TWO BINOMIAL COEFFICIENT CONJECTURES

ERIC ROWLAND

To Doron Zeilberger in honor of his 60th birthday!

Abstract. Much is known about binomial coefficients where primes are concerned, but considerably less is known regarding prime powers and composites. This paper provides two conjectures in these directions, one about counting binomial coefficients modulo 16 and one about the value of $\binom{n}{2p}$ modulo n.

1. Introduction

On the occasion of Doron Zeilberger's sixtieth birthday I present two conjectures on arithmetic properties of binomial coefficients. These conjectures epitomize the celebrated Zeilbergerian experimental approach to mathematics. They began as naive questions. Answers to these questions were computed (by a machine) in many specific instances, and the data was analyzed (by a human with the assistance of a machine) for patterns. From such experiments, and in the case of the second conjecture after a fair amount of work, the author formulated and simplified the statements of the conjectures, which were then verified against additional data.

Perhaps most importantly, the conjectures given in this paper are empirical claims and are unproven! We do however condescend to prove some propositions.

Accompanying these two conjectures are two stories. Arithmetic properties of binomial coefficients have a long and interesting history, a major theme of which is that properties of $\binom{n}{m}$ involving the prime p are related to the standard base-p representations $n_l n_{l-1} \cdots n_1 n_0$ and $m_l m_{l-1} \cdots m_1 m_0$ of n and m. The theorems of Kummer [13, pages 115–116] and Lucas [15] are important examples of this relationship.

Theorem (Kummer)**.** *Let p be a prime, and let $0 \leq m \leq n$. The exponent of the highest power of p dividing $\binom{n}{m}$ is the number of borrows involved in subtracting m from n in base p.*

Theorem (Lucas)**.** *If p is a prime and $0 \leq m \leq n$, then*

$$\binom{n}{m} \equiv \prod_{i=0}^{l} \binom{n_i}{m_i} \mod p.$$

The relationship between $\binom{n}{m}$ and the base-p representations of n and m can be thought of as a consequence of the self-similarity present in both Pascal's triangle and base-k representations of nonnegative integers. Figure 1 shows Pascal's triangle modulo powers of 2.

Moreover, this relationship provides a natural rendering of number theoretic questions about binomial coefficients in terms of combinatorial questions about

Date: February 7, 2011.

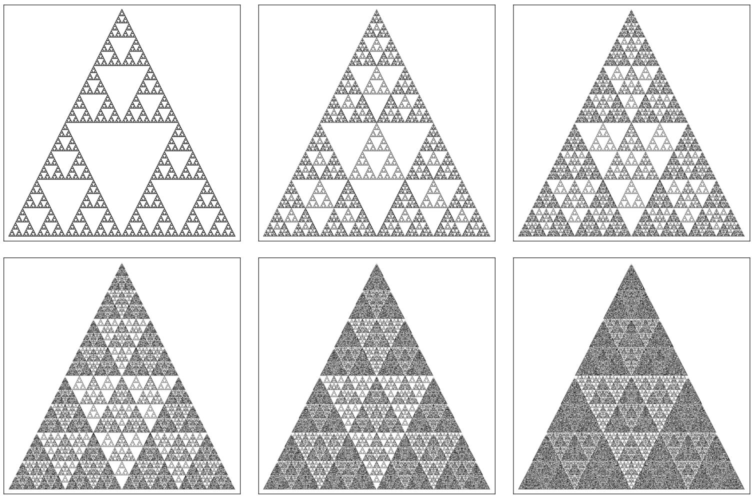

FIGURE 1. Pascal's triangle modulo 2^α for $1 \le \alpha \le 6$, in which nested structure can be seen.

words. We shall use the notation $|n|_w$ to denote the number of occurrences of the word w in the base-p representation $n_l n_{l-1} \cdots n_1 n_0$, where p is the prime implied by context.

Both conjectures in the paper are concerned with the values of $\binom{n}{m}$ modulo k. The first conjecture concerns counting binomial coefficients $\binom{n}{m}$ equivalent to a certain residue class modulo 16, for fixed n. The second conjecture concerns the value of $\binom{n}{2p}$ modulo n.

2. Counting entries modulo k

Counting binomial coefficients is a sort of "meta-combinatorics" — we are counting the counters! One basic question we can ask about Pascal's triangle modulo k is how many nonzero entries there are on row n. This question was answered for prime $k = p$ by Fine [5] and shown to be $\prod_{i=0}^{l} (n_i + 1)$. For prime powers $k = p^\alpha$ an expression was found by the author [16]. There has been no progress in the case of composite k.

