Fondamenti Matematici per l'Informatica: Teoremi e Dimostrazioni

Aymane Chabbaki

II semestre 2018/2019

Indice

1 Insiemi

1.1 Teorema del Buon ordinamento

Enunciato:

- L'insieme totalmente ordinato $(\mathbb{N}, \leq)$ è **ben ordinato**.

Dimostrazione:

- Sia A un sottoinsieme di $\mathbb{N}$ senza minimo.
- Devo provare che $A = \varnothing$ o equivalentemente $B := \mathbb{N} \setminus A = \mathbb{N}$
- Proviamo per induzione che vale $\forall n \in \mathbb{N}$, $\underbrace{\{0, 1, \ldots, n\} \subset B}_{P(n)}$
- $n = 0$ (**base dell'induzione**)
  - $\{0\} \subset B \iff 0 \in B$
  - Questo è vero, cioè $0 \in B$, altrimenti se $0 \in \mathbb{N} \setminus B = A \implies 0 = min(A)$ e questo è impossibile perchè A non ha minimo.
  - Dunque $0 \in B$
- $n \implies n + 1$
- Assumiamo che $\{0, 1, \ldots, n\} \subset B$ per qualche $n \in \mathbb{N}$ (**ipotesi induttiva**)
- Devo provare che anche $\{0, 1, \ldots, n, n + 1\} \subset B$
  - $n + 1 \notin A$ altrimenti $(n + 1) = min(A)$ visto che tutti gli altri elementi precedenti stanno in B.
  - Questo è impossibile perchè A non ha minimo.
  - Dunque $n + 1 \in B \implies \{0, 1, \ldots, n, n + 1\} \subset B$
- A è vuoto e $\mathbb{N}$ è **ben ordinato**.
- *C.V.D.*

1.2 Seconda forma del Principio di Induzione

Enunciato:

- Sia $\{P(n)\}_{n \in \mathbb{N}}$ una famiglia di affermazioni (**proposizioni**) indicizzate su $\mathbb{N}$.
- Supponiamo che:
  1. $P(0)$ è vera (**base dell'induzione**).
  2. $\forall n > 0$, $(P(k)$ è vera $\forall k < n) \implies (P(n)$ è vera$)$
- Allora $P(n)$ è vera $\forall n \in \mathbb{N}$.

Dimostrazione:

- $A := \{n \in \mathbb{N} \mid P(n) \text{ è falsa}\}$
- Supponiamo per assurdo che $A \neq \varnothing$.
- Grazie al Teorema di buon ordinamento di $(\mathbb{N}, \leq)$ si ha che $\exists n := min(A)$
- Chiaramente $0 \notin A$ poichè $P(0)$ è vera.
- Inoltre se $k < n$, allora $k \notin A$ in quanto $n = min(A)$, ma allora dalla (2) segue che $P(n)$ è vera e quindi $n \notin A$, contraddicendo il fatto che $n \in A$.
- *C.V.D.*

2 Numeri

2.1 Divisione Euclidea

Enunciato:

- Siano $n, m \in \mathbb{Z}$ con $m \neq 0$, allora esistono unici $q, r \in \mathbb{Z}$ tali che:

$$\begin{cases} n = m \cdot q + r \\ 0 \leq r < |m| \end{cases}$$

Dimostrazione Esistenza:

- Supponiamo che $n \geq 0$ e $m > 0$:
  - Procediamo per induzione su $n \geq 0$ per dimostrare che se $m > 0$ allora $\exists\, q, r \in \mathbb{N}$, tale che: $\begin{cases} n = m \cdot q + r \\ 0 \leq r < m \end{cases}$
  - $n = 0$ (**base dell'induzione**).

$$\begin{cases} n = 0 = ? \cdot m + ? = 0 \cdot m + 0 \\ 0 \leq 0 < m \end{cases}$$

  - Dunque basta prendere $n = 0$ e $r = 0$.
  - Supponiamo ora che $n > 0$, $k < m \implies n$.
  - Assumiamo l'asserto vero $\forall\, k < n$, cioè $\exists\, q', r' \in \mathbb{N}$ $tc.$ $k = q' \cdot m + r'$ e $0 \leq r' < m$ (**ipotesi induttiva**).
  - Se $n < m$ basta prendere $q = 0$ e $r = n$.
  - Se $n \geq m$ poniamo $k := n - m < n \implies 0 \leq k < n$.
  - Grazie all'ipotesi induttiva esistono $q', r' \in \mathbb{N}$ tc : $\begin{cases} k = q' \cdot m + r' \\ 0 \leq r' < m \end{cases}$
  - $n - m = k = q' \cdot m + r'$, $0 \leq r' < m$
  - Ma allora $n = k + m = m \cdot q + r' + m = (q' + 1)m + r'$, vale anche per $n \implies \forall\, n \geq 0$ è vera.
- Supponiamo ora $n < 0$ e $m > 0$:
  - Per il caso precedente si ha che esistono $q, r \in \mathbb{Z}$ tali che: $\begin{cases} -n = q \cdot m + r \\ 0 \leq r < n \end{cases}$
  - E quindi $n = (-q)m - r$.
  - Se $r = 0$ allora $-q$ è il quoziente e $r = 0$ è il resto.
  - Se $0 < r < m$:

$$n = (-q)m - m + m - r = (-q - 1)m + (m - r)$$

$$\text{con } 0 < m - r < m = |m|$$

- Sia $n \in \mathbb{Z}$ e $m < 0$:
  - Per i due casi precedenti esistomo $q, r \in \mathbb{Z}$ tali che

$$n = q(-m) + r = (-q)m + r$$

$$\text{con } 0 < r < -m = |m|$$

Dimostrazione Unicità:

- Supponiamo esistano $q, q', r, r' \in \mathbb{N}$ tale che: $q' \cdot m + r' = n = q \cdot m + r$ con $0 \leq r'$, $r < m$
- Cioè:

$$\begin{aligned} q' \cdot m + r' &= q \cdot m + r \\ q' \cdot m - q \cdot m &= r - r' \\ (q' - q) \cdot m &= r - r' \end{aligned}$$

- Supponiamo che $r' \geq r$ e passando ai moduli si ha:

$$\begin{aligned} |q' - q|\, m = |r - r'| &= r - r' < m \\ |q' - q|\, |m| < |m| &\iff |q' - q|\, m < m \\ &\iff |q' - q| < 1 \\ &\iff |q' - q| = 0 \\ &\iff q' - q = 0 \\ &\iff q' = q \end{aligned}$$

- Visto che $q' = q$ si ha che:

$$\cancel{q' \cdot m} + r' = n = \cancel{q \cdot m} + r \implies r' = r$$

- *C.V.D.*

2.2 Rappresentazione binaria dei naturali in base arbitraria

Enunciato:

- Sia $b \in \mathbb{N}$, $b \geq 2$.
- Allora ogni $n \in \mathbb{N}$ è rappresentabile, in **modo unico**, in base b. Ovvero $\exists! \{\varepsilon_i\}_{i \in \mathbb{N}}$ tale che $\varepsilon_{i \in I_b} \forall i \in \mathbb{N}$ la successione $\{\varepsilon_i\}_{i \in \mathbb{N}}$ è definitivamente nulla e vale:

$$n = \sum_{i=0}^{\infty} \varepsilon_i \cdot b^i = (\cdots \cdot \varepsilon_2 \cdot \varepsilon_1 \cdot \varepsilon_0)_b$$

Dimostrazione Esistenza:

- Procediamo per induzione (2° forma) su n:
  - $n = 0$ (**base dell'induzione**)
  - Poniamo $\varepsilon_i = 0 \ \forall i \in \mathbb{N}$. Vale:
    1. $\{\varepsilon_i\}_{i \in \mathbb{N}}$ è definitivamente nulla.
    2. $\varepsilon_i = 0 \in I_b \ \forall i \in \mathbb{N}$
    3. $n = 0 = \sum\limits_{i \in \mathbb{N}}^{\infty} 0 \cdot b^i$
  - $n > 0$, $\forall k < n \implies n$
  - Eseguiamo la divisione euclidea di n per b:

$$n = q \cdot b + r, \quad q, r \in \mathbb{N}$$

$$0 \leq r < b \quad (\iff r \in I_b)$$

  - Dico che $q < n$:

    - $*$ Se $q = 0$, allora $q = 0 < n$
    - $*$ Se $q \neq 0$ allora: $0 < q < q \cdot b + r = n$, quindi segue che $q < n$
  - Applicando l'ipotesi induttiva con $k = q$ si ha quindi che esiste $\{\zeta_i\}_{i \in \mathbb{N}}$ con $\zeta_{i \in I_b}$ definitivamente nulla e $q = \sum_{i=0}^{\infty} \zeta_i \cdot b^i$
  - Si ha:

$$\begin{aligned} n = q \cdot b + r &= \sum_{i=0}^{\infty} \left(\zeta_i \cdot b^i\right) \cdot b + r \\ &= r + \sum_{i=0}^{\infty} \zeta_i \cdot b^{i+1} \\ &= r + \sum_{i=1}^{\infty} \zeta_{i-1} \cdot b^i \end{aligned}$$

    $\implies r \in I_b$ e $\zeta_{i-1} \in Ib \ \forall i \geq 1$
  - Definiamo:
    - $*$ $\varepsilon_0 = r$
    - $*$ $\varepsilon_i = \zeta_{i-1} \ \forall i \geq 1$

    $\implies \{\varepsilon_i\}_{i \in \mathbb{N}}$ è definitivamente nulla e $\varepsilon_{i \in I_b} \forall i \in \mathbb{N} \implies n = \varepsilon_0 + \sum_{i=1}^{\infty} \varepsilon_i \cdot b^i = \sum_{i=0}^{\infty} \varepsilon_i \cdot b^i$

- Dunque esiste una scrittura in base $b \ \forall n \in \mathbb{N}$
- *C.V.D.*

Dimostrazione Unicità:

- Sia $n \in \mathbb{N}$ tale che:
  1. $\exists \{\varepsilon_i\}_{i \in \mathbb{N}}$ tale che:
     - $\{\varepsilon_i\}_{i \in \mathbb{N}}$ è definitivamente nulla
     - $\varepsilon_{i \in I_b} \ \forall i \in \mathbb{N}$
     - $n = \sum_{i \in \mathbb{N}} \varepsilon_i \cdot b^i$
  2. $\exists \{\varepsilon_i^{'}\}_{i \in \mathbb{N}}$ tale che:
     - $\{\varepsilon_i^{'}\}_{i \in \mathbb{N}}$ è definitivamente nulla.
     - $\varepsilon_{i \in I_b}^{'} \ \forall i \in \mathbb{N}$
     - $n = \sum_{i \in \mathbb{N}} \varepsilon_i^{'} \cdot b^i$

