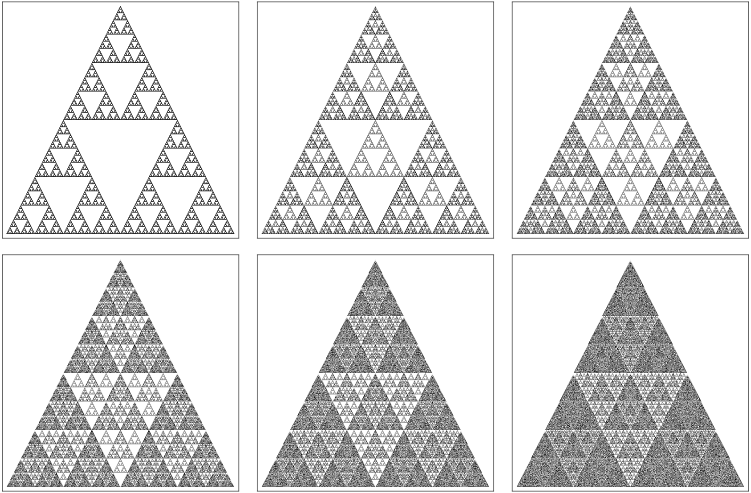
The number of nonzero binomial coefficients modulo p^α

Eric Rowland

Mathematics Department
Tulane University, New Orleans

January 14, 2010

Binomial coefficients modulo 2^α



Notation

Binomial coefficients have many nice arithmetic properties.

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 $m_l m_{l-1} \cdots m_1 m_0$.

Classic results are the theorems of Kummer and Lucas.

Let $a_k(n)$ be the number of nonzero binomial coefficients on row n of Pascal's triangle modulo k.

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: $a_2(n) = 2^{|n|_1}$.

Theorem (Lucas, 1878)

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

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

Theorem (Fine, 1947)

Let p be a prime. For $n \geq 0$, $a_p(n) = \prod_{i=0}^{l} (n_i + 1)$.

Alternate expression: $a_p(n) = \prod_{r=0}^{p-1} (r+1)^{|n|_r}$.
For example, $a_5(n) = 2^{|n|_1} 3^{|n|_2} 4^{|n|_3} 5^{|n|_4}$.

Goal: Generalize Fine's result to prime powers.

Main result

Theorem

Let p be a prime. Let $A_\epsilon(0) = 1$, let $A_\epsilon(\beta) = 0$ for $\beta \geq 1$, and for $n \geq 1$ and $\beta \geq 0$ define $A_n(\beta)$ recursively by

$$A_{n_l n_{l-1} \cdots n_0}(\beta) = (n_l + 1) A_{n_{l-1} \cdots n_0}(\beta) + n_l \sum_{i=1}^{\beta} \left(\prod_{j=1}^{i-1} (p - n_{l-j}) \right) (p - n_{l-i} - 1) A_{n_{l-i-1} \cdots n_0}(\beta - i).$$

For $\alpha \geq 0$ and $n \geq 0$,

$$a_{p^\alpha}(n) = \sum_{\beta=0}^{\alpha-1} A_n(\beta).$$

Proof

Theorem (Kummer, 1852)

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

Therefore, $\binom{n}{m} \not\equiv 0 \mod p^\alpha$ precisely when there are fewer than α borrows in $n - m$.

Let $A_n(\beta)$ be the number of integers $0 \leq m \leq n$ such that there are precisely β borrows involved in computing $n - m$.
Then $a_{p^\alpha}(n) = \sum_{\beta=0}^{\alpha-1} A_n(\beta)$.

Proof

For $n = n_l n_{l-1} \cdots n_0$, let $n' = n_{l-1} \cdots n_0$.
What is the relationship between borrows in $n - m$ and borrows in $n' - m'$?

We must distinguish between $m < n$ and $m > n$:
There is a borrow from n_{l+1} in $n - m$ if and only if $m > n$.

Let $B_n(\beta)$ be the number of integers $n < m \leq p^{l+1} - 1$ such that there are precisely β borrows up through the borrow from $n_{l+1} = 0$ involved in computing $n - m$. Then

$$A_n(\beta) = (n_l + 1)A_{n'}(\beta) + n_l B_{n'}(\beta)$$
$$B_n(\beta) = (p - n_l - 1)A_{n'}(\beta - 1) + (p - n_l)B_{n'}(\beta - 1).$$

$\alpha = 1$ and $\alpha = 2$

Fine's theorem is our first corollary:

$$a_p(n) = A_n(0) = \prod_{i=0}^{l} (n_i + 1) .$$

$\alpha = 2$:

Corollary

For $n \geq 0$,

$$a_{p^2}(n) = \left(\prod_{i=0}^{l} (n_i + 1) \right) \cdot \left(1 + \sum_{i=0}^{l-1} \frac{p - (n_i + 1)}{n_i + 1} \cdot \frac{n_{i+1}}{n_{i+1} + 1} \right) .$$

$\alpha = 2$

$p = 2$ and $p = 3$:

$$a_4(n) = 2^{|n|_1}\left(1 + \frac{1}{2}|n|_{10}\right)$$
$$a_9(n) = 2^{|n|_1}3^{|n|_2}\left(1 + |n|_{10} + \frac{1}{4}|n|_{11} + \frac{4}{3}|n|_{20} + \frac{1}{3}|n|_{21}\right)$$

$p = 5$:

$$\frac{a_{25}(n)}{2^{|n|_1}3^{|n|_2}4^{|n|_3}5^{|n|_4}} = 1 + 2|n|_{10} + \frac{3}{4}|n|_{11} + \frac{1}{3}|n|_{12} + \frac{1}{8}|n|_{13} + \frac{8}{3}|n|_{20} + |n|_{21} + \frac{4}{9}|n|_{22} + \frac{1}{6}|n|_{23} + 3|n|_{30} + \frac{9}{8}|n|_{31} + \frac{1}{2}|n|_{32} + \frac{3}{16}|n|_{33} + \frac{16}{5}|n|_{40} + \frac{6}{5}|n|_{41} + \frac{8}{15}|n|_{42} + \frac{1}{5}|n|_{43}$$

$\alpha = 3$

For $\alpha \geq 3$ the expression for $a_{p^\alpha}(n)$ contains nested sums. However, we can still evaluate in terms of $|n|_w$.

$p = 2$:

$$a_8(n) = 2^{|n|_1} \left(1 + \frac{1}{8}|n|_{10}^2 + \frac{3}{8}|n|_{10} + |n|_{100} + \frac{1}{4}|n|_{110}\right)$$

Formulas for other p can be found similarly.

$\alpha = 4$

The expression for $\alpha \geq 4$ can also be evaluated.

$p = 2$:

$$\begin{aligned}\frac{a_{16}(n)}{2^{|n|_1}} = 1 &+ \frac{5}{12}|n|_{10} + \frac{1}{2}|n|_{100} + \frac{1}{8}|n|_{110} \\ &+ 2|n|_{1000} + \frac{1}{2}|n|_{1010} + \frac{1}{2}|n|_{1100} + \frac{1}{8}|n|_{1110} + \frac{1}{16}|n|_{10}^2 \\ &+ \frac{1}{2}|n|_{10}|n|_{100} + \frac{1}{8}|n|_{10}|n|_{110} + \frac{1}{48}|n|_{10}^3\end{aligned}$$