Комбинаторни тъждества. Формула на Стирлинг. Терема на Льожандер. Теорема на Люка. Теорема на Кумер.

Лектор: д-р Д. Кралчев (2021-03-04)

$n! = (n-1)! \times n$, за $n \in \mathbb{N}_0$, като $0! = 1$, $k, n \in \mathbb{N}$.

$\binom{n}{k} = \frac{n!}{k!(n-k)!}$, $0 \le k \le n$; $k, n \in \mathbb{N}$ (като понякой път се обобщава и се приема, че при $k > n$: $\binom{n}{k} = 0$).

$\binom{n}{k}$ е броя на начините, по които може да изберем k елемента от n без да ги подреждаме. $\binom{n}{k}$ също така са биномните коефициенти:

$$(x+y) = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

$(x+1)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$, т.е. погледнато по друг начин, обикновената пораждаща функция на редицата $a_k = \binom{n}{k} x^k$ е $(x+1)^n$. А най-просто казано, това е биномната формула на Нютон.

Свойства (комбинаторни тъждества):

Методи за доказване:

- математическа индукция;
- свеждане до други тъждества, в т.ч. биномната формула;
- комбинаторни разсъждения:
    - двукратно преброяване;
    - построяване на биекция.

Тъждесво 1. $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ (Тъждество на Паскал)

Алтернативен запис: $\binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k}$

Доказателство:

I н/н: (двукратно преброяване) Знаем, че $\binom{n}{k}$ е броя на начините, по които може да изберем k елемента от общо n елемента без наредба. Тези начини може да ги преброим и по следния алтернативен начин:
Нека фиксираме един от n-те елемента. Той или е сред избраните или не е. Ако е от избраните, то от останалите $n-1$ елемента трябва да изберем $k-1$, което става по $\binom{n-1}{k-1}$ начина. Ако фиксираният елемент обаче не е от избраните, то от останалите $n-1$ елемента трябва да изберем всичките k, което става по $\binom{n-1}{k}$ начина. Следователно $\underbrace{\binom{n-1}{k-1}}_{\text{фикс. ел. е от избраните}} + \underbrace{\binom{n-1}{k}}_{\text{фикс. ел. НЕ е от избраните}} = \binom{n}{k}$, което искахме да докажем.

II н/н: (грубо прилагане на дефиницията) $\binom{n-1}{k-1} + \binom{n-1}{k} =$

$$= \frac{(n-1)!}{(k-1)!(n-\cancel{1}-k+\cancel{1})!} + \frac{(n-1)!}{k!(n-1-k)!} = \frac{(n-1)!}{(k-1)!(n-k-1)!}\left(\frac{1}{n-k}+\frac{1}{k}\right) =$$

$$= \frac{(n-1)!}{(k-1)!(n-k-1)!} \times \frac{n}{k(n-k)} = \frac{n!}{k!(n-k)!} = \binom{n}{k}.$$

Тъждесво 2. $\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n} = 2^n$.

Доказателство:

I н/н: (биномна формула)

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^k 1^{n-k} = \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n}$$

II н/н: (двукратно преброяване)

$\binom{n}{k}$ е броя на k елементните подмножества на n. Броят на всички подмножества на n елементно множество са 2^n (всеки от n-те елемента или участва или не участва: $\underbrace{2 \times 2 \times \ldots \times 2}_{n}$ възможности). Пускаме k да пробягва от 0 до n и сумираме целия брой и получаваме исканото тъждество.

Тъждесво 3. $\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$

<u>Доказателство</u>:

<u>I н/н: (прилагане на формулата от дефиницията)</u>

$$\frac{n}{k}\binom{n-1}{k-1} = \frac{n}{k} \times \frac{(n-1)!}{(k-1)!(n-\cancel{1}-k+\cancel{1})!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}.$$

Тъждесво 4. $\binom{n}{i}\binom{n-i}{j} = \binom{n}{j}\binom{n-j}{i}$.

<u>Доказателство</u>:

<u>I н/н (комбинаторни разсъждения)</u>: Няма никакво значение дали от n елемента първо ще изберем i и от останалите ще изберем j или първо ще изберем j и от останалите ще изберем i по отношение на ничините, по които може да го направим.
<u>II н/н (грубо прилагане на дефиницита)</u>:
$\binom{n}{i}\binom{n-i}{j} = \frac{n!}{i!\cancel{(n-i)!}}\frac{\cancel{(n-i)!}}{(n-i-j)!} = \frac{n!}{i!j!(n-i-j)!}$, и тъй като израза е симетричен спрямо i и j, то ще получим същия израз ако им разменим позициите, което е дясната страна на тъждеството, което искаме да докажем.