     $\implies \varepsilon_i = \varepsilon_i^{'} \quad \forall i \in \mathbb{N}$

- Procediamo per induzione su $n \in \mathbb{N}$ e dimostriamo che la rappresentazione di n in base n è unica.
  - $n = 0$ (**base dell'induzione**)

$$\begin{array}{ccc} \sum_{i \in \mathbb{N}} \varepsilon_i \cdot b^i = & 0 & = \sum_{i \in \mathbb{N}} \varepsilon_i^{'} \cdot b^i \\ \varepsilon_i \cdot b = 0 \ \forall i \in \mathbb{N} & & \varepsilon_i^{'} \cdot b = 0 \ \forall i \in \mathbb{N} \\ \varepsilon_i = 0 \ \forall i & & \varepsilon_i^{'} = 0 \ \forall i \end{array}$$

    $\implies \varepsilon_i = \varepsilon_i^{'} \ \forall i$

- $n > 0, \forall k < n \implies n$

$$\sum_{i\in\mathbb{N}} \varepsilon_i \cdot b^i = \quad n \quad = \sum_{i\in\mathbb{N}} \varepsilon_i^{'} \cdot b^i$$

$$\varepsilon_0 + \sum_{i=0}^{\infty} \varepsilon_i \cdot b^i \qquad \varepsilon_0^{'} + \sum_{i=0}^{\infty} \varepsilon_i^{'} \cdot b^i$$

$$\varepsilon_0 + \underbrace{\left(\sum_{i=1}^{\infty} \varepsilon_i \cdot b^{i-1}\right) \cdot b}_{q} \qquad \varepsilon_0^{'} + \underbrace{\left(\sum_{i=1}^{\infty} \varepsilon_i^{'} \cdot b^{i-1}\right) \cdot b}_{q'}$$

- Siccome la divisione euclidea è unica $q = q' < n \implies \varepsilon_0 = \varepsilon_0^{'}$

$$\sum_{i=1}^{\infty} \varepsilon_i \cdot b^{i-1} = \quad q \quad = \sum_{i=1}^{\infty} \varepsilon_i^{'} \cdot b^{i-1} \quad < n$$

$$\sum_{i=0}^{\infty} \varepsilon_{i-1} \cdot b^{i} = \quad q \quad = \sum_{i=0}^{\infty} \varepsilon_{i-1}^{'} \cdot b^{i}$$

- Per ipotesi induttiva $\varepsilon_{i+1} = \varepsilon_{i+1}^{'}\ \forall i \geq 0$
- *C.V.D.*

2.3 Esistenza ed unicità del Massimo Comune Divisore

Enunciato:

- Siano n, m due numeri **interi** non entrambi nulli.
- Si dice che un numero naturale d è il **massimo comune divisore** tra n e m se soddisfa:
  1. $d \,|\, n$ e $d \,|\, m$ (**comune divisore**)
  2. Se $c \in \mathbb{Z}$ tale che $c \,|\, n$ e $c \,|\, m$ allora $c \,|\, d$ (se esiste, allora d è il massimo tra i divisore comuni tra n e m)
- Se un tale d esiste, allora è **unico** (è il massimo comune divisore) e si indica con $(n, m) = d$

Dimostrazione Unicità:

- Supponiamo l'esistenza, e quindi che valgano le proprietà della definizione.
- Siano d e d' due massimi comuni divisori di n e m. Allora:

$$d \,|\, d' \begin{cases} (1) \text{ con } d \\ (2) \text{ con } d' \end{cases}$$

$$d' \,|\, d \begin{cases} (1) \text{ con } d' \\ (2) \text{ con } d \end{cases}$$

- $d = \pm d'$ ma visto che sono numeri naturali si ha che $d = d'$
- *C.V.D.*

Enunciato Esistenza MCD:

- Dati qualunque $n, m \in \mathbb{Z}$ non entrambi nulli, **esiste sempre**, ed è **unico** il massimo comune divisore tra n e m.
- Dati $n, m \in \mathbb{Z}$ vale $n \mid m \iff n \mid -m \iff -n \mid m \iff -n \mid -m$

Dimostrazione Esistenza:

- Possiamo supporre che $n \geq 0$, $m \geq 0$.
- Definiamo $S := \{s \in \mathbb{N} \setminus \{0\} \mid s = xn + ym \text{ per qualche } x, y \in \mathbb{Z}\} \subset \mathbb{N}$
- $S = \varnothing$, $n^2 + m^2 = s$ allora grazie al Teorema di buon ordinamento di $(N, \leq)$, S **ammette minimo** $d = min(S) \in S$
- Poichè $d \in S$, allora $d = xn + ym$ per qualche $x, y \in \mathbb{Z}$
- Verifichiamo che $d = (n, m)$ (M.C.D.)
- Sia $c \in \mathbb{Z}$ tale che $c \mid n$ e $c \mid m$, ovvero $\exists\ k, h \in \mathbb{Z}$ tale che $n = kc$ e $m = hc$
  - Vale:

$$\begin{aligned} d &= xn + ym \\ &= x\,(k \cdot c) + y\,(h \cdot c) \\ &= (xk + yh)\,c \end{aligned}$$

  - $\implies c \mid d$ e abbiamo dimostrato il punto (2) dell'enunciato.
- Ora proviamo il punto (1), precisamente che $d \mid n$:
  - Dobbiamo provare che il resto della divisione di n per d è 0.
  - Vale $\begin{cases} n = qd + r & \text{per qualche (unico) } q, r \in \mathbb{Z} \\ 0 \leq r < d \end{cases}$
  - Se $r = 0$, la dimostrazione è completata.
  - Supponiamo che $0 < r < d$. Osserviamo che:

$$\begin{aligned} r &= n - qd \\ &= n - q(xn + ym) \\ &= n - qxn - qym \\ &= (1 - qx)n + (-qy)m \subset S \end{aligned}$$