Here we shall be interested in a refinement of the previous question: Let $a_{k,r}(n)$ be the number of integers $0 \le m \le n$ such that $\binom{n}{m} \equiv r \mod k$; what is the structure of $a_{k,r}(n)$?

The first result on $a_{k,r}(n)$ was Glaisher's 1899 [7] discovery that $a_{2,1}(n) = 2^{|n|_1}$. After that there appears to have been no results until 1978, when Hexel and Sachs [11, §5] determined a formula for $a_{p,r^i}(n)$ for any prime p in terms of $(p-1)$th roots of unity, where r is a primitive root modulo p. From this they derived

$$a_{3,1}(n) = 2^{|n|_1 - 1} \cdot \left(3^{|n|_2} + 1\right)$$
$$a_{3,2}(n) = 2^{|n|_1 - 1} \cdot \left(3^{|n|_2} - 1\right)$$

as well as explicit formulas for $a_{5,r^i}(n)$ in terms of $|n|_1$, $|n|_2$, $|n|_3$, and $|n|_4$. Garfield and Wilf [6] exhibited a method to compute the generating function $\sum_{i=0}^{p-2} a_{p,r^i}(n)x^i$, where again r is a primitive root.

Recently, Amdeberhan and Stanley [2, Theorem 2.1] studied the number of coefficients equal to r in the nth power of a general multivariate polynomial over a finite field, where r is an invertible element of the field. They showed that if $f(\mathbf{x}) \in \mathbb{F}_q[x_1, \dots, x_m]$ then the number $a(n)$ of coefficients in $f(\mathbf{x})^n$ equal to $r \in \mathbb{F}_q^\times$ is a q-regular sequence, meaning that it satisfies linear recurrences in $a(q^e n + i)$ [1].

The first results for a non-prime modulus were formulas for $a_{4,r}(n)$ given by Davis and Webb [3]:

$$\begin{aligned}
a_{4,1}(n) &= \begin{cases} 2^{|n|_1} & \text{if } |n|_{11} = 0 \\ 2^{|n|_1 - 1} & \text{otherwise} \end{cases} \\
a_{4,2}(n) &= 2^{|n|_1 - 1} \cdot |n|_{10} \\
a_{4,3}(n) &= \begin{cases} 0 & \text{if } |n|_{11} = 0 \\ 2^{|n|_1 - 1} & \text{otherwise} \end{cases}
\end{aligned}$$

(where $|n|_w$ counts occurrences of w in the base-2 representation of n). In particular, if r is odd then $a_{4,r}(n)$ is either 0 or a power of 2.

Granville observed that in a sense the statement that $a_{4,r}(n)$ is either 0 or a power of 2 parallels Glaisher's result that $a_{2,1}(n) = 2^{|n|_1}$ is (either 0 or) a power of 2. Granville asked whether a similar statement is true modulo 8. His delightful paper "Zaphod Beeblebrox's brain and the fifty-ninth row of Pascal's triangle" [8] contains the following theorem.

Theorem (Granville)**.** *If r is odd then $a_{8,r}(n)$ is either 0 or a power of 2.*

As in the case of $a_{4,r}(n)$, for even r other values occur. For example, $a_{8,4}(12) = 5$ and $a_{8,0}(16) = 12$.

Granville goes on to consider the number of binomial coefficients congruent to an odd residue class r modulo 16, and he discovers that the analogous statement fails for $n = 59$! Granville writes: "Unbelievably, there are exactly six entries of Row 59 in each of the congruence classes 1, 11, 13, and 15 (mod 16)! Our pattern has come to an end, but not before providing us with some interesting mathematics, as well as a couple of pleasant surprises."

But this isn't the end of the story! We are now lead to ask: What values *does* $a_{16,r}(n)$ take for odd r? Explicit computation shows that up to row 2^{20} the set of values that occur is

$$\{0, 1, 2, 4, 6, 8, 12, 16, 20, 24, 32, 40, 48, 56, 64, 72, 80, 96, \dots, 65536\}.$$

This computation took nearly three CPU weeks to complete. It is clear that the only odd number that occurs is 1, since $\binom{2n}{n}$ is even for $n \geq 1$, so $a_{16,r}(n)$ is even. But the data suggests that $a_{16,r}(n)$ does not take on every even number.

