PASCAL'S TRIANGLE MODULO p

CALVIN T. LONG
Washington State University, Pullman, WA 99164

1. INTRODUCTION

In "Mathematical Games" in the December 1966 issue of *Scientific American*, Martin Gardner made the following statement regarding Pascal's triangle: "Almost anyone can study the triangle and discover more properties, but it is unlikely that they will be new, for what is said here only scratches the surface of a vast literature." But, of course, many new results have been discovered since 1966 and we present some here that were even suggested by Gardner's article, although the more immediate stimulation was the recent brief article by S. H. L. Kung [3] concerning the parity of entries in Pascal's triangle.

2. THE ITERATED TRIANGLE

Consider Pascal's triangle with its entries reduced to their least nonnegative residues modulo p, where p denotes a prime. Let k, n, and m be integers with $0 \leq k \leq n$ and $1 \leq m$, and let $\Delta_{n,k}$ denote the triangle of entries

$$\begin{array}{ccc} & \binom{np^m}{kp^m} & \\ \cdot & & \cdot \\ \binom{np^m + p^m - 1}{kp^m} & \cdots & \binom{np^m + p^m - 1}{kp^m + p^m - 1} \end{array}$$

For fixed m, we claim that all those elements not contained in one of these triangles are zeros, that there are precisely p distinct triangles $\Delta_{n,k}$, and that these triangles are in one-to-one correspondence with the residues 0, 1, 2, ..., $p - 1$ in such a way that the triangle of triangles

$$\begin{array}{ccccc} & & \Delta_{0,0} & & \\ & \Delta_{1,0} & & \Delta_{1,1} & \\ \Delta_{2,0} & & \Delta_{2,1} & & \Delta_{2,2} \\ & & \cdots & & \end{array}$$

is "isomorphic" to the original Pascal triangle. In particular, we claim that there is an element-wise addition of the triangles $\Delta_{n,k}$ which satisfies the equation

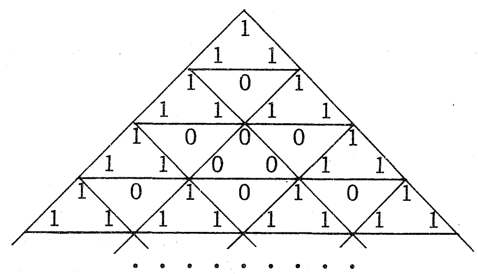
$$\Delta_{n,k} + \Delta_{n,k+1} = \Delta_{n+1,k+1}$$

where the addition is modulo p.

If we repeatedly iterate this process by mapping the triangles $\Delta_{n,k}$ onto the residues it follows that, modulo p, Pascal's triangle is a triangle that contains a Pascal triangle of triangles, that in turn contains a Pascal triangle of triangles, ..., *ad infinitum*. For example, let $m = 1$ and consider Pascal's triangle, modulo 2.

```
              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
1   1   1   1   1   1   1   1
    . . . . . . . . .
```

If we actually draw triangles around the $\Delta_{n,k}$ defined above, we obtain the following array:

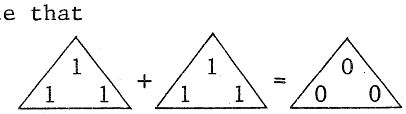


And is we suppress the triangles with a single zero (with the points pointed downward) and make the substitution indicated by the one-to-one correspondence

we obtain

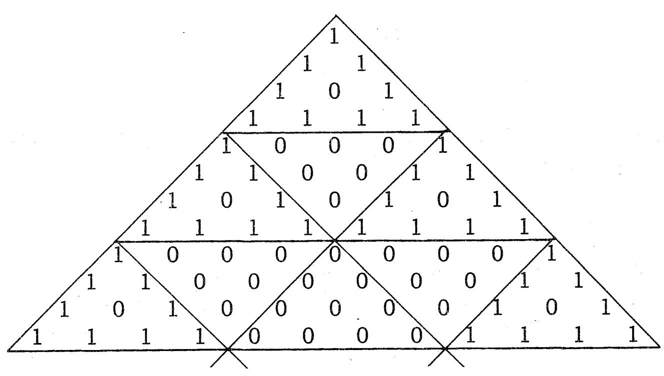
$$
\begin{array}{ccccccc}
 & & & 1 & & & \\
 & & 1 & & 1 & & \\
 & 1 & & 0 & & 1 & \\
1 & & 1 & & 1 & & 1 \\
 & & & \cdots\cdot\cdot & & &
\end{array}
$$

which is simply the original Pascal triangle modulo 2. Also, using element-wise addition modulo 2, we note that

