

## Coefficienti binomiali

### Def

- **Coefficiente binomiale**  $\binom{n}{k} := \begin{cases} \frac{n!}{k!(n-k)!} & k \leq n \\ 0 & k > n \end{cases}$

### Oss

- **Hp**
  - $n, k \in \mathbb{N}$
- **Th**
  - $\binom{n}{k} = \binom{n}{n-k}$
- **Dim**
  - $\binom{n}{n-k} = \frac{n!}{(n-k)!(n-(n-k))!} = \frac{n!}{(n-k)!k!} = \binom{n}{k}$

### Oss

- **Hp**
  - $n, k \in \mathbb{N}$
- **Th**
  - $\binom{n}{k+1} = \binom{n-1}{k+1} + \binom{n-1}{k}$
- **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**
  - $p \mid \binom{p}{k}$
- **Dim**
  - $\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p \cdot (p-1)!}{k!(p-k)!} = p \cdot \frac{(p-1)!}{k!(p-k)!} \implies p$  è nella fattorizzazione di  $\binom{p}{k}$
  - 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  $p \mid \binom{p}{k}$

### 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**
  - $p \mid n \implies \exists k \in \mathbb{Z} \mid pk = n$
  - $n \cdot [a] = [a] + \dots + [a] = [n \cdot a] = [pk \cdot a] = p \cdot [ka]$
  - $[pka]$  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**
  - $\binom{p}{k} \cdot [a] = \left[ \binom{p}{k} \cdot a \right]$
  - per la dimostrazione precedente,  $p \mid \binom{p}{k}$ , quindi  $\binom{p}{k} \cdot a$  è anch'esso multiplo di  $p$ , e di conseguenza  $\left[ \binom{p}{k} \cdot a \right] = [0]$  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  $([a] + [b])^p = \sum_{k=0}^p \binom{p}{k} [a]^k \cdot [b]^{p-k} =$   

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

## Cor

- **Hp**

- $p \in \mathbb{P}$
- $[a_1], \dots, [a_n] \in \mathbb{Z}_p$

- **Th**

- $([a_1] + \dots + [a_n])^p = [a_1]^p + \dots + [a_n]^p$  in  $\mathbb{Z}_p$

- **Dim**

- $n = 1 \implies [a_1]^p = [a_1]^p$  per dimostrazione precedente
- $n > 1 \implies ([a_1] + \dots + [a_n] + [a_{n+1}])^p = [a_1]^p + \dots + [a_n]^p + [a_{n+1}]^p$ 
  - \* per ipotesi induttiva,  $[a_1]^p + \dots + [a_n]^p + [a_{n+1}]^p = ([a_1] + \dots + [a_n])^p + [a_{n+1}]^p$
  - \* allora, ancora per ipotesi induttiva  $([a_1] + \dots + [a_n])^p + [a_{n+1}]^p = ([a_1] + \dots + [a_{n+1}])^p$