Conjecture 1. *Fix n and odd r.*
If $a_{16,r}(n)$ is divisible by 3, then it is also divisible by 2.
If $a_{16,r}(n)$ is divisible by 5, then it is also divisible by 2^2.
If $a_{16,r}(n)$ is divisible by 7, then it is also divisible by 2^3.
If $a_{16,r}(n)$ is divisible by 11, then it is also divisible by 2^5.

If $a_{16,r}(n)$ is divisible by 13*, then it is also divisible by* 2^6*.*
If $a_{16,r}(n)$ is divisible by 17*, then it is also divisible by* 2^4*.*
If $a_{16,r}(n)$ is divisible by 31*, then it is also divisible by* 2^5*.*

Moreover, these eight primes are the only primes that appear up to row 2^{20}. Of course, there is a probably a more general and more compact conjecture waiting to be discovered. However, it is not clear what the corresponding powers of 2 might be for larger primes.

Granville's analysis of $a_{8,r}(n)$ was long (and in fact incomplete [9, 12]). However, it should be possible to automate Granville's work in true Zeilberger fashion. We do not undertake this work here, but once this is done and understood, the methodology will likely be applicable to $a_{16,r}(n)$, and perhaps the statements in the conjecture and the larger context surrounding them will become clear. Hopefully a reader will take up this challenge!

3. The value of $\binom{n}{m}$ modulo n

We all know the feeling of anxiety caused by witnessing a calculus student apply the "high school dream"[1]

$$(a+b)^n = a^n + b^n,$$

in which exponentiation distributes over addition. But of course the high school dream is actually valid on occasion. In particular, $(a+b)^p \equiv a^p + b^p \mod p$, since $\binom{p}{m} \equiv 0 \mod p$ for $1 \leq m \leq p-1$.

We might then ask: How badly does the high school dream fail for non-primes? What is $\binom{n}{m}$ modulo n, and how frequently is it nonzero? With such an answer we can precisely quantify how upset at students we are entitled to get!

Rather than study $\binom{n}{m}$ modulo n directly, we divide by n and consider $\operatorname{frac}(\frac{1}{n}\binom{n}{m})$, where $\operatorname{frac}(x) = x - \lfloor x \rfloor$ is the fractional part of x. We can recover the value of $\binom{n}{m}$ modulo n from $\binom{n}{m} \equiv n \operatorname{frac}(\frac{1}{n}\binom{n}{m}) \mod n$. Figure 2 displays $\operatorname{frac}(\frac{1}{n}\binom{n}{m})$ graphically. The principal advantage of reformulating in this way is that for fixed $m \geq 1$ the sequence $\operatorname{frac}(\frac{1}{n}\binom{n}{m})$ for $n \geq 1$ is periodic, which we soon prove. For example, if $m = 4$ the sequence $\operatorname{frac}(\frac{1}{n}\binom{n}{m})$ is

$$0, 0, 0, \frac{1}{4}, 0, \frac{1}{2}, 0, \frac{3}{4}, 0, 0, 0, \frac{1}{4}, 0, \frac{1}{2}, 0, \frac{3}{4}, 0, 0, 0, \frac{1}{4}, 0, \frac{1}{2}, 0, \frac{3}{4}, \dots.$$

If $m = 5$ the sequence is

$$0, 0, 0, 0, \frac{1}{5}, 0, 0, 0, 0, \frac{1}{5}, 0, 0, 0, 0, \frac{1}{5}, 0, 0, 0, 0, \frac{1}{5}, 0, 0, 0, 0, \frac{1}{5}, \dots,$$

and if $m = 6$ it is

$$\begin{gathered} 0, 0, 0, 0, 0, \frac{1}{6}, 0, \frac{1}{2}, \frac{1}{3}, 0, 0, 0, 0, \frac{1}{2}, \frac{2}{3}, \frac{1}{2}, 0, \frac{1}{3}, 0, 0, 0, \frac{1}{2}, 0, \frac{1}{6}, \\ 0, 0, \frac{1}{3}, 0, 0, \frac{1}{2}, 0, \frac{1}{2}, \frac{2}{3}, 0, 0, \frac{1}{3}, 0, \frac{1}{2}, 0, \frac{1}{2}, 0, \frac{2}{3}, 0, 0, \frac{1}{3}, \frac{1}{2}, 0, \frac{1}{2}, \\ 0, 0, \frac{2}{3}, 0, 0, \frac{5}{6}, 0, \frac{1}{2}, 0, 0, 0, \frac{2}{3}, 0, \frac{1}{2}, \frac{1}{3}, \frac{1}{2}, 0, 0, 0, 0, \frac{2}{3}, \frac{1}{2}, 0, \frac{5}{6}, \dots \end{gathered}$$

with period length 72.

