

Math 105 TOPICS IN MATHEMATICS

REVIEW OF LECTURES – VIII

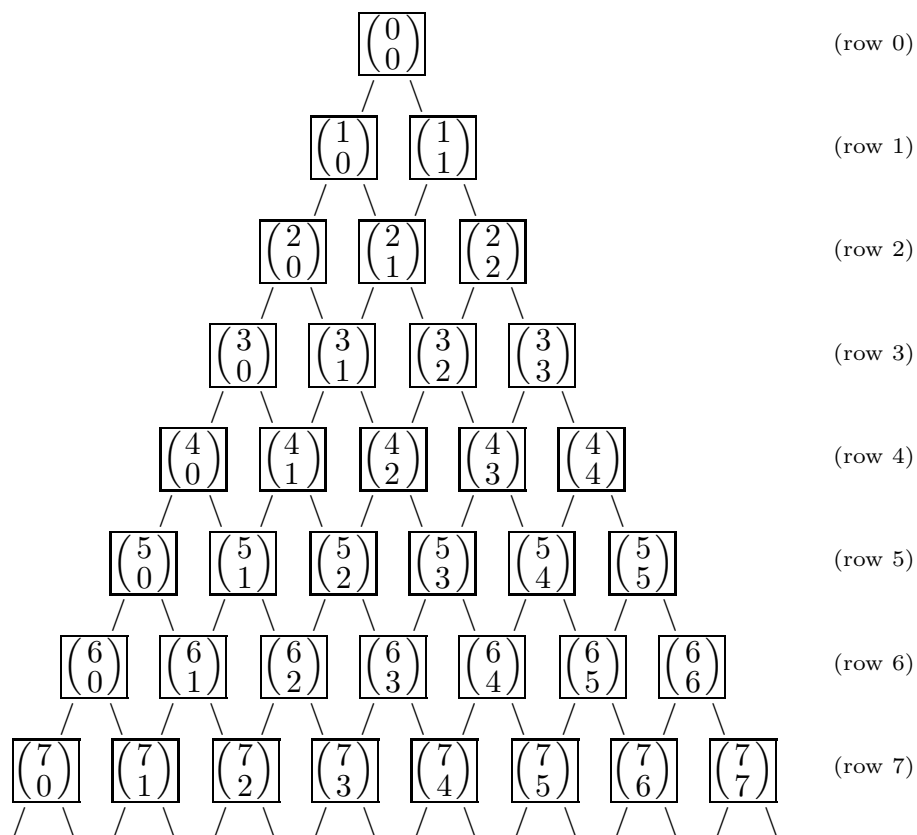
February 6 (Fri), 2015

Instructor: Yasuyuki Kachi

Line #: 52920.

§8. MORE ABOUT BINOMIAL COEFFICIENTS.

We just adopted the notation for the numbers showing up in the Pascal's triangle, namely, $\binom{n}{k}$. These fit exactly as follows:

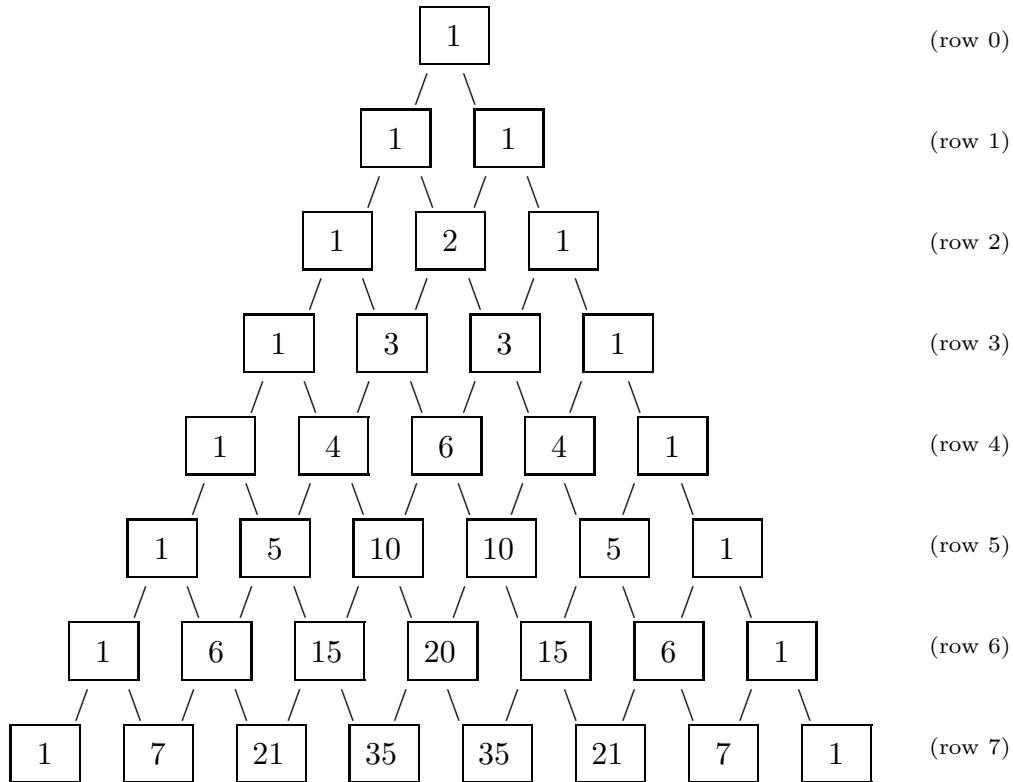


Of course, what are in those boxes are actual numbers (positive integers). Last time we highlighted a formula that allows you to figure out those actual numbers in the Pascal (“Formula A” in “Review of Lectures – VII”). Let me reproduce:

Formula A. Let n and k be integers, with $0 < k < n$. Then

$$\binom{n}{k} = \frac{n \cdot (n-1) \cdot (n-2) \cdots (n-k+1)}{1 \cdot 2 \cdot 3 \cdots k} .$$

If I base this formula, then I can easily convert the Pascal in the previous page into



This is the same Pascal we have seen before. But the real upshot of Formula A above is that the same works, namely, it instantaneously spits out the actual number at any spot of Pascal, no matter how far down it is. Last time I did not quite explain why we can safely claim that this formula is true. Today I want to offer a solid justification why the shape of the formula has to be this way. But the argument is not self-contained. We substantially rely on the content of our previous lectures. Today's lecture also serves the purpose of getting comfortable with the binomial coefficients. So, ready?

As a starter, let's accept that, the left-most and the right-most in each row equal 1. That's "pre-endowed", a part of the proviso, called the initial condition. By comparing the two versions of Pascal's, one on page 1 and one on page 2, we can offer

$$\begin{array}{ll}
 \binom{0}{0} = 1, & \\
 \binom{1}{0} = 1, & \binom{1}{1} = 1, \\
 \binom{2}{0} = 1, & \binom{2}{2} = 1, \\
 \binom{3}{0} = 1, & \binom{3}{3} = 1, \\
 \binom{4}{0} = 1, & \binom{4}{4} = 1, \\
 \binom{5}{0} = 1, & \binom{5}{5} = 1, \\
 \binom{6}{0} = 1, & \binom{6}{6} = 1, \\
 \binom{7}{0} = 1, & \binom{7}{7} = 1, \\
 \vdots & \vdots
 \end{array}$$

A way to write these simultaneously in a short form is as follows:

Initial Conditions (of the Pascal algorithm).

$$\boxed{\binom{n}{0} = 1}, \quad \boxed{\binom{n}{n} = 1}$$

$(n = 0, 1, 2, 3, \dots).$

Now, this might be repetitious, but since it is central to our on-going discussion, so let's recite the rule of Pascal:

Rule.

At every spot, that number equals the sum of two numbers right above it.

Thanks to this rule, the rest of the numbers are completely determined. From the version of the Pascal in page 1, the same rule is recaptured as the relations

$$\begin{array}{ccccccc} \binom{2}{1} = \binom{1}{0} + \binom{1}{1}, & & & & & & \\ \binom{3}{1} = \binom{2}{0} + \binom{2}{1}, & \binom{3}{2} = \binom{2}{1} + \binom{2}{2}, & & & & & \\ \binom{4}{1} = \binom{3}{0} + \binom{3}{1}, & \binom{4}{2} = \binom{3}{1} + \binom{3}{2}, & \binom{4}{3} = \binom{3}{2} + \binom{3}{3}, & & & & \\ \binom{5}{1} = \binom{4}{0} + \binom{4}{1}, & \binom{5}{2} = \binom{4}{1} + \binom{4}{2}, & \binom{5}{3} = \binom{4}{2} + \binom{4}{3}, & \binom{5}{4} = \binom{4}{3} + \binom{4}{4}, & & & \\ \vdots & \vdots & \vdots & \ddots & & & \end{array}$$

A way to write these simultaneously in a short form is

$$\boxed{\binom{n+1}{1} = \binom{n}{0} + \binom{n}{1}}, \quad \boxed{\binom{n+1}{2} = \binom{n}{1} + \binom{n}{2}}, \quad \boxed{\binom{n+1}{3} = \binom{n}{2} + \binom{n}{3}}, \quad \dots$$

$$(n = 0, 1, 2, 3, \dots).$$

Or, just simply

Rule k . $\boxed{\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}}$ $(0 < k \leq n)$.