Тъждество 5. Докажете, че $\binom{m+n}{k} = \sum_{i=0}^{k}\binom{m}{i}\binom{n}{k-i}$ (Тъждество на Вандермонд).

<u>Доказателство</u>: (двукратно преброяване)

Допускаме, че имаме множество A, което се състои от $m+n$ елемента:

$A = \{a_1, a_2, a_3, \ldots, a_m, b_1, b_2, \ldots, b_n\}$. Искаме да намерим броя на k-елементните подмножества на A. Те са $\binom{n+m}{k}$. Друг начин, по който може да го направим това е като първо изберем i елемента от $\{a_1, a_2, a_3, \ldots, a_m\}$ и след това изберем $k-i$ елемента от $\{b_1, b_2, \ldots, b_n\}$. Това може да бъде направено по $\binom{m}{i}\binom{n}{k-i}$

начина. Но i може да заема всяка стойност от 0 до k, следователно $\binom{m+n}{k} = \sum_{i=0}^{k} \binom{m}{i} \binom{n}{k-i}$.

<u>Теорема на Льожандер</u>

За всяко просто число p и всяко положително число n, нека $\nu_p(n)$ е експонентата на най-голямата степен на p, която дели n. Тогава $\nu_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$.

Формулата е записана като безкрайна сума, но за всеки две фиксирани стойности на n и p тази сума има само краен брой ненулеви събираеми: за всяко достатъчно голямо i, за което $p^i > n$, $\left\lfloor \frac{n}{p^i} \right\rfloor = 0$.

<u>Доказателство</u>: Тъй като $n!$ е произведението на целите числа от 1 до n, намираме колко от числата $\{1,2,...,n\}$ имат поне един делител p: $\left\lfloor \frac{n}{p} \right\rfloor$. За всяко число което се дели на p^2 ще имаме, че съдържа допълнителен множител p, всяко число което се дели на p^3 съдържа допълнителен множител на p и т.н. Събирайки резултатите от тези целочислени деления дава безкрайната сума за $\nu_p(n!)$.

Пример 1: На колко нули завършва числото $2021!$?

Броя на завършващите нули на едно число е равен на най-голямата степен на 10, която дели числото. Ако едно число се дели на 10, то то ще се дели на 2 и на 5, тъй като в $2021!$ (и попринцип в $n!$) четните числа се срещат много по-често от делящите се на 5, то достатъчно ще е да преброим каква е най-голямата степен на 5 която дели $2021!$.

$$\nu_5(2021!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{5^i} \right\rfloor = \left\lfloor \frac{2021}{5} \right\rfloor + \left\lfloor \frac{2021}{5^2} \right\rfloor + \left\lfloor \frac{2021}{5^3} \right\rfloor + \left\lfloor \frac{2021}{5^4} \right\rfloor + 0 + \ldots = 404 + 80 + 16 + 3 = 503$$

Приближение на биномни коефициенти (<u>Формула на Стирлинг</u>):

$$n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n.$$

Приближение 1. Намерете добро приближение на $\binom{2n}{n}$.

<u>Решение</u>:

Едно добро асимптотично приближение ще получим прилагайки формулата на Стирлинг:

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2} \sim \frac{\sqrt{4\pi n}\left(\frac{2n}{e}\right)^{2n}}{2\pi n\left(\frac{n}{e}\right)^{2n}} = \frac{4^n}{\sqrt{\pi n}}.$$

Деление на биномен коефициент (<u>Теорема на Люка</u>):

$$\binom{m}{n} \equiv \prod_{i=0}^{k-1}\binom{m_i}{n_i} \mod p,$$

където p е просто число, $m = \overline{(m_{k-1}m_{k-2}\ldots m_0)}_p$ и $n = \overline{(n_{k-1}n_{k-2}\ldots n_0)}_p$ са представянията на числата m и n в p-ична бройна система.

Пример 2:

Да се определи четността на числото $\binom{23}{16}$.

Решение:

$23 = \overline{11101}_2$, $16 = \overline{10000}_2$. Следователно от теоремата на Люка ще имаме, че:

$\binom{23}{16} \equiv \binom{1}{1}\binom{1}{0}\binom{1}{0}\binom{0}{0}\binom{1}{0} \equiv 1.1.1.1.1 \equiv 1 \mod 2$. Т.е. числото е нечетно.