The proof of periodicity follows from a result of Lu and Tsai [14].

[1] known as the "freshman dream" in countries such as the U.S. with lagging math education

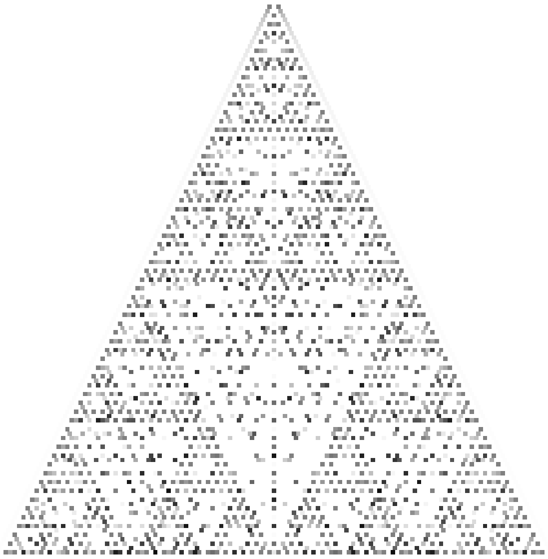

FIGURE 2. Rows 1 through $2^7 - 1$ of Pascal's triangle, where $\binom{n}{m}$ is assigned the gray value between 0 (white) and 1 (black) corresponding to $\mathrm{frac}(\frac{1}{n}\binom{n}{m})$.

Theorem (Lu and Tsai)**.** *Let $k \geq 1$ and $m \geq 1$. The sequence $\binom{n}{k}$ modulo m for $n \geq 0$ is periodic with (minimal) period length*

$$m \cdot \prod_{p|m} p^{\lfloor \log_p k \rfloor}.$$

We now apply the Lu–Tsai result to $\binom{n}{m} \mod n$.

Proposition. *Let $m \geq 1$. The sequence $\mathrm{frac}(\frac{1}{n}\binom{n}{m})$ for $n \geq 1$ is periodic with period length*

$$m \cdot \prod_{p|m} p^{\lfloor \log_p (m-1) \rfloor}.$$

The factor $p^{\lfloor \log_p (m-1) \rfloor}$ can be interpreted as the largest power of p that is strictly less than m.

Proof. We have

$$\frac{1}{n}\binom{n}{m} = \frac{1}{m}\binom{n-1}{m-1}.$$

Taking the fractional part of both sides and letting $k = m - 1$ in the previous theorem gives the desired result. □

In the remainder of the paper we aim to compute $\mathrm{frac}(\frac{1}{n}\binom{n}{m})$ in two cases — when $m = p$ and when $m = 2p$. The case when $m = p$ is fairly simple. Let δ_S be 1 if the statement S is true and 0 if S is false.

Proposition. *If p is a prime and $n \geq 1$, then*

$$\operatorname{frac}(\frac{1}{n}\binom{n}{p}) = \frac{1}{p}\delta_{p|n} = \begin{cases} 0 & \textit{if } p \nmid n \\ 1/p & \textit{if } p \mid n. \end{cases}$$

First proof. By the previous proposition, the period length of $\operatorname{frac}(\frac{1}{n}\binom{n}{p})$ is p, so the values of $\operatorname{frac}(\frac{1}{n}\binom{n}{p})$ for $n \geq 1$ are determined by the values for $1 \leq n \leq p$. For $1 \leq n \leq p-1$ we have $\binom{n}{p} = 0$, and $\binom{p}{p} = 1$. □

Therefore $\binom{n}{p}$ is zero modulo n with frequency $\frac{p-1}{p}$.

We provide a second proof of this proposition that is more similar to the proof of the final proposition of the section. We require two preliminary results. The first follows immediately from Kummer's theorem. Let $\nu_p(n)$ be the exponent of the highest power of p dividing n.