  - Dunque r è una **combinazione lineare** in $\mathbb{Z}$ di n e m e sta in S.
  - r è positivo e più piccolo di d (**assurdo** perchè per ipotesi abbiamo preso d come il $min(S)$ e risulterebbe che $r < min(S)$).
  - Quindi $r = 0 \implies d$ divide n.
- In modo analogo si prova che $d \mid m$.
- *C.V.D.*

2.4 Esistenza ed unicità del Minimo Comune Multiplo

Enunciato:

- Siano n, m due numeri **interi** non entrambi nulli.
- Si dice che $M \in \mathbb{N}$ è il **minimo comune divisore** tra n e m se soddisfa:
  1. $n \mid M$ e $m \mid M$ (**comune multiplo**)
  2. Se $c \in \mathbb{Z}$ tale che $n \mid c$ e $m \mid c$ allora $M \mid c$ (se esiste, allora d è il minimo tra i mutipli comuni tra n e m)
- Siano $n, m \in \mathbb{Z}$ allora **esiste** ed è **unico** il minimo comune multiplo e si indica con $[n, m]$.
- Inoltre vale:
  - Se $n = m = 0$, allora $[n, m] = 0$
  - Se n e m **non sono entrambi nulli**, $[n, m] = \dfrac{n \cdot m}{(n, m)}$

Dimostrazione Unicità:

- Siano M_1 e $M_2 \in \mathbb{N}$ tali da soddisfare le proprietà del minimo comune multiplo.
- Infatti se M_1 e M_2 soddifano (1) e (2) si ha:

$$M_2 \mid M_1 \begin{cases} (1) \text{ con } M_1 \\ (2) \text{ con } M_2 \end{cases}$$

$$M_1 \mid M_2 \begin{cases} (1) \text{ con } M_2 \\ (2) \text{ con } M_1 \end{cases}$$

- $M_1 = \pm M_2$ ma visto che sono numeri naturali si ha che $M_1 = M_2$
- *C.V.D.*

Dimostrazione Esistenza:

- Supponiamo che n e m non siano entrambi nulli. Osserviamo che $(n, m) \mid n$ e $(n, m) \mid m \iff \exists\, n', m' \in \mathbb{Z}$ tale che:
  - $n = n'(n, m)$
  - $m = m'(n, m)$
- Definiamo $M := \dfrac{n \cdot m}{(n, m)}$ con $n \geq 0$, $m \geq 0$
- Dimostriamo:
  1. Vale:

$$M = \frac{n'(n,m) \cdot m' \cancel{(n,m)}}{\cancel{(n,m)}} = n' \cdot m'(n,m) = n \cdot m'$$
$$= n' \cdot m$$

     - M è multiplo sia di n che di m.
  2. Sia $c \in \mathbb{Z}$ tale che $n \mid c$ e $m \mid c$, valgono:

$$(n, m) \mid n \text{ e } n \mid c \implies (n, m) \mid c \iff c = c'(n, m) \quad \text{per qualche } c' \in \mathbb{Z}$$

- Segue che:
  - $n \mid c \Longleftrightarrow n' \cancel{(n,m)} \mid c' \cancel{(n,m)} \Longleftrightarrow n' \mid c'$
  - $m \mid c \Longleftrightarrow m' \cancel{(n,m)} \mid c' \cancel{(n,m)} \Longleftrightarrow m' \mid c'$
- Vale:
  - $(n', m') = \left(\underbrace{\frac{n}{(n,m)}, \frac{m}{(n,m)}}_{\text{coppia coprima (Prop. 9.12)}} \right) = 1$
  - $n' \mid c'$ e $m' \mid c' \xRightarrow[\text{Teorema 10.1}]{} n' \cdot m' \mid c' \Longleftrightarrow \underbrace{n' \cdot m'(n,m)}_{M} \mid \underbrace{c'(n,m)}_{c}$
- $\implies M \mid c$

- Abbiamo completato la dimostrazione, in quanto le proprietà (1) e (2) sono state dimostrate.
- *C.V.D.*

2.5 Teorema Fondamentale dell'Algebra

Enunciato:

- Ogni **numero naturale** $n \geq 2$ si può scrivere come **prodotto di un numero finito di primi** (eventualmente ripetuti), tali che $n = p_1 \cdots p_k$
- Se esiste un'altra famiglia finita $\{q_1, \dots, q_h\}$ di primi (eventualmente ripetuti) tale che: $n = q_1 \dots q_h$, allora $k = h$ ed **esiste** una **bigezione** $\varphi : \{1, \dots, k\} \longrightarrow \{1, \dots, k = h\}$ tale che $p_i = q_{\varphi(i)} \rightarrow$(prendo indici q, li permuto usando φ e ottengo p_i)
- Le due scritture sono **permutate**, cioè sono **uniche** a meno di ordinamento.
- In altre parole, ogni **numero maggiore** di 1 si scrive in **modo unico** a meno dell'ordine, come **prodotto di numeri primi positivi**.

