DIVISIBILITY OF BINOMIAL COEFFICIENTS AT $p = 2$

BAILEY SWINFORD

Abstract. This paper will look at the binomial coefficients divisible by the prime number 2. The paper will seek to understand and explain a case when each entry in a row of Pascal's triangle will be divisible by one of two primes, 2 and r.

1. Introduction

This paper was first and foremost inspired by the work of John Shareshian and Russ Woodroofe. In their paper [2], they considered the following condition that a natural number n may or may not satisfy.

Condition 1. There exist primes p and r (depending on n) such that for every k with $1 \leq k \leq n-1$, the binomial coefficient $\binom{n}{k}$ is divisible by at least one of p and r.

They asked when the condition would hold for given values of p and r. They developed a sieve that would help them answer the question. From several properties and theorems outlined in the paper, the case where $p = 2$ should garner special attention. Indeed, from computational work done with the help of a program, it was discovered that 2 satisfied the conditions in roughly 86.7% of the cases where $n \leq 1000000$. This discovery is what led me to work on this project. I wanted to further explore where $p = 2$ holds and, perhaps more importantly, where it fails.

In this paper, I will be attempting to show where 2 satisfies the conditions in all cases. In Section 2, I will prove a lemma that will be important to the argument of the later proof. In Section 3, I will give a brief explanation of the computer programming and results that motivated this paper and some tables that show interesting values returned by the program. In Section 4, I will be giving a short bit of background into the mathematics that will help to prove the theorem in the paper, as well as proving the theorem of the paper.

2. Preliminaries

We are interested in satisfying Condition 1 from [2]. Recall:

Lemma 2 (Shareshian and Woodroofe [2, Lemma 1.8])**.** *Let n, a, and b be positive integers and p and r be primes. Suppose n is not a prime power. If $p^a \mid n$ and $r^b < n < r^b + p^a$, then n satisfies Condition 1 with p and r. In particular, if $2^a \mid n$ and $r^b < n < r^b + 2^a$, then n satisfies Condition 1 with 2 and r.*

From here on in, we will be referring to Lemma 2 as the sieve. We noticed that if n satisfies Lemma 2 with 2 and r, then frequently $2n$ satisfies Condition 1 with 2 and r. The following theorem gives some circumstances in which this phenomena occurs.

Our main theorem relies heavily on combinatorial theorems and algebra involving primes. A well-known lemma from [1] is particularly useful. The following is a statement and proof of the lemma.

Lemma 3. *Let p be a prime and a be a natural number. Then*

$$(1+x)^{p^a} \equiv (1+x^{p^a}) \mod p.$$

Proof. Let x be an integer, p be a prime, and a be a natural number. By the Binomial Theorem,

$$(1+x)^{p^a} = 1^{p^a} + \binom{p^a}{1} 1^{p^a} x^{p^a-1} + \ldots + \binom{p^a}{p^a-1} 1^1 x^{p^a-1} + x^{p^a}.$$

We must prove that p divides every term on the right-hand side except 1^{p^a} and x^{p^a}. Recall for $1 \leq k < p^a - 1$

$$\binom{p^a}{k} = \frac{(p^a)!}{k!(p^a-k)!}.$$

We will prove this using induction. The first case to consider is when $a = 1$. Hence, we have $(1+x)^p$ and the Binomial Theorem says

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}.$$

Notice in the above expression that there is a factor of p in the numerator, but there is not one in the denominator since p is a prime number. Thus, the coefficients of the expanded polynomial will all be divisible by p except the trivial cases where the coefficients are 1. So, we have $(1+x)^p \equiv_p (1+x^p)$. Now, since we have proved the base case, we may assume that $(1+x)^{p^a} \equiv_p (1+x^{p^a})$ is true. It is our goal to prove the case where we have $(1+x)^{p^{a+1}}$. Notice that $(1+x)^{p^{a+1}}$ is the same as $((1+x)^{p^a})^p$. We may begin with $(1+x)^{p^a}$ and remember that $(1+x)^{p^a} \equiv_p (1+x^{p^a})$. Therefore, we have $((1+x)^{p^a})^p \equiv_p (1+x^{p^a})^p$. From the base case, we know that $(1+x)^p \equiv_p (1+x^p)$. By reducing again $\mod p$, we have $(1+x^{p^a})^p \equiv_p (1+x^{p^a \cdot p}) = (1+x^{p^{a+1}})$. $\square$

3. Computer algorithms

In the very beginning of this project, I used the GAP code SgdivPartnersLucas [3] developed by Shareshian and Woodroofe to generate values of r that satisfy the sieve and Condition 1 with 2 for the values input for n. I began with 3927 because $3927 \cdot 2^3$ was the first number that fails to satisfy Condition 1 with its largest prime-power divisor. I took 3927 and continued to multiply it by powers of 2 while pairing it with $p = 2$ in the function. For the first four iterations, the program would only return a single number, 7853. However, after this, the numbers returned by the program increased greatly from one iteration to the next. Not all of these numbers satisfied the sieve. In each list of numbers, there was a small range, sometimes as small as one number, where the values of r could be found. I, manually, examined those that satisfied the sieve to see how many generations r "survives". For my purposes, I am defining a generation to be the number of subsequent values of 2^a that are multiplied by 3927 to get a value for the prime r that satisfies Condition 1. The first time a prime r appears is generation 1. I prove in Section 3 that for values of r satisfying the sieve, these numbers will survive at least one generation.