Lemma. *If p is a prime and $0 \leq m \leq n$, then $\nu_p(\binom{pn}{pm}) = \nu_p(\binom{n}{m})$.*

The second is a result discovered by Anton in 1869 and rediscovered by both Stickelberger and Hensel that determines the value modulo p of a binomial coefficient removed of its p factors [4, 10]. Recall that $n_l n_{l-1} \cdots n_1 n_0$ and $m_l m_{l-1} \cdots m_1 m_0$ are the representations of n and m in base p. We write $(n-m)_i$ for the ith base-p digit of $n-m$.

Theorem (Anton). *Let p be a prime, and let $0 \leq m \leq n$. We have*

$$\frac{1}{(-p)^{\nu_p(\binom{n}{m})}}\binom{n}{m} \equiv \prod_{i=0}^{l} \frac{n_i!}{m_i!(n-m)_i!} \mod p.$$

Note that the arithmetic on the right side of the congruence takes place in $\mathbb{Z}/p\mathbb{Z}$, not $\mathbb{R}/p\mathbb{Z}$.

We are now ready to give the second proof.

Second proof of the proposition. We show that $\binom{n}{p} \equiv \frac{n}{p}\delta_{p|n} \mod n$.

For any integer m, $\frac{m}{n}\binom{n}{m} = \binom{n-1}{m-1} \in \mathbb{Z}$, so in particular $p\binom{n}{p} \equiv 0 \mod n$.

If $p \nmid n$ then p is invertible modulo n, so $\binom{n}{p} \equiv 0 \mod n$.

If $p \mid n$, let $\nu = \nu_p(n)$ and write $n = p^\nu n'$. We show that $\binom{n}{p} \equiv \frac{n}{p} \mod n$. Since $n' \mid \binom{n}{p}$ and $n' \mid \frac{n}{p}$, we have $\binom{n}{p} \equiv \frac{n}{p} \mod n'$. It remains to show that $\binom{n}{p} \equiv \frac{n}{p} \mod p^\nu$. By the lemma, $\nu_p(\binom{n}{p}) = \nu_p(\binom{n/p}{1}) = \nu_p(n) - 1$. Write $\binom{n}{p} = p^{\nu-1}b'$. One checks that the ratio in Anton's theorem is

$$\frac{n_i!}{p_i!(n-p)_i!} \equiv \begin{cases} 1 & \text{if } i = 0 \\ -1 & \text{if } 1 \leq i < \nu \\ n_\nu & \text{if } i = \nu \\ 1 & \text{if } i > \nu \end{cases} \mod p.$$

It follows that $b' \equiv n' \mod p$, so multiplying by $p^{\nu-1}$ gives $\binom{n}{p} \equiv \frac{n}{p} \mod p^\nu$. □

When m is not prime, the behavior of $\operatorname{frac}(\frac{1}{n}\binom{n}{m})$ is more complex. Our second conjecture concerns the case $m = 2p$. The period length of $\operatorname{frac}(\frac{1}{n}\binom{n}{2p})$ for $p \neq 2$ is $2^{\lfloor \log_2(2p-1) \rfloor + 1} p^2$. However, the conjecture states that we may specify these

$2^{\lfloor \log_2(2p-1)\rfloor+1}p^2$ values in a more concise way than by listing them explicitly. First we prove a result for $\operatorname{frac}(\frac{2}{n}\binom{n}{2p})$.

Proposition. *If p is a prime and $n \geq 1$, then*

$$\operatorname{frac}(\frac{2}{n}\binom{n}{2p}) = \operatorname{frac}(\frac{n_1-1}{p})\delta_{p|n}.$$

For example, if $p=3$ then the sequence $\operatorname{frac}(\frac{2}{n}\binom{n}{2p})$ is

$$0,0,0,0,0,\frac{1}{3},0,0,\frac{2}{3},0,0,0,0,0,\frac{1}{3},0,0,\frac{2}{3},0,0,0,0,0,\frac{1}{3},0,0,\frac{2}{3},\dots.$$

Proof. As in the proof of the previous proposition, $\frac{2p}{n}\binom{n}{2p} \in \mathbb{Z}$, so $2p\binom{n}{2p} \equiv 0 \mod n$.

First consider $p=2$. The period length of $\operatorname{frac}(\frac{2}{n}\binom{n}{4})$ is 4. The period length of $\operatorname{frac}(\frac{n_1-1}{2})\delta_{2|n}$ is also 4, so one checks that the first 4 values of the two sequences agree.

Let $p \neq 2$.

If $p \nmid n$ then $2\binom{n}{2p} \equiv 0 \mod n$.

