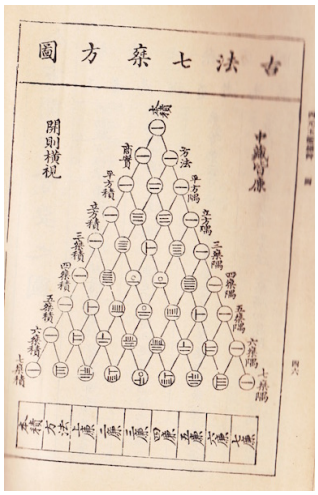
Mathematical Foundations of Computer Science

CS 499, Shanghai Jiaotong University, Dominik Scheder

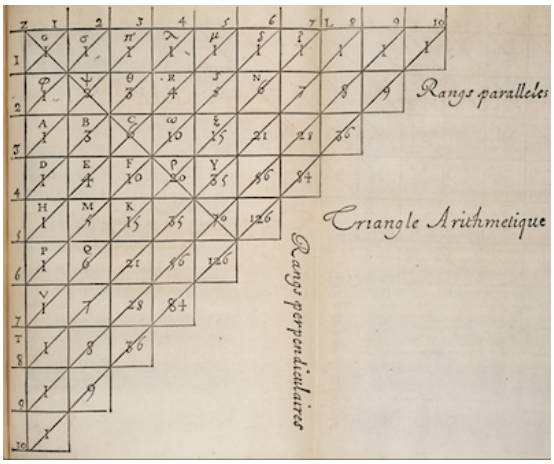
- Monday, 2018-03-19, homework handed out
- Sunday, 2018-03-25, 12:00: submit questions and first submissions. You'll get feedback until Wednesday.
- Sunday, 2018-03-29 (Wednesday), 18:00: submit your review of the other group's first submission.
- 2018-04-01: submit final solution.

4 Pascal's Triangle Modulo 2

Here are two early tables of the binomial coefficient:

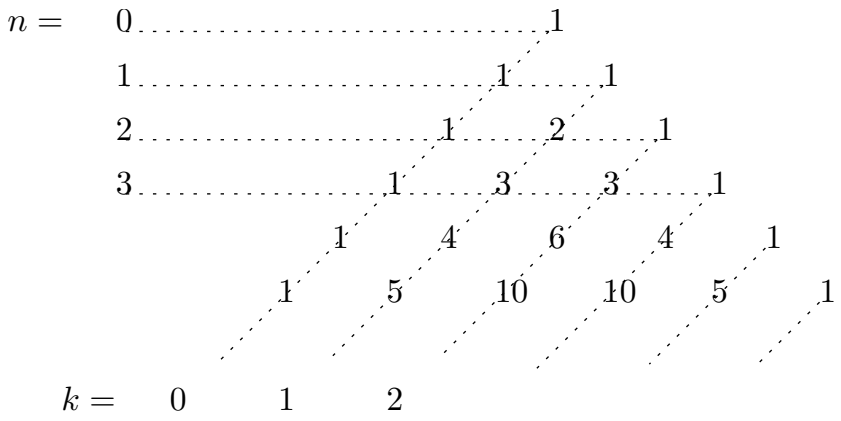


Yang Hui triangle from the book "Jade Mirror of the Four Unknowns" by Zhu Shijie, 1303 (Wikimedia)



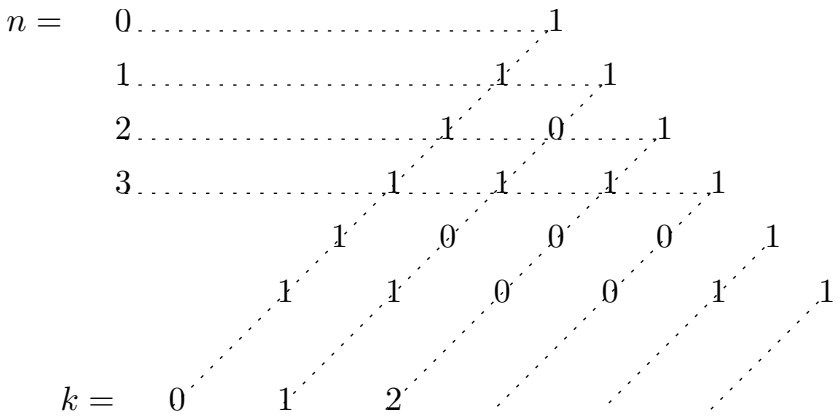
Blaise Pascals version of the triangle (Source: Wikimedia)

