5.3 If n is even and p_i is not 2

By Lemma 5.2 we only need to consider the central binomial coefficient $\binom{n}{n/2}$, because the only multiple of $p_i^{a_i}$ in the interval $(q_2, n/2]$ is $n/2$. We claim the following proposition, using Legendre's Theorem for its proof.

Proposition 5.4. *The prime factor p_i divides $\binom{n}{n/2}$ if and only if at least one of the fractions $\lfloor n/p^\alpha \rfloor$ with $\alpha \geq 1$ is odd.*

Proof. When we compare $v_{p_i}(n!)$ and $v_{p_i}((n/2)!)$ we see that, for each α,

$$\left\lfloor \frac{n}{p^\alpha} \right\rfloor = 2 \left\lfloor \frac{n/2}{p^\alpha} \right\rfloor$$

if $\lfloor n/p^\alpha \rfloor$ is even. If $\lfloor n/p^\alpha \rfloor$ is even for all α, we conclude that $v_{p_i}(n!) = 2v_{p_i}((n/2)!)$, and hence p_i does not divide $\binom{n}{n/2}$. However, if $\lfloor n/p^\alpha \rfloor$ is odd, then

$$\left\lfloor \frac{n}{p^\alpha} \right\rfloor = 2 \left\lfloor \frac{n/2}{p^\alpha} \right\rfloor + 1.$$

Therefore, $v_{p_i}(n!)$ is greater than $2v_{p_i}((n/2)!)$. □

Corollary 5.5. *Let $S_{p_i}(n)$ be the base p_i representation of n. If $\frac{n - S_p(n)}{p-1}$ is odd then p_i divides $\binom{n}{n/2}$.*

Corollary 5.5 is shown using Legendre's formula.

Corollary 5.6. *If any of the digits in the base p_i representation of $n/2$ is larger than $\lfloor p_i/2 \rfloor$, then the binomial coefficient $\binom{n}{n/2}$ is divisible by p_i.*

Corollary 5.7. *If one of the digits in the base p_i representation of n is odd, then the prime p_i divides $\binom{n}{n/2}$.*

Proof. The proofs of Corollaries 5.6 and 5.7 are similar. If a digit of $n/2$ is larger than $\lfloor p_i/2 \rfloor$, when we add $n/2$ to itself in base p_i to obtain n there at least one carry. Similarly, if n has an odd digit in base p_i, it means that there has been a carry when adding $n/2$ and $n/2$ in base p_i. By Kummer's Theorem with $k = n/2$, if there is at least one carry when adding $n/2$ to itself in base p_i, then p_i divides the binomial coefficient $\binom{n}{n/2}$. □

Corollary 5.8. *If $p_i^{\left\lfloor \frac{\log(n)}{\log(p_i)} \right\rfloor} > n/2$ and $n - q > p_i^{a_i} > n - 2q_2$, then p_i divides $\binom{n}{n/2}$ and therefore n satisfies Condition 1 with p_i and q_2.*

Proof. The largest α such that $p_i^\alpha < n < p_i^{\alpha+1}$ is $\left\lfloor \frac{\log(n)}{\log(p_i)} \right\rfloor$. Therefore, in Proposition 5.4, α is bounded by $1 \leq \alpha \leq \left\lfloor \frac{\log(n)}{\log(p_i)} \right\rfloor$. Also note that $\alpha \geq a_i$, where a_i is the exponent of p_i. If $p_i^{\left\lfloor \frac{\log(n)}{\log(p_i)} \right\rfloor} > n/2$ then $\lfloor n/p_i^\alpha \rfloor = 1$. Because this is odd, p_i divides $\binom{n}{n/2}$ by Proposition 5.4. □

5.4 Some cases in which $2n$ implies n

In this section we denote by $p_{i_k}^{a_i}$ and q_k any prime power factor of k and the largest prime smaller than k respectively. For integers that satisfy the inequality $n - q > p_i^{a_i} > n - 2q_2$, we observe three cases in which if $2n$ satisfies Condition 1 and $p_{i_{2n}} \neq 2$, then n also satisfies Condition 1. Note that since p_i is not 2, then $p_{i_{2n}} = p_{i_n}$. Also, $q_{2_{2n}} = q_n$. Therefore we claim:

Claim 5.9. *If $2n$ satisfies the inequality $2n - 2q_{2_{2n}} < 2n - q_{2n} < p_{i_{2n}}^{a_{i_{2n}}}$, then n satisfies Condition 1 with p_i and q.*

Proof. We rewrite the inequality above as $n - q_n < 2(n - q_n) < 2n - q_{2n} < p_{i_n}^{a_{i_n}}$. Therefore, $n - q_n < p_{i_n}^{a_{i_n}}$, and, by Theorem 4.2, n satisfies Condition 1 with the primes p_i and q. □

Claim 5.10. *If $2n$ satisfies the inequality $2n - q_{2n} < 2n - q_{2_{2n}} < p_{i_{2n}}^{a_{i_{2n}}}$, then n satisfies Condition 1 with p_i and q.*

Claim 5.11. *If $2n$ satisfies the inequality $2n - 2q_{2_{2n}} < p_{i_{2n}}^{a_{i_{2n}}} < 2n - q_{2n}$, then n satisfies Condition 1 with p_i and q.*

The proofs of Claims 5.10 and 5.11 follow the same steps as the one of Claim 5.9.

6 Large multiples of n satisfying Condition 1 with prime gap conjectures

In this section we always denote the t^{th} prime as $\hat{p}_t$.

