Two Theorems on Binomial Coefficients

Karen Ge

August 26, 2016

Abstract

Given natural numbers $m$ and $n$ and a prime $p$, is the binomial coefficient $\binom{m+n}{n}$ divisible by $p$? If so, what is the highest power of $p$ that divides $\binom{m+n}{n}$? If it is not divisible by $p$, then what is its remainder modulo $p$? We investigate this question with the help of Kummer’s Theorem and Lucas’ Theorem.

Keywords: binomial coefficients, $p$-adic valuation, Pascal’s triangle, Kummer’s Theorem, Lucas’ Theorem

1 Introduction

We will investigate the following question throughout this talk.

Question. Is $\binom{1749}{355}$ divisible by 5? Furthermore,

A. If it is divisible by 5, then what is the largest integer $v$ such that $5^v | \binom{1749}{355}$?
B. If it is not divisible by 5, then what is its remainder when divided by 5?

Part A of the question above can be answered using elementary calculation. We start with a definition. Given a non-zero integer $n$ and a prime $p$, we define the $p$-adic valuation of $n$ as the highest power of $p$ that divides $n$, and write it as $v_p(n)$. For example, the 5-adic valuation of 355! is:

$$v_5(355!) = \left\lfloor \frac{355}{5} \right\rfloor + \left\lfloor \frac{355}{5^2} \right\rfloor + \left\lfloor \frac{355}{5^3} \right\rfloor + \left\lfloor \frac{355}{5^4} \right\rfloor = 71 + 14 + 2 + 0 = 87.$$  

In general, for any non-zero integer $n$ and prime number $p$, we have

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$
Solution to Part A. Let $N = \binom{1749}{355}$. We are asked to find $v_5(N)$. Since $\binom{1749}{355} = \frac{1749!}{355! \cdot 1394!}$, we have $v_5(N) = v_5(1749!) - [v_5(355!) + v_5(1394!)]$.

$$v_5(1749!) = \left\lfloor \frac{1749}{5} \right\rfloor + \left\lfloor \frac{1749}{25} \right\rfloor + \left\lfloor \frac{1749}{125} \right\rfloor + \left\lfloor \frac{1749}{625} \right\rfloor + \left\lfloor \frac{1749}{3125} \right\rfloor = 349 + 69 + 13 + 2 + 0 = 433,$$

$$v_5(1394!) = \left\lfloor \frac{1394}{5} \right\rfloor + \left\lfloor \frac{1394}{25} \right\rfloor + \left\lfloor \frac{1394}{125} \right\rfloor + \left\lfloor \frac{1394}{625} \right\rfloor + \left\lfloor \frac{1394}{3125} \right\rfloor = 278 + 55 + 11 + 2 + 0 = 346.$$

Recall from our previous example that $v_5(355!) = 87$. Now we have

$$v_5(N) = v_5(1749!) - (v_5(355!) + v_5(1394!)) = 433 - 346 - 87 = 0.$$

Thus, the largest integer $v$ such that $5^v | \binom{1749}{355}$ is $0$. That is, $\binom{1749}{355}$ is not divisible by $5$.

In the next section, we will introduce Kummer’s Theorem. It gives us a shortcut to answer Part A.

## 2 Kummer’s Theorem

**Theorem 1 (Kummer’s Theorem).** Let $m, n$ be natural numbers and $p$ be a prime. Then $v_p(\binom{m+n}{n})$ is the number of carries when adding $m$ and $n$ in base $p$.

