Cheerful facts about Pascal's triangle

Eric Rowland
Hofstra University

Many Cheerful Facts — Summer Seminar
Hofstra University, 2020–6–8

Binomial coefficients

What do powers of $x + y$ look like?

$$\begin{aligned}
(x+y)^0 &= 1 \\
(x+y)^1 &= x + y \\
(x+y)^2 &= x^2 + 2xy + y^2 \\
(x+y)^3 &= x^3 + 3x^2y + 3xy^2 + y^3 \\
(x+y)^4 &= x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4
\end{aligned}$$

Coefficient of $x^{n-m}y^m$ in $(x+y)^n$:

	$m = 0$	1	2	3	4
$n = 0$	1	0	0	0	0
1	1	1	0	0	0
2	1	2	1	0	0
3	1	3	3	1	0
4	1	4	6	4	1

The number at position (n, m) is denoted $\binom{n}{m}$. For example, $\binom{4}{2} = 6$.

Pascal's triangle

$$\begin{array}{ccccccccc} &&&&1&&&& \\ &&&1&&1&&& \\ &&1&&2&&1&& \\ &1&&3&&3&&1& \\ 1&&4&&6&&4&&1 \end{array}$$

Blaise Pascal (1623–1662)
Portrait by an unknown artist (public domain)

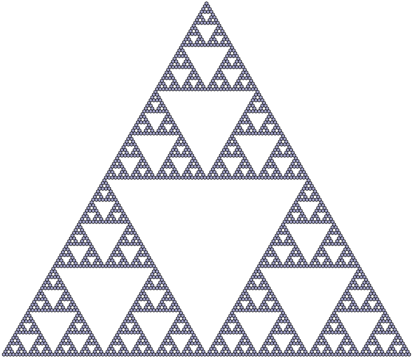
Reflection symmetry: $\binom{n}{m} = \binom{n}{n-m}$. For example, $\binom{4}{1} = 4 = \binom{4}{3}$.

Why?

$$\begin{aligned} \binom{n}{m} &= \text{coefficient of } x^{n-m}y^m \text{ in } (x+y)^n && \text{(definition)} \\ &= \text{coefficient of } y^{n-m}x^m \text{ in } (y+x)^n && \text{(swap } x, y\text{)} \\ &= \text{coefficient of } x^m y^{n-m} \text{ in } (x+y)^n && \text{(rearrange)} \\ &= \binom{n}{n-m}. \end{aligned}$$

Odd binomial coefficients

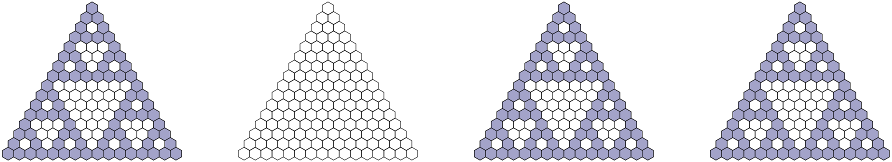
Which numbers in Pascal's triangle are odd? First 128 rows:



This is a fractal — we see the same features on different scales.

Four slices

$\binom{2n+0}{2m+0}$ $\binom{2n+0}{2m+1}$ $\binom{2n+1}{2m+0}$ $\binom{2n+1}{2m+1}$



If $r = 0$ and $s = 1$, then $\binom{2n+r}{2m+s} = \binom{2n+0}{2m+1}$ is even.
Otherwise, $\binom{2n+r}{2m+s}$ has the same parity as $\binom{n}{m}$.

What's special about $r = 0, s = 1$?

$\binom{0}{0} = 1$ $\binom{0}{1} = 0$ $\binom{1}{0} = 1$ $\binom{1}{1} = 1$

Parity

We write $a \equiv b \mod 2$ if a and b have the same parity.

If $0 \leq r \leq 1$ and $0 \leq s \leq 1$, then

$$\binom{2n+r}{2m+s} \equiv \begin{cases} 0 \mod 2 & \text{if } r = 0, s = 1 \\ \binom{n}{m} \mod 2 & \text{otherwise} \end{cases}$$
$$\equiv \binom{n}{m}\binom{r}{s} \mod 2.$$

Can we generalize 2?

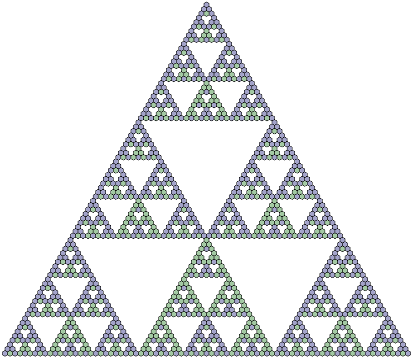
$$\begin{array}{ccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & \cdots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & \cdots \end{array}$$

Even numbers leave remainder 0 when divided by 2;
odd numbers leave remainder 1.