Ако се случи така, че числата да не са с равен брой цифри, тогава може или да запълним липсващите цифри с нули или тъй като всяко число над 0 винаги дава единица, то може просто да не взимаме предвит тези числа, които са в повече.

Нека например проверим каква е четността на $\binom{23}{4}$:

$23 = \overline{11101}_2$, $16 = \overline{100}_2$

$\binom{23}{4} \equiv \binom{1}{1}\binom{0}{0}\binom{1}{0} \equiv 1.1.1 \equiv 1 \mod 2$, т.е. и това число не е четно.

С други думи, приемаме, че и двете числа са в p-ична бройна система.

Пример 3: Какъв остатък дава числото $\binom{588}{277}$ при деление на 5?

<u>Решение</u>: Имаме, че $588 = \overline{4323}_5$ и $277 = \overline{2102}_5$. Следователно , от теоремата на Люка, $\binom{588}{277} \equiv \binom{4}{2}\binom{3}{1}\binom{2}{0}\binom{3}{2} = 6 \times 3 \times 1 \times 3 = 54 \equiv 4 \mod 5.$

Доказателство (Теорема на Люка):

$\binom{n}{k} \equiv 0 \mod n$, винаги когато n е просто число и $0 < k < n$ (т.е. $k \neq 0$ и $k \neq n$).

Простият факт по-горе следва директно от елементарни разсъждения по формулата $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$ и допълнителни условия за n и k. В числителя, n ще остане несъкратено до последното съкращение.

Нека $f(x)$ и $g(x)$ са полиноми. Ще казваме, че $f(x) \equiv g(x) \mod p$, ако коефициентите пред k-тите им степени, където k пробягва от 0 до $\max\Big((\deg\big(f(x)\big), \deg\big(g(x)\big)\Big)$, са сравними по модул от p ($\equiv \mod p$).

$$(1+x)^p \equiv 1^p + \binom{p}{1} x^{p-1} + \binom{p}{2} x^{p-2} + \ldots + x^p \equiv 1 + x^p \mod p$$
$$(1+x)^{p^2} \equiv \big((1+x)^p\big)^p \equiv (1+x^p)^p \equiv 1 + x^{p^2} \mod p$$
$$\ldots$$
$$(1+x)^{p^k} \equiv 1 + x^{p^k} \mod p$$

Нека $m = m_0 + m_1 p + m_2 p^2 + \ldots + m_k p^k = \sum_{i=0}^{k} m_i p^i$ е представянето на числото n в p-ична бройна система. От предходната лекция ние знаем, че всяко число има единствено представяне в такъв вид.

Тогава,

$$\sum_{n=0}^{m} \binom{m}{n} x^n = (1+x)^m = (1+x)^{\left(m_0 + m_1 p + \ldots + m_k p^k\right)} = \prod_{i=0}^{k} \left((1+x)^{p^i}\right)^{m_i} \equiv$$

$$\equiv \prod_{i=0}^{k} \left(1 + x^{p^i}\right)^{m_i} = \prod_{i=0}^{k} \left(\sum_{n_i=0}^{m_i} \binom{m_i}{n_i} x^{n_i p^i} \right) = \prod_{i=0}^{k} \left(\sum_{n_i=0}^{p-1} \binom{m_i}{n_i} x^{n_i p^i} \right) =$$

$$\sum_{n=0}^{m} \left(\prod_{i=0}^{k} \binom{m_i}{n_i} \right) x^n \mod p.$$

Задача 1. (**следствие на Люка**) Колко от биномните коефициенти в n-тия ред на триъгълника на Паскал се делят на p, където p е просто число?

Решение:

Т.е. искаме да видим колко биномни коефициенти от вида $\binom{n}{m}$, за $m = 0,1,2,...,n$, **не** се делят на просто число p, тъй като знаем, че на всеки ред има $n + 1$ числа.

От теоремата на Люка, знаем че $\binom{n}{m} \equiv \binom{n_0}{m_0}\binom{n_1}{m_1}\dots\binom{n_k}{m_k} \mod p$, където $n = (\overline{n_0 n_1 \dots n_k})_p$ и $m = (\overline{m_0 m_1 \dots m_k})_p$ са записите на числата n и m в p-ична бройна система.

