Two binomial coefficient conjectures

Eric Rowland

Mathematics Department
Tulane University, New Orleans

May 27, 2010

Outline

1. Counting entries modulo m

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

First question

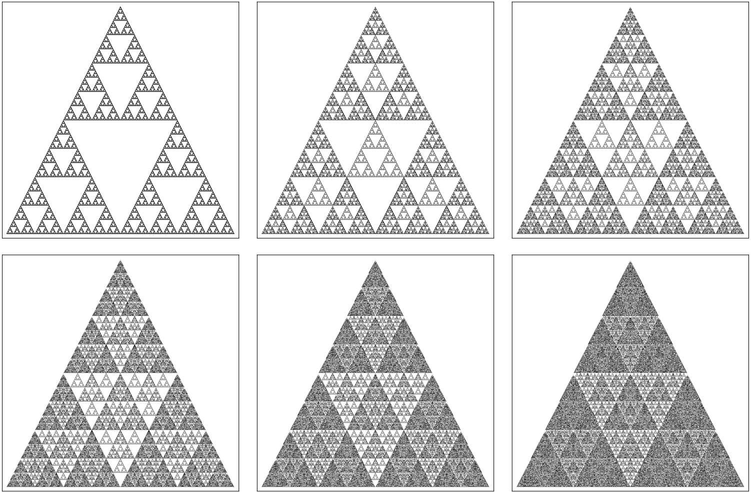
Arithmetic properties of binomial coefficients have a long history, the theorems of Kummer and Lucas being classical results.

Main theme:
Properties of $\binom{n}{m}$ modulo p are related to the base-p representations $n_l n_{l-1} \cdots n_1 n_0$ and $m_l m_{l-1} \cdots m_1 m_0$.

Let $a_{k,r}(n)$ be the number of $0 \leq m \leq n$ such that $\binom{n}{m} \equiv r \mod k$.

What is the structure of $a_{k,r}(n)$?

Binomial coefficients modulo 2^α



Modulo p

Let $|n|_w$ be the number of occurrences of the word w in $n_l n_{l-1} \cdots n_1 n_0$.

- Glaisher, 1899:
  $a_{2,1}(n) = 2^{|n|_1}$
- Hexel and Sachs, 1978:
  - formula for $a_{p,r^i}(n)$ in terms of $(p-1)$th roots of unity
  - $a_{3,1}(n) = 2^{|n|_1 - 1} \cdot \left(3^{|n|_2} + 1\right)$ and $a_{3,2}(n) = 2^{|n|_1 - 1} \cdot \left(3^{|n|_2} - 1\right)$
  - explicit formulas for $a_{5,r^i}(n)$ in terms of $|n|_1$, $|n|_2$, $|n|_3$, and $|n|_4$
- Garfield and Wilf, 1992:
  method to compute the generating function $\sum_{i=0}^{p-2} a_{p,r^i}(n) x^i$
- Amdeberhan and Stanley:
  Let $f(\mathbf{x}) \in \mathbb{F}_q[x_1, \ldots, x_m]$. The number of coefficients in $f(\mathbf{x})^n$ equal to $r \in \mathbb{F}_q^\times$ is a q-regular sequence.

Modulo 4

Davis and Webb, 1991:

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

(Here $|n|_w$ counts occurrences 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.

By Glaisher's result, $a_{2,1}(n) = 2^{|n|_1}$ is (either 0 or) a power of 2.

Granville's paper

"Zaphod Beeblebrox's brain and the fifty-ninth row of Pascal's triangle"

Theorem (Granville, 1992)

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

So what about modulo 16?
The statement fails for $n = 59$!

"Unbelievably, there are exactly six entries of Row 59 in each of the congruence classes 1, 11, 13, and 15 $\pmod{16}$! Our pattern has come to an end, but not before providing us with some interesting mathematics, as well as a couple of pleasant surprises."

Modulo 16

This may not be the end of the story ...

What values does $a_{16,r}(n)$ take for odd r? Up to row 2^{19}:
$\{0, 1, 2, 4, 6, 8, 12, 16, 20, 24, 32, 40, 48, 56, 64, 72, 80, 96, \dots, 65536\}$

Conjecture

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.

Second question

The "high school dream"

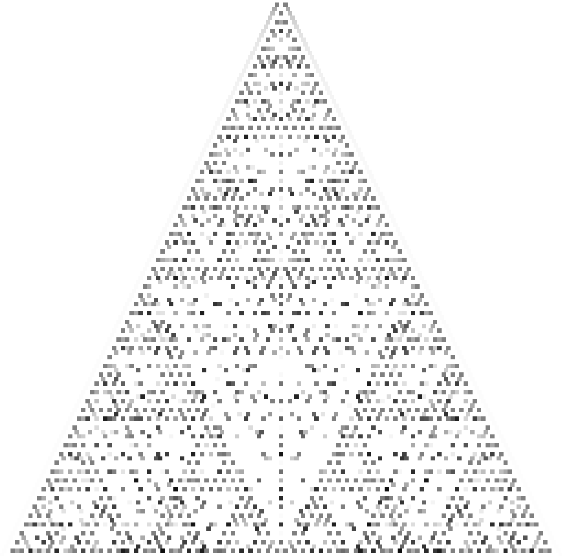
$$(a+b)^n = a^n + b^n$$

actually works sometimes.

Namely, $(a+b)^p \equiv a^p + b^p \mod p$, since $\binom{p}{m} \equiv 0 \mod p$ for $1 \leq m \leq p-1$.

How badly does the high school dream fail for non-primes?
What is $\binom{n}{m} \mod n$?

$\binom{n}{m} \bmod n$



$\binom{n}{p}$ mod n

Rather than fixing n and varying m, let us fix m and vary n.

Let frac(x) be the fractional part of x.
Rather than looking at $\binom{n}{m} \mod n$, let us look at $\mathrm{frac}(\frac{1}{n}\binom{n}{m})$.
For fixed $m \geq 1$, $\mathrm{frac}(\frac{1}{n}\binom{n}{m}) = \mathrm{frac}(\frac{1}{m}\binom{n-1}{m-1})$ is periodic.

Let δ_S be 1 if S is true and 0 if S is false.

Proposition

Let p be a prime, and let $n \geq 1$. Then

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

So $\binom{n}{p} \equiv \frac{n}{p}\delta_{p|n} \mod n$.

$\binom{n}{m} \mod n$

$\binom{n}{2p}$ mod n

What about non-primes? What is $\mathrm{frac}(\frac{1}{n}\binom{n}{2p})$?

Conjecture

Let $p \neq 2$ be a prime, and let $n \geq 1$. Then

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

...where $m_l \cdots m_1 m_0$ is the binary representation of $m = 2p$ and $\mathrm{exceptional}_{2p}(n)$ is the statement that

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

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

Crazy condition

The expression

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

is *almost* the product of $2p$ and j ...

For example, let $p = 197$ and $j = 27$.

$$\begin{array}{r}
110001010_2 \\
\times \qquad\qquad 11011_2 \\
\hline
11011 \\
11011 \\
11011 \\
+\ 11011 \\
\hline
1010011000111 0_2
\end{array}$$

Crazy condition

The expression

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

is *almost* the product of $2p$ and j . . .

. . . except we delete some digits:

$$\begin{array}{lr}
 & 110001010_2 \\
※ & 11011_2 \\ \hline
 & 11011 \\
 & 110\cancel{11} \\
 & \cancel{11011} \\
+ & \cancel{11011} \\ \hline
 & 1100110_2
\end{array}$$