ARS MATHEMATICA CONTEMPORANEA

ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 19 (2020) 297–309
https://doi.org/10.26493/1855-3974.2103.e84
(Also available at http://amc-journal.eu)

On the divisibility of binomial coefficients

Sílvia Casacuberta *

Harvard University, 1 Oxford Street, Cambridge, MA, USA

Received 30 August 2019, accepted 16 August 2020, published online 18 November 2020

Abstract

Shareshian and Woodroofe asked if for every positive integer n there exist primes p and q 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 q. We give conditions under which a number n has this property and discuss a variant of this problem involving more than two primes. We prove that every positive integer n has infinitely many multiples with this property.

Keywords: Binomial coefficients, divisibility, primorials.

Math. Subj. Class. (2020): 11B65, 05A10

1 Introduction

Binomial coefficients display interesting divisibility properties. Conditions under which a prime power p^a divides a binomial coefficient $\binom{n}{k}$ are given by Kummer's Theorem [10] and also by a generalized form of Lucas' Theorem [5, 13].

Still, there are problems involving divisibility of binomial coefficients that remain unsolved. In this article we investigate the following question, which was asked by Shareshian and Woodroofe in [16].

Question 1.1. Is it true that for every positive integer n there exist primes p and q such that, for all integers k with $1 \leq k \leq n-1$, the binomial coefficient $\binom{n}{k}$ is divisible by p or q?

As in [16], we say that n *satisfies Condition* 1 if such primes p and q exist for n. In this article we discuss sufficient conditions under which an integer n satisfies Condition 1. In Sections 2 and 3 we prove a variation of the Sieve Lemma from [16] and use it to show that

*I am indebted to my mentor Oscar Mickelin for his guidance throughout this research and to Prof. Russ Woodroofe for correspondence and kind suggestions. This work was carried out during the Research Science Program at MIT in the summer of 2017 and was supported by the Center for Excellence in Education, the MIT Mathematics Department, and the Youth and Science Program of Fundació Catalunya La Pedrera (Barcelona).

E-mail address: scasacubertapuig@college.harvard.edu (Sílvia Casacuberta)

n satisfies Condition 1 if certain inequalities hold. In Section 5 we infer that every positive integer has infinitely many multiples for which Condition 1 is satisfied.

The collection of numbers for which Condition 1 is not known to hold has asymptotic density 0 assuming the truth of Cramér's conjecture (as first shown in [16]) and includes most *primorials* $p_1p_2\cdots p_i$, where $p_1,\dots,p_i$ are the first i primes, namely those primorials such that $(p_1p_2\cdots p_i)-1$ is not a prime.

In addition, we introduce the following variant of Condition 1:

Definition 1.2. A positive integer n satisfies the N*-variation* of Condition 1 if there exist N different primes $p_1,\dots,p_N$ such that if $1\le k\le n-1$ then $\binom{n}{k}$ is divisible by at least one of $p_1,\dots,p_N$.

For example, it follows from Kummer's Theorem or from Lucas' Theorem that a positive integer n satisfies the 1-variation of Condition 1 if and only if n is a prime power, and every integer n satisfies the m-variation of Condition 1 if $n = p_1^{a_1}\cdots p_m^{a_m}$ where $p_1,\dots,p_m$ are distinct primes. In Section 4 we discuss upper bounds on N so that a given n satisfies the N-variation of Condition 1.

2 An extended Sieve Lemma

Our results in this section will be based on Lucas' Theorem:

Theorem 2.1 (Lucas [13])**.** *Let p be a prime and let*

$$n = n_rp^r + n_{r-1}p^{r-1} + \cdots + n_1p + n_0$$
$$k = k_rp^r + k_{r-1}p^{r-1} + \cdots + k_1p + k_0$$

be base p expansions of two positive integers, where $0\le n_i<p$ and $0\le k_i<p$ for all i, and $n_r\ne 0$. Then

$$\binom{n}{k}\equiv\prod_{i=0}^{r}\binom{n_i}{k_i}\pmod{p}.$$

By convention, a binomial coefficient $\binom{n_i}{k_i}$ is zero if $n_i<k_i$. Hence, if any of the digits of the base p expansion of n is 0 whereas the corresponding digit in the base p expansion of k is nonzero, then $\binom{n}{k}$ is divisible by p. As a particular case, if a prime power p^a with $a>0$ divides n and does not divide k, then $\binom{n}{k}$ is divisible by p.

Observe that, if n satisfies Condition 1 with two primes p and q, then at least one of these primes has to be a divisor of n, because otherwise $\binom{n}{1}$ would not be divisible by any of them. The next two results are elementary consequences of Lucas' Theorem.