**Solution to Part A using Kummer’s Theorem.** In base $5$,

$$1394 = 210345, \text{ and } 355 = 24105.$$

Adding these two numbers gives no carries in base $5$, so

$$v_5 \left( \binom{1394 + 355}{355} \right) = v_5 \left( \binom{1749}{355} \right) = 0.$$

Theorem 1 holds for our specific example, but is it true in general? The answer is yes, and we will give a proof of Kummer’s Theorem using Legendre’s Formula.
Theorem 2 (Legendre’s Formula). Let \( n \) be a natural number and \( p \) be a prime. Let \( s_p(n) \) be the sum of the digits of \( n \) in base \( p \). Then

\[
v_p(n!) = \frac{n - s_p(n)}{p - 1}.
\]

Proof of Legendre’s Formula. Let the base \( p \) representation of \( n \) be

\[
a_k p^k + a_{k-1} p^{k-1} + \cdots + a_0.
\]

Note that \( s_p(n) \) is just \( a_k + a_{k-1} + \cdots + a_0 \). By our observation in the introduction,

\[
v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots
\]

\[
= (a_k p^{k-1} + a_{k-1} p^{k-2} + \cdots + a_1)
\]

\[
+ (a_k p^{k-2} + a_{k-1} p^{k-3} + \cdots + a_2) + \cdots + (a_k p + a_{k-1}) + a_k
\]

\[
= a_k (p^{k-1} + p^{k-2} + \cdots + 1) + a_{k-1} (p^{k-2} + \cdots + 1) + \cdots + a_1
\]

\[
= a_k \frac{p^k - 1}{p - 1} + a_{k-1} \frac{p^{k-1} - 1}{p - 1} + \cdots + a_1
\]

\[
= a_k \frac{(p^k - 1)}{p - 1}
\]

\[
= \frac{a_k p^k + a_{k-1} p^{k-1} + \cdots + a_1 p + a_0 - (a_k + a_{k-1} + \cdots + a_0)}{p - 1}
\]

\[
= \frac{n - (a_k + a_{k-1} + \cdots + a_0)}{p - 1}
\]

\[
= \frac{n - s_p(n)}{p - 1}.
\]

Now we are ready to prove Kummer’s Theorem.

Proof of Kummer’s Theorem. First we write each of \( m + n, m, \) and \( n \) in base \( p \).

\[
m + n = a_r p^r + a_{r-1} p^{r-1} + \cdots + a_1 p + a_0,
\]

\[
m = b_r p^r + b_{r-1} p^{r-1} + \cdots + b_1 p + b_0,
\]

\[
n = c_r p^r + c_{r-1} p^{r-1} + \cdots + c_1 p + c_0.
\]
Note that we can assume \( m + n, m, \) and \( n \) all have \( r \) digits in base \( p \) by adding leading 0’s. We define the carry function \( \gamma: \gamma_0 = 0 \) if \( b_0 + c_0 < p \) and \( \gamma_0 = 1 \) otherwise. For \( 1 \leq i < r \), we define
\[
\gamma_i = \begin{cases} 
1 & \text{if } b_i + c_i + \gamma_{i-1} \geq p, \\
0 & \text{if } b_i + c_i + \gamma_{i-1} < p.
\end{cases}
\]

Note that since \( a_r \) is the leading coefficient of \( m + n \) in base \( p \), \( \gamma_r = 0 \) and \( a_r = b_r + c_r + \gamma_{r-1} \). Comparing the digits of \( m + n, m, \) and \( n \) in base \( p \), we see that
\[
a_0 = b_0 + c_0 - p\gamma_0, \\
a_i = b_i + c_i + \gamma_{i-1} - p\gamma_i, \quad \text{for all } 1 \leq i \leq r - 1.
\]

Therefore, by Legendre’s Formula, we have
\[
\nu_p\left(\binom{m+n}{n}\right) = \nu_p((m+n)!) - \nu_p(m!) - \nu_p(n!) \\
= \frac{m+n - s_p(m+n)}{p-1} - \frac{m - s_p(m)}{p-1} - \frac{n - s_p(n)}{p-1} \\
= \frac{s_p(m) + s_p(n) - s_p(m+n)}{p-1} \\
= \frac{\gamma_0 + (p\gamma_1 - \gamma_0) + \cdots + (p\gamma_{r-1} - \gamma_{r-2}) - \gamma_{r-1}}{p-1} \\
= \gamma_0 + \gamma_1 + \cdots + \gamma_{r-1}.
\]

That is, \( \nu_p\left(\binom{m+n}{n}\right) \) is the number of carries when adding \( m \) and \( n \) in base \( p \). \( \square \)

Since we know that \( \binom{1749}{355} \) is not divisible by 5, we would naturally like to know what its remainder is when divided by 5. To answer Part B of our question, we need Lucas’ Theorem.