Dimostrazione: Esistenza fattorizzazione

- Procediamo per induzione (di 2° forma) su $n \geq 2$:
  - $n = 2$ (**base dell'induzione**).
  - Si ha: $2 = 2 \rightarrow p_i$
  - $P(2)$ è vera.
  - $n > 2$, $k < n \implies n$
  - Assumiamo per tutti i $k < n$ sia **possibile** trovare una **fattorizzazione** in numeri primi (**ipotesi induttiva**).
  - Devo provare l'esistenza di tale fattorizzazione anche per n.
  - Se n **è primo** si ha che $n = n \rightarrow p_i$
  - Supponiamo che n **non sia primo**. Allora $\exists\, k_1, k_2 \in \mathbb{Z}$ tale che: $\begin{cases} 1 < k_1 < n \\ 1 < k_2 < n \end{cases}$
  - $n = k_1 \cdot k_2$
  - Per **ipotesi induttiva** $k_1 = p_1 \cdots p_k$ e $k_2 = q_1 \cdots q_h$ dove p_i e q_j sono primi.
  - n è un **prodotto di numeri primi**:

$$n = p_1 \cdots p_k \cdot q_1 \cdots q_h$$

$\implies$ Fattorizzazione esiste sempre *C.V.D.*

Dimostrazione: Unicità della fattorizzazione

- Siano $p_1, \cdots p_k$ e $q_1 \cdots q_h$
- $p_1 \cdots p_k = n = q_1 \cdots q_h \qquad k \leq h$
- Procediamo per induzione su $k \geq 1$:
  - $k = 1$
$$p_1 = q_1 \cdot q_2 \ldots q_h \underset{?}{\Rightarrow} h = 1$$
$$\implies p_1 \,|\, q_1 \text{ a meno di riordinare (permutare) i vari } q_j$$
$$(p_1 \geq 2 \text{ ed è primo, mentre } q_1 \text{ è primo, dunque ha come divisori 1 e se stesso.})$$
$$\implies p_1 = q_1$$
  - Dunque $h = 1$ perchè $1 = q_2 \cdots q_h \geq 2$ è assurdo, non può essere.
  - $k = k + 1$
  - Assumiamo che se $p_1 \cdots p_k = q_1 \cdots q_h$
  - $ksh \underset{\text{ip. ind.}}{\Longrightarrow} k = h$ e a meno di riordinamento, $p_i = q_i \, \forall i = 1, \ldots, k$
  - Supponiamo che $p_1 \cdots p_{k+1} = q_1 \cdots q_h$ con $k + 1 \leq h$
  - Vale:
    * $p_{k+1} \,|\, p_1 \cdots p_{k+1} = q_1 \cdots q_h$ (numero primo che divide un prodotto)
    * A meno di riordinamento, posso assumere $p_{k+1} \,|\, q_h = p_{k+1} = q_h$
    * Si ha $p_1 \cdots \cancel{p_{k+1}} = q_1 \cdots q_h$
      $\implies p_1 \cdots p_k = q_1 \cdots q_{h-1}$ con $k < h - 1 \underset{\text{ip. ind.}}{\Longrightarrow} k = h - 1$
  - Dunque $p_i = q_i \forall i = 1, \ldots, k$
- *C.V.D.*

3 RSA

3.1 Teorema Cinese del Resto

Enunciato:

- Siano $a, b, n, m \in \mathbb{Z}$ con $n > 0$ e $m > 0$
- Consideriamo il seguente sistema di congruenze: $(S) \begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{cases}$
- Il sistema (S) è **compatibile** (ovvero $Sol(S) \neq \varnothing$) se e solo se $(n, m) \mid a - b$
- Supponiamo che esista almeno una **soluzione** c, ovvero $c \in Sol(S)$
- Allora $Sol(S) = [c]_{[n,m]} = \{c + k\,[n, m] \subset \mathbb{Z} \mid,\ k \in \mathbb{Z}\}$

Dimostrazione:

1. $Sol(S) \neq \varnothing \implies (n, m) \mid a - b$
   - Supponiamo che $Sol(S) \neq \varnothing$, ovvero $\exists\ c \in Sol(S)$
   - Valgono le seguenti proprietà: $\begin{cases} c \equiv a \pmod{n} \\ c \equiv b \pmod{m} \end{cases} \iff \begin{cases} c = a + kn & \text{per qualche } k \in \mathbb{Z} \\ c = b + hm & \text{per qualche } h \in \mathbb{Z} \end{cases}$
   - $\implies a + kn = b + hm \iff a - b = hm - kn$
   - Dunque $(n, m) \mid n$ e $(n, m) \mid m \implies (n, m) \mid hm - kn = a - b$
   - Visto che $(n, m) \mid a - b$, abbiamo dimostrato la prima implicazione del teorema.
2. $(n, m) \mid a - b \implies Sol(S) \neq \varnothing$
   - Supponiamo che $(n, m) \mid a - b$, cioè **(1)**: $a - b = k(n, m)$ per qualche $k \in \mathbb{Z}$
   - Ricordiamo che esistono $x, y \in \mathbb{Z}$ tale che **(2)**: $xn + ym = (n, m)$ dall'algoritmo di Euclide
   - Dalla **(1)** e **(2)** segue che:

$$a - b = k(xn + ym) = (kx)n + (ky)m$$
$$a - \underbrace{b}_{\rightarrow} = \underbrace{(kx)n}_{\leftarrow} + (ky)m$$

