Lucas' Theorem

Lucas' theorem is a result about binomial coefficients modulo a prime p. It answers questions like:

- For which m and n is $\binom{m}{n}$ even?
- What is the remainder when a binomial coefficient like $\binom{100}{30}$ is divided by a prime number like 13?
- How many entries in the 34^{th} row of Pascal's triangle are divisible by 11? Which entries are not? What are they cong to mod 11?

Contents

Statement of the Theorem

Lucas' theorem states that for non-negative integers m and n, and a prime p,

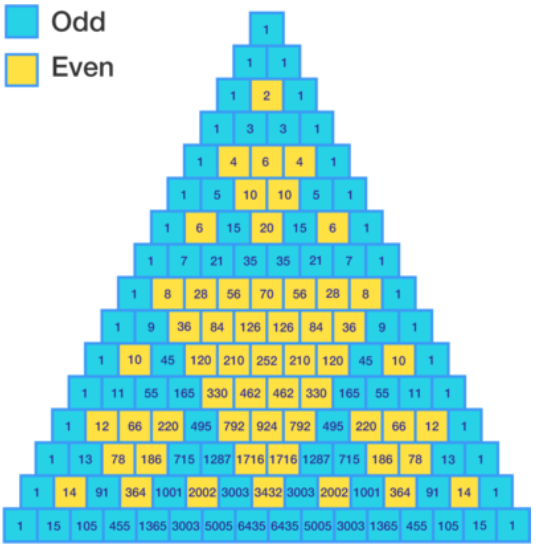
$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \pmod{p},$$

where $m = m_k p^k + m_{k-1} p^{k-1} + \cdots + m_1 p + m_0$ and $n = n_k p^k + n_{k-1} p^{k-1} + \cdots + n_1 p + n_0$ are the base p expansions of m and n, respectively. This uses the convention that $\binom{m}{n}$=0 when $m < n$.

In particular, $\binom{m}{n}$ is divisible by p if and only if **at least one** of the base-p digits of n is greater than the corresponding digit of m.

To look at a tangible example, take $p = 2$. Then $\binom{m}{n}$ is even if and only if **at least one** of the binary digits of n is greate corresponding binary digits of m. So, $\binom{8}{3} = 56$ is even because $3 = 0011_2$ has a greater digit than $8 = 1000_2$ (spec rightmost digit).

Another interesting consequence is that $\binom{2^k-1}{m}$ is always odd, since $2^k - 1$ is all 1s when written in binary; e.g., $\binom{31}{m}$ is odd.



Applications

One of the most common problems to tackle is a direct application of Lucas' theorem: what is the remainder of a binc coefficient when divided by a prime number?

EXAMPLE

Find the remainder when $\binom{1000}{300}$ is divided by 13.

We first write both 1000 and 300 in terms of the sum of powers of 13:

$$1000 = 5(13^2) + 11(13) + 12 \quad \text{and} \quad 300 = 1(13^2) + 10(13) + 1.$$

Then apply Lucas' theorem:

$$\begin{aligned} \binom{1000}{300} \equiv \binom{5}{1} \cdot \binom{11}{10} \cdot \binom{12}{1} &\equiv 5 \cdot 11 \cdot 12 \\ &\equiv 5 \cdot (-2) \cdot (-1) \\ &= 10, \end{aligned}$$

implying the remainder is 10. □

Note: Looking deeper, it is possible to further explore these coefficients throughout Pascal's triangle.

TRY IT YOURSELF

- 0
- 2
- 4
- 6

The oranges are stacked as a triangular-based pyramid such that there is one orange on the top, 2 more oranges on the second layer, yet 3 more oranges on the third, and so on until there are 200 pyramidal layers of oranges.

If this big lot is distributed into boxes of 7 oranges each, how many oranges will remain undistributed?

EXAMPLE

Find a formula for the number of entries in the n^{th} row of Pascal's triangle that are not divisible by p, in terms of the expansion of n.

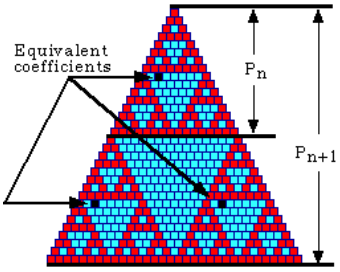
Write $n = n_k p^k + \cdots + n_0$, $r = r_k p^k + \cdots + r_0$. Then $\binom{n}{r}$ is not divisible by p if and only if $r_i \leq n_i$ for $0 \leq i \leq$ are $n_i + 1$ choices for each r_i (it can be $0, 1, \ldots, n_i$). So the answer is

$$\prod_{i=0}^{k} (n_i + 1). \ \square$$

Note that in particular if $n = p^{k+1} - 1$, then all the n_i are equal to $p - 1$, so the product is p^{k+1}; that is, all p^{k+1} of entries in the $\left(p^{k+1} - 1\right)^{\text{th}}$ row are not divisible by p.