6.1 Cramér's Conjecture

Conjecture 6.1. (Cramér [5]) *There exist constants M and N such that if $\hat{p}_t \geq N$ then $\hat{p}_{t+1} - \hat{p}_t \leq M(\log \hat{p}_t)^2$.*

We claim the following:

Proposition 6.2. *If Cramér's conjecture is true, then for every positive integer n and every prime p dividing n, the number np^k satisfies Condition 1 for all sufficiently large values of k.*

Proof. Let M and N be the constants given by Cramér's conjecture. Given a positive integer n which is not a prime power and a prime divisor p of n, we write $n = mp^a$ where p does not divide m, and compare $M(\log nx)^2$ with $p^a x$ as x goes to infinity. Using L'Hôpital's rule, we find that

$$\lim_{x\to\infty} \frac{p^a x}{M(\log nx)^2} = \lim_{x\to\infty} \frac{p^a nx}{2Mn \log nx} = \lim_{x\to\infty} \frac{p^a x}{2M \log nx}$$

$$= \lim_{x\to\infty} \frac{p^a nx}{2Mn} = \lim_{x\to\infty} \frac{p^a x}{2M} = \infty.$$

Therefore, $p^a x$ is bigger than $M(\log nx)^2$ when x is sufficiently large. Hence we can choose any k large enough so that $p^{a+k} > M(\log np^k)^2$ and furthermore, if q denotes the largest prime smaller than np^k, then $q \geq N$. Now, if r denotes the smallest prime larger than np^k, we infer that, if Cramér's conjecture holds, then, since $q \geq N$,

$$np^k - q \leq r - q \leq M(\log q)^2.$$

Moreover

$$M(\log q)^2 < M(\log np^k)^2 < p^{a+k}.$$

Hence $np^k - q < p^{a+k}$ and, since p^{a+k} is the highest power of p dividing np^k, Theorem 3.4 implies that np^k satisfies Condition 1. □

Cramér's conjecture also proves the following proposition:

Proposition 6.3. *Let m denote the number of distinct prime factors of n. If Cramér's conjecture is true and n grows sufficiently large keeping m fixed, then n satisfies Condition* 1*.*

Proof. If n has m distinct prime factors, we define the *average prime factor* of n as $\sqrt[m]{n}$ because if n were formed by m equal prime factors each one would equal $\sqrt[m]{n}$. It is true that $\sqrt[m]{n} \leq p_j^{a_j}$, where $p_j^{a_j}$ denotes the largest prime power divisor of n. Hence we must see if $M(\log n)^2 < \sqrt[m]{n}$ for large values of n. We apply again L'Hôpital's rule to compute the limit

$$\lim_{x\to\infty} \frac{\sqrt[m]{nx}}{M(\log nx)^2}$$

and we obtain that $M(\log n)^2 < \sqrt[m]{n}$ holds when n is sufficiently large. □

6.2 Oppermann's Conjecture

A weaker conjecture on prime gaps by Oppermann states the following:

Conjecture 6.4. (Oppermann [12]) For some constant M, $\hat{p}_{t+1} - \hat{p}_t \leq M\sqrt{\hat{p}_t}$.

Proposition 6.5. *If Oppermann's conjecture is true, then for every positive integer n and every prime p dividing n, the number np^k satisfies Condition* 1 *for all sufficiently large values of k.*

Proof. The proof is similar to the proof of Proposition 6.2. We apply L'Hôpital's rule once to solve the indetermination in

$$\lim_{x\to\infty} \frac{p^a x}{M\sqrt{nx}},$$

where p^a is the highest power of p dividing n. Since the ratio goes to infinity our inequality is satisfied, and by choosing $x = p^k$ with k large enough the proof is complete. □

6.3 Riemann's Hypothesis

The following conjecture is a consequence of Riemann's Hypothesis.

Conjecture 6.6. (Riemann [6]) *For some constant M, $\hat{p}_{t+1} - \hat{p}_t \leq M(\log \hat{p}_t)\sqrt{\hat{p}_t}$.*

This bound can be used to prove the following:

Proposition 6.7. *If Riemann's conjecture is true, then for every positive integer n and every prime p dividing n, the number np^k satisfies Condition 1 for all sufficiently large values of k.*

Proof. We apply again L'Hôpital's rule to solve the indetermination in

$$\lim_{x\to\infty} \frac{p^a x}{M(\log nx)\sqrt{nx}}$$

The limit goes to infinity and hence, by choosing $x = p^k$ with k large enough, the proof is complete. □

Due to the similarities of the inequalities, we skip the calculations of Propositions 6.5 and 6.7.

7 Using other primes to satisfy Condition 1

In Sections 3 and 5 we analyzed inequalities involving $n-q$ and $n-2q_2$. In general, for any positive integer d, we can study the function $n - dq_d$, where q_d refers to the largest prime smaller than n/d (when writing q_1 we omitted the subindex 1).

We consider the integers n that do not satisfy the inequality $p_i^{a_i} > n - 2q_2$. Up to 1,000,000 there are only 88 integers that do not satisfy $p_i^{a_i} > n - 2q_2$. The On-Line Encyclopedia of Integer Sequences (OEIS) has accepted our submission of these numbers [3] with the reference A290290. Up to 1,000,000, there are 25 integers that do not satisfy the inequality $p_i^{a_i} > n - 3q_3$; 7 integers that do not satisfy the inequality $p_i^{a_i} > n - 4q_4$; 5 integers that do not satisfy the inequality $p_i^{a_i} > n - 5q_5$, and only 1 integer that does not satisfy the inequality $p_i^{a_i} > n - 6q_6$. Figure 1 shows the number of integers up to 1,000,000 that do not satisfy the inequality $p_i^{a_i} > n - dq_d$ depending on d.

We also observe that the function $n - dq_d$ tends to 0 as d increases, which means that it is likely that at some point the inequality is achieved. This is explained with the properties of the function n/d, which behaves in the same way as the function $1/x$ except for the constant n. As d grows large, the difference between n/d and $n/(d+1)$ grows smaller. Hence, the closest prime to n/d is the same one for all the n/d that are close. Then, when d increases, p_d decreases much more slowly, and because it is multiplied by d, which grows linearly, dp_d tends to n. Figure 2 shows how $n - dp_d$ tends to 0 as d increases taking 330 as an example. All the points correspond to values of d such that p_d satisfies Condition 1 with another prime. Note that if $n - dp_d$ is exactly zero then d is a divisor of n such that n/d is a prime.