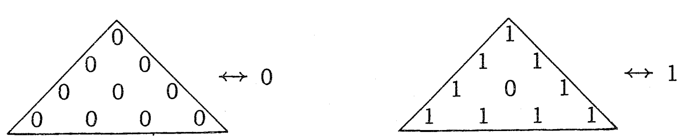


and similarly for the other "digit" sums.

Iterating a second time (or, equivalently, taking $m = 2$) amounts to partitioning the original triangle as follows:



This time, suppressing the inverted triangles of zeros and making the replacement indicated by the correspondence



we obtain

$$\begin{array}{ccccc} & & 1 & & \\ & 1 & & 1 & \\ 1 & & 0 & & 1 \\ & & \cdots & & \end{array}$$

which is again the original Pascal triangle modulo 2. Also, again adding element-wise modulo 2, we have

$$\begin{array}{ccccccc} & & & 1 & & & \\ & & 1 & & 1 & & \\ & 1 & & 0 & & 1 & \\ 1 & & 1 & & 1 & & 1 \end{array} + \begin{array}{ccccccc} & & & 1 & & & \\ & & 1 & & 1 & & \\ & 1 & & 0 & & 1 & \\ 1 & & 1 & & 1 & & 1 \end{array} = \begin{array}{ccccccc} & & & 0 & & & \\ & & 0 & & 0 & & \\ & 0 & & 0 & & 0 & \\ 0 & & 0 & & 0 & & 0 \end{array}$$

as required by the Pascal recurrence.

These results are summarized for any prime p in the following theorem.

Theorem 1: Let p be a prime and let $\Delta_{n,k}$ be defined as above for $0 \le k \le n$ and $1 \le m$. Then $\Delta_{n,k}$ is the triangle

$$\begin{array}{ccc} & \binom{n}{k}\binom{0}{0} & \\ \binom{n}{k}\binom{1}{0} & & \binom{n}{k}\binom{1}{1} \\ \vdots & & \vdots \\ \binom{n}{k}\binom{p^m - 1}{0} & \cdots & \binom{n}{k}\binom{p^m - 1}{p^m - 1} \end{array}$$

with all the products reduced modulo p and

$$\Delta_{n,k} + \Delta_{n,k+1} = \Delta_{n+1,k+1}$$

where the addition is element-wise addition modulo p. Finally, every element in Pascal's triangle and not in one of the $\Delta_{n,k}$ is congruent to zero modulo p.

Proof: The elements of $\Delta_{n,k}$ are the binomial coefficients

$$\binom{np^m + r}{kp^m + s}, \quad 0 \le s \le r < p^m,$$

and, by Lucas' theorem for binomial coefficients [1], [5, p. 230],

$$\binom{np^m + r}{kp^m + s} \equiv \binom{n}{k}\binom{r}{s} \pmod{p}.$$

This gives the first assertion of the theorem and also implies the second, since

$$\begin{aligned} \binom{np^m + r}{kp^m + s} + \binom{np^m + r}{(k + 1)p^m + s} &\equiv \binom{n}{k}\binom{r}{s} + \binom{n}{k + 1}\binom{r}{s} \\ &= \binom{n + 1}{k + 1}\binom{r}{s} \\ &\equiv \binom{(n + 1)p^m + r}{(k + 1)p^m + s} \pmod{p}. \end{aligned}$$

Finally, the entries of Pascal's triangle not included in any of the $\Delta_{n,k}$ form triangles $\nabla_{n,k}$ of the form shown below.

$$\begin{matrix} \binom{np^m}{kp^m+1} & \cdots\cdots & \binom{np^m}{kp^m+p^m-1} \\ & \ddots \quad \therefore & \\ & \binom{np^m+p^m-2}{kp^m+p^m-1} & \end{matrix}$$

with the elements reduced modulo p. Thus, every element in $\nabla_{n,k}$ is of the form

$$\binom{np^m+r}{kp^m+s}, \quad 0 \le r < s \le p^m - 1$$

and, again from Lucas' theorem,

$$\binom{np^m+r}{kp^m+s} \equiv \binom{n}{k}\binom{r}{s} \equiv 0 \pmod{p}.$$

since $r < s$. This completes the proof.