### 3 Lucas’ Theorem

Before we dive into Lucas’ Theorem, let’s first prove a lemma.
Lemma. For any natural number \( n \) and any prime \( p \), we have

\[
(1 + x)^p \equiv 1 + x^p \pmod{p}.
\]

Proof. For any \( 1 < k < p^n \), we have

\[
\binom{p^n}{k} = \frac{p^n!}{k!(p^n - k)!} = \frac{p^n}{k} \binom{p^n - 1}{k - 1}.
\]

That is,

\[
k \binom{p^n}{k} = p^n \binom{p^n - 1}{k - 1}.
\]

Since \( 1 < k < p^n \), at most \( n - 1 \) powers of \( p \) divide \( k \). But at least \( n \) powers of \( p \) divide the RHS. Thus \( p \) must divide \( \binom{p^n}{k} \). That is, \( \binom{p^n}{k} \equiv 0 \pmod{p} \).

Now we expand \( (1 + x)^{p^n} \) using the binomial theorem and see that the coefficients of all the terms other than the first and the last are 0 modulo \( p \). Thus,

\[
(1 + x)^{p^n} \equiv 1 + x^{p^n} \pmod{p}. \quad \square
\]

Question Part B. What is the remainder when \( \binom{1749}{355} \) is divided by 5?

Solution to Part B. When we write 1749 and 355 in base 5, we get:

\[
1749 = 2 \cdot 5^4 + 3 \cdot 5^3 + 4 \cdot 5^2 + 4 \cdot 5^1 + 4,
\]

\[
355 = 2 \cdot 5^3 + 4 \cdot 5^2 + 1 \cdot 5^1 + 0.
\]

Therefore, by our lemma,

\[
(1 + x)^{1749} = (1 + x)^{2 \cdot 5^4 + 3 \cdot 5^3 + 4 \cdot 5^2 + 4 \cdot 5^1 + 4}
\]

\[
= (1 + x)^{2 \cdot 625} (1 + x)^{3 \cdot 125} (1 + x)^{4 \cdot 25} (1 + x)^{4 \cdot 5} (1 + x)^4
\]

\[
\equiv (1 + x)^{625} (1 + x)^{125} (1 + x)^{25} (1 + x)^5 (1 + x)^4 \pmod{5}.
\]

Similarly, we have

\[
(1 + x)^{355} = (1 + x)^{2 \cdot 5^3 + 4 \cdot 5^2 + 1 \cdot 5^1 + 0}
\]

\[
= (1 + x)^{2 \cdot 125} (1 + x)^{4 \cdot 25} (1 + x)^{1 \cdot 5} (1 + x)^0
\]

\[
\equiv (1 + x)^{125} (1 + x)^{25} (1 + x)^{10} (1 + x)^0 \pmod{5}.
\]
Note that $\binom{1749}{355}$ is the coefficient of $x^{355}$ in the expansion of $(1 + x)^{1749}$. We see that $(1 + x)^{1749}$ has two terms of $x^{625}$, three terms of $x^{125}$, four terms each of $x^{25}$, $x^5$, and $x$. We note that a term of $x^{355}$ is generated by using exactly zero terms of $x^{625}$, two terms of $x^{125}$, four terms of $x^{25}$, one term of $x^5$, and zero terms of $x$. Thus, the coefficient of $x^{355}$ is:

$$\binom{1749}{355} \equiv \binom{2}{0} \binom{3}{2} \binom{4}{4} \binom{4}{1} \binom{4}{0} \equiv 2 \pmod{5}.$$ 

Therefore, $\binom{1749}{355}$ gives a reminder of 2 when divided by 5.

Now are are ready to state and prove Lucas’ Theorem. We note that $\binom{m}{n}$ is defined to be 0 when $m < n$.

