$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : a^{-1} \bmod n \text{ istnieje}\} = \{a \in \mathbb{Z}_n : a \perp n\}$

$\varphi(n) = |\mathbb{Z}_n^*|$

$n = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_k^{n_k} \Rightarrow \varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right)$

Twierdzenie Eulera:

$$a \perp n \Rightarrow n \mid a^{\varphi(n)} - 1$$

Dowód: $n \mid a^{\varphi(n)} - 1 \iff a^{\varphi(n)} \equiv 1 \bmod n \iff a^{\varphi(n)} \bmod n = 1$

$$\prod_{x \in \mathbb{Z}_n^*} x \bmod n = \prod_{x \in \mathbb{Z}_n^*} (x \cdot a) \bmod n = a^{|\mathbb{Z}_n^*|} \prod_{x \in \mathbb{Z}_n^*} x \bmod n$$

$$\prod_{x \in \mathbb{Z}_n^*} x = a^{\varphi(n)} \prod_{x \in \mathbb{Z}_n^*} x \Rightarrow 1 = a^{\varphi(n)} \quad \blacksquare$$

Małe twierdzenie Fermata:

$$\boxed{a \perp p \equiv p \nmid a}$$

$$(a \perp p \Rightarrow p \mid a^{p-1} - 1) \equiv (p \mid a^p - a)$$

dwa równoważne twierdzenia

$$p \nmid a \iff a \perp p \Rightarrow p \mid a^{\varphi(n)} - 1 \quad i \quad \varphi(p) = p - 1$$

Zasada szufladkowa Dirichleta:

Mamy k szufladek i (k+1) kulek, wtedy istnieje szufladka, w której są dwie kulki. Jeśli mamy (sk+1) kulek, to istnieje szufladka, w której jest s+1 kulek.

Twierdzenie:

$$a \perp n \Rightarrow \exists x \;\; n \mid a^x - 1$$

Dowód: Rozważamy reszty $a^i \bmod n$ dla $i = 0, 1, \ldots, n$ (n+1 kulek). Reszty te przyjmują wartości należące do $\mathbb{Z}_n$ (n różnych możliwych wartości → n szufladek). Z zasady szufladkowej istnieją dwie kulki w jednej szufladce, czyli:

$\exists\, i < j : a^i \bmod n = a^j \bmod n$. Wtedy $a^{j-i} \bmod n = 1$,
czyli $n \mid a^{j-i} - 1$.

$$(a^{-1})^i a^i = (a^{-1})^i a^j$$

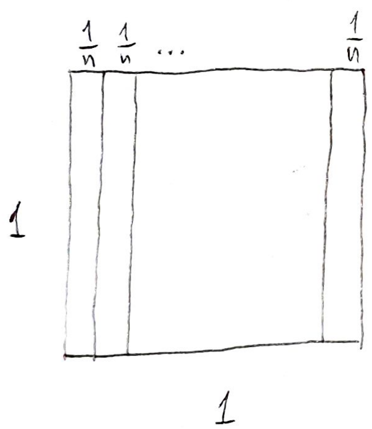
$$\cancel{\underbrace{a \cdot a \cdot a \cdot \ldots \cdot a}_{i}}\ \cancel{\underbrace{a^{-1} \cdot a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1}}_{i}} = \underbrace{a \cdot a \cdot a \ldots}_{j-i}\ \cancel{\underbrace{a \cdot a \ldots}_{i}}\ \cancel{\underbrace{a^{-1} a^{-1} \ldots}_{i}}$$

$$1 = a^{j-1}$$

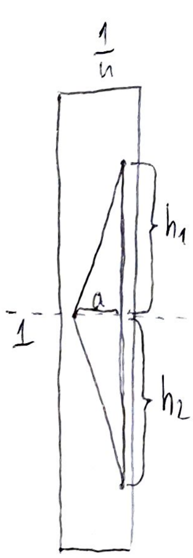
■

Twierdzenie: W kwadracie jednostkowym jest $2n+1$ punktów, z których żadne 3 nie są współliniowe. Istnieją wtedy 3 punkty, które są wierzchołkami trójkąta o polu co najwyżej $\frac{1}{2n}$.

Dowód:



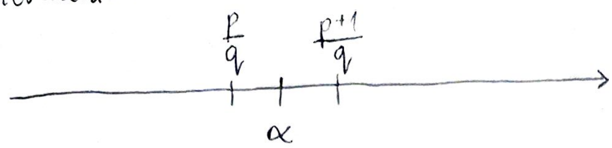

Dzielimy kwadrat na $n$ pasków.
Z zasady szufladkowej istnieje pasek zawierający trzy z $2n+1$ punktów.
Te trzy punkty są wierzchołkami trójkąta o polu mniejszym/równym $\frac{1}{2n}$.




$$P_\Delta = \frac{1}{2} a h_1 + \frac{1}{2} a h_2 = \frac{1}{2} a (h_1 + h_2) \leq \frac{1}{2n},$$

ponieważ $a \leq \frac{1}{n}$, $(h_1 + h_2) \leq 1$.