   - Si ha che $c := a + (-kx)n = b + (ky)m \implies \begin{cases} c \equiv a \pmod{n} \\ c \equiv b \pmod{n} \end{cases}$
   - Visto che c è una **soluzione** e sta in $Sol(S)$, abbiamo dimostrato anche la seconda implicazione.
3. Resta da dimostrare che $Sol(S) = [c]_{[n,m]}\ (\in \mathbb{Z})$, dove $c \in Sol(S)$
   - $Sol(S) \subset [c]_{[n,m]}$
     - Sia $c' \in Sol(S)$
     - Perchè $c, c' \in Sol(S)$, valgono: $\begin{cases} c \equiv a \pmod{n} \\ c \equiv b \pmod{m} \\ c' \equiv a \ (\mathrm{mod}\ n \\ c' \equiv b \pmod{m} \end{cases} \iff \exists\ h, k, h', k' \in \mathbb{Z}$ tale che $\begin{cases} (1)\ c = a + hn \\ (2)\ c' = a + h'n \\ (3)\ c = b + km \\ (4)\ c' = b + k'm \end{cases}$

- Effettuiamo la sottrazione tra $(2)-(1)$ e $(4)-(3)$, si ha:

$$c'-c=(h'-h)n$$
$$c'-c=(k'-k)m$$

$\implies n \mid c'-c$ e $m \mid c'-c$
$\implies [n,m] \mid c'-c \iff c' \equiv c \pmod{[n,m]}$
$\implies c' \in [c]_{[n,m]}$

- $Sol(S) \supset [c]_{[n,m]}$
  - Sia $c' \in [c]_{[n,m]}$ ovvero $c' = c + k\,[n,m]$ per qualche $k \in \mathbb{Z}$
  - Vale:

$$\begin{aligned}[c']_n = [c+k\,[n,m]]_n &= [c]_n + [k]_n \cdot [[n,m]]_n \\ &= [c]_n + [k]_n \cdot [0]_n \\ &= [a]_n + [k]_n \cdot [0]_n \\ &= [a + k \cdot 0]_n \\ &= [a]_n\end{aligned}$$

  - Dunque si ha $[c']_n = [a]_n$
  - Stesso procedimento per dimostrare che $[c']_m = [b]_m$
- Poichè $Sol(S) \subset [c]_{[n,m]}$ e $[c]_{[n,m]} \subset Sol(S)$ allora $Sol(S) = [c]_{[n,m]}$ e così si conclude la dimostrazione.
- *C.V.D.*

3.2 Teorema di Fermat-Eulero

Enunciato:

- Sia $n > 0$, per ogni classe α invertibile, $\alpha \in (\mathbb{Z}/_{n\mathbb{Z}})^*$, vale:

$$\alpha^{\phi(n)} = [1]_n \in (\mathbb{Z}/_{n\mathbb{Z}})^*$$

- Equivalentemente, per ogni $\alpha \in \mathbb{Z}$ tale che: $(\alpha, n) = 1$ vale:

$$\alpha^{\phi(n)} \equiv 1 \pmod{n}$$

Dimostrazione:

- Sia $\alpha \in \left(\mathbb{Z}/_{n\mathbb{Z}}\right)^*$
- Definiamo la seguente funzione:

$$\begin{aligned}L_\alpha : (\mathbb{Z}/_{n\mathbb{Z}})^* &\longrightarrow (\mathbb{Z}/_{n\mathbb{Z}})^* \\ \beta &\longmapsto \alpha \cdot \beta\end{aligned}$$

- Ponendo $L_\alpha(\beta) = \alpha \cdot \beta \quad \forall\, \beta \in (\mathbb{Z}/_{n\mathbb{Z}})^*$
- Dobbiamo dimostrare che L_α è una **bigezione**, poichè $(\mathbb{Z}/_{n\mathbb{Z}})^*$ è finita, è sufficente verificare che L_α sia **iniettiva**:
  - Prendiamo $\beta_1, \beta_2 \in (\mathbb{Z}/_{n\mathbb{Z}})^*$ e siano $L_\alpha(\beta_1)$ e $L_\alpha(\beta_2)$

– Vogliamo dimostrare che $\beta_1 = \beta_2$:

$$\begin{aligned} L_\alpha(\beta_1) &= L_\alpha(\beta_2) \\ \alpha \cdot \beta_1 &= \alpha \cdot \beta_2 \quad (\alpha \text{ è invertibile}) \\ (\alpha^{-1} \cdot \alpha)\beta_1 &= (\alpha^{-1} \cdot \alpha)\beta_2 \\ [1]_n \cdot \beta_1 &= [1]_n \cdot \beta_2 \\ \beta_1 &= \beta_2 \end{aligned}$$

- L_α è **iniettiva** e **surgettiva** $\implies$ L_α è una **bigezione**.
- Scriviamo $(\mathbb{Z}/_{n\mathbb{Z}})^* = \{\beta_1, \beta_2, \dots, \beta_k\}$ dove $k = \phi(n)$

$$\begin{aligned} \implies \beta_1 \cdot \beta_2 \cdots \beta_k &= L_\alpha(\beta_1) \cdot L_\alpha(\beta_2) \cdots L_\alpha(\beta_k) \\ &= (\alpha \cdot \beta_1) \cdot (\alpha \cdot \beta_2) \cdots (\alpha \cdot \beta_k) \\ &= \alpha^k \cdot (\beta_1 \cdot \beta_2 \cdots \beta_k) \\ &= \alpha^{\phi(n)} \cdot (\beta_1 \cdot \beta_2 \cdots \beta_k) \end{aligned}$$

$$\begin{aligned} &\implies (\beta_1 \cdot \beta_2 \cdots \beta_k)(\beta_k^{-1} \cdot \beta_{k-1}^{-1} \cdots \beta_1^{-1}) = \alpha^{\phi(n)} \cdot (\beta_1 \cdot \beta_2 \cdots \beta_k)(\beta_k^{-1} \cdot \beta_{k-1}^{-1} \cdots \beta_1^{-1}) \\ &\implies (\cancel{\beta_1} \cdot \cancel{\beta_2} \cdots \cancel{\beta_k})(\cancel{\beta_k^{-1}} \cdot \cancel{\beta_{k-1}^{-1}} \cdots \cancel{\beta_1^{-1}}) = \alpha^{\phi(n)} \cdot (\cancel{\beta_1} \cdot \cancel{\beta_2} \cdots \cancel{\beta_k})(\cancel{\beta_k^{-1}} \cdot \cancel{\beta_{k-1}^{-1}} \cdots \cancel{\beta_1^{-1}}) \\ &\implies [1]_n = \alpha^{\phi(n)} \end{aligned}$$