Also, it is thanks to the same rule (taking the initial condition aforementioned into account), that Pascal exhibits the left-to-right symmetry:

$$\begin{array}{ccc}
 \binom{3}{1} = \binom{3}{2}, & & \\
 \binom{4}{1} = \binom{4}{3}, & & \\
 \binom{5}{1} = \binom{5}{4}, & \binom{5}{2} = \binom{5}{3}, & \\
 \binom{6}{1} = \binom{6}{5}, & \binom{6}{2} = \binom{6}{4}, & \\
 \binom{7}{1} = \binom{7}{6}, & \binom{7}{2} = \binom{7}{5}, & \binom{7}{3} = \binom{7}{4}, \\
 \binom{8}{1} = \binom{8}{7}, & \binom{8}{2} = \binom{8}{6}, & \binom{8}{3} = \binom{8}{5}, \\
 \vdots & \vdots & \vdots
 \end{array}$$

A way to write these simultaneously in a short form is

$$\boxed{\binom{n}{1} = \binom{n}{n-1}}, \quad \boxed{\binom{n}{2} = \binom{n}{n-2}}, \quad \boxed{\binom{n}{3} = \binom{n}{n-3}}, \quad \dots$$

$$(n = 0, 1, 2, 3, \dots).$$

Or, just simply

Symmetry. $\boxed{\binom{n}{k} = \binom{n}{n-k}} \quad (0 \leq k \leq n).$

- Now I want to incorporate this perspective, and recapture the essence of the previous argument which we have extensively covered (in “Review of Lectures – II, III and IV”) that will lead up to Formula A. The argument below looks different from the previous lectures due to the new notation, but you can see the same narrative. It will go step by step.

First, let’s try to dissect $\binom{n}{1}$. We are going to use

Rule 1.
$$\boxed{\binom{n+1}{1} = \binom{n}{0} + \binom{n}{1}}$$

(‘Rule k ’ in page 4 with $k = 1$). Below “*” underneath ‘=’ is where I have applied Rule 1.

$$\begin{aligned} \binom{2}{1} &\underset{*}{=} \binom{1}{0} + \binom{1}{1} = 1 + 1 && \left(\text{since } \binom{n}{0} = \binom{n}{n} = 1 \right) \\ &= 2, \end{aligned}$$

$$\begin{aligned} \binom{3}{1} &\underset{*}{=} \binom{2}{0} + \binom{2}{1} = 1 + 2 && \left(\text{since } \binom{n}{0} = 1 \text{ and} \right. \\ & && \left. \binom{2}{1} = 2 \text{ as shown above} \right) \\ &= 3, \end{aligned}$$

$$\begin{aligned} \binom{4}{1} &\underset{*}{=} \binom{3}{0} + \binom{3}{1} = 1 + 3 && \left(\text{since } \binom{n}{0} = 1 \text{ and} \right. \\ & && \left. \binom{3}{1} = 3 \text{ as shown above} \right) \\ &= 4, \end{aligned}$$

$$\begin{aligned} \binom{5}{1} & \underset{*}{=} \binom{4}{0} + \binom{4}{1} = 1 + 4 && \left(\text{since } \binom{n}{0} = 1 \text{ and} \right. \\ & && \left. \binom{4}{1} = 4 \text{ as shown above} \right) \\ & = 5, \end{aligned}$$

$$\begin{aligned} \binom{6}{1} & \underset{*}{=} \binom{5}{0} + \binom{5}{1} = 1 + 5 && \left(\text{since } \binom{n}{0} = 1 \text{ and} \right. \\ & && \left. \binom{5}{1} = 5 \text{ as shown above} \right) \\ & = 6, \end{aligned}$$

⋮

In sum,

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

$$\binom{2}{1} = 2,$$

$$\binom{3}{1} = 3,$$

$$\binom{4}{1} = 4,$$

$$\binom{5}{1} = 5,$$

$$\binom{6}{1} = 6,$$

⋮

So, we can extrapolate and conclude

$$\boxed{\binom{n}{1} = n} \quad (n = 1, 2, 3, 4, \dots).$$

Since we already have $\binom{n}{1} = \binom{n}{n-1}$, that is,

$$\binom{1}{1} = \binom{1}{0},$$

$$\binom{2}{1} = \binom{2}{1},$$

$$\binom{3}{1} = \binom{3}{2},$$

$$\binom{4}{1} = \binom{4}{3},$$

$$\binom{5}{1} = \binom{5}{4},$$

$$\binom{6}{1} = \binom{6}{5},$$

$$\binom{7}{1} = \binom{7}{6},$$

\vdots

we conclude

$$\boxed{\binom{n}{1} = n}, \quad \boxed{\binom{n}{n-1} = n} \quad (n = 0, 1, 2, 3, \dots).$$

- Next, let's dissect $\binom{n}{2}$. We are going to use

Rule 2. $\binom{n+1}{2} = \binom{n}{1} + \binom{n}{2}$

(‘Rule k ’ in page 4 with $k = 2$). Below “*” underneath ‘=’ is where I have applied Rule 2.