Тъй като записите са в p-ична бройна система, то всяко едно от числата n_i и m_i за $i = \overline{1,k}$ ще е най-много $p - 1$. Т.е. за да **не** се дели $\binom{n_0}{m_0}\binom{n_1}{m_1}\dots\binom{n_k}{m_k}$ на p е необходимо нито един от множителите $\binom{n_i}{m_i}$, за $i = \overline{1,k}$ да не се нулира. За да бъде изпълнено последното е необходимо да се удовлетворява условието: $m_i \leq n_i$. Тъй като n_i и m_i са цифри, то тогава ще имаме:

$m_0 : 0,1,2,...,n_0$ - общо $n_0 + 1$ възможности за m_0
$m_1 : 0,1,2,...,n_1$ - общо $n_1 + 1$ възможности за m_1
$\dots$
$m_k : 0,1,2,...,n_k$ - общо $n_k + 1$ възможности за m_k

Тоест ще имаме общо $(n_0 + 1)(n_1 + 1)\dots(n_k + 1) = \prod_{i=0}^{k}(n_i + 1)$ възможности за числата m, при които $\binom{n}{m}$ **не** се дели на p, а при всички останали случай ще имаме поне едно $j : 0 < j < k$ и $m_j > n_j \longrightarrow \binom{n_j}{m_j} = 0$.

Отговор: $n + 1 - \prod_{i=0}^{k}(n_i + 1)$, където n_i е i-тата цифра в представянето на числото n в p-ична бройна система.

Пример 4:

Колко от числата на седмия ред от триъгълника на Паскал се делят на 7, а на 5 ?
$7 = \overline{10}_7$ и $7 = \overline{12}_5$

Следователно броя на числата от седмия ред, които се делят на 7 е:
$7 + 1 - (1 + 1)(0 + 1) = 6,$
а броя на числата от седмиця ред, които се делят на 5 е:
$7 + 1 - (1 + 1)(1 + 2) = 2$

В действителност:

$$
\begin{array}{cccccccccccccccccc}
 & & & & & & & & 1 & & & & & & & & & \longleftarrow 0 \\
 & & & & & & & 1 & & 1 & & & & & & & & \longleftarrow 1 \\
 & & & & & & 1 & & 2 & & 1 & & & & & & & \longleftarrow 2 \\
 & & & & & 1 & & 3 & & 3 & & 1 & & & & & & \longleftarrow 3 \\
 & & & & 1 & & 4 & & 6 & & 4 & & 1 & & & & & \longleftarrow 4 \\
 & & & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & & & & \longleftarrow 5 \\
 & & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 & & & \longleftarrow 6 \\
 & 1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1 & & \longleftarrow 7 \\
\dots & & \dots & & \dots & & \dots & & \dots & & \dots & & \dots & & \dots & & & \dots
\end{array}
$$

Пример 5:

Колко от числата на 2021-вия ред от триъгълника на Паскал **не** се делят на 13?
$2021 \,|\, 13 = 155 \,|\, 13 = 11 \,|\, 13 = \mathbf{11}$

$$
\begin{array}{r}
\underline{13\ } \\
72 \\
\underline{65} \\
\mathbf{6}
\end{array}
\qquad
\begin{array}{r}
\underline{13\ } \\
25 \\
\underline{13} \\
\mathbf{12}
\end{array}
$$

Т.е. $2021 = \overline{11\ 12\ 6}_{13}$. По следствието от теоремата на Люка, броя на търсените числа е равен на: $(11 + 1)(12 + 1)(6 + 1) = 12 \times 13 \times 7 = \mathbf{1092}$. А пък останалите, които се делят

на 13 са $\;\begin{array}{r} \overset{...}{2021} \\ -\ \underline{1092} \\ 0939 \end{array}$, т.е. $\mathbf{939}$.

Пример 6:

Колко от числата от 5-тия ред на триъгълника на паскал са нечетни?

$5 = \overline{101}_2$, следователно от следствието на теоремата на Люка ще имаме, че точно $(1 + 1)(1 + 0)(1 + 1)$ ще е броя на числата, които не се делят на 2 в 5-тия ред. Т.е. 4 числа.

Пример 7: Може ли ред от триъгълника на Паскал да има точно 1000 нечетни числа?

Не, тъй като в двойчна бройна система, всяко едно естествено число ще има представяне само с 0 и 1. Добавяйки 1-ци към всяка една цифра от това представяне ще получим само 1-ци и 2-ки, чието произведение ще резултира единствено в точни степени на двойката, каквато числото 1000 не е.