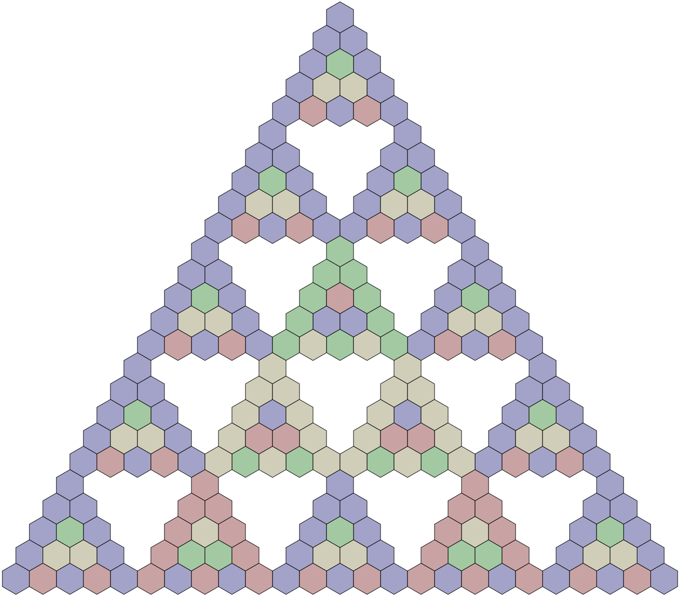
Modulo 3

Every number leaves remainder 0, 1, or 2 when divided by 3.

$$\begin{array}{cccccccc} 0 & 1 & 2 & 3 & 4 & 5 & \cdots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ 0 & 1 & 2 & 0 & 1 & 2 & \cdots \end{array}$$



Modulo 5



Lucas' theorem

$a \equiv b \mod m$ if a and b leave the same remainder when divided by m.

Theorem (Édouard Lucas, 1878)

Let p be a prime number.
If $0 \leq r \leq p-1$, $0 \leq s \leq p-1$, $n \geq 0$, and $m \geq 0$, then

$$\binom{pn+r}{pm+s} \equiv \binom{n}{m}\binom{r}{s} \mod p.$$

Example

Let $p = 5$.
Directly: $\binom{19}{6} = 27132 \equiv 2 \mod 5$.
By Lucas' theorem: $\binom{19}{6} = \binom{3\cdot5+4}{1\cdot5+1} \equiv \binom{3}{1}\binom{4}{1} = 3 \cdot 4 = 12 \equiv 2 \mod 5$.

Iterating Lucas' theorem

Example

Computing $\binom{1956}{1865}$ mod 7 is easy, though $\binom{1956}{1865} \approx 2.88 \times 10^{158}$ is large:

$$\binom{1956}{1865} = \binom{279 \cdot 7 + 3}{266 \cdot 7 + 3} \equiv \binom{39 \cdot 7 + 6}{38 \cdot 7 + 0}\binom{3}{3} \equiv \binom{5 \cdot 7 + 4}{5 \cdot 7 + 3}\binom{6}{0}\binom{3}{3}$$
$$\equiv \binom{5}{5}\binom{4}{3}\binom{6}{0}\binom{3}{3} \equiv 1 \cdot 4 \cdot 1 \cdot 1 = 4 \mod 7.$$

This is equivalent to writing 1956 and 1865 in base 7:

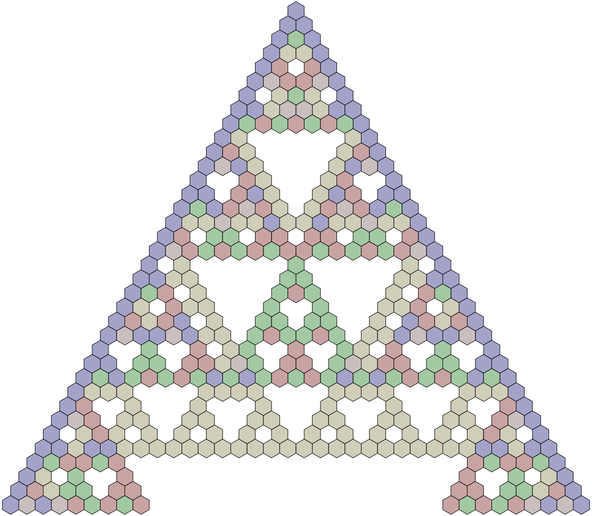
$$1956 = 5 \cdot 7^3 + 4 \cdot 7^2 + 6 \cdot 7 + 3$$
$$1865 = 5 \cdot 7^3 + 3 \cdot 7^2 + 0 \cdot 7 + 3.$$