Here is my version of "Pascal's triangle", indicating that rows are indexes by n and "columns" by k:

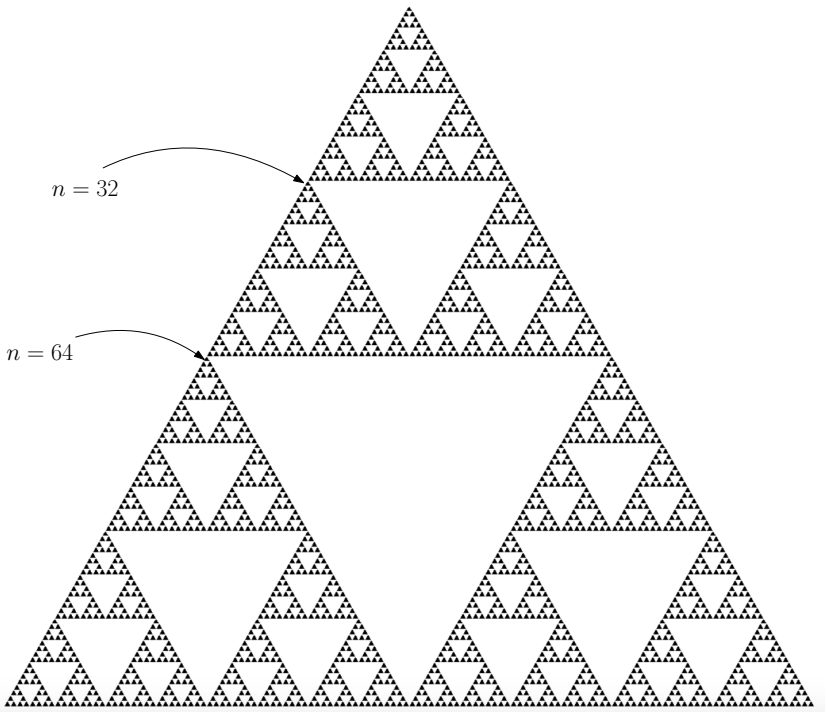


4.1 Lucas Theorem: $\binom{n}{k}$ mod 2

Something interesting happens when we take the triangle modulo 2, that is, we replace even numbers by 0 and odd numbers by 1:



If we draw a black dot for every 1 and look at a larger section of this triangle, we get the following pattern, known as the Sierpinski triangle:



Note the amazing recursive structure. This suggests we should be able to compute $\binom{n}{k} \mod 2$ without actually computing $\binom{n}{k}$, by somehow employing this structure. In fact, here is a cool result by Édouard Lucas, which we state here in a simpler, more special version:

The set $\mathbb{N}_0$ comes equipped with a partial ordering $\preceq$, in which $x \preceq y$ if for every i, the i^{th} least significant bit of x is at most that of y. Put in a simpler way, we write x and y as bit strings in binary. If their length differ, we put a bunch of 0's in front of the smaller number to make both strings of equal length d. Then we simply compare those strings using the usual partial ordering $\preceq$ on $\{0,1\}^d$. For example, $3 \preceq 7$ since $011 \preceq 111$, and $5 \preceq 23$ since $00101 \preceq 10111$, but $7 \not\preceq 8$ since $0111 \not\preceq 1000$.