Proposition 2.2. *If $n=p^a+1$ with p a prime and $a>0$, then n satisfies Condition 1 with p and any prime dividing n.*

Proof. If $n-1$ is a prime power then the two summands in the left-hand term of the equality

$$\binom{n-1}{k-1}+\binom{n-1}{k}=\binom{n}{k}$$

are divisible by p by Lucas' Theorem if $2\le k\le n-2$, and hence $\binom{n}{k}$ is also divisible by p. If $k=1$ or $k=n-1$, then $\binom{n}{k}=n$, so any prime factor of n divides $\binom{n}{k}$. □

Proposition 2.3. *If a positive integer n is equal to the product of two prime powers p_1^a and p_2^b with $a > 0$, $b > 0$, and $p_1 \neq p_2$, then n satisfies Condition 1 with p_1 and p_2.*

Proof. The base p_1 expansion of n ends with a zeroes and the base p_2 expansion of n ends with b zeroes. Because a positive integer k smaller than n cannot be divisible by both p_1^a and p_2^b, it is not possible that k ends with a zeroes in base p_1 and b zeroes in base p_2. Consequently, we can apply Lucas' Theorem modulo p_1 if p_1^a does not divide k or modulo p_2 if p_2^b does not divide k. □

Proposition 2.3 generalizes as follows.

Proposition 2.4. *If $p_1, \ldots, p_m$ are distinct primes and $n = p_1^{a_1} \cdots p_m^{a_m}$ with $a_i > 0$ for all i, then n satisfies the m-variation of Condition 1 with $p_1 \ldots, p_m$.*

Proof. If $1 \leq k \leq n-1$, then the base p_i expansion of k ends with less zeroes than the base p_i expansion of n for at least one prime factor p_i of n. □

The following result extends [16, Lemma 4.3]. It is the starting point of our discussion of Question 1.1 in the next sections. By symmetry, we only need to consider those values of k with $k \leq n/2$. Moreover, we may restrict our study further to those values of k that are multiples of p^a, since otherwise $\binom{n}{k}$ is divisible by p.

Theorem 2.5. *Let n be a positive integer and suppose that p^a divides n where p is a prime and $a > 0$. Suppose that there is a prime q with $n/(d+1) < q < n/d$, where $d \geq 1$, and let $k \leq n/2$. Then $\binom{n}{k}$ is divisible by p or q except possibly when k is a multiple of p^a belonging to one of the intervals $[cq, cq+\beta]$ with $\beta = n - dq$ and $0 \leq c < (d+1)/2$.*

Proof. Since $q < n/d$, the number $\beta = n - dq$ is positive. If $k \leq \beta$ then k is in the interval $[0, \beta]$, which is the case $c = 0$ in the statement of the theorem.

The assumption that $n/(d+1) < q$ is equivalent to assuming the inequality $n - dq < q$, which implies that the last digit in the base q expansion of n is equal to β. Hence, if $\beta < k < q$ then we may infer from Lucas' Theorem that $\binom{n}{k}$ is divisible by q.

The remaining range of values of k to be considered is $q \leq k \leq n/2$. In this case we look at the last digit of the base q expansion of k. If this last digit is bigger than β, then $\binom{n}{k}$ is again divisible by q. Thus the undecided cases are those in which the residue of k modulo q is smaller than or equal to β. This happens when $cq \leq k \leq cq + \beta$ for some positive integer c, and if $cq \leq k \leq n/2$ then $c \leq n/(2q) < (d+1)/2$. □

By the Bertrand-Chebyshev Theorem [2], for every integer $n > 2$ there exists a prime q such that $n/2 < q < n$. This yields the following particular instance of Theorem 2.5, which is also a special case of [16, Lemma 4.3].

Corollary 2.6. *For a positive integer n, suppose that p^a divides n where p is a prime and $a > 0$. If q is a prime such that $n/2 < q < n$ and $n - q < p^a$, then n satisfies Condition 1 with p and q.*

Proof. Pick $d = 1$ in Theorem 2.5. □

Note that, under the assumptions of Corollary 2.6, the equality $n - q = p^a$ cannot hold, since p divides n and $p \neq q$ because q does not divide n. Hence there remains to study the case when $n - q > p^a$ and q is the largest prime smaller than n while p^a is the largest prime power dividing n. In other words, Condition 1 holds for n whenever there is a prime between $n - p^a$ and n.

The sequence of integers n for which there is no prime between $n - p^a$ and n can be found in the On-Line Encyclopedia of Integer Sequences (OEIS) [17] with the reference A290203 [3]. Its first terms are the following:

$$126, 210, 330, 630, 1144, 1360, 2520, 2574, 2992, 3432, 3960, 4199, \dots \tag{2.1}$$

Banderier's conjecture [1] claims that if $p_n\#$ denotes the n-th *primorial*, that is,

$$p_n\# = p_1 p_2 \cdots p_n$$

where $p_1, \dots, p_n$ are the first n primes, and q is the largest prime below $p_n\#$, then either $p_n\# - q = 1$ or $p_n\# - q$ is a prime.

Proposition 2.7. *If Banderier's conjecture is true, then the sequence* (2.1) *contains all primorials $p_n\#$ such that $p_n\# - 1$ is not a prime.*

Proof. If $p_n\# - 1$ is not a prime, then $p_n\# - q$ is a prime according to Banderier's conjecture. Since $p_n\# - q$ does not divide $p_n\#$, we infer that $p_n\# - q$ is bigger than p_n, which is the largest prime power dividing $p_n\#$. □

The first primorials $p_n\#$ such that $p_n\# - 1$ is not a prime are

$$p_4\# = 210, \quad p_7\# = 510510, \quad p_8\# = 9699690, \quad p_9\# = 223092870.$$

Inspecting this list could be a strategy to seek for a counterexample for Question 1.1. The complementary list of primorials can be found in OEIS with reference A057704 [11].