- Visto che $[1]_n = \alpha^{\phi(n)}$ abbiamo dimostrato il teorema.
- *C.V.D.*

3.3 Teorema Fondamentale della Crittografia RSA

Enunciato:

- Sia $n > 0$ e sia $c \in \mathbb{N} \setminus \{0\}$ tale che $(c, \phi(n)) = 1$ $(\exists\ [c]_{\phi(n)}^{-1})$
- E sia $d \in \mathbb{N}$, $d > 0$ con $d \in [c]_{\phi(n)}^{-1}$
- Allora P_c è una **procedura bigettiva** e $P_c^{-1} = P_d$

$$\begin{aligned} (\mathbb{Z}/_{n\mathbb{Z}})^* &\xrightarrow{P_c} (\mathbb{Z}/_{n\mathbb{Z}})^* \\ \alpha &\longmapsto \alpha^c \end{aligned}$$

$$\begin{aligned} (\mathbb{Z}/_{n\mathbb{Z}})^* &\xleftarrow{P_d} (\mathbb{Z}/_{n\mathbb{Z}})^* \\ \beta^d &\xleftarrow{P_d} \beta \end{aligned}$$

Dimostrazione:

- Devo provare: $P_d \circ P_c = id_{(\mathbb{Z}/_{n\mathbb{Z}})^*} = P_c \circ P_d \ \forall\, \alpha \in (\mathbb{Z}/_{n\mathbb{Z}})^*$
- Poichè $d > 0$, $d \in [c]_{\phi(n)}^{-1}$ si ha:

$$\begin{aligned} [d]_{\phi(n)} \cdot [c]_{\phi(n)} &= [1]_{\phi(n)} \\ cd &\equiv 1 \pmod{\phi(n)} \end{aligned}$$

- Per definizione di congruenza:

$$cd = 1 + h\,\phi(n) \text{ per qualche } h \in \mathbb{N} \text{ (con } cd > 0 \text{ e } h > 0)$$

- Quindi:

$$
\begin{aligned}
P_d(P_c(\alpha)) = P_d(\alpha^c) &= (\alpha^c)^d \\
&= \alpha^{cd} \\
&= \alpha^{1+h\phi(n)} \\
&= \alpha^1 \cdot \left(\alpha^{\phi(n)}\right)^h \\
&= \alpha \cdot [1]^h_{\phi(n)} \\
&= \alpha \cdot [1]_{\phi(n)} \\
&= \alpha
\end{aligned}
$$

- *C.V.D.*

4 Grafi

4.1 Equivalenze tra congiungibilità per cammini e passeggiate

ENUNCIATO:

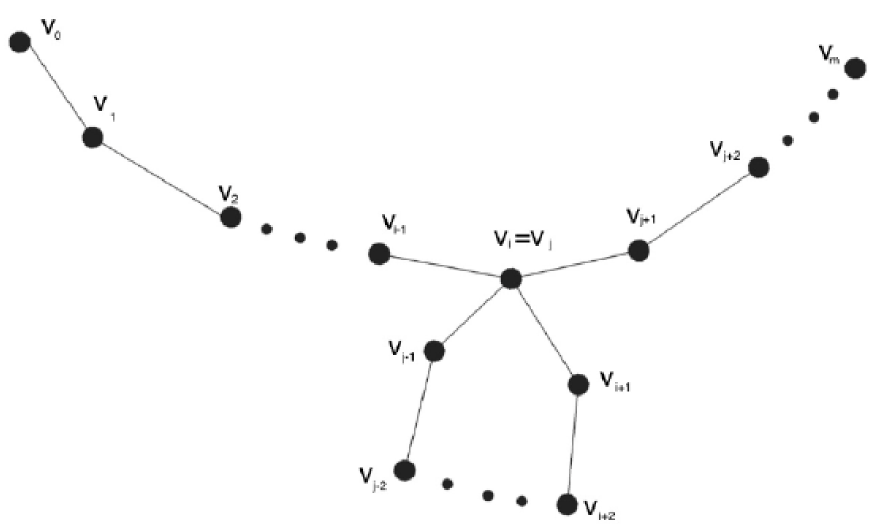
- Sia $G = (V, E)$ e siano $v, w \in V$ (non necessariamente distinti).
- v e w sono **congiungibili** per **passeggiata** in G **se e solo se** lo sono per **cammini**.
- Cioè, sono congiungibili se esiste una passeggiata (cammino) $P \in G$, $P = (V_0, \dots, V_k)$ tale che il vertice di partenza sia v e quello di arrivo sia w.