Then there are two conditions that we use for p_i and q_d to satisfy Condition 1.

Condition 2. *For any integer n to satisfy Condition 1 with p_i and q_d we require that $p_i^{a_i} > n - dq_d$ and $n - dq_d < q_d$.*

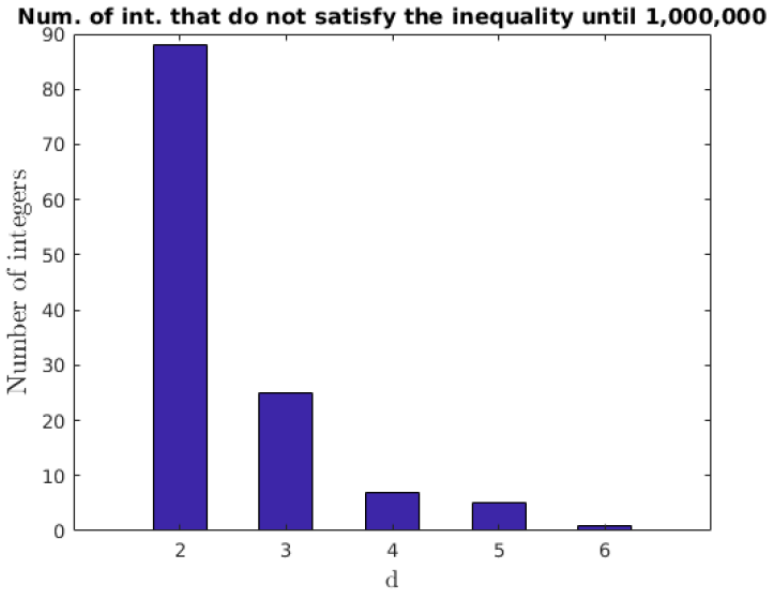

Figure 1: Number of integers up to 1,000,000 that do not satisfy the inequality $p_i^{a_i} > n - dq_d$ as a function of d.

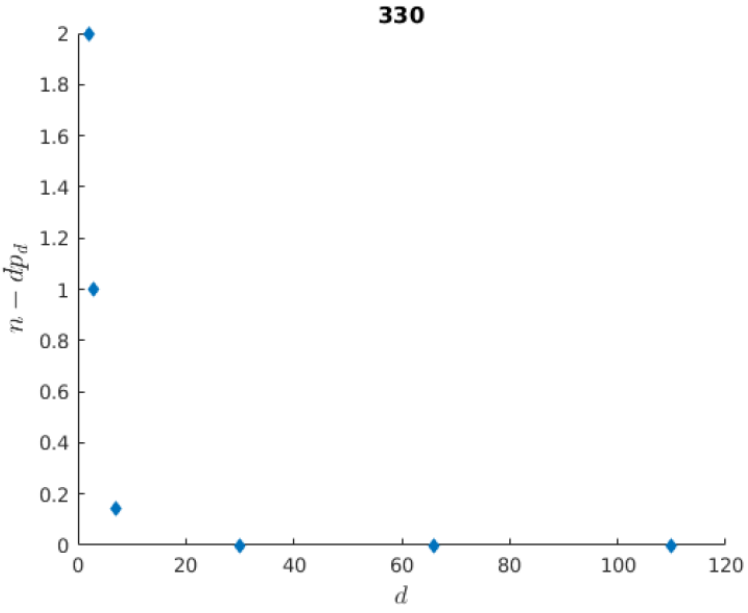

Figure 2: Decrease of $n - dp_d$ for $n = 330$.

When k is larger than $p_i^{a_i}$, we rely on the fact that k is larger than $n - dq_d$ to justify that the binomial coefficient $\binom{n}{k}$ is divisible by q_d using Lucas' Theorem unless if k is a multiple of q_d. However, if $n - dq_d$ were larger than q_d, when writing n in base q_d the inequality $p_i^{a_i} > n - dq_d$ would not hold.

Lemma 7.1. *If $n \geq 30$ and $d < 5$, then $n - dq_d < q_d$.*

Proof. By Lemma 4.2, if $n \geq 25$, $5n/6d < q_d < n/d$. Therefore, $n/6 > n - dq_d$.

Now we need to show that $q_d > n - dq_d$. It follows that $n < q_d + dq_d$ and thus $n < q_d(1+d)$. Using Lemma 4.2,

$$n < \frac{5n(d+1)}{6d} < q_d(1+d).$$

Therefore, $6d < 5d + 5$ and we get that $d < 5$. □

Lemma 7.2. *If $n \geq$ 2,010,882 and $d <$ 16,597, then $n - dq_d < q_d$.*

The proof is the same one as the one for Lemma 7.1, except that by Lemma 4.3, the initial inequality is $16{,}597n/16{,}598d < q_d < n/d$.

Corollary 7.3. *The integer $\lfloor d/2 \rfloor q_d$ is the largest multiple of q_d smaller than or equal to $n/2$.*

Proof. We apply the definition of q_d to obtain that $n \geq dq_d$. Assume, towards a contradiction, that $n > q_d(d+1)$. By Lemmas 7.1 and 7.2, $n - dq_d < q_d$ and therefore $n < q_d(d+1)$. This contradicts the inequality $n > q_d(d+1)$. □

7.1 The 3-variation of Condition 1

In Section 5 we proved that many integers that satisfy the inequalities

$$n - q > p_i^{a_i} > n - 2q_2$$

also satisfy Condition 1 with p_i and q_2. In this section we prove some cases in which an integer n satisfies the 3-variation of Condition 1 (as stated in Definition 1.2 in the Introduction).