If $n_\ell, \dots, n_1, n_0, m_\ell, \dots, m_1, m_0$ are numbers between 0 and $p - 1$, then

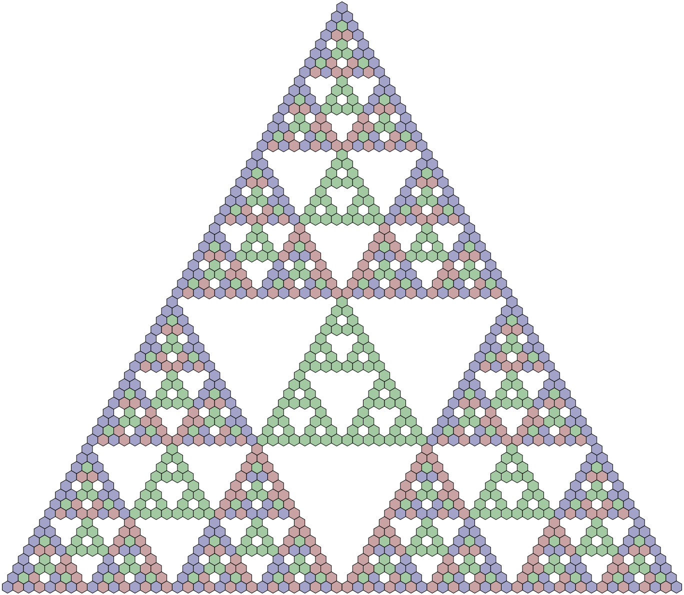
$$\binom{n_\ell p^\ell + \cdots + n_1 p + n_0}{m_\ell p^\ell + \cdots + m_1 p + m_0} \equiv \binom{n_\ell}{m_\ell} \cdots \binom{n_1}{m_1}\binom{n_0}{m_0} \mod p.$$

Modulo 6

What about non-primes?



Modulo 4



Squares of primes

Does Lucas' theorem work modulo p^2?

That is,

$$\binom{pn+r}{pm+s} \stackrel{?}{\equiv} \binom{n}{m}\binom{r}{s} \mod p^{2}.$$

Example

Let $p = 2$.

$$\binom{2\cdot 1+0}{2\cdot 0+1} = \binom{2}{1} = 2 \not\equiv 0 = \binom{1}{0}\binom{0}{1} \mod 4$$

It doesn't work!

Partial generalizations

However, for the digits $r = 0$ and $s = 0$,

$$\binom{pn}{pm} \equiv \binom{n}{m} \mod p^2.$$

$\binom{0}{0} = 1$

Ljunggren (1949): If $p \geq 5$, then

$$\binom{pn}{pm} \equiv \binom{n}{m} \mod p^3.$$

Bailey (1990): If $p \geq 5$, $0 \leq r \leq p - 1$, and $0 \leq s \leq p - 1$, then

$$\binom{p^3 n + r}{p^3 m + s} \equiv \binom{n}{m}\binom{r}{s} \mod p^3.$$

Restricted digits

For which digit pairs (r, s) does Lucas' theorem hold modulo p^2?

Let $D(p)$ be the set of pairs (r, s) such that

$$\binom{pn+r}{pm+s} \equiv \binom{n}{m}\binom{r}{s} \mod p^2$$

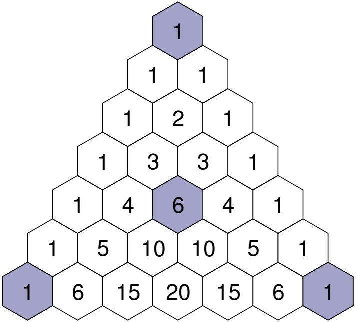
for all $n \geq 0$ and $m \geq 0$.

Experimentally...
$D(2) = \{(0,0)\}$
$D(3) = \{(0,0),(2,0),(2,2)\}$
$D(5) = \{(0,0),(4,0),(4,4)\}$

Since $\binom{pn}{pm} \equiv \binom{n}{m} \mod p^2$, $D(p)$ contains the pair $(0,0)$.