For any fixed value of d, the number β in Theorem 2.5 is smallest when q is as close as possible to n/d. For this reason, we focus our attention on the largest prime q_d below n/d for various values of d. This motivates the next definition.

Definition 2.8. For positive integers n and $1 \le d < n/2$, let q_d be the largest prime smaller than n/d and let $\beta_d = n - dq_d$. For each integer c with $0 \le c < (d+1)/2$, we call $[cq_d,\ cq_d + \beta_d]$ a *dangerous interval*.

By Theorem 2.5, if we attempt to prove that Condition 1 holds with p and q_d assuming that $q_d > n/(d+1)$ —that is, assuming that the dangerous intervals are disjoint— we only need to care about values of k that lie in a dangerous interval and are multiples of the largest power of p dividing n.

In the case $d = 1$, the only dangerous interval below $n/2$ is $[0, n - q_1]$. When $d = 2$, we have that $[0, n - 2q_2]$ and $[q_2, n - q_2]$ are dangerous intervals. Since $n - q_2 > n/2$, the second interval may be replaced by $[q_2, n/2]$ to carry our study further, as we do in the next section.

Example 2.9. The largest prime below $n = p_7\# = 510510$ is $q_1 = 510481$ and the largest prime dividing n is $p = 17$. Here $n - q_1 = 29$ and therefore $\binom{n}{k}$ is divisible by 17 or 510481 for all k except for $k = 17$.

On the other hand, the largest prime below $n/2 = 255255$ is $q_2 = 255253$. Thus $\beta_2 = n - 2q_2 = 4$ and therefore $[0, 4]$ and $[255253,\ 255257]$ are dangerous intervals. The second interval contains a multiple of 17, namely $n/2$. However, since

$$510510 = 6 \cdot 17^4 + 1 \cdot 17^3 + 15 \cdot 17^2 + 8 \cdot 17,$$
$$255255 = 3 \cdot 17^4 + 0 \cdot 17^3 + 16 \cdot 17^2 + 4 \cdot 17,$$

we infer from Lucas' Theorem that $\binom{510510}{255255}$ is divisible by 17. Consequently, $\binom{n}{k}$ is divisible by 17 or 255253 for all k.

3 Using the nearest prime below $n/2$

Nagura showed in [14] that, if $m \geq 25$, then there is a prime between m and $(1 + 1/5)m$. Therefore, there is a prime q such that $5n/6 < q < n$ when $n \geq 30$. This implies that, if $n \geq 30$ and the largest prime-power divisor p^a of n satisfies $p^a \geq n/6$, then there is a prime q between $n - p^a$ and n and hence Condition 1 holds for n with p and q.

The following result is sharper.

Proposition 3.1. *If $n \geq 2010882$ and the largest prime-power divisor p^a of n satisfies $p^a \geq n/16598$, then n satisfies Condition 1 with p and the nearest prime q below n.*

Proof. Schoenfeld proved in [15] that for $m \geq 2010760$ there is a prime between m and $(1 + 1/16597)m$. Hence, if $n \geq 2010882$ and the largest prime-power divisor p^a of n satisfies $p^a \geq n/16598$ then there is a prime between $n - p^a$ and n, and therefore Condition 1 holds for n by Corollary 2.6. □

The following are consequences of Nagura's and Schoenfeld's bounds.

Lemma 3.2. *Let q_d be the largest prime below n/d for positive integers n and d.*

(a) If $n \geq 120$ and $d < 5$, then $n/(d+1) < q_d$.
(b) If $n \geq 3.34 \cdot 10^{10}$ and $d < 16597$, then $n/(d+1) < q_d$.

Proof. By Nagura's bound [14], if $n/d \geq 30$, then $5n/6d < q_d < n/d$. Therefore, $n - dq_d < n/6$. If $d < 5$, then $6d < 5(d+1)$ and hence

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

as claimed. The proof of part (b) is analogous using Schoenfeld's bound [15]. □

In order to apply Theorem 2.5 with $d = 2$ for a given n, we need that there is a prime q such that $n/3 < q < n/2$. If q_2 denotes the nearest prime below $n/2$, then the inequality $n/3 < q_2$ holds if $n \geq 120$ by Lemma 3.2. Since by (2.1) we have that $n - q_1 < p^a$ if $n < 126$, we may assume that $n/3 < q_2$ without any loss of generality.

Note that the inequality $n/3 < q$ is equivalent to $n - 2q < q$, so the intervals $[0, n-2q]$ and $[q, n-q]$ are disjoint.