3. A GREATEST COMMON DIVISION PROPERTY

In this section, we need the following remarkable lemma [4, p. 57, Prob. 16] which is readily derived from Lucas' theorem. Note that by $p^f \| n$ we mean that $p^f | n$ and $p^{f+1} \nmid n$.

Lemma: Let p be a prime and let n and k be integers with $0 \le k \le n$. If $p^f \| \binom{n}{k}$, then f is the number of carries one makes when adding k to $n - k$ in base p.

We now prove an interesting greatest common divisor property for the binomial coefficients in the triangular array

$$\begin{matrix} \binom{m}{1} & \cdots\cdots\cdots & \binom{m}{m-1} \\ \binom{m+1}{2} & \cdots & \binom{m+1}{m-1} \\ & \ddots \quad \therefore & \\ & \binom{2m-2}{m-1} & \end{matrix}$$

which we denote by ∇_m.

Theorem 2: Let p be a prime, let d be the greatest common divisor of all elements in ∇_m, and let D denote the greatest common divisor of the three corner elements

$$\binom{m}{1}, \binom{m}{m-1}, \text{ and } \binom{2m-2}{m-1}.$$

Then,
(i) $d = D = p$ if $m = p$,
(ii) $d = p$ and $D = p$ if $m = p^\alpha$, where $\alpha > 1$ is an integer, and
(iii) $d = 1$ and $D = m$ for all other integers $m \ge 2$.

Proof: (i) Since $\binom{m}{1} = \binom{p}{1} = p$ and $d | D | \binom{m}{1}$, it suffices to show that $p | d$. Consider an arbitrary element

$$\binom{p+k}{h}, \quad 0 \le k \le p-2, \quad k+1 \le h \le p-1$$

of ∇_p. By Lucas' formula

$$\binom{p+k}{h} \equiv \binom{k}{h} \equiv 0 \pmod{p},$$

since $k < h$. Thus, p divides every element of ∇_p and so $p|d$ as required.

(ii) Here the elements of ∇_{p^α} are the form

$$\binom{p^\alpha + k}{h},\ 0 \le k \le p - 2,\ k + 1 \le h \le p - 1$$

and, again by Lucas' theorem,

$$\binom{p^\alpha + k}{h} \equiv \binom{k}{h} \equiv 0 \pmod{p},$$

since $k < h$. Thus, $p|d|D$. On the other hand, $p \| \binom{p^\alpha}{p^{\alpha-1}}$, since the only carry you make in adding $p^{\alpha-1}$ to $p^\alpha - p^{\alpha-1} = (p-1)p^{\alpha-1}$ is just 1. This implies that $d|p$, and hence that $d = p$. Furthermore,

$$\binom{p^\alpha}{1} = \binom{p^\alpha}{p^\alpha - 1} = p^\alpha \quad \text{and} \quad p^\alpha \| \binom{2p^\alpha - 2}{p^\alpha - 1},$$

since

$$p^\alpha - 1 = \sum_{i=0}^{\alpha-1} (p-1)p^i$$

so that you carry precisely α times when adding $p^\alpha - 1$ to $p^\alpha - 1$ in base p. Therefore, $D = p^\alpha$ as claimed.

(iii) In this case, m is not a prime power. Since

$$\binom{m}{1} = \binom{m}{m-1} = m,$$

we have that $D|m$. Thus, to show that $D = m$, it suffices to show that $m|D$. This will clearly be the case if we show that $m \Big| \binom{2m-2}{m-1}$ and for this it suffices to show that

$$p_i^{\alpha_i} \Big| \binom{2m-2}{m-1},\ 1 \le i \le r,$$

where

$$m = \prod_{i=1}^{r} p_i^{\alpha_i}$$

is the canonical representation of m. Let $m = kp$, where k is an integer and $p \nmid k$. Since

$$kp^\alpha - 1 = (k-1)p^\alpha + p^\alpha - 1 = (k-1)p^\alpha + \sum_{i=0}^{\alpha-1} (p-1)p,$$

it is clear that the number of carries made in adding $kp^\alpha - 1$ to $kp^\alpha - 1$ in base p is at least α. Therefore,

$$p^\alpha \Big| \binom{2kp^\alpha - 2}{kp^\alpha - 1}$$

and the result follows.

