Appendix 3A: Factoring binomial coefficients, and Pascal's Triangle mod p

3.10. The prime powers dividing a given binomial coefficient

Lemma 3.10.1. *The power of prime p that divides $n!$ is $\sum_{k\geq 1}[n/p^k]$. In other words*

$$n! = \prod_{p\ prime} p^{\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\dots}$$

Proof. We wish to determine the power of p dividing $n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n$. If p^k is the power of p dividing m then we will count 1 for p dividing m, then 1 for p^2 dividing m,..., and finally 1 for p^k dividing m. Therefore the power of p dividing $n!$ equals the number of integers m, $1 \leq m \leq n$ that are divisible by p, plus the number of integers m, $1 \leq m \leq n$ that are divisible by p^2, plus etc. The result follows as there are $[n/p^j]$ integers m, $1 \leq m \leq n$, that are divisible by p^j for each $j \geq 1$, by exercise 1.7.6(c). $\square$

Exercise 3.10.1. Write $n = n_0 + n_1 p + \ldots + n_d p^d$ in base p so that each $n_j \in \{0, 1, \ldots, p-1\}$.

(a) Prove that $[n/p^k] = (n - (n_0 + n_1 p + \ldots + n_{k-1}p^{k-1}))/p^k$.
The *sum of the digits of n in base p* is defined to be $s_p(n) := n_0 + n_1 + \ldots + n_d$.

(b) Prove that the exact power of prime p that divides $n!$ is $\frac{n - s_p(n)}{p-1}$.

Theorem 3.7 (Kummer's Theorem)**.** *The largest power of prime p that divides the binomial coefficient $\binom{a+b}{a}$ is given by the number of carries when adding a and b in base p.*

Example: To recover the factorization of $\binom{14}{6}$ we add 6 and 8 in each prime base ≤ 14:

$$\begin{array}{cccccc} 0101 & 020 & 11 & 06 & 06 & 06 \\ \underline{1000_2} & \underline{022_3} & \underline{13_5} & \underline{11_7} & \underline{08_{11}} & \underline{08_{13}} \\ 1101 & 112 & 24 & 20 & 13 & 11 \end{array}$$

We see that there are no carries in base 2, 1 carry in base 3, no carries in base 5, 1 carry in base 7, 1 carry in base 11, and 1 carry in base 13, so we deduce that $\binom{14}{6} = 3^1 \cdot 7^1 \cdot 11^1 \cdot 13^1$.

Proof. For given integer $k \geq 1$, let $q = p^k$. Then let A and B be the least non-negative residue of a and b (mod q), respectively, so that $0 \leq A, B \leq q-1$. Note that A and B give the first k digits (from the right) of a and b in base p. If C is the first k digits of $a+b$ in base p then C is the least non-negative residue of $a+b$ (mod q), that is of $A+B$ (mod q). Now $0 \leq A+B < 2q$:

• If $A+B < q$ then $C = A+B$ and there is no carry in the kth digit when we add a and b in base p.

• If $A+B \geq q$ then $C = A+B-q$ and so there is a carry of 1 in the kth digit when we add a and b in base p.

We need to relate these observations to the formula in Lemma 3.10.1. The trick comes in noticing that $A = a - p^k \left[\frac{a}{p^k}\right]$, and similarly $B = b - p^k \left[\frac{b}{p^k}\right]$ and $C = a + b - p^k \left[\frac{a+b}{p^k}\right]$. Therefore

$$\left[\frac{a+b}{p^k}\right] - \left[\frac{a}{p^k}\right] - \left[\frac{b}{p^k}\right] = \frac{A+B-C}{p^k} = \begin{cases} 1 & \text{if there is a carry in the kth digit;} \\ 0 & \text{if not;} \end{cases}$$

and so

$$\sum_{k \geq 1} \left(\left[\frac{a+b}{p^k}\right] - \left[\frac{a}{p^k}\right] - \left[\frac{b}{p^k}\right] \right)$$

equals the number of carries when adding a and b in base p. However Lemma 3.10.1 implies that this also equals the exact power of p dividing $\frac{(a+b)!}{a!b!} = \binom{a+b}{a}$, and the result follows. □

Exercise 3.10.2. State, with proof, the analogy to Kummer's Theorem for trinomial coefficients $n!/(a!b!c!)$ where $a+b+c=n$.