**Theorem 3 (Lucas’ Theorem).** Given natural numbers $m$ and $n$ expressed in base $p$,

$$m = m_k p^k + m_{k-1} p^{k-1} + \cdots + m_1 p + m_0,$$

$$n = n_k p^k + n_{k-1} p^{k-1} + \cdots + n_1 p + n_0,$$

where $p$ is a prime, we have

$$\binom{m}{n} \equiv \binom{m_k}{n_k} \binom{m_{k-1}}{n_{k-1}} \cdots \binom{m_0}{n_0} \pmod{p}.$$ 

The investigation above of the Part B of our original question can be generalized to prove Lucas’ Theorem (see Exercise 4). Here we will give a different proof of Lucas’ Theorem using Pascal’s triangle. Recall that the binomial coefficient $\binom{m}{n}$ is the $n$th entry in the $m$th row of Pascal’s triangle. By convention, the top entry of a Pascal’s triangle is the entry at the zeroth row and zeroth column.

**Proof.** Let $m = Mp + i$ and $n = Np + j$. Let’s look at the $p$th row of Pascal’s triangle (mod $p$). By our lemma, it starts and ends with 1 and has $p-1$ 0’s in between. Now let’s look at the $(2p)$th row of Pascal’s triangle. Since each entry of Pascal’s triangle is the sum of the two entries immediately above it, the $(2p)$th row starts with 1, followed by a block of $p-1$ 0’s, followed by 2 in the middle column, followed by a second block of $p-1$ 0’s, and ends with 1 (mod $p$).
Similarly, in base $p$, the $(Mp)$th row of Pascal’s triangle is a copy of the $M$th row of Pascal’s triangle with each entry separated by a block of $p - 1$ 0’s. That is, it looks like this:

\[
\binom{M}{0}00\cdots0\binom{M}{1}00\cdots\binom{M}{N}00\cdots0\binom{M}{M}.
\]

From row $Mp$ to row $Mp+p−1$, $M+1$ small Pascal’s triangles are formed each with the non-zero entry of the $(Mp)$th row as its top entry. For example, the entries in leftmost, or zeroth, small triangle in the $(Mp+i)$th row are:

\[
\binom{i}{0}, \binom{i}{1}, \ldots, \binom{i}{j}, \ldots, \binom{i}{i}.
\]

In general, the entries in the $N$th small triangle in the $(Mp+i)$th row are:

\[
\binom{M}{N}\binom{i}{0}, \binom{M}{N}\binom{i}{1}, \ldots, \binom{M}{N}\binom{i}{j}, \ldots, \binom{M}{N}\binom{i}{i}.
\]

Since $m = Mp + i$ and $n = Np + j$, the binomial coefficient $\binom{m}{n}$ is the $j$th entry in the $N$th small triangle in the $(Mp+i)$th row of Pascal’s triangle. It is exactly the entry with value $\binom{M}{N}\binom{i}{j}$. Therefore,

\[
\binom{Mp+i}{Np+j} \equiv \binom{M}{N}\binom{i}{j}, \pmod{p}.
\]

Now Lucas’ Theorem follows by induction. \qed

## 4 Exercises

0. Why is $\binom{m}{n}$ an integer when $m, n$ are natural numbers?

1. Is the binomial coefficient $\binom{125}{64}$ divisible by 10? If so, how many trailing zeros does it have? If not, what is its last digit in base 10?

2. Let $a, b$ be natural numbers and $p$ be a prime. Prove that

\[
\binom{pa}{pb} \equiv \binom{a}{b} \pmod{p}.
\]

3. Compute the last digit of $\binom{250}{125}$ in base 10.

4. Give an alternate proof of Lucas’ Theorem.
5. Consider a number line consisting of all positive integers greater than 7. Olaf traverses the number line, starting from 8 and working up. He checks each positive integer \( n \) and marks it if and only if \( \binom{n}{7} \) is divisible by 12. As Olaf marks more and more numbers, the fraction of checked numbers that are marked approaches a fixed number \( \rho \). What is \( \rho \)?

5 References