We now show that $d = 1$. Since

$$\binom{m}{1} = m = \prod_{i=1}^{r} p_i^{\alpha_i},\ r > 1,$$

it suffices to show that

$$p_i \nmid \binom{m}{p_i^{\alpha_i}},\ 1 \le i \le r.$$

If we fix i, we may write $m = hp_i^{\alpha_i}$ with $h > 1$ and $(h, p_i) = 1$. The question will then be settled if we show that there are *no* carries when adding $p_i^{\alpha_i}$ to $m - p_i^{\alpha_i} = (h - 1)p_i^{\alpha_i}$ in base p. Since the only nonzero digit in the representation of $p_i^{\alpha_i}$ to base $p_i^{\alpha_i}$ is the 1 that multiplies p_i^{α}, we need consider only the digit that multiplies $p_i^{\alpha_i}$ in the base p_i representation of $(h - 1)p_i^{\alpha_i}$. Indeed, it is clear that we have a carry if and only if $h - 1 = qp_i + (p_i - 1)$ for some integer q. But this is so if and only if $h = (q + 1)p_i$, and this contradicts the fact that $(h, p_i) = 1$. Thus,

$$p_i \nmid \binom{m}{p_i^{\alpha_i}}$$

for $1 \leq i \leq r$, and the proof is complete.

REFERENCES

1. N. J. Fine. "Binomial Coefficients Modulo a Prime." *Amer. Math. Monthly* 14 (1947):589-92.
2. Martin Gardner. "Mathematical Games." *Scientific American* 215 (Dec. 1966): 128-32.
3. S. H. L. Kung. "Parity Triangles of Pascal's Triangle." *The Fibonacci Quarterly* 14 (1976):54.
4. C. T. Long. *Elementary Introduction to the Theory of Numbers*. 2nd ed. Lexington: D. C. Heath & Co., 1972.
5. E. Lucas. "Théorie des functions numériques simplement périodiques." *Amer. J. Math.* 1 (1878):184-240.

*****

ON THE NUMBER OF FIBONACCI PARTITIONS OF A SET

HELMUT PRODINGER

Institut für Mathematische Logik und Formale Sprachen, 1040 Wien, Austria

1. PARTITIONS OF $\overline{n}$ IN FIBONACCI SETS

Let $\overline{n} := \{1, 2, \ldots, n\}$. It is well known [1] that the number of sets $A \subseteq \overline{n}$, with

(1) $$i, j \in A,\ i \neq j \text{ implies } |i - j| \geq 2,$$

is the Fibonacci number F_{n+1}. ($F_0 = F_1 = 1$, $F_{n+2} = F_{n+1} + F_n$.)

A set $A \subseteq \overline{n}$ with the property (1) will be called a Fibonacci set.

A partition of $\overline{n}$ is a family of disjoint (nonempty) subsets of $\overline{n}$ whose union is $\overline{n}$. The number of partitions of $\overline{n}$ is B_n, the nth Bell number [2].

In this section the number C_n of partitions of $\overline{n}$ in Fibonacci subsets will be considered. There exists an interesting connection with B_n.

Theorem 1: $C_n = B_{n-1}$.

Proof: This will be proved by arguments analogous to Rota's in [2]. First, the number of functions $f: \overline{n} \to U$ (U has u elements) with $f(i) \neq f(i + 1)$ for all i is determined: for $f(1)$ there are u possibilities; for $f(2)$ there are $u - 1$ possibilities; for $f(3)$ there are $u - 1$ possibilities, and so on. The desired number of functions is $u(u - 1)^{n-1}$.

These functions are partitioned with respect to their kernels. (Note that exactly those kernels appear which are Fibonacci sets!)

(2) $$\sum (u)_{N(\pi)} = u(n - 1)^{n-1},$$