Corollary 3.10.1. *If p^e divides the binomial coefficient $\binom{n}{m}$ then $p^e \leq n$.*

Proof. There are $k+1$ digits in the base p expansion of n when $p^k \leq n < p^{k+1}$. When adding m and $n-m$ there can be carries in every digit except the $(k+1)$st (which corresponds to the number of multiples of p^k). Therefore there are no more than k carries when adding m to $n-m$ in base p, and so the result follows from Kummer's Theorem. □

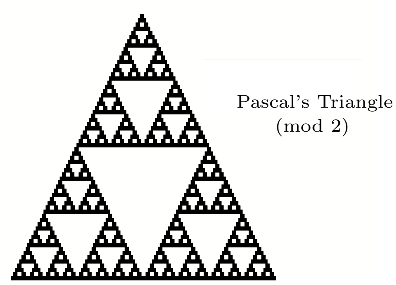
Exercise 3.10.3. Prove that if $0 \leq k \leq n$ then $\binom{n}{k}$ divides $\mathrm{lcm}[m : m \leq n]$.

3.11. Pascal's Triangle mod 2

In section 0.3 we explained the theory and practice of constructing Pascal's Triangle. We are now interested in constructing Pascal's Triangle modulo 2, mod 3, mod 4, etc. To do so one can either reduce the binomial coefficients mod m (for $m = 2, 3, 4, \ldots$), or one can rework Pascal's Triangle, starting with a 1 in the top row and then obtaining a row from the previous one by adding the two entries immediately above the given entry, modulo m. For example, Pascal's Triangle mod 2, starts with the rows

$$\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 0 & & 1 & & & & \\
 & & & 1 & & 1 & & 1 & & 1 & & & \\
 & & 1 & & 0 & & 0 & & 0 & & 1 & & \\
 & 1 & & 1 & & 0 & & 0 & & 1 & & 1 & \\
1 & & 0 & & 1 & & 0 & & 1 & & 0 & & 1
\end{array}$$

It is perhaps easiest to visualize this by replacing 1 (mod 2) by a dark square; and otherwise, a white square, as in the following fascinating diagram:[13]



One can see patterns emerging. For example the rows corresponding to $n = 1, 3, 7, 15, \ldots$ are all 1's, and the next rows, $n = 2, 4, 8, 16, \ldots$ start and end with a 1, and have all 0's in-between. Even more: The two 1's at either end of row $n = 4$ seem to each be the first entry of a (four line) triangle, which is an exact copy of the first four rows of Pascal's Triangle mod 2. Similarly the two 1's at either end of row $n = 8$, and the eight-line triangles beneath (and including) them. In general if T_k denotes the top 2^k rows of Pascal's triangle mod 2, then T_{k+1} is given by a triangle of copies of T_k, with an inverted triangle of zeros in the middle, as in the following diagram:

[13]These and other images in this section reproduced from `http://www-math.ucdenver.edu/~wcherowi/jcorm5.html`, with kind permission of Bill Cherowitzo

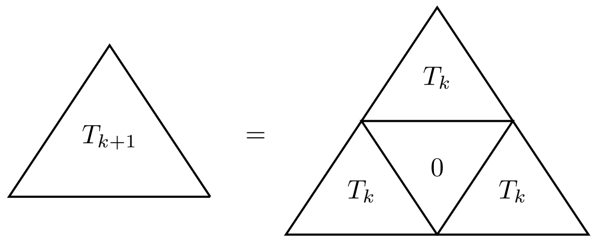
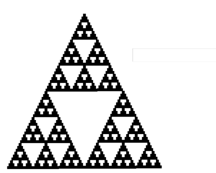


Figure 1. The top 2^{k+1} rows of Pascal's Triangle mod 2, in terms of the top 2^k rows.