$p = 7$

$D(7) = \{(0,0), (4,2), (6,0), (6,6)\}$



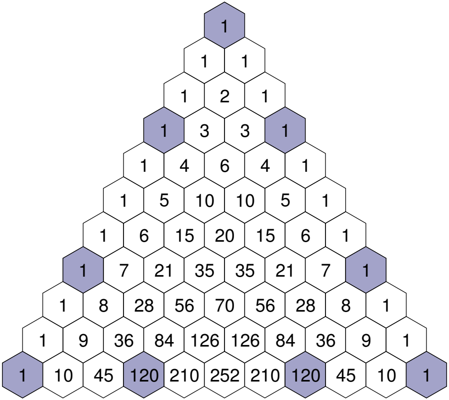
Example

$\binom{12002}{7156} \equiv \binom{4}{2}\binom{6}{6}\binom{6}{6}\binom{6}{0}\binom{4}{2} \equiv 6 \cdot 1 \cdot 1 \cdot 1 \cdot 6 = 36 \mod 7^2.$

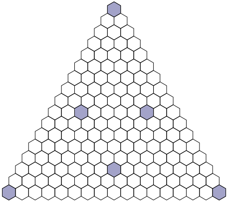
$p = 11$

$D(11) =$

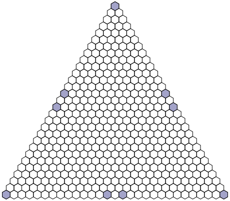
$$\{(0,0),(3,0),(3,3),(7,0),(7,7),(10,0),(10,3),(10,7),(10,10)\}$$



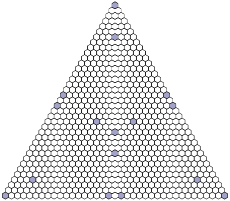
Other primes



$p = 17$



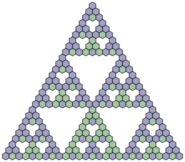
$p = 29$



$p = 37$

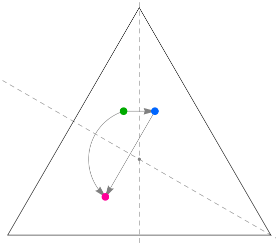
$D(p)$ seems to possess the symmetries of the equilateral triangle!

Reflection symmetry through the vertical axis follows (after a little work) from reflection symmetry in Pascal's triangle.



Rotation

Where does rotation by 120° take a point (r, s)?



The first reflection maps (r, s) to $(r, r - s)$.
The second reflection maps (r, s) to $(p - 1 - r + s, s)$.
The rotation maps (r, s) to $(p - 1 - s, r - s)$.

The three binomial coefficients visited by the orbit of (r, s) are

$$\binom{r}{s}, \binom{p-1-s}{r-s}, \binom{p-1-r+s}{p-1-r}.$$

Lucas' theorem modulo p^2

If $0 \le s \le r \le p - 1$, then

$$\binom{r}{s} \equiv (-1)^{r-s} \binom{p-1-s}{r-s} \mod p.$$

Theorem (Rowland, 2020+)

Let p be a prime number, let $0 \le r \le p-1$, and let $0 \le s \le p-1$. The statement

$$\binom{pn+r}{pm+s} \equiv \binom{n}{m}\binom{r}{s} \mod p^2$$

holds for all $n \ge 0$ and $m \ge 0$ precisely when $s \le r$ and

$$\binom{r}{s} \equiv (-1)^{r-s}\binom{p-1-s}{r-s} \equiv (-1)^{s}\binom{p-1-r+s}{p-1-r} \mod p^2.$$

A general congruence

Let $H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ be the nth harmonic number.

n	0	1	2	3	4	5	6	7	$\cdots$
H_n	0	1	$\frac{3}{2}$	$\frac{11}{6}$	$\frac{25}{12}$	$\frac{137}{60}$	$\frac{49}{20}$	$\frac{363}{140}$	$\cdots$

If $0 \le r \le p-1$, the denominator of H_r is not divisible by p.
So we can interpret H_r modulo p by clearing denominators.

Theorem

Let p be a prime number.
If $0 \le s \le r \le p-1$, $n \ge 0$, and $m \ge 0$, then

$$\binom{pn+r}{pm+s} \equiv \binom{n}{m}\binom{r}{s}\left(1 + pn\left(H_r - H_{r-s}\right) + pm\left(H_{r-s} - H_s\right)\right) \mod p^2.$$

Conversion

Lemma

If $0 \le s \le r \le p-1$*, then* $H_r \equiv H_s \mod p$ *precisely when*

$$\binom{r}{s} \equiv (-1)^{r-s}\binom{p-1-s}{r-s} \mod p^2.$$

Why do harmonic numbers arise? $\binom{n}{m} = \frac{n!}{m!(n-m)!}$

$$\begin{aligned}(p-1-s)! &= \prod_{i=s+1}^{p-1}(p-i) \\ &\equiv \prod_{i=s+1}^{p-1}(-i) + p(-1)^{p-1-s}\frac{(p-1)!}{s!}\sum_{i=s+1}^{p-1}\frac{1}{-i} \mod p^2 \\ &= (-1)^{p-1-s}\frac{(p-1)!}{s!}\left(1 - p\left(H_{p-1} - H_s\right)\right).\end{aligned}$$