In fact, for the previous example, taking $p = 2$ gives the following result:

Picture for $p = 2$: If we draw a picture of the odd entries in the n^{th} row of Pascal's triangle ($p = 2$), we get an image looks very much like the Sierpinski gasket:



source: http://ecademy.agnesscott.edu/~lriddle/ifs/siertri/pascalmath.htm

This fractality comes from the fact that if $k \leq a < 2^n$, then

$$\binom{a}{k} \equiv \binom{a + 2^n}{k} \equiv \binom{a + 2^n}{k + 2^n} \pmod 2$$

by Lucas' theorem, so the top 2^n rows are reproduced twice side-by-side in the next 2^n rows.
What about the middle section? This consists of elements of the form $\binom{a+2^n}{r}$, where $a < r < 2^n$. In this case, since at least one of the binary digits of r will be greater than the corresponding binary digit of a, so that part of the prod Lucas' theorem will be $\binom{0}{1} \equiv 0$, so all of the entries in the middle section will be even.

TRY IT YOURSELF

Find the largest $n < 10,000$ such that $\displaystyle\prod_{k=0}^{n} \binom{n}{k}$ is an odd number.

Submit your answ

EXAMPLE

Show that $\binom{n}{p} \equiv \left\lfloor \frac{n}{p} \right\rfloor \pmod p$.

Let $n = n_k p^k + \cdots + n_1 p + n_0$ be the expansion of n in base p. Then Lucas' theorem says

$$\binom{n}{p} \equiv \binom{n_1}{1}\binom{n_0}{0} \equiv n_1 \pmod p$$

and $\left\lfloor \frac{n}{p} \right\rfloor = n_k p^{k-1} + \cdots + n_1 \equiv n_1 \pmod p$, so both sides are equal. $\square$

TRY IT YOURSELF

What is the remainder when $\binom{2013}{101}$ is divided by 101?

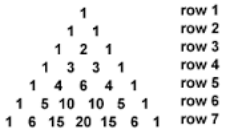
Submit your answ

Hint:
You may use the fact that 101 is a prime.

TRY IT YOURSELF

These are the first few rows of Pascal's triangle:

Submit your answ



Each number is derived by adding up the two numbers just above it (and to the left and right) in the previous row. (The numbers on the ends remain 1).

Of the first 1000 rows, as labeled above, how many of them contain all odd numbers?

Image credit: http://www.daviddarling.info/

Proof of the Theorem

There are several proofs, but the most down-to-earth one proceeds by induction. The idea is to write $n = Np + n_0$, $k = Kp + k_0$ by the division algorithm, and then to prove that

$$\binom{Np+n_0}{Kp+k_0} \equiv \binom{N}{K}\binom{n_0}{k_0} \pmod{p},$$

where $0 \leq n_0, k_0 < p$. The result will follow by induction since N, K are smaller than n, k, respectively, and the base-p expansions of N and K are just the base-p expansions of n and k with the respective rightmost digits omitted.

To see that the formula above is true, write the left side as

$$\frac{(Np+n_0)(\cdots)((N-K)p+n_0-k_0+1)}{(Kp+k_0)!},$$

and separate out the first k_0 terms on top and bottom. These are

$$\frac{(Np+n_0)(\cdots)(Np+n_0-k_0+1)}{(Kp+k_0)(\cdots)(Kp+1)}.$$

The denominator is not divisible by p, so this is just $\binom{n_0}{k_0} \pmod{p}$.

Now the remaining terms come in consecutive groups of p; in each group of p there is one term on top and on bottom divisible by p, and the rest are products of every nonzero element mod p, i.e. $(p-1)!$ mod p. The $(p-1)!$ on top and bottom will cancel mod p, and we can take the p factors out of each of the terms divisible by p. What is left is

$$\begin{cases} \frac{N(N-1)(\cdots)(N-K+1)}{K!} & \text{if } n_0 \geq k_0 \\ \frac{(N-1)(N-2)(\cdots)(N-K)}{K!} & \text{if } n_0 < k_0. \end{cases}$$

So we get

$$\binom{n}{k} = \begin{cases} \binom{N}{K}\binom{n_0}{k_0} & \text{if } n_0 \geq k_0 \\ \binom{N-1}{K}\binom{n_0}{k_0} & \text{if } n_0 < k_0, \end{cases}$$

but in the second case, this also equals $\binom{N}{K}\binom{n_0}{k_0}$ because both are 0. So the theorem is true by induction. $\square$