Theorem 3.3. *For an odd positive integer n and a prime power p^a dividing n, suppose that there is a prime q with $n/3 < q < n/2$ and $n - 2q < p^a$. Then n satisfies Condition 1 with p and q.*

Proof. By Theorem 2.5, in order to infer that $\binom{n}{k}$ is divisible by p or q, the only cases that we need to discuss are those values of k that are multiples of p^a with $k \in [0, n-2q]$ or $k \in [q, n-q]$. By assumption, there are no multiples of p^a in $[0, n-2q]$. Since $n-q > n/2$, we may focus on the interval $[q, n/2]$. Since n is odd, $n/2$ is not an integer; hence we are only left to prove that there is no multiple k of p^a with $q \le k < n/2$. We will prove this by contradiction.

Thus suppose that $q \le \lambda p^a < n/2$ for some integer λ. The assumption that $n-2q < p^a$ implies that $n - p^a < 2q$ and hence

$$n/2 - p^a/2 < q \le \lambda p^a.$$

Consequently, $\lambda p^a < n/2 < (\lambda + 1/2)p^a$. If we now write $n = mp^a$, we obtain that $2\lambda < m < 2\lambda + 1$, which is impossible for an integer m. □

The rest of this section is devoted to the case when n is even.

Lemma 3.4. *Suppose that n is even and there is a prime q with $q < n/2$ and $n - 2q < p^a$, where p^a is the largest power of p dividing n. If there is a multiple k of p^a in the interval $[q, n/2]$, then p is odd and $k = n/2$.*

Proof. Suppose first that p is odd. Then the integer $n/2$ is a multiple of p^a, so we may write $n/2 = \lambda p^a$ for some integer λ. If there is another multiple of p^a in the interval $[q, n/2]$, then $q \le (\lambda - 1)p^a < n/2$, and this implies that

$$n/2 - p^a = \lambda p^a - p^a = (\lambda - 1)p^a \ge q.$$

Hence $n - 2q \ge 2p^a$, which is incompatible with our assumption that $n - 2q < p^a$.

In the case $p = 2$ (so that 2^a is the largest power of 2 dividing n), we have that $n/2$ is divisible by 2^{a-1}, and we may write $n/2 = \lambda 2^{a-1}$ with λ odd. If there is a multiple of 2^a in the interval $[q, n/2)$, then $q \le \mu 2^a < n/2$, so $\mu < \lambda/2$ and $\mu \le (\lambda - 1)/2$ because λ is odd. Therefore

$$n/2 - 2^{a-1} = (\lambda - 1)2^{a-1} \ge \mu 2^a \ge q.$$

Hence, as above, $n - 2q \ge 2^a$, which contradicts that $n - 2q < 2^a$. □

Theorem 3.5. *For an even positive integer n, suppose that there is a prime q such that $n/3 < q < n/2$ and $n - 2q < p^a$, where p^a is the largest power of p dividing n.*

(a) If $p = 2$, then n satisfies Condition 1 with 2 and q.

(b) If $p \ne 2$, then n satisfies Condition 1 with p and q if and only if $\binom{n}{n/2}$ is divisible by p.

Proof. By Theorem 2.5 and Lemma 3.4, the only case left is $k = n/2$ for p odd. Consequently, if $\binom{n}{n/2}$ is divisible by p, then n satisfies Condition 1 with p and q. Moreover, $\binom{n}{n/2}$ is not divisible by q, since the base q expansions of n and $n/2$ are, respectively, $2 \cdot q + (n - 2q)$ and $1 \cdot q + (n/2 - q)$. Hence the assumption that $\binom{n}{n/2}$ be divisible by p is necessary. □

Our last remarks in this section correspond to the case when n is even, and they are only relevant if $p \neq 2$, by Theorem 3.5. Next we give sufficient conditions to infer that a prime p divides $\binom{n}{n/2}$. The greatest integer less than or equal to a real number x is denoted by $\lfloor x \rfloor$, and we write $v_p(n) = a$ if p^a is the maximum power of p such that p^a divides n.

Recall from [12] that

$$v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \frac{n - s_p(n)}{p-1}, \tag{3.1}$$

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

Proposition 3.6. *Suppose that n is even. A prime p divides $\binom{n}{n/2}$ if and only if at least one of the numbers $\lfloor n/p^r \rfloor$ with $r \geq 1$ is odd.*

Proof. By comparing $v_p(n!)$ and $v_p((n/2)!)$ we see that, for each r,

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

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

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

and consequently $v_p(n!)$ is greater than $2v_p((n/2)!)$. □

Corollary 3.7. *If n is even and $(n - s_p(n))/(p-1)$ is odd, then p divides $\binom{n}{n/2}$.*

Proof. This follows from Proposition 3.6 and Legendre's formula (3.1). □

Corollary 3.8. *Suppose that n is even.*

(a) If any of the digits in the base p expansion of $n/2$ is larger than $\lfloor p/2 \rfloor$, then p divides $\binom{n}{n/2}$.

(b) If one of the digits in the base p expansion of n is odd, then p divides $\binom{n}{n/2}$.