Twierdzenie:




$\alpha \in \mathbb{R}$, $p \in \mathbb{Z}$, $q \in \mathbb{N}$ — ta część nie jest częścią twierdzenia, lecz stałym oszacowaniem

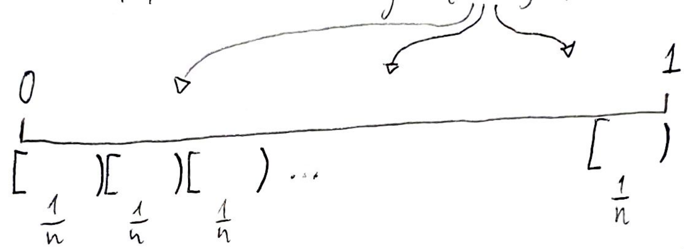
$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q}$$

Istnieją jednak mianowniki $q$, dla których $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$:

Niech $\alpha \in \mathbb{R}$ i $n \in \mathbb{N}$. Istnieją $p \in \mathbb{Z}$, $q \in \mathbb{N}$ takie, że

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{nq}.$$

Dowód: dla $i = 0, 1, \ldots, n$ rozważamy $\{\alpha \cdot i\}$ (części ułamkowe):




Z zasady szufladkowej dwie reszty $\{\alpha i\}, \{\alpha j\}$ dla $i < j$ wpadną do tej samej szufladki.

$$\left|\{\alpha j\} - \{\alpha i\}\right| < \frac{1}{n} \iff \left|\alpha j - \lfloor \alpha j \rfloor - \alpha i + \lfloor \alpha i \rfloor\right| < \frac{1}{n}$$

$$\iff \left|\alpha(j-i) - (\lfloor \alpha j \rfloor - \lfloor \alpha i \rfloor)\right| < \frac{1}{n}.$$

$(\lfloor \alpha j \rfloor - \lfloor \alpha i \rfloor = p, (j-i) = q)$

$$\iff \left|\alpha - \frac{\lfloor \alpha j \rfloor - \lfloor \alpha i \rfloor}{j-i}\right| < \frac{1}{n(j-i)}$$

∎

Zliczanie:

- Liczba ciągów $a_1, a_2, \dots, a_k$ gdzie $a_i \in \{1,2,3,\dots,n\}$ wynosi $n^k$
- Liczba takich ciągów jeśli $a_1, \dots, a_k$ mają być różne to

$n(n-1)(n-2)\dots(n-k+1)$: $n$ do potęgi $k$-tej ubywającej

$$n^{\underline{k}} = n(n-1)\dots(n-k+1) = \frac{n!}{(n-k)!} \qquad (n^{\underline{n}} = n!)$$

- Liczba podzbiorów $\{a_1, a_2, \dots, a_k\}$ zbioru $\{1,2,\dots,n\}$ wynosi

$$\binom{n}{k} = \frac{n^{\underline{k}}}{k!} = \frac{n!}{k!\,(n-k)!} \qquad (0 \leq k \leq n)$$

$\binom{n}{k}$ - liczba $k$-elementowych podzbiorów zbioru $n$-elementowego,
np. $\{1,2,3,\dots,n\}$

$\binom{n}{k} = 0$ dla $n < k$ lub $k < 0$.

Inna interpretacja $\binom{n}{k}$ - liczba ciągów zero-jedynkowych długości $n$ zawierających $k$ jedynek (dokładnie), czyli $\binom{n}{k}$ to liczba sposobów wybrania $k$ pozycji (spośród $n$), na których są jedynki.

Liczba ciągów złożonych z $n_1$-jedynek, $n_2$-dwójek, ..., $n_k$-liczb $k$ bywa oznaczana jako:

multinomial coefficient

$$\binom{n}{n_1 n_2 \dots n_k} = \binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\dots\binom{n-n_1-\dots-n_{k-1}}{n_k} = \frac{n!}{n_1!\,n_2!\dots n_k!}$$

gdzie $n = n_1 + n_2 + \dots + n_k$.

uogólniony symbol Newtona

Liczba układów kart w pokerze (5 kart z 52):

1° wszystkich: $\binom{52}{5} = \frac{52^{\underline{5}}}{5!}$

2° as, król, dama, walet, 10 w jednym kolorze (poker królewski): 4

3° jak wyżej, inne kolory (poker): $4 \cdot 9$ (bez królewskiego $4 \cdot 8$)

4° czwórka (kareta): $13 \cdot 48$ (13 - rodzaje kart, 48 - pozostała karta)