If $p \mid n$, let $\nu = \nu_p(n)$ and write $n = p^\nu n'$. We show that $2\binom{n}{2p} \equiv \frac{n}{p}(\frac{n}{p}-1) \mod n$. Since $2\binom{n}{2p} \equiv 0 \mod n'$ and $\frac{n}{p}(\frac{n}{p}-1) \equiv 0 \mod n'$, it suffices to show that $2\binom{n}{2p} \equiv \frac{n}{p}(\frac{n}{p}-1) \mod p^\nu$. Let $\beta = \nu_p(2\binom{n}{2p})$, and write $2\binom{n}{2p} = p^\beta b'$. By the lemma, $\beta = \nu_p(\frac{n}{p}(\frac{n}{p}-1)) = \nu - 1 + \nu_p(\frac{n}{p}-1)$. We consider two cases. If $n_1 \geq 2$, the ratio in Anton's theorem is

$$\frac{n_i!}{(2p)_i!(n-2p)_i!} \equiv \begin{cases} 1 & \text{if } i=0 \\ \frac{1}{2}\frac{n}{p}(\frac{n}{p}-1) & \text{if } i=1 \\ 1 & \text{if } i>1 \end{cases} \mod p;$$

in this case $\nu = 1$ and $\beta = 0$, so

$$2\binom{n}{2p} \equiv \frac{n}{p}\left(\frac{n}{p}-1\right) \mod p$$

as desired. Alternatively, if $n_1 < 2$, the ratio is

$$\frac{n_i!}{(2p)_i!(n-2p)_i!} \equiv \begin{cases} 1 & \text{if } i=0 \\ \frac{1}{2!(n_1+p-2)!} & \text{if } i=1 \\ -1 & \text{if } 2 \leq i \leq \beta \\ \lfloor \frac{n}{p^i} \rfloor & \text{if } i = \beta+1 \\ 1 & \text{if } i > \beta+1 \end{cases} \mod p,$$

so (since $(n_1+p-2)! \equiv (-1)^{n_1} \mod p$)

$$2\binom{n}{2p} \equiv -(-1)^{n_1}p^\beta \left\lfloor \frac{n}{p^{\beta+1}} \right\rfloor \mod p^{\beta+1}.$$

Now if $n_1 = 1$ then $\beta = \nu_p(n-p)-1$, so this becomes

$$2\binom{n}{2p} \equiv p^{\nu_p(n-p)-1}\left\lfloor \frac{n}{p^{\nu_p(n-p)}} \right\rfloor = \frac{n-p}{p} \equiv \frac{n}{p}\left(\frac{n}{p}-1\right) \mod p^{\nu_p(n-p)},$$

which is sufficient since $\nu_p(n-p) > 1 = \nu_p(n)$. If on the other hand $n_1 = 0$ then $\beta = \nu_p(n) - 1$, so we have

$$2\binom{n}{2p} \equiv -p^{\nu_p(n)-1} \left\lfloor \frac{n}{p^{\nu_p(n)}} \right\rfloor = -\frac{n}{p} \equiv \frac{n}{p}\left(\frac{n}{p} - 1\right) \mod p^{\nu_p(n)}. \qquad \square$$

Since $\operatorname{frac}(\frac{2}{n}\binom{n}{2p}) = \operatorname{frac}(\frac{n_1-1}{p})\delta_{p|n}$, it follows that, for a given n and p, $\operatorname{frac}(\frac{1}{n}\binom{n}{2p})$ is either $\operatorname{frac}(\frac{n_1-1}{2p}\delta_{p|n})$ or $\operatorname{frac}(\frac{n_1-1}{2p}\delta_{p|n}+\frac{1}{2})$, depending on whether $\frac{2}{n}\binom{n}{2p} - \frac{n_1-1}{p}\delta_{p|n}$ is even or odd. For example, if $p = 3$ then $\frac{2}{n}\binom{n}{2p} - \frac{n_1-1}{p}\delta_{p|n}$ is even unless n is congruent to one of

$$8, 9, 14, 15, 16, 18, 22, 27, 30, 32, 33, 36, 38, 40, 42, 45, 46, 48, 51, 56, 60, 62, 63, 64, 69, 70$$

modulo 72.