$$\binom{2}{2} = 1 \quad \left(\text{since } \binom{n}{n} = 1 \text{ as shown above} \right),$$

$$\binom{3}{2} = 3 \quad \left(\text{since } \binom{n}{n-1} = n \text{ as shown above} \right),$$

$$\begin{aligned} \binom{4}{2} & \underset{*}{=} \binom{3}{1} + \binom{3}{2} = 3 + 3 \quad \left(\text{since } \binom{n}{1} = n \text{ and} \right. \\ & \qquad \qquad \qquad \left. \binom{3}{2} = 3 \text{ as shown above} \right) \\ & = 6, \end{aligned}$$

$$\begin{aligned} \binom{5}{2} & \underset{*}{=} \binom{4}{1} + \binom{4}{2} = 4 + 6 \quad \left(\text{since } \binom{n}{1} = n \text{ and} \right. \\ & \qquad \qquad \qquad \left. \binom{4}{2} = 6 \text{ as shown above} \right) \\ & = 10, \end{aligned}$$

$$\binom{6}{2} \stackrel{*}{=} \binom{5}{1} + \binom{5}{2} = 10 + 5 \left(\text{since } \binom{n}{1} = n \text{ and} \right. \\ \left. \binom{5}{2} = 10 \text{ as shown above} \right) \\ = 15,$$

$$\binom{7}{2} \stackrel{*}{=} \binom{6}{1} + \binom{6}{2} = 15 + 6 \left(\text{since } \binom{n}{1} = n \text{ and} \right. \\ \left. \binom{6}{2} = 15 \text{ as shown above} \right) \\ = 21,$$

$$\binom{8}{2} \stackrel{*}{=} \binom{7}{1} + \binom{7}{2} = 21 + 7 \left(\text{since } \binom{n}{1} = n \text{ and} \right. \\ \left. \binom{7}{2} = 21 \text{ as shown above} \right) \\ = 28,$$

$$\binom{9}{2} \stackrel{*}{=} \binom{8}{1} + \binom{8}{2} = 28 + 8 \left(\text{since } \binom{n}{1} = n \text{ and} \right. \\ \left. \binom{8}{2} = 28 \text{ as shown above} \right) \\ = 36,$$

⋮

In sum,

$$\binom{2}{2} = 1,$$

$$\binom{3}{2} = 3,$$

$$\binom{4}{2} = 6,$$

$$\binom{5}{2} = 10,$$

$$\binom{6}{2} = 15,$$

$$\binom{7}{2} = 21,$$

$$\binom{8}{2} = 28,$$

⋮

As you can see, this is exactly the subject previously addressed (in “Review of Lectures — II”): The above is nothing else but the algorithm that yields

$$1 = 1,$$

$$1 + 2 = 3,$$

$$1 + 2 + 3 = 6,$$

$$1 + 2 + 3 + 4 = 10,$$

$$1 + 2 + 3 + 4 + 5 = 15,$$

$$1 + 2 + 3 + 4 + 5 + 6 = 21,$$

$$1 + 2 + 3 + 4 + 5 + 6 + 7 = 28,$$

⋮

⋮

The patterns which we already figured out in “Review of Lectures — II” for this sequence are

$$\begin{aligned}1 &= \frac{1}{2} \cdot 1 \cdot 2, \\3 &= \frac{1}{2} \cdot 2 \cdot 3, \\6 &= \frac{1}{2} \cdot 3 \cdot 4, \\10 &= \frac{1}{2} \cdot 4 \cdot 5, \\15 &= \frac{1}{2} \cdot 5 \cdot 6, \\21 &= \frac{1}{2} \cdot 6 \cdot 7, \\28 &= \frac{1}{2} \cdot 7 \cdot 8, \\&\vdots\end{aligned}$$

So,

$$\begin{aligned}\binom{2}{2} &= \frac{1}{2} \cdot 1 \cdot 2, \\ \binom{3}{2} &= \frac{1}{2} \cdot 2 \cdot 3, \\ \binom{4}{2} &= \frac{1}{2} \cdot 3 \cdot 4, \\ \binom{5}{2} &= \frac{1}{2} \cdot 4 \cdot 5, \\ \binom{6}{2} &= \frac{1}{2} \cdot 5 \cdot 6, \\ \binom{7}{2} &= \frac{1}{2} \cdot 6 \cdot 7, \\ \binom{8}{2} &= \frac{1}{2} \cdot 7 \cdot 8, \\ &\vdots\end{aligned}$$

These translate into

$$\boxed{\binom{n+1}{2} = \frac{1}{2}n(n+1)} \quad (n = 1, 2, 3, 4, \dots),$$

or the same

$$\boxed{\binom{n}{2} = \frac{1}{2}n(n-1)} \quad (n = 2, 3, 4, 5, \dots).$$

(As you can see, these two are mutually the shifting of n of each other.)