Theorem 7.4. *If an even integer n satisfies the inequality $n - q > p_i^{a_i} > n - 2q_2$ and $p_i \neq 2$, then n satisfies the 3-variation of Condition 1 with p_i, q_2 and any prime that divides $\binom{n}{n/2}$.*

Proof. In Section 5.2 we show that if n satisfies the inequality $n - q > p_i^{a_i} > n - 2q_2$ and p_i is not 2, the only binomial coefficient we could not prove that was divisible by either p_i or q_2 is the central binomial coefficient. Thus, for such n to satisfy the 3-variation of Condition 1 it suffices to add an extra prime that divides the central binomial coefficient. □

7.1.1 Regarding the two highest prime powers of n

For any n, let q be the largest prime smaller than n, let p_j be the prime factor of n such that $p_j^{a_j}$ is the largest prime power of n, and let p_r be the prime factor of n such that $p_r^{a_r}$ is the second largest prime power divisor of n. We then claim the following:

Proposition 7.5. *If $p_j^{a_j} p_r^{a_r} > n/6$, then n satisfies the 3-variation of Condition 1 with p_j, p_r and q.*

Proof. By Lucas' Theorem, for any k such that $1 \leq k \leq p_j^{a_j}$, the binomial coefficient $\binom{n}{k}$ is divisible by p_j. For the same reason, by Lucas' Theorem, for any k such that $n-q < k \leq n/2$ the binomial coefficient $\binom{n}{k}$ is divisible by p_j. Then we need a prime that divides at least the binomial coefficients $\binom{n}{k}$ with $p_j^{a_j} \leq k \leq n-q$ such that k is a multiple of $p_j^{a_j}$. Now take p_r as the third prime such that n might satisfy the 3-variation of Condition 1 with p_j, q and p_r. For the same reasoning, in this interval we only consider the k that are multiples of $p_r^{a_r}$. The only k such that the binomial coefficient $\binom{n}{k}$ is not divisible by either p_j of p_r are those k that are multiples of both $p_j^{a_j}$ and $p_r^{a_r}$. The least k that is multiple of both prime powers is $p_j^{a_j} p_r^{a_r}$. By Lemma 4.2 we know that $n-q < n/6$. Therefore, if $p_j^{a_j} p_r^{a_r} > n/6$, this integer is larger than $n-q$ and hence it is not part of the interval that we are considering. Thus, all the k lying in the interval $p_j^{a_j} \leq k \leq n-q$ are such that the binomial coefficient $\binom{n}{k}$ is divisible by either p_j or p_r. □

Moreover, using the bounds described in Lemma 4.2, we use the primes p_j, q and q_d for n to satisfy the 3-variation of Condition 1.

Proposition 7.6. *Let q_d be the largest prime smaller than n/d. If $q_d > n/6$, then n satisfies the 3-variation of Condition 1 with p_j, q and q_d.*

Proof. The prime q fails to divide $\binom{n}{k}$ only if $1 \leq k \leq n-q$. Similarly, by Lucas' Theorem, the prime q_d fails to divide $\binom{n}{k}$ only if $cq_d \leq k \leq cq_d + (n - dq_d)$, where cq_d refers to any positive multiple of q_d. This is because $n - dq_d$ is the last digit of the base q_d representation of n. But because by assumption $q_d > n - p_j$, the intervals $[1, n-q]$ and $[cq_d, cq_d + (n - dq_d)]$ are disjoint. □

8 Bounds on the number of primes needed to satisfy the N-variation of Condition 1

For each positive integer n, we are interested in the minimum number N of primes such that n satisfies the N-variation of Condition 1. In this section we provide four upper bounds for N. Because in all four bounds N is a function of n, the suitability of each bound depends on n; some bounds may be better for certain values of n.

8.1 First upper bound with prime factors of n

Claim 8.1. *If n has m different prime factors, then these prime factors satisfy the m-variation of Condition 1.*

Proof. The proof is similar to the one described when n is a product of two prime powers. The smallest integer divisible by all the m prime powers of n is n. The base p representation of all $k < n$ has less zeroes than the base p representation of n for at least one prime factor p of n. Using Lucas' Theorem, Claim 8.1 is proven. □

8.2 Second upper bound with d

Proposition 8.2. *Let q_d be the largest prime smaller than n/d and let $p_i^{a_i}$ be any prime power divisor of n such that $p_i^{a_i} > n - dq_d$. If $p_i^{a_i} > q_d + n - dq_d$, then n satisfies the N-variation of Condition 1 with $N = 2 + \lfloor d/2 \rfloor$.*

For the subsequent proofs we use the following definition:

Definition 8.3. Let cq_d be any multiple of q_d and let β be $n - dq_d$. We call the interval $[cq_d, cq_d + \beta]$ a *dangerous interval*.

Note that for every time that $p_i^{a_i}$ falls into a dangerous interval we need to add an extra prime.

Proof. By Lucas' Theorem all the binomial coefficients $\binom{n}{k}$ are divisible by q_d except if k lies in a dangerous interval. In these dangerous intervals we only consider the integers that are multiples of $p_i^{a_i}$ because if k is not a multiple of $p_i^{a_i}$, then by Lucas' Theorem the binomial coefficient $\binom{n}{k}$ is divisible by p_i. Because $p_i^{a_i} > \beta$ we know that in any dangerous interval there is at most one multiple of $p_i^{a_i}$. This means that the worst case is the one in which there is a multiple of $p_i^{a_i}$ in every dangerous interval until $c \leq \lfloor d/2 \rfloor$. Thus we need at most one extra prime each time that there is a multiple of $p_i^{a_i}$ in a dangerous interval. □

Claim 8.4. *If $d < 5$ and $p_i^{a_i} > q_d + \beta$, then n satisfies Condition 1 with q_d and p_i.*

Proof. If $d < 5$, then $\lfloor d/2 \rfloor$ equals either 1 or 2. If it equals one, then by assumption $p_i^{a_i} > q_d + \beta$, which means that no multiple of $p_i^{a_i}$ falls in any dangerous interval until $n/2$. If d equals 2, then we need to check that $2p_i^{a_i} > 2q_d + \beta$. This means that we want to see that the next multiple of $p_i^{a_i}$ does not fall into the second dangerous interval. The minimum value of $p_i^{a_i}$ such that our assumption $p_i^{a_i} > q_d + \beta$ holds is $q_d + \beta + 1$. The next multiple of $q_d + \beta + 1$ is $2q_d + 2\beta + 2$. This last expression is greater than $2q_d + \beta$, which means that $2p_i^{a_i}$ does not fall into the second dangerous interval. □

8.3 Third upper bound

In this subsection we consider the generalization of the cases that have been discussed so far. Let d be a natural number and let q_d be the largest prime number smaller or equal to n/d. Let β denote $n - dq_d$, let $p_i^{a_i}$ be any prime power divisor of n, and let $\gamma = p_i^{a_i} - cq_d$. In Sections 8.3 and 8.4 we do not consider the cases in which $q_d = p_i$ because the proofs hold by taking any other prime factor of n that is not p_i.