Proof. If a digit of $n/2$ in base p is larger than $\lfloor p/2 \rfloor$, then when we add $n/2$ to itself in base p to obtain n there is at least one carry. Similarly, if n has an odd digit in base p, then there is a carry when adding $n/2$ and $n/2$ in base p. Hence, by Kummer's Theorem [10] with $k = n/2$, if there is at least one carry when adding $n/2$ to itself in base p, then p divides $\binom{n}{n/2}$. □

Corollary 3.9. *Let n be an even positive integer. Suppose that there is a prime q such that $n/3 < q < n/2$ and $n - 2q < p^a$, where p^a denotes the largest power of p dividing n. If $p^{\lfloor \log n/ \log p \rfloor} > n/2$, then p divides $\binom{n}{n/2}$ and therefore n satisfies Condition 1 with p and q.*

Proof. The largest value of r such that $p^r < n < p^{r+1}$ is $\lfloor \log n/ \log p \rfloor$. Therefore, in Proposition 3.6, the exponent r is bounded by $\lfloor \log n/ \log p \rfloor$. Also note that $r \geq a$, where a is the largest exponent of p such that p^a divides n. If $p^{\lfloor \log n/ \log p \rfloor} > n/2$, then $\lfloor n/p^r \rfloor = 1$. Because this is odd, p divides $\binom{n}{n/2}$ by Proposition 3.6. □

In those cases when the inequalities $n - q_1 < p^a$ and $n - 2q_2 < p^a$ both fail for the largest prime power p^a dividing n, a possible strategy would be to analyze the inequality $n - dq_d < p^a$ for bigger values of d, where q_d is the largest prime below n/d.

Up to 1,000,000 there are 88 integers that do not satisfy $n - 2q_2 < p^a$, where p^a is the largest prime power dividing n. The On-Line Encyclopedia of Integer Sequences has published these numbers with the reference A290290 [4]. Among these, there are 25 that do not satisfy the inequality $n - 3q_3 < p^a$; there are 7 that do not satisfy the inequality $n - 4q_4 < p^a$ either; there are 5 for which the inequality $n - 5q_5 < p^a$ also fails, and there is only one integer for which the inequality $n - 6q_6 < p^a$ still fails (namely, $n = 875160$). However, the value of $n - dq_d$ need not decrease as d grows, and the number of dangerous intervals that one needs to inspect when $n - dq_d < p^a$ increases linearly with d. Therefore this strategy is not conclusive, although it often works in practice.

Example 3.10. The largest prime power dividing $n = p_{14}\# = 13082761331670030$ is $p = 43$. In this case, $n - q_1 = 89$ and $n - 2q_2 = 268$. Thus, Condition 1 fails for p and q_1 and it also fails for p and q_2. Nevertheless, $n - 3q_3 = 27$ works, as the dangerous interval $[q_3, n - 2q_3]$ contains one multiple of 43, namely $n/3$, and $\binom{n}{n/3}$ is divisible by 43. Therefore Condition 1 holds for $p = 43$ and $q_3 = 4360920443890001$.

Example 3.11. For $n = 210$, the inequality $n - q_1 < 7$ fails while $n - 2q_2 < 7$ is true. However, $\binom{210}{105}$ is not divisible by 7. Hence we look for greater values of d and find that $n - 5q_5 < 7$ with $q_5 = 41$. Now $42 \in [41, 46]$ and $84 \in [82, 87]$, yet $\binom{210}{42}$ and $\binom{210}{84}$ are both divisible by 7. Hence Condition 1 is satisfied with $p = 7$ and $q_5 = 41$.

Example 3.12. For $n = 875160$, the inequality $n - dq_d < 17$ is satisfied with $d = 11$ but not with any smaller value of d. There are 6 dangerous intervals of length $n - 11q_{11} = 11$. Each of these intervals (except the first) contains one multiple of 17, and in each case the corresponding binomial coefficient $\binom{n}{k}$ happens to be divisible by 17. Therefore Condition 1 is satisfied with $p = 17$ and $q_{11} = 79559$.

4 On the N-variation of Condition 1

Recall from Definition 1.2 that n satisfies the *N-variation* of Condition 1 if there are N primes $p_1, \dots, p_N$ such that if $1 \le k \le n - 1$ then $\binom{n}{k}$ is divisible by at least one of $p_1, \dots, p_N$.

Theorem 4.1. *If an even positive integer n satisfies $n - 2q < p^a$ for a prime q with $n/3 < q < n/2$, where p^a is the largest power of p dividing n and $p \neq 2$, then n satisfies the 3-variation of Condition 1 with p, q and any prime that divides $\binom{n}{n/2}$.*

Proof. According to the statement of part (b) of Theorem 3.5, the only binomial coefficient $\binom{n}{k}$ with $1 \le k \le n - 1$ that might fail to be divisible by p or q is $\binom{n}{n/2}$. Hence it suffices to add an extra prime with this purpose. □

Proposition 4.2. *For a positive integer n, let q_1 be the largest prime smaller than n, let $p_1^{a_1}$ be the largest prime-power divisor of n and let $p_2^{a_2}$ be the second largest prime-power divisor of n. If $p_1^{a_1} p_2^{a_2} > n - q_1$, then n satisfies the 3-variation of Condition 1 with p_1, p_2 and q_1.*