The following table contains some of the numbers satisfying Lemma 2 along with the number of generations r survives computation.

n	r	# generations
$(3927 * 2)$	7853	5
$(3927 * 2^4)$	62819	5
$(3927 * 2^5)$	125639	5
$(3927 * 2^8)$	1005312	6

Next, I have included a table displaying primes r that appear during computations, but where 2 and r do not satisfy the sieve. These are found in the same way as in the first table, using SgdivPartnersLucas. It is notable that these numbers show a greater variation of generations survived, with 41887 surviving the longest of numbers studied.

n	r	# generations
$(3927 * 2^5)$	20939	3
$(3927 * 2^5)$	41887	8
$(3927 * 2^9)$	1005217	4
$(3927 * 2^4)$	20939	4

The final table exhibits the number of primes r such that the given n satisfies Condition 1 of the SgdivPartnersLucas program. The values for the size are found by simply calling the size function in GAP after each subsequent iteration of the SgdivPartnersLucas function. It is of interest that the values of the size appear to grow very quickly.

n	size
$(3927 * 2^2)$	1
$(3927 * 2^4)$	8
$(3927 * 2^6)$	28
$(3927 * 2^8)$	90
$(3927 * 2^{10})$	331

4. Main theorem

Theorem 4. *Let n be a positive integer. Let 2^a be the highest power that divides n. Suppose $r^b < n < r^b + 2^a$ where r is a prime. Then $2n$ also satisfies Condition 1 with 2 and r.*

Proof. From Lemma 2, we know if n is not a prime power and $r^b < n < r^b + p^a$, then n satisfies Condition 1. We are interested in studying the case where $p = 2$. Thus, we have

$$r^b < n < r^b + 2^a$$

where $2^a | n$. Therefore, by multiplying through by 2, we have

$$2r^b < 2n < 2r^b + 2^{a+1}.$$

Next, we can subtract through by $2r^b$ and get

$$0 < 2n - 2r^b < 2^{a+1}.$$

The simplest way to prove the idea is using the Binomial Theorem and Lemma 3 to check divisibility of coefficients.

If $n = 2^a$, then $\binom{2n}{k}$ is divisible by 2 for all $1 \leq k \leq 2n - 1$, because we have

$$(1 + x)^{2^a} \equiv_2 (1 + x^{2^a}).$$

We are left with the trivial cases where the coefficients are 1.

If $n \neq 2^a$, then there exists an integer $m \neq 1$ such that $n = 2^a m$. Thus,

$$(1 + x)^n = (1 + x)^{2^a m}$$
$$(1 + x)^{2n} = (1 + x)^{2^{a+1} m}.$$

By reducing modulo 2, we have

$$(1 + x)^{2n} \equiv_2 (1 + x^{2^{a+1}})^m.$$

Thus, $\binom{2n}{k}$ fails to be divisible by 2 only when k is a multiple of 2^{a+1}. Further,

$$(1 + x)^{2n} = (1 + x)^{2n-2r^b} (1 + x)^{2r^b},$$

and this time, we can reduce modulo r to get

$$(1 + x)^{2n} \equiv_r (1 + x)^{2n-2r^b} (1 + x^{r^b})^2.$$

Therefore, $\binom{2n}{k}$ fails to be divisible by r only when

(1) $k \leq 2n - 2r^b$,
(2) $k \geq 2r^b$, or
(3) $0 \leq k - r^b \leq 2n - 2r^b$, i.e. $r^b \leq k \leq 2n - r^b$.

It suffices to show that k is not a multiple of 2^{a+1} (and hence, that 2 divides k) in the above cases. By the hypotheses on n and r, we have $0 < n - r^b < 2^a$. Thus, in case 1, we have $0 < k \leq 2n - 2r^b < 2^{a+1}$. Case 2 follows by symmetry between k and $2n - k$. Since 2^a is the highest power dividing n, n is not a multiple of 2^{a+1}. However, $n - 2^a$ and $n + 2^a$ are multiples of 2^{a+1}. Thus, we have

$$n - 2^a < r^b < n < n + (n - r^b) = 2n - r^b < n + 2^a.$$

We know that in Case 3 that k is contained in the interval $r^b \leq k \leq 2n - r^b$. Therefore, k cannot be a multiple of 2^{a+1}, as $n - 2^a$ and $n + 2^a$ are the adjacent multiples of 2^{a+1}. □

References

[1] I. Martin Isaacs, *Algebra: a graduate course*, Graduate Studies in Mathematics, vol. 100, American Mathematical Society, Providence, RI, 2009, Reprint of the 1994 original.

[2] John Shareshian and Russ Woodroofe, *Divisibility of binomial coefficients and generation of alternating groups*, arXiv:1505.05143.

[3] John Shareshian and Russ Woodroofe, *Ancillary file to arXiv:1505.05143*, May 2015.