Theorem 4.1. *Let $n, k \in \mathbb{N}_0$. Then $\binom{n}{k}$ is odd if $k \preceq n$ and even otherwise.*

Note that this theorem lets us compute $\binom{n}{k} \mod 2$ quickly for numbers n, k having millions of digits, whereas no computer on Earth has the memory to evaluate the formula

$$\binom{n}{k} = \frac{n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot (n-k+2) \cdot (n-k+1)}{k \cdot (k-1) \cdot (k-2) \cdot \cdots \cdot 2 \cdot 1}$$

for values that large. Let me now walk you through a proof of this theorem.

Definition 4.2. *For a natural number $n \in \mathbb{N}$, let $|n|_1$ be the number of 1's in the binary representation of n. For example, $|1|_1 = |2|_1 = |4|_1 = 1$ but $|3|_1 = 2$ and $|7|_1 = 3$.*

Definition 4.3. *For a natural number $a \in \mathbb{N}$ define $f(a)$ as the number of times the factor 2 appears in a. Formally,*

$$f(a) := \max\{k \mid 2^k \text{ divides } a\} .$$

For example, $f(24) = 3$ since 8 divides 24 but 16 does not.

Exercise 4.4. Find a closed formula for $f(n!)$ in terms of n and $|n|_1$.

Solution.

From the rule we find, we can easily find the formula $n - |n|_1$

We can prove this by induction.

Basic step. When n=1, it is obvious that $f(1!) = 1 - |1|_1 = 0$

Induction Hypothesis. We assume that when n=k, $f(k!) = k - |k|_1 = 0$.

Now let's prove that $n = k+1$, $f((k+1)!) = k+1-|k+1|_1 = 0$ is true.

If k is even, then $k+1$ is odd, the lowest bit of the binary form of $k+1$ is 1(changed from 0) with other bits unchanged, so $|k+1|_1 = |k| + 1$, so $f((k+1)!) = f(k!)$ and it is true for the even number k.

If k is odd, then $k+1$ is even, the situation is a little complex. It is obvious that $k+1$ can be changed into a form such that $k+1 = 2^m \times p$ (m is an integer and p is an odd number). Thus, $f((k+1)!) = f(k!)+m$. $k+1$ can be divided by 2^m, so the first m^{th} bits of the binary form of $k+1$ is 0(all changed from 1), and the $m+1^{th}$ bit is 1(changed from 0) with other bits unchanged. Therefore, we get one 1 but lose m 1s instead. $|k+1|_1 = |k|_1 - (m-1)$, so $f((k+1)!) = f(k!) + m = k+1-|k|_1+m-1 = k+1-|k+1|_1$

Exercise 4.5. Find a closed formula for $f\left(\binom{n}{k}\right)$ in terms of $n, k, |n|_1$, and so on.

Solution. According to the exercise above, $f(n!) = n - |n|_1$.

$$\begin{aligned} f\left(\binom{n}{k}\right) &= f\left(\binom{n!}{k!(n-k)!}\right) \\ &= f(n!) - f(k!) - f((n-k)!) \\ &= -|n|_1 + |k|_1 + |n-k|_1 \end{aligned}$$

Exercise 4.6. Prove Theorem 4.1. With our new notation, prove that $f\left(\binom{n}{k}\right)$ is 0 if $k \preceq n$ and at least 1 if $k \not\preceq n$.

Proof. If $k \preceq n$, $n-k$ will have exactly the same 1s with $|n|_1 - |k|_1$.

Otherwise, every same bit in n and k with 1 will reduce $|n|_1$ no more than the number of these bits, and we call the number i_1. Every bit with 1 in k and 0 in n will result in at least 1 carry which replaces 0 in n with 1, and we call the number of these bits i_0 and the number of carries c, obviously $c \geq i_0$ and $i_0 \geq 1$. Note that

$$|n-k|_1 = |n|_1 - i_1 - i_0 + c = |n|_1 - |k|_1 + c \geq |n|_1 - |k|_1 + 1,$$

so

$$f\left(\binom{n}{k}\right) = -|n|_1 + |k|_1 + |n-k|_1 > 0.$$

4.2 Almost Empty Rows

One feature of the Sierpinski triangle is that some rows are almost empty. For example, row 64 has a black dot at the very left and the very right, and only white space in between. This is because

Theorem 4.7. *Let $d \in \mathbb{N}_0$ and $0 < k < 2^d$. Then $\binom{2^d}{k}$ is even.*

Although this theorem follows easily from Lucas' Theorem, I want you to think about an alternative proof. Intuitively, if some number is even, then one suspects it can be proved by "pairing things up" perfectly. After all, if you can prove that in a set S, every element can be "married" to another element, you have partitioned S into couples and thus $|S|$ must be even. So let's see whether there is a proof of Theorem 4.7 along these lines. This is also valuable because it lets you practice with notions of sets and functions.