Proof. By Lucas' Theorem, for any k such that $1 \le k < p_1^{a_1}$, the binomial coefficient $\binom{n}{k}$ is divisible by p_1, and for any k such that $n - q_1 < k \le n/2$ the binomial coefficient $\binom{n}{k}$ is divisible by q_1. Thus we need to add a prime that divides at least the binomial coefficients $\binom{n}{k}$ with $p_1^{a_1} \le k \le n - q_1$ in which k is a multiple of $p_1^{a_1}$. For this, we pick p_2 and therefore we only need to consider those values of k that are, in addition, multiples of $p_2^{a_2}$. The least k that is a multiple of both prime powers is $p_1^{a_1}p_2^{a_2}$. Therefore, if $p_1^{a_1}p_2^{a_2} > n-q_1$, then all values of k lying in the interval $p_1^{a_1} \le k \le n - q_1$ are such that $\binom{n}{k}$ is divisible by p_1 or p_2. □

In the statement of Proposition 4.2, the condition that $p_1^{a_1}p_2^{a_2} > n - q_1$ holds by Nagura's bound [14] if we impose instead that $p_1^{a_1}p_2^{a_2} > n/6$.

For each n, we are interested in the minimum number N of primes such that n satisfies the N-variation of Condition 1. We next discuss upper bounds for N.

Proposition 4.3. *For positive integers n and d, suppose that there is a prime q such that $n/(d+1) < q < n/d$ and a prime-power divisor p^a of n such that $n - dq < p^a$. Then n satisfies the N-variation of Condition 1 with $N = 2 + \lfloor d/2 \rfloor$.*

Proof. By Theorem 2.5, the binomial coefficients $\binom{n}{k}$ are divisible by q except possibly if k lies in a dangerous interval. In the dangerous intervals we only need to consider those integers that are multiples of p^a, since otherwise $\binom{n}{k}$ is divisible by p. Since we are assuming that $n - dq < p^a$, we know that in each dangerous interval there is at most one multiple of p^a. This means that the worst case is the one in which there is a multiple of p^a in every dangerous interval $[cq, cq + \beta]$ with $1 \le c \le \lfloor d/2 \rfloor$. Hence we pick one extra prime for each such interval. □

Corollary 4.4. *If $1 < d < 5$ and $p^a > q_d + \beta_d$ where p^a divides n and q_d is the largest prime below n/d, and $\beta_d = n - dq_d$, then n satisfies Condition 1 with p and q_d.*

Proof. By Lemma 3.2, we may assume that $n/(d+1) < q_d$. If $1 < d < 5$, then $\lfloor d/2 \rfloor$ equals 1 or 2. If $\lfloor d/2 \rfloor = 1$, then the assumption that $p^a > q_d + \beta_d$ implies that no multiple of p^a falls into any dangerous interval until $n/2$. If $\lfloor d/2 \rfloor = 2$, then we need to check that $2p^a > 2q_d + \beta_d$ in order to ensure that $2p^a$ does not fall into the third dangerous interval. The minimum value of p^a such that our assumption $p^a > q_d + \beta_d$ holds is $q_d + \beta_d + 1$. The next multiple of $q_d + \beta_d + 1$ is $2q_d + 2\beta_d + 2$, which is greater than $2q_d + \beta_d$ and therefore $2p^a$ does not fall into the third dangerous interval. □

In order to refine the conclusion of Proposition 4.3, we consider the Diophantine equation

$$p^a x - q_d y = \delta, \tag{4.1}$$

for $0 \le \delta \le \beta_d = n - dq_d$, where p^a is a prime-power divisor of a given number n and q_d is the largest prime below n/d with $d \ge 1$. We keep assuming, as above, that $q_d > n/(d+1)$. We will also assume that $p \ne q_d$, which guarantees that (4.1) has infinitely many solutions for each value of δ. Specifically, if (x_1, y_1) is a particular solution for some value of δ, then the general solution for this δ is

$$x = x_1 + rq_d, \qquad y = y_1 + rp^a,$$

where r is any integer. In the next theorem we denote by $N(\delta)$ the number of solutions (x, y) of (4.1) with $x > 0$ and $0 \le y \le \lfloor d/2 \rfloor$ for each value of δ with $0 \le \delta \le \beta_d$. Thus $N(\delta) = 0$ precisely when (4.1) has no solution (x, y) subject to these conditions.

Theorem 4.5. *For positive integers n and d, suppose that the largest prime q_d below n/d satisfies $q_d > n/(d+1)$, and let $\beta_d = n - dq_d$. Let p^a be a prime power dividing n with $p \neq q_d$. Then n satisfies the N-variation of Condition 1 with*

$$N = 2 + \sum_{\delta=0}^{\beta_d} N(\delta),$$

where $N(\delta)$ is the number of solutions (x, y) of $p^a x - q_d y = \delta$ with $x > 0$ and $0 \leq y \leq \lfloor d/2 \rfloor$ for each value of δ with $0 \leq \delta \leq \beta_d$.