Theorem 8.5. *For all $c \geq 0$, n satisfies the N-variation of Condition 1 with*

$$N = 2 + \left\lfloor \frac{k\gamma q_d - (c-1)}{\gamma q_d} \right\rfloor \beta,$$

where $k = \left\lfloor \dfrac{d}{2q_d\gamma} \right\rfloor$.

Proof. We first consider the case in which $p_i^{a_i} = q_d + \gamma$ and $\gamma \leq \beta$. This means that $p_i^{a_i}$ falls in the first dangerous interval. Any subsequent multiple of $p_i^{a_i}$ is of the form $rp_i^{a_i} = rq_d + r\gamma$. Note that we only need to analyze $r\gamma$ because this is what determines if $p_i^{a_i}$ falls in a dangerous interval.

Lemma 8.6. *The prime power divisor $p_i^{a_i}$ falls into a dangerous interval if and only if $r\gamma \pmod{q_d} \leq \beta$.*

The proof of Lemma 8.6 comes from the definition of a dangerous interval (see Definition 8.3). Now consider all the possible values of $r\gamma$ modulo q_d from γ until γq_d. Note the following:

Remark 8.7. *The numbers γ and q_d are always coprime.*

For the proof of the remark it suffices to see that q_d is a prime number. This means that all the numbers from 1 to $q_d - 1$ appear exactly once in the interval $[\gamma, \gamma q_d)$. Therefore, by Lemma 8.6 the number of integers that fall into a dangerous interval are those such that $r\gamma \pmod{q_d} \leq \beta$. By Remark 8.7 we know there are only β such integers in the interval $[\gamma, \gamma q_d)$. Thus, if $\gamma q_d > d/2$, we only need $2 + \beta$ primes. We add 2 to β because we also need to count q_d and p_i. Note that this is an upper bound and therefore in some cases several of the primes that we use for the dangerous intervals are repeated.

Now we consider the general case in which $p_i^{a_i} = cq_d + \gamma$. We need to count the multiples of γq_d from cq_d until $k\gamma q_d$ (k has the same definition as in Theorem 7.1). This gives us the bound stated in Theorem 8.5. □

Note that, in Theorem 8.5, γ cannot be 0 because otherwise by definition p_i would be equal to q_d. This is a case that we are not considering (see the beginning of Section 8.3).

8.4 Fourth upper bound with Diophantine equations

We consider the Diophantine equation $p_i^{a_i} k_1 - q_d \alpha = \delta$, where $0 \leq \delta \leq \beta$. Let $x = k_1$ and let $y = \alpha$. The general solutions of these Diophantine equation depending on the particular solutions x_1 and y_1 are well-known:

$$x = x_1 - rq_d$$
$$y = y_1 + rp_i^{a_i}$$

Let $\hat{y}(\delta)$ denote the largest $y \leq \lfloor d/2 \rfloor$ depending on δ. Note that for all $y_1(\delta)$ we can add or subtract a certain number of $p_i^{a_i}$ until we reach $\hat{y}(\delta)$.

Theorem 8.8. *All integers n satisfy the N-variation of Condition 1 with*

$$N = 2 + \sum_{\delta=0}^{\beta} \left\lfloor \frac{\hat{y}(\delta)}{p_i^{a_i}} \right\rfloor \leq 2 + (\beta + 1) \left\lfloor \frac{d}{2p_i^{a_i}} \right\rfloor.$$

Proof. Note that the solutions of the Diophantine equation correspond to all the cases in which a multiple of $p_i^{a_i}$ falls in some dangerous interval. It is known that a Diophantine equation $ax + by = c$ has infinitely many solutions if $\gcd(a, b)$ divides c.

Therefore, for all δ such that $0 \leq \delta \leq \beta$ there exists a particular solution $y_1(\delta)$ for y in Equation 6 because $\gcd(p_i^{a_i}, q_d) = 1$ (recall that we do not consider the case in which $p_i = q_d$). Thus, for each $\hat{y}(\delta)$ we count the number of multiples of $p_i^{a_i}$ in the interval $[1, \hat{y}(\delta)]$. This is the number of times that $p_i^{a_i}$ falls into a dangerous interval and hence we need to add an extra prime. We also add 2 to count p_d and p_i. Moreover, note that by definition $\hat{y}(\delta) \leq \lfloor d/2 \rfloor$. This gives us the expression stated in Theorem 8.8. □

9 Computational results

In order to obtain more information about which primes make n satisfy Condition 1 we wrote some C++ programs. The results are presented in this section.

9.1 When we fix a prime

In the original article of Shareshian and Woodroofe [13], the authors computed the percentage of integers below 1,000,000 that satisfy Condition 1 if p_1 is fixed to be 2, and they found a percentage of 86.7%. We compute the percentage of integers until 10,000 that satisfy Condition 1 fixing one prime to be not only 2 but also 3, 5, 7 and 11. Table 2 shows the number of integers below 10,000 that do not satisfy Condition 1 fixing one prime to be 2, 3, 5, 7 and 11 respectively. It also shows the percentage of integers satisfying Condition 1 fixing each prime. Figure 3 shows the percentage of integers until 10,000 that satisfy Condition 1 depending on the fixed prime.