Извод: Броя на нечетните числа във всеки ред от триъгълника на паскал е точна степен на двойката!

<u>**Треорема на Кумер**</u>

Теоремата на Кумер ни дава коя е най-високата степен на p, която дели биномния коефициент $\binom{m}{n}$, където p е просто число.

Ако p не дели $\binom{m}{n}$, то отговора ще е 0. С други думи, теоремата на Кумер е интересна само в случая когато от теоремата на Люка получим остатък 0.

<u>Формулата гласи следното</u>: Записваме m и n в p-ична бройна система и изваждаме m от n $(m > n)$. Броя на пътите, в които взимаме „едно на ум“ (едно на заем от по-старшата цифра) е равен на най-високата степен на p, която дели биномния коефициент.

Пример 8: Коя е най-високата степен на 3, която дели $\binom{100}{50}$?

Решение:

$$
\begin{array}{llll}
100\,|\,3 = & 33\,|\,3 = & 11\,|\,3 = & 3\,|\,3 = \mathbf{1} \\
\underline{\;9\;} & \underline{33} & \underline{\;9\;} & \underline{\;3\;} \\
10 & \mathbf{0} & \mathbf{2} & \mathbf{0} \\
\underline{\;9\;} & & & \\
\mathbf{1} & & &
\end{array}
\qquad
\begin{array}{lll}
50\,|\,3 = & 16\,|\,3 = & 5\,|\,3 = \mathbf{1} \\
\underline{\;3\;} & \underline{15} & \underline{\;3\;} \\
20 & \mathbf{1} & \mathbf{2} \\
\underline{18} & & \\
\mathbf{2} & &
\end{array}
$$

Т.е. получихме, че $100 = \overline{10201}_3$ и $50 = \overline{1212}_3$

$$
\begin{array}{r}
\_\,\dot{1}\dot{0}\dot{2}\dot{0}1 \\
\underline{01212} \\
01212
\end{array}
$$

Следователно 3^4 дели C_{100}^{50}, но 3^5 **не** го дели. Т.е. отговора е 4.

Доказателството на теоремата на Кумер става чрез теоремата на Люжандер.

Доказателство (Теорема на Кумер):

$\binom{n}{m} = \dfrac{n!}{m!(n-m)!}$, проверяваме колко пъти множителя p се среща в числителя и колко

в знаменателя. Следователно $\nu_p\left(\binom{n}{m}\right) = \nu_p(n!) - \nu_p(m!) - \nu_p\left((n-m)!\right)$. Т.е. имаме, че: $\nu_p\left(\binom{n}{m}\right) = \sum_{i=1}^{\infty}\left\lfloor \dfrac{n}{p^i}\right\rfloor - \sum_{i=1}^{\infty}\left\lfloor \dfrac{m}{p^i}\right\rfloor - \sum_{i=1}^{\infty}\left\lfloor \dfrac{n-m}{p^i}\right\rfloor =$

(n и m са по-малки от p^{k+1} и щом са по-малки знаем, че многоточието в сумата ще има значение само до степен k)

$$= \left\lfloor \frac{n}{p}\right\rfloor + \left\lfloor \frac{n}{p^2}\right\rfloor + \ldots + \left\lfloor \frac{n}{p^k}\right\rfloor$$

$$- \left\lfloor \frac{m}{p}\right\rfloor - \left\lfloor \frac{m}{p^2}\right\rfloor - \ldots - \left\lfloor \frac{m}{k}\right\rfloor$$

$$-\left\lfloor \frac{n-m}{p}\right\rfloor - \left\lfloor \frac{n-m}{p^2}\right\rfloor - \ldots - \left\lfloor \frac{n-m}{p^k}\right\rfloor =$$

Записваме n и m в p-ична бройна система:

$$n = n_0 + n_1p + n_2p^2 + \ldots + n_kp^k$$
$$m = m_0 + m_1p + m_2p^2 + \ldots + m_kp^k$$

Б.о.о. може да считаме, че m и n имат равен брой цифри в p-ична бройна система (ако нямат-допълваме с водещи нули по-късия запис)

$$\left(\left\lfloor \frac{n}{p}\right\rfloor = \left\lfloor \frac{n_0}{p} + n_1 + n_2p + \ldots + n_kp^{k-1}\right\rfloor = \left\lfloor n_1 + n_2p + \ldots + n_kp^k\right\rfloor\right)$$

$$= \begin{array}{lll} \overline{n_k\ldots n_2n_1}_p + & \overline{n_k\ldots n_2}_p + & \ldots + n_k \\ -\overline{m_k\ldots m_2m_1}_p - & \overline{m_k\ldots m_2}_p - & \ldots - m_k = \\ -\overline{z_k\ldots z_2z_1}_p - & \overline{z_k\ldots z_2}_p - & \ldots - z_k \end{array}$$