Consider the set $\{0,1\}^d$. You can view this as the set of all binary strings of length d. This set has size $2^d = n$. For $1 \leq i \leq d$ and $x \in \{0,1\}^d$ let $f_i(x)$ be x with the i^{th} position flipped. For example, $f_3(11011) = 11111$.

Exercise 4.8. Show that f_i is an involution without a fixed point. That is, $f(f(x)) = x$ and $f(x) \neq x$ for all $x \in \{0,1\}^d$.

Proof. According to definition, $f_i(x)$ is x with i^{th} position flipped, so $f_i(x) \neq x$. And $f_i(f_i(x))$ is x with i^{th} position flipped twice, which goes back to x, so $f_i(f_i(x)) = x$.Therefore, f_i is an involution without a fixed point. □

Let $S \subseteq \{0,1\}^d$. We define $f_i(S)$ as the set arising from applying f_i to every element of S. Formally,

$$f_i(S) := \{f_i(x) \mid x \in S\} .$$

Given a set $S \subseteq \{0,1\}^d$, we call an index $i \in [n]$ *active* for S if $f_i(S) \neq S$.

Exercise 4.9. Let $d = 3$ and $S = \{000, 100\}$. Which of the indices $1, 2, 3$ are active?

Proof. Let least significant digit be the 1'st position.

$$f_1(S) = \{001, 101\} \neq S$$
$$f_2(S) = \{010, 110\} \neq S$$
$$f_3(S) = \{100, 000\} = S$$

So 1 and 2 are active. □

Exercise 4.10. Show that f is an involution. That is, $f(f(S)) = S$. Furthermore, show that the only fixed points of f are $\emptyset$ and $\{0,1\}^d$.

Proof.

$$\forall x \in S, f(f(x)) = x \Rightarrow f(f(S)) = S$$

Let's suppose that f(S)=S when $S \neq \{0,1\}^d and S \neq \emptyset$.Thus, there must exist an element $x \in S$ and an element $y \in \{0,1\}^d \backslash S$.Define a step as changing one number's 1 bit, such as 00000 $\rightarrow$ 00001.Obviously, one figure can walk into any other one in at most n steps(n is the number of bits).The path from x to y is followed, and the distance of neighbours is one step, which means $t_{k+1} = f_{i_k}(t_k)$.

$$x = t_0 \rightarrow t_1 \rightarrow \ldots \rightarrow t_n \rightarrow t_{n+1} = y$$

Since f(S)=S, $t_{k+1} \in S \Rightarrow t_{k+1} = f_{i_k}(t_k) \in S$.By induction, we can know that $y \in S$ on the base of $x \in S$,which results in conflict with the claim $y \in \{0,1\}^d \backslash S$. Therefore, the only fixed points of f are $\emptyset$ and $\{0,1\}^d$. □

Exercise 4.11. Let $\mathcal{S} = \binom{\{0,1\}^d}{k}$. This is a set of sets, and each set $S \in \mathcal{S}$ consists of exactly k strings from $\{0,1\}^d$. Prove the following statements:

1. f is a bijection from $\mathcal{S}$ to $\mathcal{S}$.
2. For $1 \leq k \leq 2^d - 1$, this bijection is an involution without fixed points.
3. $|\mathcal{S}|$ is even for $1 \leq k \leq 2^d - 1$.