Since we already have $\binom{n}{2} = \binom{n}{n-2}$, that is,

$$\binom{2}{2} = \binom{2}{0},$$

$$\binom{3}{2} = \binom{3}{1},$$

$$\binom{4}{2} = \binom{4}{2},$$

$$\binom{5}{2} = \binom{5}{3},$$

$$\binom{6}{2} = \binom{6}{4},$$

$$\binom{7}{2} = \binom{7}{5},$$

⋮

we conclude

$$\boxed{\binom{n}{2} = \frac{1}{2}n(n-1)},$$

$$\boxed{\binom{n}{n-2} = \frac{1}{2}n(n-1)}$$

$$(n = 2, 3, 4, 5, \dots).$$

- Next, let's dissect $\binom{n}{3}$. We are going to use

Rule 3. $\binom{n+1}{3} = \binom{n}{2} + \binom{n}{3}$

(‘Rule k ’ in page 4 with $k = 3$). Below “*” underneath ‘=’ is where I have applied Rule 3.

$$\binom{3}{3} = 1 \quad \left(\text{since } \binom{n}{n} = 1 \text{ as shown above} \right),$$

$$\binom{4}{3} = 4 \quad \left(\text{since } \binom{n}{n-1} = n \text{ as shown above} \right),$$

$$\binom{5}{3} = 10 \quad \left(\text{since } \binom{n}{n-2} = \frac{1}{2}n(n-1) \text{ as shown above} \right),$$

$$\begin{aligned} \binom{6}{3} &\stackrel{*}{=} \binom{5}{2} + \binom{5}{3} \\ &= 10 + 10 \quad \left(\text{since } \binom{n}{2} = \frac{1}{2}n(n-1) \text{ and} \right. \\ &\quad \left. \binom{5}{3} = 10 \text{ as shown above} \right) \\ &= 20, \end{aligned}$$

$$\begin{aligned}
\binom{7}{3} &\stackrel{*}{=} \binom{6}{2} + \binom{6}{3} \\
&= 15 + 20 && \left(\text{since } \binom{n}{2} = \frac{1}{2}n(n-1) \text{ and} \right. \\
& && \left. \binom{6}{3} = 20 \text{ as shown above} \right) \\
&= 35,
\end{aligned}$$

$$\begin{aligned}
\binom{8}{3} &\stackrel{*}{=} \binom{7}{2} + \binom{7}{3} \\
&= 21 + 35 && \left(\text{since } \binom{n}{2} = \frac{1}{2}n(n-1) \text{ and} \right. \\
& && \left. \binom{7}{3} = 35 \text{ as shown above} \right) \\
&= 56,
\end{aligned}$$

$$\begin{aligned}
\binom{9}{3} &\stackrel{*}{=} \binom{8}{2} + \binom{8}{3} \\
&= 28 + 56 && \left(\text{since } \binom{n}{2} = \frac{1}{2}n(n-1) \text{ and} \right. \\
& && \left. \binom{8}{3} = 56 \text{ as shown above} \right) \\
&= 84,
\end{aligned}$$

In sum,

$$\binom{3}{3} = 1,$$

$$\binom{4}{3} = 4,$$

$$\binom{5}{3} = 10,$$

$$\binom{6}{3} = 20,$$

$$\binom{7}{3} = 35,$$

$$\binom{8}{3} = 56,$$

$$\binom{9}{3} = 84,$$

⋮

As you can see, this is exactly the subject previously addressed (in “Review of Lectures — III”): The above is nothing else but the algorithm that yields

$$1 = 1,$$

$$1 + 3 = 4,$$

$$1 + 3 + 6 = 10,$$

$$1 + 3 + 6 + 10 = 20,$$

$$1 + 3 + 6 + 10 + 15 = 35,$$

$$1 + 3 + 6 + 10 + 15 + 21 = 56,$$

$$1 + 3 + 6 + 10 + 15 + 21 + 28 = 84,$$

⋮

⋮

The patterns which we already figured out in “Review of Lectures — III” for this sequence are

$$\begin{aligned}1 &= \frac{1}{6} \cdot 1 \cdot 2 \cdot 3, \\4 &= \frac{1}{6} \cdot 2 \cdot 3 \cdot 4, \\10 &= \frac{1}{6} \cdot 3 \cdot 4 \cdot 5, \\20 &= \frac{1}{6} \cdot 4 \cdot 5 \cdot 6, \\35 &= \frac{1}{6} \cdot 5 \cdot 6 \cdot 7, \\56 &= \frac{1}{6} \cdot 6 \cdot 7 \cdot 8, \\84 &= \frac{1}{6} \cdot 7 \cdot 8 \cdot 9, \\&\vdots\end{aligned}$$