However, we can significantly simplify this condition by rewriting the previous proposition instead as $\operatorname{frac}(\frac{2}{n}\binom{n}{2p}) = \operatorname{frac}(\frac{(p+1)(n_1-1)}{p})\delta_{p|n}$. Now $\operatorname{frac}(\frac{1}{n}\binom{n}{2p})$ is either $\operatorname{frac}(\frac{(p+1)(n_1-1)}{p}\delta_{p|n})$ or $\operatorname{frac}(\frac{(p+1)(n_1-1)}{p}\delta_{p|n} + \frac{1}{2})$, depending on whether $\frac{2}{n}\binom{n}{2p} - \frac{(p+1)(n_1-1)}{p}\delta_{p|n}$ is even or odd. Taking $p = 3$ again, $\frac{2}{n}\binom{n}{2p} - \frac{(p+1)(n_1-1)}{p}\delta_{p|n}$ is even unless n is congruent to one of $6, 8$ modulo 8.

The following conjecture claims that we can determine when this second criterion holds — and thereby compute $\operatorname{frac}(\frac{1}{n}\binom{n}{2p})$ — by examining the binary representation of p. Let $\operatorname{mod}(a, b)$ be the number $x \equiv a \mod b$ such that $0 \le x < b$. By '$|m|_0$' we mean the number of zeros in the standard binary representation of m (with no leading zeros). Note however that 'n_1' still refers to the base-p representation of n.

Conjecture 2. *Let $p \neq 2$ be a prime, let $m = 2p$, and let $m_l m_{l-1} \cdots m_1 m_0$ be the standard base-2 representation of m. Let $n \ge 1$. Then*

$$\frac{2}{n}\binom{n}{2p} - \frac{(p+1)(n_1-1)}{p}\delta_{p|n}$$

is odd if and only if

$$n \equiv 2p + \sum_{i=0}^{l} \left\lfloor \frac{j}{2^{|\operatorname{mod}(2p,2^{i+1})|_0 - \delta_{i=1}}} \right\rfloor m_i 2^i \mod 2^{\lfloor \log_2(2p) \rfloor + 1}$$

for some $0 \le j \le 2^{|2p|_0} - 1$.

Letting $\operatorname{exceptional}_{2p}(n)$ be the statement that $\frac{2}{n}\binom{n}{2p} - \frac{(p+1)(n_1-1)}{p}\delta_{p|n}$ is odd, it follows from the conjecture that

$$\operatorname{frac}(\frac{1}{n}\binom{n}{2p}) = \operatorname{frac}(\frac{(p+1)(n_1-1)}{2p}\,\delta_{p|n} + \frac{1}{2}\,\delta_{\operatorname{exceptional}_{2p}(n)}).$$

Let us compute some examples of the exceptional residue classes given by the conjecture. Let $p = 3$. For $j = 0$ we obtain

$$\begin{aligned} n &\equiv 6 + \sum_{i=0}^{2} \left\lfloor \frac{0}{2^{|\operatorname{mod}(6,2^{i+1})|_0 - \delta_{i=1}}} \right\rfloor m_i 2^i \mod 8 \\ &= 6 + 0 \cdot 0 \cdot 2^0 + 0 \cdot 1 \cdot 2^1 + 0 \cdot 1 \cdot 2^2 \\ &= 6. \end{aligned}$$

For $j = 1$ the exceptional residue class is

$$\begin{aligned}
n &\equiv 6 + \sum_{i=0}^{2} \left\lfloor \frac{1}{2^{|\mathrm{mod}(6,2^{i+1})|_0 - \delta_{i=1}}} \right\rfloor m_i 2^i \mod 8 \\
&= 6 + \left\lfloor \frac{1}{2^{|0|_0}} \right\rfloor \cdot 0 \cdot 2^0 + \left\lfloor \frac{1}{2^{|2|_0 - 1}} \right\rfloor \cdot 1 \cdot 2^1 + \left\lfloor \frac{1}{2^{|6|_0}} \right\rfloor \cdot 1 \cdot 2^2 \\
&= 6 + \lfloor 1 \rfloor \cdot 0 \cdot 2^0 + \lfloor 1 \rfloor \cdot 1 \cdot 2^1 + \left\lfloor \frac{1}{2} \right\rfloor \cdot 1 \cdot 2^2 \\
&= 8.
\end{aligned}$$

In general, one can think of the sum in the conjecture as performing an operation similar to the product $\sum_{i=0}^{l} j m_i 2^i$ of $2p$ and j in base 2. For example, let $p = 173$ and $j = 13$. The product $2p \cdot j$ is computed as follows using the standard multiplication algorithm.