Proof. 1. $\forall S_1 \neq S_2 \in \mathcal{S}, \exists x_1 \in S_1, x_1 \notin S_2 \Rightarrow f(x_1) \in f(S_1), f(x_1) \notin f(S_2) \Rightarrow f(S_1) \neq f(S_2)$.So f is an injective. And $|\mathcal{S}| = |\mathcal{S}|$, so f is a surjective. Thus, f is a bijection from $\mathcal{S}$ to $\mathcal{S}$. □

Proof. 2. According to Exercise 4.10, For $1 \leq k \leq 2^d - 1$, which means $S \neq \emptyset and S \neq \{0,1\}^d$, $f(S) \neq S$.So f is an bijection without fixed point. □

Proof. 3. Since $f(S) \neq S$and $f(f(S)) = S$, we say every S can be "married" with f(S).Thus,$|\mathcal{S}|$ is even for $1 \leq k \leq 2^d - 1$. □

Exercise 4.12. Complete the proof of Theorem 4.7.

Proof.

$$|\{0,1\}^d| = 2^d$$

$$|S| = k$$

So every S can be considered as a choice of selecting k strings from 2^d strings. The number of S is the choices.

Thus,

$$\binom{2^d}{k} = |\mathcal{S}|$$

Since we prove that $|\mathcal{S}|$ is even for $1 \leq k \leq 2^d - 1$ in Exercise 4.12, $\binom{2^d}{k}$ is even for $0 < k < 2^d$. □

***Exercise 4.13.** *Generalize the above "combinatorial" proof to show the following theorem:*

Theorem 4.14. *Let $n = p^d$ where p is a prime number. Then p divides $\binom{n}{k}$ unless $k = 0$ or $k = n$.*

Consider the set $\{0, 1, \ldots, p-1\}^d$. We view this as the set of all p-based strings of length d. This set has size $p^d = n$. For $1 \leq i \leq d$ and $x \in \{0, 1, \ldots, p\}^d$ let $f_i(x)$ be x with the i_{th} position $\hat{k} = (k+1) \mod p$. For example, when $p = 6$, $f_3(12345) = 12445$, $f_3(12545) = 12045$

Step 1

Let's prove that f_i is an involution without a fixed point. That is, $f(\ldots f(x)) = f^p(x) = x$ and $f(x) \neq x$ for all $x \in \{0, 1, \ldots, p-1\}^d$.

Proof. Since number at the i^{th} position is changed, obviously, $f(x) \neq x$.

For the number of the t^{th} position, after p functions, $\hat{k} = ((k+1) \mod p \cdots + 1) \mod p = (k+p) \mod p = k$, so $f^p(x) = x$. □

Step 2

Let $S \subseteq \{0, 1, \ldots, p-1\}^d$. Define $f_i(S) := \{f_i(x) | x \in S\}$. We call an index $i \in [n]$ *active* for S if $f_i(S) \neq S$.

Let's prove that if $S \neq 0$ and $S \neq \{0, 1, \ldots, p-1\}^d$ then S has at least one active index.

Proof. Contradiction.

If S has no active index, then $\forall i, f_i(S) = S$.

Since $S \neq 0$, $\exists \xi \in S$. So $f_i(\xi), f_i(f_i(\xi)), \ldots, f_i^{d-1}(\xi) \in S$. Thus, every position can be number $0, 1, \ldots, p-1$, which contradicts $S \neq \{0, 1, \ldots, p-1\}^d$. □

Step 3

Given $S \subseteq \{0, 1, \ldots, p-1\}^d$, define $f(S)$ as follows: if $S = \emptyset$ or $S = \{0, 1, \ldots, p-1\}^d$ define $f(S) = S$. Otherwise, let $f(S) := f_i(S)$ where i is the smallest active index of S.

Let's prove that f is an involution. That is, $f(\dots f(S)) = f^d(S) = S$. Furthermore, let's prove that the only fixed points of f are $\emptyset$ and $\{0,1\}^d$.

Proof. $\forall x \in S$, since $f^d(x) = x$, $f^d(x) \in S$. So $f^d(S) = S$.