So,

$$\begin{aligned}\binom{3}{3} &= \frac{1}{6} \cdot 1 \cdot 2 \cdot 3, \\ \binom{4}{3} &= \frac{1}{6} \cdot 2 \cdot 3 \cdot 4, \\ \binom{5}{3} &= \frac{1}{6} \cdot 3 \cdot 4 \cdot 5, \\ \binom{6}{3} &= \frac{1}{6} \cdot 4 \cdot 5 \cdot 6, \\ \binom{7}{3} &= \frac{1}{6} \cdot 5 \cdot 6 \cdot 7, \\ \binom{8}{3} &= \frac{1}{6} \cdot 6 \cdot 7 \cdot 8, \\ \binom{9}{3} &= \frac{1}{6} \cdot 7 \cdot 8 \cdot 9, \\ &\vdots\end{aligned}$$

These translate into

$$\boxed{\binom{n+2}{3} = \frac{1}{6}n(n+1)(n+2)} \quad (n = 1, 2, 3, 4, \dots),$$

or the same

$$\boxed{\binom{n}{3} = \frac{1}{6}n(n-1)(n-2)} \quad (n = 3, 4, 5, 6, \dots).$$

(As you can see, these two are mutually the shifting of n of each other.)

Since we already have $\binom{n}{3} = \binom{n}{n-3}$, that is,

$$\binom{3}{3} = \binom{3}{0},$$

$$\binom{4}{3} = \binom{4}{1},$$

$$\binom{5}{3} = \binom{5}{2},$$

$$\binom{6}{3} = \binom{6}{3},$$

$$\binom{7}{3} = \binom{7}{4},$$

$$\binom{8}{3} = \binom{8}{5},$$

⋮

we conclude

$$\boxed{\binom{n}{3} = \frac{1}{6}n(n-1)(n-2)}, \quad \boxed{\binom{n}{n-3} = \frac{1}{6}n(n-1)(n-2)}$$

$$(n = 3, 4, 5, 6, \dots).$$

- And you know where I'm going. The next will be to dissect $\binom{n}{4}$. I would run the same argument, with necessary tweaks, relying on the result which we previously worked out in "Review of Lectures – IV", and conclude

$$\boxed{\binom{n}{4} = \frac{1}{24}n(n-1)(n-2)(n-3)}, \quad \boxed{\binom{n}{n-4} = \frac{1}{24}n(n-1)(n-2)(n-3)}$$

$$(n = 4, 5, 6, 7, \dots),$$

and so on so forth.

- **Summary.** Here is what we've got so far.

$$\binom{n}{0} = 1,$$

$$\binom{n}{n} = 1,$$

$$\binom{n}{1} = n,$$

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

$$\binom{n}{2} = \frac{1}{2}n(n-1),$$

$$\binom{n}{n-2} = \frac{1}{2}n(n-1),$$

$$\binom{n}{3} = \frac{1}{6}n(n-1)(n-2),$$

$$\binom{n}{n-3} = \frac{1}{6}n(n-1)(n-2),$$

$$\binom{n}{4} = \frac{1}{24}n(n-1)(n-2)(n-3),$$

$$\binom{n}{n-4} = \frac{1}{24}n(n-1)(n-2)(n-3),$$

$$\binom{n}{5} = \frac{1}{120}n(n-1)(n-2)(n-3)(n-4),$$

$$\binom{n}{n-5} = \frac{1}{120}n(n-1)(n-2)(n-3)(n-4),$$

⋮

⋮

Here, the progression of the denominator is

$$\begin{aligned}1 &= 1, \\2 &= 1 \cdot 2, \\6 &= 1 \cdot 2 \cdot 3, \\24 &= 1 \cdot 2 \cdot 3 \cdot 4, \\120 &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5, \\&\vdots \qquad \qquad \qquad \ddots\end{aligned}$$

Actually, if you want to see more of these

$$\begin{aligned}1 &= 1, \\2 &= 1 \cdot 2, \\6 &= 1 \cdot 2 \cdot 3, \\24 &= 1 \cdot 2 \cdot 3 \cdot 4, \\120 &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5, \\720 &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6, \\5040 &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7, \\40320 &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8, \\362880 &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9, \\3628800 &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10, \\&\vdots \qquad \qquad \qquad \ddots\end{aligned}$$

By the way, how do these numbers grow? Is there any patterns?

$$\left(\begin{array}{l} \text{One way to look at it is it is } \underline{\text{the multiplication version}} \text{ of} \\ \\ 1 = 1, \\ 3 = 1 + 2, \\ 6 = 1 + 2 + 3, \\ 10 = 1 + 2 + 3 + 4, \\ 15 = 1 + 2 + 3 + 4 + 5, \\ 21 = 1 + 2 + 3 + 4 + 5 + 6, \\ 28 = 1 + 2 + 3 + 4 + 5 + 6 + 7, \\ 36 = 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8, \\ \vdots \qquad \qquad \qquad \ddots \end{array} \right)$$

You might ask: “Is there a formula?” “How fast is the growth rate?” Excellent questions. Actually, these numbers play very special and important roles in mathematics. They make frequent appearances in all corners of mathematics. Besides, they are interesting in their own right. So, I am going to revisit this subject later.