$$\begin{array}{r}
101011010_2 \\
\times \qquad\qquad 1101_2 \\
\hline
1101 \\
1101 \\
1101 \\
1101 \\
+\ 1101 \\
\hline
1000110010010_2
\end{array}$$

To compute the expression

$$\sum_{i=0}^{l} \left\lfloor \frac{j}{2^{|\mathrm{mod}(2p,2^{i+1})|_0 - \delta_{i=1}}} \right\rfloor m_i 2^i$$

we truncate and shift each instance of j as follows.

$$\begin{array}{r}
101011010_2 \\
⋇ \qquad\qquad 1101_2 \\
\hline
1101 \\
11\cancel{01} \\
11\cancel{01} \\
1\cancel{101} \\
+\ \cancel{1101} \\
\hline
10100010_2
\end{array}$$

As with Conjecture 1, a proof of Conjecture 2 will undoubtedly provide more context for the result and will perhaps reveal a more natural formulation. We have also not addressed the computational feasibility of computing $\mathrm{frac}(\frac{1}{n}\binom{n}{2p})$ using Conjecture 2. In particular, there is no obvious way of quickly determining whether there is an appropriate j establishing that n belongs to an exceptional residue class.

However, Conjecture 2 is suggestive in its departure from traditional results for prime power moduli. The immediate question is whether it can be generalized to $\mathrm{frac}(\frac{1}{n}\binom{n}{pq})$. The author does not know the answer.

Acknowledgement

I would like to thank Andrew Granville for several discussions about the arithmetic of binomial coefficients.

References

[1] Jean-Paul Allouche and Jeffrey Shallit, The ring of k-regular sequences, *Theoretical Computer Science* **98** (1992) 163–197.
[2] Tewodros Amdeberhan and Richard Stanley, Polynomial coefficient enumeration, `http://arxiv.org/abs/0811.3652v1`.
[3] Kenneth Davis and William Webb, Pascal's triangle modulo 4, *The Fibonacci Quarterly* **29** (1989) 79–83.
[4] Leonard Dickson, Divisibility of factorials and multinomial coefficients (Chapter IX), *History of the Theory of Numbers* **I** (1919), Chelsea Publishing Company, New York.
[5] Nathan Fine, Binomial coefficients modulo a prime, *The American Mathematical Monthly* **54** (1947) 589–592.
[6] Richard Garfield and Herbert Wilf, The distribution of the binomial coefficients modulo p, *Journal of Number Theory* **41** (1992) 1–5.
[7] James Glaisher, On the residue of a binomial-theorem coefficient with respect to a prime modulus, *Quarterly Journal of Pure and Applied Mathematics* **30** (1899) 150–156.
[8] Andrew Granville, Zaphod Beeblebrox's brain and the fifty-ninth row of Pascal's triangle, *The American Mathematical Monthly* **99** (1992) 318–331.
[9] Andrew Granville, Correction to: Zaphod Beeblebrox's brain and the fifty-ninth row of Pascal's triangle, *The American Mathematical Monthly* **104** (1997) 848–851.
[10] Andrew Granville, Binomial coefficients modulo prime powers, *Canadian Mathematical Society Conference Proceedings* **20** (1997) 253–275.
[11] Erhard Hexel and Horst Sachs, Counting residues modulo a prime in Pascal's triangle, *Indian Journal of Mathematics* **20** (1978) 91–105.
[12] James Huard, Blair Spearman, and Kenneth Williams, Pascal's triangle (mod 8), *European Journal of Combinatorics* **19** (1998) 45–62.
[13] Ernst Kummer, Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen, *Journal für die reine und angewandte Mathematik* **44** (1852) 93–146.
[14] Chi-Jen Lu and Shi-Chun Tsai, The periodic property of binomial coefficients modulo m and its applications, 10th SIAM Conference on Discrete Mathematics (2000), Minneapolis, Minnesota, USA.
[15] Édouard Lucas, Sur les congruences des nombres eulériens et les coefficients différentiels des functions trigonométriques suivant un module premier, *Bulletin de la Société Mathématique de France* **6** (1878) 49–54.
[16] Eric Rowland, The number of nonzero binomial coefficients modulo p^α, `http://arxiv.org/abs/1001.1783`.

Mathematics Department, Tulane University, New Orleans, LA 70118, USA