Since $f(S) = S$ for $S = \emptyset$ or $S = \{0, 1, \dots, p-1\}^d$, $\emptyset$ and $\{0, 1, \dots, p-1\}^d$ are fixed points.

According to the last step, $f(S) \neq S$ for $S \neq \emptyset$ and $S \neq \{0, 1, \dots, p-1\}^d$, so $\emptyset$ and $\{0, 1, \dots, p-1\}^d$ are the only fixed points. □

Step 4

Let $\mathcal{S} = \binom{\{0,1,\dots,p-1\}^d}{k}$. This is a set of sets, and each set $S \in \mathcal{S}$ consists of exactly k strings from $\{0, 1, \dots, p-1\}^d$. Let's prove the following statements:

1. f is a bijection from $\mathcal{S}$ to $\mathcal{S}$.

   Proof. $\forall S \in \mathcal{S}$, $f(S)$ is also a set consisting of exactly k strings from $\{0, 1, \dots, p-1\}^d$, so $f(S) \in \mathcal{S}$. Thus, f is a bijection from $\mathcal{S}$ to $\mathcal{S}$. □

2. For $1 \leq k \leq p^d - 1$, this bijection is an involution without fixed points.

   Proof. $f^d(S) = S$ as showed in **Step 3**, so f is an involution.

   Since $1 \leq k \leq p^d - 1$, $\forall S \in \mathcal{S}$, $S \neq \emptyset$ and $S \neq \{0, 1, \dots, p-1\}^d$. Thus, $f(S) \neq S$. This bijection has no fixed points.

   □

3. $S, f(S), f(f(S)), \dots, f^{p-1}(S)$ are all different.

   Proof. Contradiction.

   Define *Period* as the smallest $t \geq 1$ that $f^t(S) = S$.

   If $S, f(S), \dots, f^{p-1}(S)$ are not all different, then *Period* of S is t and $t < p$. As $f(S) \neq S$ is proved before, $1 < t < p$.

   So $f^t(S) = S$ and $f^p(S) = S$.

   Let's prove $f^{p-kt}(S) = S$ for $1 \leq k \leq p-1$.

   Base Step. Since $f^p(S) = f^{p-t}(f^t(S)) = S$, $f^{p-t}(S) = S$.

   Induction Hypothesis. When $f^{p-qt}(S) = S$, $1 \leq q \leq p-2$, according to the definition, t is the smallest, so $t \leq p - qt$, $t \leq \frac{p}{q+1}$.

Proof of Induction Step. Since p is a prime number and $q+1 < p$, p has no factor of $q+1$, so $t < \frac{p}{q+1}$.

$f^p(S) = f^{p-(q+1)t}(f^{(q+1)t}(S)) = S$, so $f^{p-(q+1)t}(S) = S$.

Thus, $f^{p-(p-1)t}(S) = S$. Since t is the smallest, $t \leq p-(p-1)t$, $pt \leq p$, which contradicts $t > 1$.

Therefore, *Period* of S is p. $S, f(S), \ldots, f^{p-1}(S)$ are all different. □

4. $|\mathcal{S}|$ can be divided by p for $1 \leq k \leq p^d - 1$.

   Proof. $\forall S \in \mathcal{S}$, $f(S), f(f(S)), \ldots f^{d-1}(S)$ construct a cluster of size p. f can transform S within the cluster and cannot transform out of the cluster, so the clusters are independent to each other. The number of clusters $\mathcal{S}$ have is an integer, so $|\mathcal{S}|$ can be divided by p. □

Last Step

Proof. When $k = 0$ or $k = n$, $\binom{n}{k} = 1$ cannot be divided by p.

$$|\{0, 1, \ldots, p-1\}^d| = p^d = n$$
$$|S| = k$$

So every S can be considered as a choice of selecting k strings from n strings. The number of S is the choices.

Thus,

$$\binom{n}{k} = |\mathcal{S}|$$

Since we prove that $|\mathcal{S}|$ can be devided by p for $1 \leq k \leq p^d - 1$, $\binom{n}{k}$ can be divided by p unless $k = 0$ or $k = n$. □