- So, in any case, the above results (‘Summary’ two pages ago) are compressed in one single line, and that is our Formula A. Let’s duplicate it:

Formula A (binomial coefficients).

Let n and k be integers, with $0 < k < n$. Then

$$\boxed{\binom{n}{k} = \frac{n (n-1) (n-2) \cdots (n-k+1)}{1 \cdot 2 \cdot 3 \cdots k}} .$$

Last time I did not quite explain why this formula is true. Now the above is why this is true. The argument relied on our previous lectures (“Review of Lectures — II, III and IV”).

- **Fermat Primes, Mersenne Primes.**

Change the subject. Do you remember 2-to-the-powers? Yes, they are

$$\begin{aligned} 2^1 &= 2, \\ 2^2 &= 4, \\ 2^3 &= 8, \\ 2^4 &= 16, \\ 2^5 &= 32, \\ 2^6 &= 64, \\ 2^7 &= 128, \\ 2^8 &= 256, \\ 2^9 &= 512, \\ 2^{10} &= 1024, \\ 2^{11} &= 2048, \\ 2^{12} &= 4096, \\ 2^{13} &= 8192, \\ 2^{14} &= 16384, \\ 2^{15} &= 32768, \\ 2^{16} &= 65536, \\ \vdots &\quad \quad \quad \vdots \end{aligned}$$

Now, just out of the blue, do you remember that, on Day 1, I talked a little bit about how vexing the prime number distribution is? Yes? Good. But what do the 2-to-the-powers have to do with it? They seemingly have nothing to do with each other, because (with the obvious exception of 2) none of the 2-to-the-powers is a prime. Not so fast. Let me answer it. Adding 1 to, or subtracting 1 from, those 2-to-the-powers suddenly have a bearing on the business of the mystery of primes. Historically speaking, the following types of numbers drew attention of mathematicians in relation to large primes.

Definition. (1) A number of the form

$$\boxed{2^n + 1}, \quad n: \text{ a positive integer}$$

is called a Fermat number .*

- If it is a prime, then it is called a Fermat prime .*

(2) A number of the form

$$\boxed{2^n - 1}, \quad n: \text{ a positive integer}$$

is called a Mersenne number .**

- If it is a prime, then it is called a Mersenne prime .**

On Day 1 I said there are infinitely many primes, and that fact has been long known since Euclid (B.C. 300, c.). But what I didn't say is that does not mean that we have a list that contains infinitely many concrete examples of primes. In fact, no one has (on this planet). Indeed, what I am going to say next is potentially confusing, so listen carefully:

There is such a thing called '*the largest known prime*'.

It means as follows: Somebody has offered one particular number (a positive integer), a very very large number, and has mathematically proved that it is indeed a prime. Moreover, no one has offered another, larger, number and has mathematically proved that it is a prime. So, 'the largest known prime' is dependent on time, it keeps getting replaced by larger ones as the time progresses, because people are working on getting hold of larger and larger primes. So, the nature of 'the largest known prime' is, it is not permanent, but it is constantly updated. The largest known prime today may not be the largest known prime tomorrow. Now, this process (of getting hold of larger primes) is heavily computer-dependent. But I am going to say something equally important about the roles of computers in a little bit.

*Named after Pierre de Fermat (1601(?)–1665).

**Named after Marin Mersenne (1548–1648).

The reason why I say this is potentially confusing is that we know for fact that there are indeed infinitely many primes. But the crux of the matter is, for each given prime p , we, human being, do not know of a concrete formula for the next prime, or not even a formula that generates any prime larger than p . So that's why it makes sense to recognize such and such number is a prime, and it is "so far" the largest prime known to us, human beings. Maybe somewhere out in the universe, there is a planet where there is an intelligence, something like us, humans, live there, and they do know such a formula. Who knows. Now, the largest known primes are typically (here I say 'typically' because like I said, this is constantly updated) a Mersenne prime. That's one reason (one of the many reasons) why Mersenne primes draw public attention.

Meanwhile, Fermat primes, "kissing cousins" of Mersenne primes, are of special interest after the striking discovery by a mathematician named Gauss*: Gauss has answered one problem famous at that time (the late 18th century, that is), that, if N is a Fermat prime, then a regular polygon with N edges, namely, a figure inscribed in a circle that has N straight edges and N vertices, and those N vertices are evenly distributed on the perimeter of the circle, is drawn only using straightedge and compass. So, for example, a regular heptadecagon (a regular polygon with $N = 2^{2^2} + 1 = 17$ edges) can be drawn only with straightedge and compass.*

Here, please don't dismiss it by saying "computers can draw just about any of those figures". I want to elaborate this point, because this is important. There is a precise mathematical meaning attached to the expression "*something can be drawn only with straightedge and compass.*" When I talk about drawings of figures, what you are thinking is either an ink spead on a sheet or a collection of dots, or 'pixels', in case it is digitally drawn. But every stroke has thickness, no matter how thin it is, just that the thickness is thin enough so from a distance it looks like lines and circles but they are actually 'bands', and moreover the width of the bands is not exactly even, if you care to use a microscope to magnify it, partially because the surface of the paper (or LCD screen) is not exactly even or flat. But we draw figures in math classes, and our stance is we '*pretend*' that those strokes have no width.