Fixed prime	2	3	5	7	11
Number of integers not satisfying 1	1144	1633	2626	3259	4180
Percentage of integers satisfying 1	88.56%	83.67%	73.74%	67.41%	58.20%

Table 2: Number of integers that do not satisfy Condition 1 and percentage of integers that do satisfy Condition 1 fixing one prime until 10,000.

9.2 How many pairs of primes satisfy Condition 1

Given a positive integer n, multiple pairs of primes p_1 and p_2 can satisfy Condition 1. We have found computationally all the possible pairs of primes that satisfy Condition 1 with a given $n \leq 3{,}000$. This findings helped us conjecture and then prove Theorem 3.4. Figure 4 shows the data for n up to 3,000. We note four main tendencies. The one with the greatest slope corresponds to the one formed with prime numbers and prime powers. This is explained by Proposition 3.1. Because only one prime is needed to satisfy the 1-variation of Condition 1 if n is a prime power, the other prime can be any prime smaller than n. Thus, this first tendency follows the function $f(n) = n/\log n$ disregarding the prime powers [7]. The second greatest slope is formed with even numbers that satisfy Condition 1 with one prime being 2. The third one is formed by numbers that satisfy Condition 1 with one

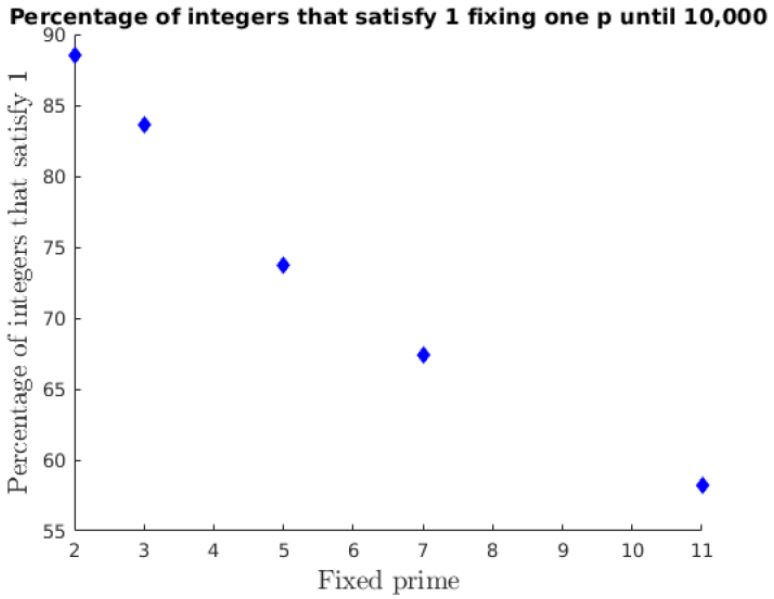

Figure 3: Percentage of integers until 10,000 that satisfy Condition 1 fixing one prime to be 2, 3, 5, 7 and 11 respectively.

prime being 3 and the following one with numbers that satisfy Condition 1 with one prime being 5.

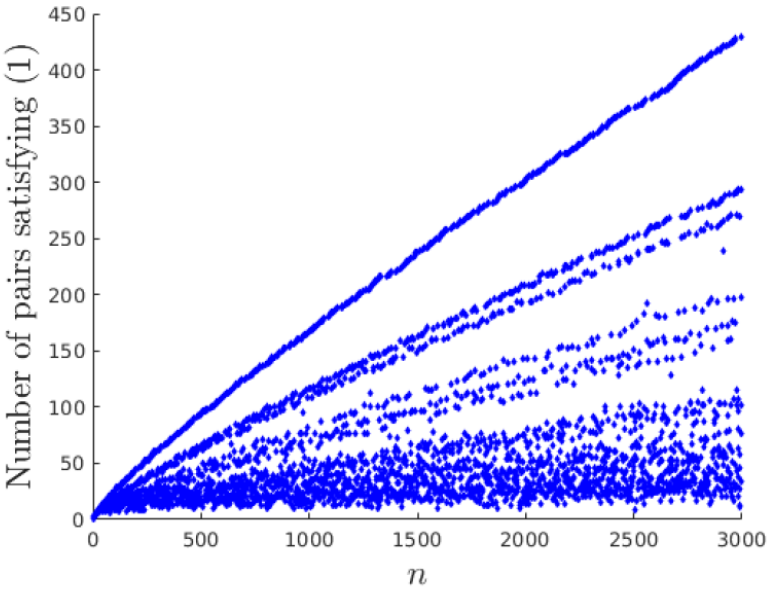

Figure 4: Number of pairs of primes that satisfy Condition 1 depending on the integer n until 3,000.

In order to fit a function for each curve, we approximated the function $n/\log n$ for each branch using Matlab, and we obtained the following functions:

First branch: $\dfrac{0.97n^{0.96}}{(\log n)^{0.75}}$ Second branch: $\dfrac{0.80n^{0.96}}{(\log n)^{0.84}}$

Third branch: $\dfrac{3.30n^{1.14}}{(\log n)^{2.27}}$ Fourth branch: $\dfrac{35.48n^{1.47}}{(\log n)^{4.81}}$

Figure 5 shows a plot of each separate branch with its corresponding curve.

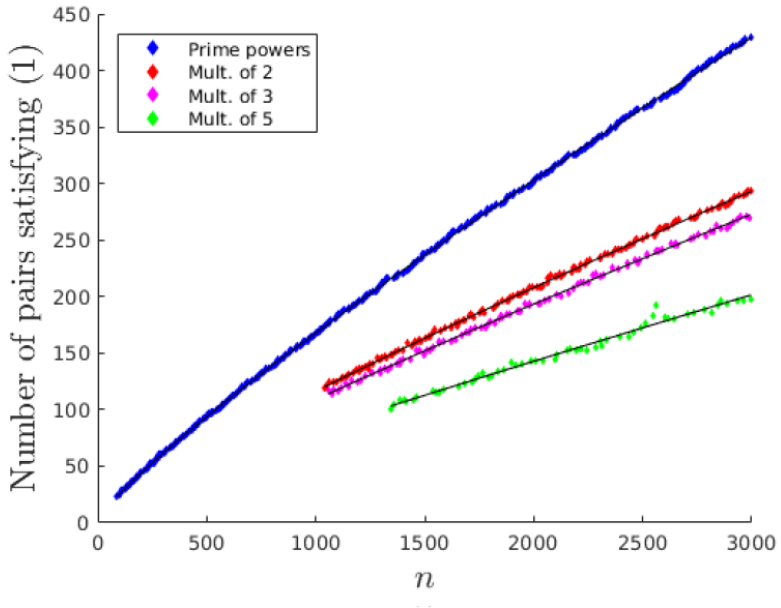

Figure 5: The four branches of Figure 4 separated and fitted with a curve.

