Coefficienti binomiali

Def

- **Coefficiente binomiale** > - $0! := 1$ > - $n, k \in \mathbb{N}$ > - $\left(\begin{array}{c} n \\ k \end{array} \right) := \begin{cases} \frac{n!}{n!(n-k)!} & k \leqslant n \\ 0 & k > n \end{cases}$

Oss

- **Hp**
  - $n, k \in \mathbb{N}$
- **Th**
  - $\left(\begin{array}{c} n \\ k \end{array} \right) = \left(\begin{array}{c} n \\ n-k \end{array} \right)$
- **Dim**
  - $\left(\begin{array}{c} n \\ n-k \end{array} \right) = \dfrac{n!}{(n-k)!(n-(n-k))!} = \dfrac{n!}{(n-k)!k!} = \left(\begin{array}{c} n \\ n \end{array} \right)$

Oss

- **Hp**
  - $n, k \in \mathbb{N}$
- **Th**
  - $\left(\begin{array}{c} n \\ k+1 \end{array} \right) = \left(\begin{array}{c} n-1 \\ k+1 \end{array} \right) + \left(\begin{array}{c} n-1 \\ k \end{array} \right)$
- **Dim**
  - $\binom{n-1}{k+1} + \binom{n-1}{k} = \frac{(n-1)!}{(k+1)!(n-1-(k+1))!} + \frac{(n-1)!}{k!(n-1-k)!} = \frac{(n-1)!}{(k+1)k!(n-2-k)!} + \frac{(n-1)!}{k!(n-1-k)!} = \frac{(n-1-k)(n-1)!+(k+1)(n-1)!}{(k+1)!(n-k-1)!} = \frac{(n-1)!(n-1-k+k+1)}{(k+1)!(n-1-k)!} = \frac{(n-1)! \cdot n}{(n+1)!(n-1-k)!} = \frac{n!}{(k+1)!(n-k-1)!} = \binom{n}{k+1}$

Lem

- **Hp**
  - $p \in \mathbb{P}$
  - $k \in \mathbb{N} \mid 0 < k < p$
- **Th**
  - $p \left| \left(\begin{array}{c} p \\ k \end{array} \right) \right.$
- **Dim**
  - $\begin{pmatrix} p \\ k \end{pmatrix} = \dfrac{p!}{k!(p-k)!} = \dfrac{p \cdot (p-1)!}{k!(p-k)!} = p \cdot \dfrac{(p-1)!}{k!(p-k)!} \implies p$ è nella fattorizzazione di $\begin{pmatrix} p \\ k \end{pmatrix}$
  - poiché p è primo in ipotesi, non è possibile semplificarlo con nessun fattore del denominatore

    * $k < p \implies p$ non può essere nella fattorizzazione di $k!$
    * $p - k < p \implies p$ non può essere nella fattorizzazione di $(p - k)!$
  - quindi necessariamente $p \left| \left(\begin{array}{c} p \\ k \end{array} \right) \right.$

Oss

- **Hp**
  - $n \in \mathbb{Z}$
  - $p \in \mathbb{P} : p \mid n$
  - $[a] \in \mathbb{Z}_p$
- **Th**
  - $n \cdot [a] = [0]$ in $\mathbb{Z}_p$
- **Dim**
  - $p \mid n \implies \exists k \in \mathbb{Z} \mid pk = n$
  - $n \cdot [a] = [a] + \ldots + [a] = [n \cdot a] = [pk \cdot a] = p \cdot [ka]$
  - $[pka]$ è multiplo di p per definizione, e quindi $[pka] = [0]$ in $\mathbb{Z}_p$, quindi $n \cdot [a] = [pka] = [0]$ in $\mathbb{Z}_p$

Oss

- **Hp**
  - $n \in \mathbb{Z}$
  - $p \in \mathbb{P} : p \mid n$
  - $[a] \in \mathbb{Z}_p$
  - $k \in \mathbb{N} \mid 0 < k < p$
- **Th**
  - $\binom{p}{k} \cdot [a] = [0]$ in $\mathbb{Z}_p$
- **Dim**
  - $\left(\begin{array}{c} p \\ k \end{array} \right) \cdot [a] = \left[\left(\begin{array}{c} p \\ k \end{array} \right) \cdot a \right]$
  - per il dimostrazione precedente, $p \left| \binom{p}{k} \right.$, quindi $\left(\begin{array}{c} p \\ k \end{array} \right) \cdot a$ è anch'esso multiplo di p, e di conseguenza $\left[\left(\begin{array}{c} p \\ k \end{array} \right) \cdot a \right] = [0]$ in $\mathbb{Z}_p$

Cor

- **Hp**
  - $p \in \mathbb{P}$
  - $[a], [b] \in \mathbb{Z}_p$
- **Th**
  - $([a] + [b])^p = [a]^p + [b]^p$ in $\mathbb{Z}_p$
- **Dim**

- per il teorema del binomio di Newton $([a]+[b])^p = \sum_{k=0}^{p} \begin{pmatrix} p \\ k \end{pmatrix} [a]^k \cdot [b]^{p-k} = \sum_{k=0}^{p} \begin{pmatrix} p \\ k \end{pmatrix} \left[a^k \cdot b^{p-k}\right]$
- per dimostrazione precedente $p \in \mathbb{P} \implies \begin{pmatrix} p \\ k \end{pmatrix} \left[\ a^k \cdot b^{p-k}\ \right] = [0] \quad \forall k \in \mathbb{Z} \mid 0 < k < p$
- di conseguenza, nella sommatoria del binomio di Newton tutti i termini con $k \in (0, p)$ si annullano, in quanto congruenti a $[0]$ in $\mathbb{Z}_p$
- $([a]+[b])^p = \sum_{k=0}^{p} \begin{pmatrix} p \\ k \end{pmatrix} \left[a^k \cdot b^{p-k}\right] = \begin{pmatrix} p \\ 0 \end{pmatrix} [b]^p + \begin{pmatrix} p \\ p \end{pmatrix} [a]^p = [a]^p + [b]^p$

Cor

- **Hp**
  - $p \in \mathbb{P}$
  - $[a_1], \ldots, [a_n] \in \mathbb{Z}_p$
- **Th**
  - $([a_1] + \ldots + [a_n])^p = [a_1]^p + \ldots + [a_n]^p$ in $\mathbb{Z}_p$
- **Dim**
  - $n = 1 \implies [a_1]^p = [a_1]^p$ per dimostrazione precedente
  - $n > 1 \implies ([a_1] + \ldots + [a_n] + [a_{n+1}])^p = [a_1]^p + \ldots + [a_n]^p + [a_{n+1}]^p$
    * per ipotesi induttiva, $[a_1]^p + \ldots + [a_n]^p + [a_{n+1}]^p = ([a_1] + \ldots + [a_n])^p + [a_{n+1}]^p$
    * allora, ancora per ipotesi induttiva $([a_1] + \ldots + [a_n])^p + [a_{n+1}]^p = ([a_1] + \ldots + [a_{n+1}])^p$