Proof. The number $N(\delta)$ counts how many times a multiple of p^a falls into a dangerous interval $[cq_d, cq_d + \beta_d]$ at a distance δ from the origin of that interval. Thus we pick an extra prime for each such case, and add two to the sum in order to account for p and q_d. □

Example 4.6. The largest prime-power divisor of $n = 96135$ is $p = 29$. For $d = 4$ we find that $q_4 = 24029$ and $\beta_4 = 19$. Since $24029 \equiv 17 \pmod{29}$, the only solution (x, y) of the Diophantine equation $29x - 24029y = \delta$ with $x > 0$ and $0 \leq y \leq 2$ is $(829, 1)$ for $\delta = 12$. Thus, $N(12) = 1$ and $N = 3$ for $d = 4$. In other words, the only occurrence of a multiple of 29 in a dangerous interval for $d = 4$ is $24041 \in [24029,\ 24048]$. This example shows that the bound $2 + \lfloor d/2 \rfloor$ given in Proposition 4.3 can be lowered.

The number N given by Theorem 4.5 is not a sharp bound. For those multiples $p^a x$ of p^a falling into a dangerous interval $[cq_d, cq_d + \beta_d]$, it often happens that the corresponding binomial coefficient $\binom{n}{p^a x}$ is divisible by p, as in Example 4.6 or in other examples given in the previous sections. It could also be divisible by q_d if $d \geq q_d$. When $d < q_d$, we have that n satisfies Condition 1 with p and q_d if and only if the binomial coefficient $\binom{n}{p^a x}$ is divisible by p for every solution (x, y) of (4.1) with $x > 0$ and $0 \leq y \leq \lfloor d/2 \rfloor$, since $n = dq_d + \beta_d$ and $p^a x = yq_d + \delta$ with $\delta \leq \beta_d < q_d$ and $y \leq \lfloor d/2 \rfloor < d$, so $\binom{n}{p^a x}$ is not divisible by q_d by Lucas' Theorem. Note also, for practical purposes, that $\binom{n}{p^a x} \equiv \binom{n/p^a}{x} \pmod{p}$.

5 Every number has multiples for which Condition 1 holds

We next prove that every positive integer n has infinitely many multiples for which Condition 1 holds. We are indebted to R. Woodroofe for simplifying and improving our earlier statement of this result, which was based on prime gap conjectures.

It follows from the Prime Number Theorem [7] that, given any real number $\varepsilon > 0$, there is a prime between m and $m(1 + \varepsilon)$ for sufficiently large m. This fact can be used to prove the following:

Theorem 5.1. *For every positive integer n and every prime p, the number np^k satisfies Condition 1 with p and another prime, for all sufficiently large values of k.*

Proof. For any prime p and any $k > 0$, let $m = np^k - p^k = p^k(n-1)$. Then

$$np^k = m + p^k = m\left(1 + \frac{1}{n-1}\right).$$

Therefore, by the Prime Number Theorem, there is a prime between m and np^k for all sufficiently large values of k. Choose the largest prime q with this property. Thus,

$$np^k - p^k < q < np^k,$$

so $np^k - q < p^k$, from which it follows, according to Corollary 2.6, that np^k satisfies Condition 1 with p and q. □

Theorem 5.2. *For every positive integer n there is a number M such that if p is any prime with $p > M$ then np satisfies Condition 1 with p and another prime.*

Proof. Given n, let $\varepsilon = 1/(n-1)$. Choose m_0 such that there is a prime between m and $m(1+\varepsilon)$ for all $m \geq m_0$, and let $M = \varepsilon m_0$. If p is any prime such that $p > M$, then for $m = p(n-1)$ we have

$$np = m + p = m\left(1 + \frac{p}{m}\right) = m\left(1 + \frac{1}{n-1}\right) = m(1+\varepsilon).$$

Therefore, by our choice of m_0, there is a prime between m and np. If q is the largest prime with this property, then $np - p < q < np$, and consequently np satisfies Condition 1 with p and q. □

Prime gap conjectures provide information relevant to our problem. For example, if p_i denotes the i-th prime, then Cramér's conjecture [6] claims that there exist constants M and N such that if $p_i \geq N$ then

$$p_{i+1} - p_i \leq M(\log p_i)^2.$$

Proposition 5.3. *Let m be 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, then $\sqrt[m]{n} \leq p^a$, where p^a is the largest prime-power divisor of n. Let M and N be the constants given by Cramér's conjecture. Pick n_0 such that if $n \geq n_0$ then $M(\log n)^2 < \sqrt[m]{n}$. For every n such that $n \geq n_0$ and $N \leq p_i < n \leq p_{i+1}$ (where p_i denotes the i-th prime), we have

$$n - p_i \leq p_{i+1} - p_i \leq M(\log p_i)^2 < M(\log n)^2 < \sqrt[m]{n} \leq p^a,$$

from which it follows that n satisfies Condition 1 with p and p_i. □

We note that the argument used in the proof of Proposition 5.3 yields an alternative proof of the fact that Condition 1 holds for a set of integers of asymptotic density 1 if Cramér's conjecture holds, a result first found in [16, § 5]:

Theorem 5.4 ([16]). *If Cramér's conjecture is true, then the set of numbers in the sequence (2.1) has asymptotic density zero.*

Proof. Suppose that Cramér's conjecture holds with constants M and N, and denote by $\omega(n)$ the number of distinct prime divisors of n. Thus $n^{1/\omega(n)} \leq p^a$, where p^a is the largest prime-power divisor of n. According to [8, § 3.2], for every $\varepsilon > 0$ the inequality

$$\omega(n) < (1+\varepsilon)\log\log n \tag{5.1}$$

holds for all n except those of a set of asymptotic density zero. Since

$$\lim_{n\to\infty} \frac{n^{1/\log\log n}}{(\log n)^k} = \infty$$

for all k, there is an n_0 such that $n^{1/\omega(n)} > M(\log n)^2$ if $n \geq n_0$. Now, if n is bigger than n_0 and satisfies $N \leq p_i < n \leq p_{i+1}$, and moreover n is not in the set of integers for which (5.1) fails, then

$$n - p_i \leq p_{i+1} - p_i \leq M(\log p_i)^2 < M(\log n)^2 < n^{1/w(n)} \leq p^a.$$

Therefore, n satisfies Condition 1 with p and p_i. □

6 Multinomials

We also consider a generalization of Condition 1 to multinomials. We say that a positive integer n satisfies *Condition* 1 *for multinomials of order* m if there are primes p and q such that the multinomial coefficient

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

is divisible by either p or q whenever $k_1 + \cdots + k_m = n$ with $1 \leq k_i \leq n - 1$ for all i.

Proposition 6.1. *If n satisfies Condition 1 with two primes p and q, then n satisfies Condition 1 for multinomials of any order $m \leq n$ with p and q.*

Proof. This follows from the equality

$$\binom{n}{k_1, k_2, \ldots, k_m} = \binom{n}{k_1}\binom{n-k_1}{k_2}\binom{n-k_1-k_2}{k_3}\cdots\binom{k_m}{k_m},$$

and the fact that $\binom{n}{k_1}$ is divisible by p or q by assumption. □

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

ORCID iDs

Sílvia Casacuberta https://orcid.org/0000-0001-5684-4585

References

[1] C. Banderier, Fortune's conjecture (Fortunate and unfortunate primes : Nearest primes from a prime factorial), https://lipn.univ-paris13.fr/~banderier/Computations/prime_factorial.html, last consulted on 11 August 2018.

[2] J. Bertrand, Mémoire sur le nombre de valeurs que peut prendre une fonction quand on y permute les lettres qu'elle renferme, *J. École Roy. Polytechnique* **18** (1845), 123–140.

[3] S. Casacuberta, Sequence A290203 in The On-Line Encyclopedia of Integer Sequences, published electronically at https://oeis.org.

[4] S. Casacuberta, Sequence A290290 in The On-Line Encyclopedia of Integer Sequences, published electronically at https://oeis.org.

[5] K. S. Davis and W. A. Webb, Lucas' theorem for prime powers, *European J. Combin.* **11** (1990), 229–233, doi:10.1016/s0195-6698(13)80122-9.

[6] A. Granville, Harald Cramér and the distribution of prime numbers, *Scand. Actuar. J.* **1995** (1995), 12–28, doi:10.1080/03461238.1995.10413946.

[7] G. H. Hardy and J. E. Littlewood, Contributions to the theory of the Riemann zeta-function and the theory of the distribution of primes, *Acta Math.* **41** (1916), 119–196, doi:10.1007/bf02422942.

[8] G. H. Hardy and S. Ramanujan, The normal number of prime factors of a number n, *Quart. J. Pure Appl. Math.* **48** (1917), 76–92.

[9] A. E. Ingham, *The Distribution of Prime Numbers*, Cambridge Tracts in Mathematics and Mathematical Physics, Cambridge University Press, Cambridge, 1932.

[10] E. E. Kummer, Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen, *J. Reine Angew. Math.* **44** (1852), 93–146, doi:10.1515/crll.1852.44.93.

[11] E. Labos, Sequence A057704 in The On-Line Encyclopedia of Integer Sequences, published electronically at https://oeis.org.

[12] A.-M. Legendre, *Théorie des nombres*, Firmin Didot frères, Paris, 3rd edition, 1830.

[13] E. Lucas, Théorie des fonctions numériques simplement périodiques, *Amer. J. Math.* **1** (1878), 184–196, doi:10.2307/2369308.

[14] J. Nagura, On the interval containing at least one prime number, *Proc. Japan Acad.* **28** (1952), 177–181, doi:10.3792/pja/1195570997.

[15] L. Schoenfeld, Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II, *Math. Comp.* **30** (1976), 337–360, doi:10.2307/2005976.

[16] J. Shareshian and R. Woodroofe, Divisibility of binomial coefficients and generation of alternating groups, *Pacific J. Math.* **292** (2018), 223–238, doi:10.2140/pjm.2018.292.223.

[17] N. J. A. Sloane (ed.), The On-Line Encyclopedia of Integer Sequences, published electronically at https://oeis.org.