10 Multinomials

We also consider a generalization of Condition 1 to multinomials. We investigate the following condition that some integer n might satisfy:

Condition 3. *For a given fixed integer m there exist primes p_1 and p_2 such that whenever $k_1 + \cdots + k_m = n$ for $1 \leq k_i \leq n-1$, $\binom{n}{k_1,k_2,\ldots,k_m}$ is divisible by either p_1 or p_2.*

A very natural question follows:

Question 10.1. *Does Condition 3 hold for all positive integers n?*

Here we show that Condition 1 implies Condition 3. We claim the following:

Proposition 10.2. *If n satisfies Condition 1 with p_1 and p_2, then n also satisfies Condition 3 with these two primes and any $m \leq n$.*

Proof. We assume that p_1 and p_2 satisfy Condition 1 for a given n. We then take the multinomial

$$\binom{n}{k_1, k_2, \ldots, k_m} = \frac{n!}{k_1!k_2!\cdots k_m!}$$

with the same n and any $m \leq n$. We see that we can decompose the multinomial into a product of m binomials:

$$\frac{n!}{k_1!k_2!\cdots k_m!} = \frac{n(n-1)\cdots(n-k_1+1)}{k_1!}\cdot$$

$$\frac{(n-k_1)(n-k_1-1)\cdots(n-k_1-k_2+1)}{k_2!}\cdots\frac{(k_{m-1}+k_m)(k_{m-1}+k_m-1)\cdots 1}{(k_{m-1}!k_m!}$$

$$= \binom{n}{k_1}\binom{n-k_1-1}{k_2}\cdots\binom{k_{m-1}+k_m}{k_m}.$$

Because by assumption $\binom{m}{k_1}$ is divisible by either p_1 or p_2, the previous multinomial coefficient is also divisible by at least one of them. This decomposition can be used for any m and the first binomial coefficient can be $\binom{n}{k_i}$, k_i being any of the k in the denominator. □

Therefore, if Condition 1 is proven for binomial coefficients, then it automatically holds for multinomial coefficients.

11 Conclusions

In this paper we have obtained results that significantly contribute to the unsolved conjecture that motivated our research (see Condition 1 in the Introduction), which was proposed in a recent article by Shareshian and Woodroofe [13]. After having obtained all these research results, we have analyzed how much we have contributed to the open problem addressed in this paper. Up to 1,000,000, there are less than 50 numbers that do not fit into any of the cases that we have solved. We consider this to be a very substantial outcome. Moreover, our proofs concerning prime gap conjectures potentially have stronger implications, as we believe that we are very close to proving that all integers larger than a fixed constant satisfy Condition 1.

Acknowledgements

I would like to express my gratitude towards my mentor Oscar Mickelin, whose advice, help, and guidance have been absolutely crucial for his work. I would also like to thank my tutor Dr. John Rickert and Dr. Tanya Khovanova for their valuable and insightful comments on this project. I would like to recognize Professors Dr. David Jerison and Dr. Slava Gerovitch for organizing and coordinating the math mentorships. I would also like to thank Anqi Li, Michelle Shen, Jordan Lee and Óscar Rivero for their remarks. I would like to acknowledge the Center for Excellence in Education, the Research Science Program, and the Massachusetts Institute of Technology for giving me the once in a lifetime opportunity to conduct research during the summer. Finally, I would like to recognize and thank Ms. Perceries, the Director of Youth and Science Programs, and Fundació Catalunya la Pedrera for sponsoring me.

12 Appendix

12.1 Sequences of integers that do not satisfy the inequality for $n - dp_d$

In Section 7 we mentioned that the set of integers that do not satisfy the inequality for $n - dp_d$ becomes smaller when d increases. In this appendix we display the first terms of the sequence of integers that do not satisfy the inequality $n - dp_d < p_i^{a_i}$ when d equals 1, 2, 3, 4 and 5. The On-Line Encyclopedia of Integer Sequences has published our sequence in the cases when d equals 1 (see A290203) and when d equals 2 (see A290290).

When $d = 1$: 126, 210, 330, 630, 1144, 1360, 2520, 2574, 2992, 3432, 3960, 4199, 4620, 5544, 5610, 5775, 5980, 6006, 6930, 7280, 8008, 8415, 9576, 10005, 10032, 12870, 12880, 13090, 14280, 14586, 15708, 15725, 16182, 17290, 18480, 18837, 19635, 19656, 20475, 20592, 22610, 24310, 25296, 25300, 25520, 25840, 27170, 27720, 27846, 28272, 28275, 29716, 30628, 31416, 31450, 31464, 31465, 32292, 34086, 34100, 34580, 35568, 35650, 35670, 35728, 36036, 36432, 37944, 37950.

When $d = 2$: 3432, 5980, 12870, 12880, 13090, 14280, 14586, 20475, 28272, 28275, 31416, 31450, 34580, 35650, 39270, 45045, 45220, 72072, 76076, 96135, 97812, 106080, 106590, 120120, 121992, 125580, 132804, 139230, 173420, 181350, 185640, 191400, 195624, 202275, 203112, 215050, 216315, 222768, 232254, 240240, 266475, 271320, 291720, 293930, 336490, 338086, 350064, 351120, 358150, 371280, 388455, 408595, 421600, 430236, 447051, 447304, 471240, 480624.