5° full (trójka + para): $13 \cdot \binom{4}{3} \cdot 12 \cdot \binom{4}{3}$ ($\binom{4}{3}$ - 3 z 4 kolorów)

6° kolor (nie poker): $4 \cdot \binom{13}{5} - 4 \cdot 9$

7° strit (5 kolejnych kart, ale nie poker): $9 \cdot 4^5 - 4 \cdot 9$

8° trójka (nie full): $13 \cdot \binom{4}{3} \cdot \binom{12}{2} \cdot 4^2$

9° dwie pary: $\binom{13}{2} \cdot \binom{4}{2}^2 \cdot 44$

W pudełku mieści się 5 kulek, na ile sposobów można wybrać zestaw 5 kulek, jeśli dysponujemy nieograniczonymi liczbami kulek białych, czerwonych, zielonych i niebieskich (2 kulki tego samego koloru są nierozróżnialne)?

$\cancel{\frac{4^5}{5!}}$ ← jakaś propozycja

Odpowiedź i uzasadnienie: $\binom{5+3}{5}$ ← # ciągów

B C Z N ← zestawy kulek

Mamy zależność wzajemnie jednoznaczną między zestawami kulek i ciągami złożonymi z trzech zer i pięciu jedynek (0 - idź dalej, 1 - weź kulkę).

Wzór dwumienny Newtona:

$$(a+b)^2 = a^2 + 2ab + b^2$$

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$$

$$\vdots$$

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

$$= \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = \underbrace{\sum_{k} \binom{n}{k} a^{n-k} b^k}$$

suma niezerowych wyrazów

$$(a+b)^n = a \cdot a \cdot \ldots \cdot a + a \cdot a \cdot \ldots \cdot a \cdot b + a \cdot \ldots \cdot a \cdot b \cdot a + \ldots + a \cdot a \cdot b \cdot b \cdot a \cdot b \cdots a + \ldots + b \cdot b \cdot \ldots \cdot b =$$

$$= \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n}b^n$$

Wnioski ze wzoru dwumiennego Newtona:

- $\sum_{i} \binom{n}{i} = (1+1)^n = 2^n$
- $\sum_{i} (-1)^i \binom{n}{i} = (0-0)^n = \begin{cases} 1 & : n = 0 \\ 0 & : n \geq 1 \end{cases}$

Lemat: $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$

Dowód rachunkowy:

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

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

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

TRÓJKĄT PASCALA

$$\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & 1 & & 1 & & & \\
 & & 1 & & 2 & & 1 & & \\
 & 1 & & 3 & & 3 & & 1 & \\
1 & & 4 & & 6 & & 4 & & 1
\end{array}$$

$$\begin{array}{ccccccccc}
 & & & & \binom{0}{1} & & & & \\
 & & & \binom{1}{0} & & \binom{1}{1} & & & \\
 & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & \\
 & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4}
\end{array}$$

Dowód algebraiczny:

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \dots + \boxed{\binom{n}{k}} x^k + \dots$$

$$(1+x)^n = (1+x)(1+x)^{n-1} = (1+x)^{n-1} + x(1-x)^{n-1} =$$

$$= \binom{n-1}{0} + \binom{n-1}{1}x + \dots + \boxed{\binom{n-1}{k}} x^k + \dots$$

$$+ \binom{n-1}{0}x + \binom{n-1}{1}x^2 + \dots + \boxed{\binom{n-1}{k-1}} x^k + \dots \quad \blacksquare$$

Dowód kombinatoryczny:

Liczba k-elementowych podzbiorów $\{1,2,\dots,n\}$ wynosi $\binom{n}{k}$.

Liczba k-elementowych podzbiorów $\{1,2,\dots,n\}$ zawierających $n$ to $\binom{n-1}{k-1}$.

Liczba k-elementowych podzbiorów $\{1,2,\dots,n\}$ niezawierających $n$ to $\binom{n-1}{k}$.

Stąd mamy, że $\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}$ $\blacksquare$

$$\sum_k k\binom{n}{k} = \sum_k k\frac{n^{\underline{k}}}{k!} = \sum_k n\frac{(n-1)^{\underline{k-1}}}{(k-1)!} = \sum_k n\binom{n-1}{k-1} =$$

$$= n\sum_k \binom{n-1}{k-1} = n\cdot 2^{n-1}$$

Ile wynosi $0^{\underline{0}}$?

$$x^{\underline{k}} = x(x-1)\dots(x-k+1) = x^{\underline{k-1}}(x-k+1) = x\cdot(x-1)^{\underline{k-1}}$$

Mamy więc: $1^{\underline{1}} = 1\cdot 0^{\underline{0}}$

$1 = 1\cdot X \Rightarrow X = 1$