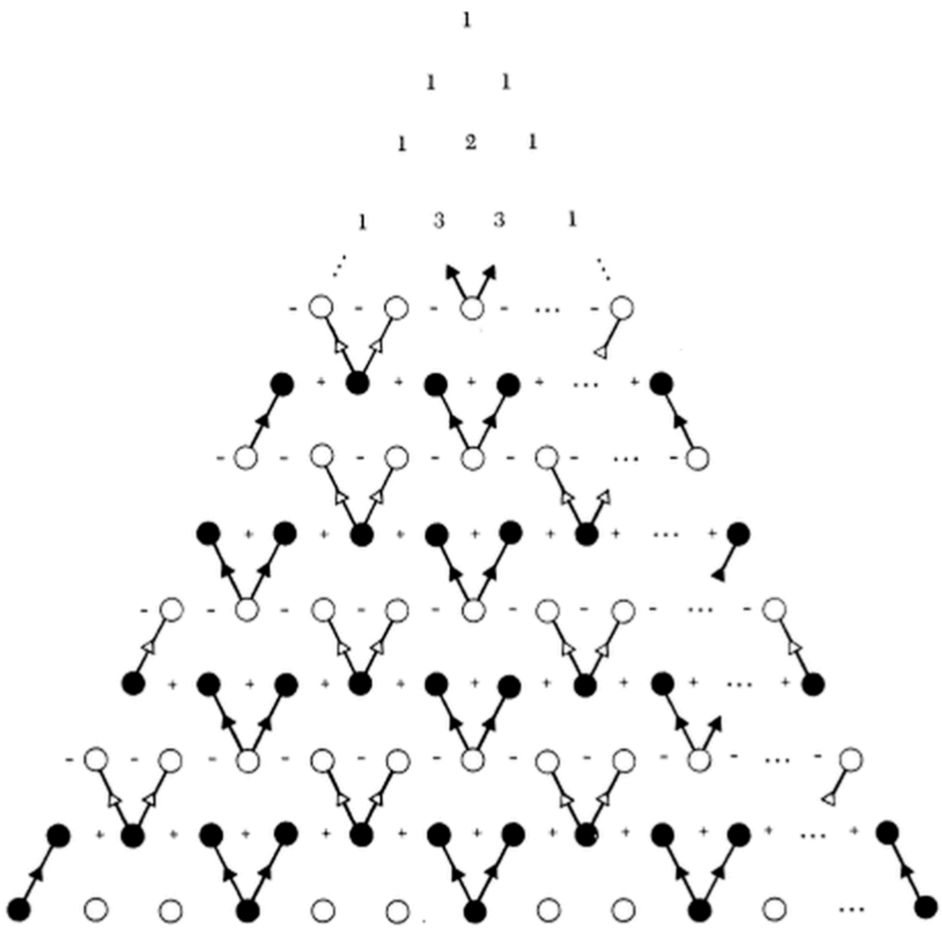
$$= \underbrace{\text{или 0 или 1}}_{\substack{\text{в зависимост от това} \\ \text{дали сме взели „едно на ум“)} \\ \text{когато сме изваждали } m_0 \text{ от } n_0}} + (0 \text{ или } 1) + \ldots + (0 \text{ или } 1) = \sum 1, \text{ което}$$

съответства на броя на броя на преносите, което искахме да докажем.

$\square$

Доказателство без думи на едно тъждество.

Доказателство без думи на тъждеството: $3\sum_{j=0}^{n}\binom{3n}{3j} = 8^n + 2(-1)^n$, чрез включване и изключване в триъгълника на Паскал.



$$\sum_{j=0}^{n}\binom{3n}{3j} = \sum_{j=1}^{3n-1}(-1)^{j-1}2^{3n-j} = -\,2^{3n}\sum_{j=1}^{3n-1}\left(-\frac{1}{2}\right) = \frac{8^n + 2(-1)^n}{3}.$$

- Dean S. Clark (University of Rhode Island, Kingston, RI 02881)

$\square$