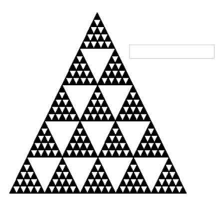
This is called *self-similarity*. One immediate consequence is that one can determine the number of 1's in a given row: If $2^k \leq n < 2^{k+1}$ then row n consists of two copies of row m $(:= n - 2^k)$ with some 0's in-between.

Exercise 3.11.1. Prove that there are 2^k odd entries in the nth row of Pascal's triangle, where $k = s_2(n)$, the number of 1's in the binary expansion of n.

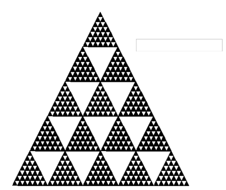
This self-similarity generalizes nicely for other primes p, where we again replace integers divisible by p by a white square, and those not divisible by p by a black square.



Pascal's Triangle (mod 3)



Pascal's Triangle (mod 5)



Pascal's Triangle (mod 7)

The top p rows are all black since the entries $\binom{n}{m}$ with $0 \leq m \leq n \leq p-1$ are never divisible by p. Let T_k denote the top p^k rows of Pascal's triangle. Then T_{k+1} is given by an array of p rows of triangles, in which the nth row contains n copies of T_k, with inverted triangles of 0's in-between.

Pascal's Triangle modulo primes p is a bit more complicated; we wish to color in the black squares with one of $p-1$ colors, each representing a different reduced residue class mod p. Call the top row, the 0th row, and the leftmost entry of the each row, its 0th entry. Therefore the mth entry of the nth row is $\binom{n}{m}$. By Lucas' Theorem (exercise 2.5.10) the value of $\binom{rp^k+s}{ap^k+b} \pmod p$, which is the bth entry of the sth row of the copy of T_k which is the ath entry of the rth row of the copies of T_k that make up T_{k+1}, is $\equiv \binom{r}{a}\binom{s}{b} \pmod p$. In other words, the values in the copy of T_k which is the ath entry of the rth row of the copies of T_k, are $\binom{r}{a}$ times the values in T_k.

The odd entries in Pascal's Triangle mod 4 make even more interesting patterns, but this will take us too far afield; see [**2**] for a detailed discussion.

Reading each row of Pascal's Triangle mod 2 as the binary expansion of an integer, we obtain the numbers

$$1,\ 11_2 = 3,\ 101_2 = 5,\ 1111_2 = 15,\ 10001_2 = 17,\ 110011_2 = 51,\ 1010101_2 = 85, \ldots$$

Do you recognize these numbers? If you factor them you obtain

$$1, \quad F_0, \quad F_1, \quad F_0F_1 \quad F_2, \quad F_0F_2, \quad F_1F_2, \quad F_0F_1F_2, \ldots$$

where $F_m = 2^{2^m} + 1$ are the Fermat numbers (introduced in exercise 0.4.14). It appears that all are products of Fermat numbers, and one can even guess at which Fermat numbers. For example the 6th row is F_2F_1 and $6 = 2^2+2^1$ in base 2, whereas the 7th row is $F_2F_1F_0$ and $7 = 2^2+2^1+2^0$ in base 2, and our other examples follow this same pattern. This leads to the following challenging problem:

Exercise 3.11.2.† Show that the nth row of Pascal's Triangle mod 2, considered as a binary number, is given by $\prod_{j=0}^{k} F_{n_j}$, where $n = 2^{n_0} + 2^{n_1} + \ldots + 2^{n_k}$, with $0 \le n_0 < n_1 < \ldots < n_k$ (i.e. the binary expansion of n).[14]

References for this chapter

[1] Andrew Granville, *Zaphod Beeblebrox's brain and the fifty-ninth row of Pascal's triangle*, Amer. Math. Monthly **99** (1992), 318–331 (preprint).

[2] Kathleen M. Shannon and Michael J. Bardzell, *Patterns in Pascal's Triangle - with a Twist - First Twist: What is It?*, Convergence (December 2004).

[14] An m-sided regular polygon with m odd is constructible with ruler and compass (see section 0.18 of appendix 0G) if and only if m is the product of distinct Fermat primes. Therefore the integers m created here include all of the odd m-sided, constructible, regular polygons.