When $d = 3$: 3432, 31416, 34580, 35650, 39270, 96135, 121992, 125580, 139230, 215050, 222768, 291720, 358150, 388455, 471240, 513590, 516120, 542640, 569296, 638001, 720720, 813960, 875160, 891480, 969969, 1046175, 1113840, 1153680, 1227600, 1343160, 1448655, 1557192, 1575860, 1745424, 1908816.

12.2 C++ code for finding all the possible pairs

Here we provide the C++ code that we used to find all the possible pairs of primes that satisfy Condition 1 for each integer. This code has been used to plot Figure 4.

The code for the data on how many integers satisfy Condition 1 if we fix one prime is quite similar and is therefore not included.

```cpp
#include<iostream>
#include<vector>
#include<cmath>
#include<set>
#include<string>
#include<sstream>
#include <bits/stdc++.h>
#include "BigIntegerLibrary.hh"

using namespace std;

vector <bool> v;
vector <unsigned long long int> primers;
vector <vector <unsigned long long int> > factors;
vector <vector <unsigned long long int> > factorsrepet;
vector <vector <BigInteger> > bino;

string int2string(int n){
    stringstream s;
    s << n;
    return(s.str());
}

void garbell(){
    v[0]=false;
    v[1]=false;
    factors[0].push_back(0);
    factors[1].push_back(1);
    for(unsigned long long int i=2; i<v.size(); i++){
        if(v[i]){
            primers.push_back(i);
            factors[i].push_back(i);
            for(unsigned long long int h=2; h*i<v.size(); h++){
                v[i*h] = 0;
                factors[i*h].push_back(i);
            }
        }
    }
```

```cpp

int main(){
    ofstream cout("HowManyPrimes.txt");
    int n;
    cin >> n;
    v = vector <bool> (n, true);
    primers = vector <unsigned long long int> ();
    factors = vector <vector <unsigned long long int>> (n);
    factorsrepet = vector <vector <unsigned long long int>> (n);
    garbell();
    bino = vector <vector <BigInteger> > (n);
    bino[0].push_back(1);
    bino[1].push_back(1);
    bino[1].push_back(1);
    for(unsigned long long int i=2; i<n; i++) {
        //cout<<endl<<endl<<i<<" ";
        bino[i].push_back(1);
        for(unsigned long long int j=1; j<i; j++){
            bino[i].push_back(bino[i-1][j-1]+bino[i-1][j]);
            //cout<<bino[i][j]<<" ";
        }
        bino[i].push_back(1);
    }
    for(unsigned long long int i=2; i<n; i++) {
        cout<<"n =      "<<i;
        unsigned long long int aa = 0;
        unsigned long long int bb = 1;
        unsigned long long int p1 = primers[aa];
        unsigned long long int p2 = primers[bb];
        unsigned long long int res = 0;
        int howmany = 0;
        while(res==0){
                string pp1 = int2string(p1);
                BigInteger ppp1 =stringToBigInteger(pp1);
                string pp2= int2string(p2);
                BigInteger ppp2 =stringToBigInteger(pp2);
                for(unsigned long long int q=1; q<=i/2; q++){
```

```cpp
                    if((bino[i][q]%ppp1!=0)and(bino[i][q]%ppp2!=0)){
                        res = 1;
                        break;
                    }
                }
            if(res==0){
                cout<<"PRIMES: "<<pp1<<"       "<<pp2<<endl;
                howmany++;
            }
            if(((bb+1==primers.size())and(aa+1==primers.size()-1))or(primers[aa+1]==i)){
                    res=1;
                }
                else{
                if((bb+1==primers.size())or(primers[bb+1]>i)){
                    aa++;
                    p1 = primers[aa];
                    bb = aa+1;
                    p2 = primers[bb];
                    res = 0;
                }
                else{
                    bb++;
                    p2 = primers[bb];
                    res = 0;
                }
            }
    }
    cout<<"              "<<howmany<<endl;
    }
}
```

References

[1] J. Bertrand. Mémoire sur le nombre de valeurs que peut prendre une fonction quand on y permute les lettres qu'elle renferme. *Journal de l'École Royale Polytechnique*, 30:123–140, 1845.

[2] S. Casacuberta. Sequence A290203 in The On-Line Encyclopedia of Integer Sequences. Published electronically at `http://oeis.org/A290203`.

[3] S. Casacuberta. Sequence A290290 in the On-Line Encyclopedia of Integer Sequences. Published electronically at `http://oeis.org/A290290`.

[4] K. S. Davis and W. A. Webb. Lucas' theorem for prime powers. *European Journal of Combinatorics*, 11:229–233, 1990.

[5] A. Granville. Harald Cramér and the distribution of prime numbers. *Scandinavian Actuarial Journal*, 1995:337–360, 1995.

[6] D. Heath-Brown. Gaps between primes, and the pair correlation of zeros of the zeta-function. *Acta Arithmetica*, 41:85–99, 1982.

[7] A. E. Ingham. *The Distribution of Prime Numbers*. Cambridge University Press, 1932.

[8] E. Kummer. Über die Ergänzungssätze zu den allgemeinen Reziprozitätsgesetzen. *Journal für die reine und angewandte Mathematik*, 44:93–146, 1852.

[9] A. M. Legendre. *Théorie des Nombres*. Paris: Firmin Didot Frères, 1932.

[10] E. Lucas. Théorie des fonctions numériques simplement périodiques. *American Journal of Mathematics*, 44:184–196, 1878.

[11] J. Nagura. On the interval containing at least one prime number, Proceedings of the Japan Academy, 1952.

[12] G. Paz. On Legendre's, Bocard's, Andrica's and Oppermann's Conjectures. arXiv:1310.1323, 2014.

[13] J. Shareshian and R. Woodroofe. Divisibility of binomial coefficients and generation of alternating groups. *Pacific Journal of Mathematics*, 292:223–238, 2018.

[14] L. Shoenfeld. Sharper bounds for Chebyshev functions $\psi(x)$ and $\theta(x)$, ii. Mathematics of Computation, 1976.