Mathematical Foundations of Computer Science

CS 499, Shanghai Jiaotong University, Dominik Scheder

Version C

This homework is special. First of all, it is more difficult than the previous ones. Second, you will have two weeks time to work on them. Third, different groups will get different problem sets. Your solution will be given to two other groups, who give you feedback. Similarly, you will have to read two other groups' solutions and give them feedback.

You have to solve only one version (the one assigned to you), but you have to understand the questions all four versions, since you have to give feedback / grade them, and since all versions might be part of the exam.

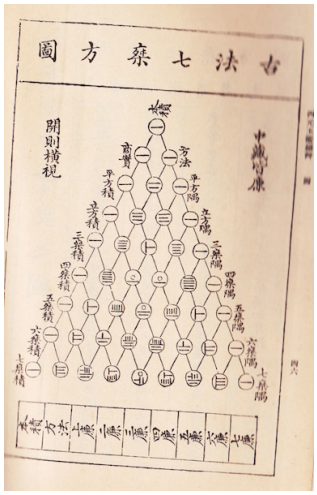
Do include your team name in filename of the the pdf file you submit, but NOT in the content of the pdf. The feedback / grading process will be anonymous, i.e., you will not know which group you are reviewing.

- 2017-03-20 (Monday): homework handed out
- 2017-03-22 (Wednesday), 18:00: submit questions
- 2017-03-26 (Sunday), 18:00: submit first solution.
- 2017-03-29 (Wednesday), 18:00: submit your review of the other group's first submission.
- 2017-04-02 (Sunday), 18:00: submit second solution.

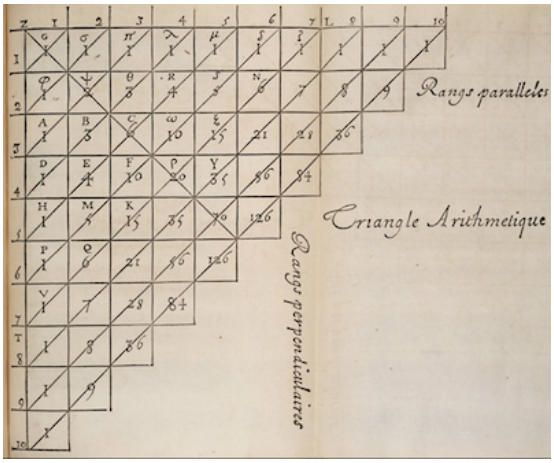
- 2017-04-05 (Wednesdy), 18:00: submit your review of the other group's second submission.
- 2017-04-09 (Sunday), 18:00: submit your final solution.

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

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 (Source: Wikimedia)

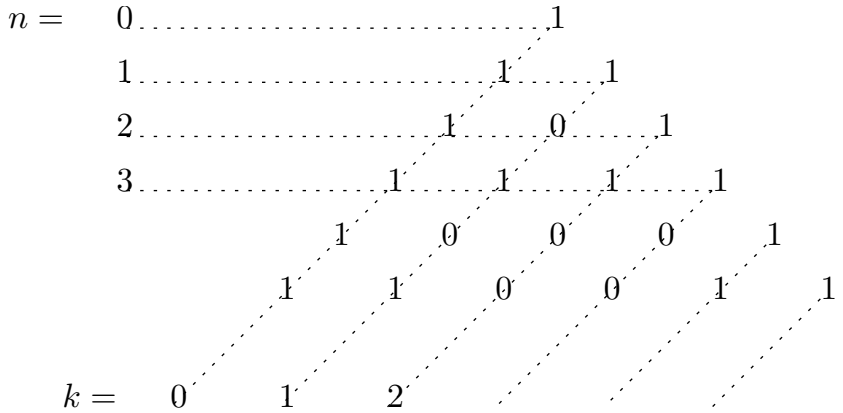


Blaise Pascals version of the triangle (Source: Wikimedia)

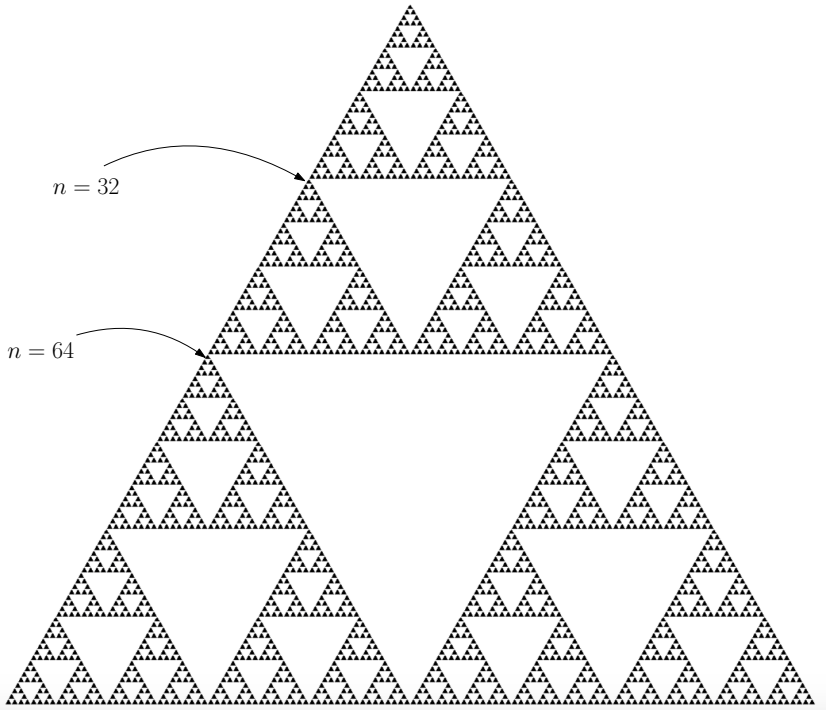
Here is my version of "Pascal's triangle", indicating that rows are indexes by n and "columns" by k:

$$
\begin{array}{lccccccccccc}
n = & 0 & & & & & 1 & & & & & \\
& 1 & & & & 1 & & 1 & & & & \\
& 2 & & & 1 & & 2 & & 1 & & & \\
& 3 & & 1 & & 3 & & 3 & & 1 & & \\
& & 1 & & 4 & & 6 & & 4 & & 1 & \\
& 1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
k = & 0 & & 1 & & 2 & & & & & &
\end{array}
$$

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 5.1. *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 5.2. *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 5.3. *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 5.4. Find a closed formula for $f(n!)$ in terms of n and $|n|_1$.

Exercise 5.5. Find a closed formula for $f\left(\binom{n}{k}\right)$ in terms of $n, k, |n|_1$, and so on.

Exercise 5.6. Prove Theorem 5.1. With our new notation, prove that $f\left(\binom{n}{k}\right)$ is 0 if $k \preceq n$ and at least 1 if $k \not\preceq n$.