*Carl Friedrich Gauss (1777–1855). B. Riemann (1826–1866) is Gauss' disciple.

*Someone has created a visual motion picture of 64 steps to draw the regular heptadecagon based on Gauss' formula:

<http://en.wikipedia.org/wiki/File:HeptadecagonConstructionAni.gif>

Now, keeping that scope intact, yes, of course, your computer can draw an ‘*approximate*’ figure within the margin of the thickness of a stroke. But what I am talking about is something else. In mathematics, a statement “such and such polygon is drawn only with straightedge and compass” means that the pair of numbers that pinpoint the location of any of its vertices relative to the origin of the coordinate (the coordinate readings of the referenced vertex) both belong to a sequence of numbers where each member in that sequence arises as a root of a certain quadratic equation whose coefficients reside in a ‘field generated by’ the previous member of the same sequence, where a field generated by a certain number means the smallest number system that contains that number and all integers that is closed under addition, subtraction, multiplication, and division. So, in the context of feasibility of drawing figures, the computer’s drawing ability is irrelevant. A side note: As you can probably extrapolate from my tone, mathematicians are actually more interested in the ‘feasibility’ of drawing more so than the actual process of drawing when feasible. And that ‘feasibility’ part is highly ‘theoretical’. Certain polygons are mathematically proved to be impossible to be drawn. And when I state something like that, I strictly adhere to the above definition as to the interpretation of ‘impossible’. Computers do not make a difference in this case. The simplest regular polygon (a regular polygon with fewest number of edges) that is proved to be impossible to be drawn is a regular heptagon (seven vertices evenly distributed across the perimeter of a circle). So, folks, seven is not feasible whereas seventeen is feasible. Interesting, huh?

Now, no body has managed to answer the following fundamental questions:

(Open) Question 1. Are there infinitely many Fermat primes?

(Open) Question 2. Are there infinitely many Mersenne primes?

As for Question 1, it is well-known that in order for a Fermat number $2^n + 1$ to be a prime, n has to be a 2-to-the-power in itself. So we denote

$$\begin{aligned}
 F_1 &= 2^{2^1} + 1 = 2^2 + 1 = 5, \\
 F_2 &= 2^{2^2} + 1 = 2^4 + 1 = 17, \\
 F_3 &= 2^{2^3} + 1 = 2^8 + 1 = 257, \\
 F_4 &= 2^{2^4} + 1 = 2^{16} + 1 = 65537, \\
 F_5 &= 2^{2^5} + 1 = 2^{32} + 1 = 4294967297, \\
 &\vdots
 \end{aligned}$$

Fermat, a 17-th century mathematician, has observed that F_1 , F_2 , F_3 , and F_4 are all primes. Then he rushed to conclusion that all F_k are primes. Alas, as it turned out, F_5 was a non-prime:

$$4294967297 = 641 \cdot 6700417.$$

This factorization was discovered by Euler*, thus Euler has refuted what Fermat was falsely led to believe. Now, today with all the modern computer technology, all F_k s up to F_{42} are computed. Surprisingly enough, none of them except the first four: F_1 , F_2 , F_3 , and F_4 , are primes. To this day no one knows if there is a Fermat prime other than F_1 , F_2 , F_3 , and F_4 . (You will become instantly famous if you discover one. But there is no guarantee that there is indeed one. Alternatively, if you manage to prove that the only Fermat primes are F_1 , F_2 , F_3 and F_4 , then you will become famous. But of course there is no guarantee that that statement is true.)

As for Question 2, it is well-known that, in order for a Mersenne number $2^n - 1$ to be a prime, n has to be a prime in itself. However, the subtlety of the matter is, not all numbers of the form $2^p - 1$, with p prime, is a Mersenne prime. For example, even though $p = 11$ is a prime,

$$2^{11} - 1 = 2047 = 23 \cdot 89$$

is not a prime. That's why Question 2 makes sense. According to Wikipedia, the largest known prime as of December, 2014, is actually a Mersenne prime, and it is

$$2^{57885161} - 1.$$

This is a number that carries 17425170 digits.

Mersenne primes are of interest because it is closely related to another famous open problem: "*Are all perfect numbers even?*" Here, a perfect number is a positive integer k such that, if you add up all of its divisors, including 1 and excluding k itself, then the sum equals k . But that's a whole nother subject. I shall stop here.

*Leonhard Euler (1707–1783).