DIMOSTRAZIONE:

- $\Leftarrow$) Ovvio in quanto per definizione il cammino è una passseggiata, allora se sono congiungibili per cammino lo sono anche per passseggiata.
- $\Rightarrow$) Supponiamo che esista una passeggiata $P = (V_0, \dots, V_k)$ in G tale che $V_0 = v$ e $V_k = w$.
  - Indichiamo con $\mathbb{P}$ l'insieme di tutte le passeggiate Q in G che partono da v e arrivano in w.
  - Per ipotesi $P \in \mathbb{P} \neq \varnothing$
  - Dunque $A := \{\ell(Q) \in \mathbb{N} \,|\, Q \in \mathbb{P}\} \neq \varnothing$
  - Poichè $(N, \leq)$ è **ben ordinato** (ordinamento totale e ogni sottoinsieme ammette minimo) $\exists\, min(A) = \ell(P_0)$ (passeggiata con il minor numero di lati da v a w).
  - Segue che $\exists\, P_0 \in \mathbb{P}$ tale che:
    * P_0 è una passeggiata in G che parte da v e arriva in w.
    * $\ell(P_0) \leq \ell(Q)\ \forall\, Q \in \mathbb{P}$
  - Proviamo che P_0 è un **cammino**.
  - Scriviamo P_0 esplicitamente:

$$P_0 = (y_0, y_1, \dots, y_h) \text{ dove } y_0 = v \text{ e } y_h = w$$

  - Se P_0 non fosse un cammino esisterebbero $i, j \in \{0, 1, \dots, h\}$ tali che $i \neq j$, $i < j$ e $y_i \leq y_j$



– Dunque possiamo definire una nuova passeggiata $P \supset P_1 = (y_0, y_1, \ldots, y_i, y_{j+1}, y_{j+2}, \ldots, y_h$ in cui sono stati tolti tutti i vertici tra v_i e v_j
– In particolare si ha che:
$$\ell(P_1) = \ell(P_0) - (j - i) < \ell(P_0) \leq \ell(P_1)$$
– Ma ciò è impossibile in quanto avevamo dimostrato come P_0 fosse il minimo dei cammini possibili.
– Abbiamo dimostrato che P_0 è un cammino.

- *C.V.D.*

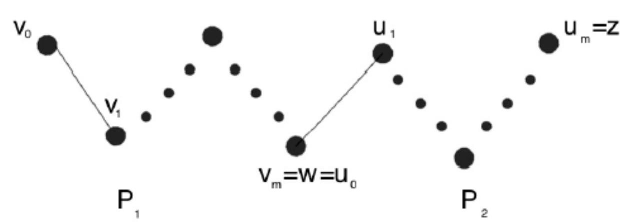
4.2 Congiungibilità è una relazione di equivalenza

Enunciato:

- La relazione di essere **congiungibili** (per passeggiata o per cammino) è di **equivalenza** sui vertici di un grafo.

Dimostrazione:

- $G = (V, E)$ grafo.
- $v, w \in V$, $v \sim w$ se v e w sono **congiungibili** in G.
- $v, w, z \in V$, affinchè sia una relazione deve soddisfare le tre proprietà:
  1. Riflessiva:
     – $v \sim v \;\forall v \in V$? Vero in quanto $\exists P = (v)$ che è una passeggiata da v in v.
  2. Simmetrica:
     – Supponiamo $v \sim w$, ovvero $\exists$ $(V_0, V_1, \ldots, V_k)$ passeggiata (dove $V_0 = v$ e $V_k = w$).
     $\implies$ $(V_k, V_{k-1}, \ldots, V_0)$ passeggiata in G (dove $V_k = w$ e $V_0 = v$).
     $\implies$ $w \sim v$
  3. Transitiva:
     – Supponiamo $v \sim w$ e $w \sim z$, dunque esistono due passeggiate in G tali che:
       * $P_1 = (v_0 = v, v_1, \ldots, v_n = w)$
       * $P_2 = (y_0 = w, y_1, \ldots, y_h = z)$



     – Si può dunque definire una terza passeggiata in G:
$$(v_0 = v, v_1, \ldots, v_k = w = y_0, y_1, \ldots, y_h)$$
     $\implies$ $v \sim z$

- *C.V.D.*

4.3 Relazione fondamentale tra gradi e numero di lati di un grafo finito

ENUNCIATO:

- Sia $G = (V, E)$ un grafo **finito**, allora:

$$\sum_{v \in V} deg_G(v) = 2\,|E|$$

DIMOSTRAZIONE:

- Siano $(v_1, \ldots, v_n)$ i **vertici** di G e siano $(e_1, \ldots, e_k)$ i **lati** di G.
- Per ogni $i \in \{1, \ldots, n\}$ e per ogni $j \in \{1, \ldots, k\}$, definiamo $m_{i,j} \in \{0, 1\}$ come segue:

$$m_{i,j} \begin{cases} 0 \text{ se } v_i \neq e_j \\ 1 \text{ se } v_i = e_j \end{cases}$$

- Prendiamo un piano cartesiano: lungo le x scorre l'indice i e lungo le y scorre l'indice j.
- Vale allora:

$$\sum_{j=1}^{k} \left(\sum_{i=1}^{n} m_{i,j} \right) = \sum_{i=1}^{n} \left(\sum_{j=1}^{k} m_{i,j} \right)$$

- Dove il primo membro ha il seguente significato:
  - $\sum_{i=1}^{n} m_{i,j}$ è il numero di vertici di un lato, che è sempre 2 (la j è bloccata).
  - $\sum_{j=1}^{k} \left(\sum_{i=1}^{n} m_{i,j} \right)$ si sommano k volte ($j \in \{1, \ldots, k\}$) il numero di vertici per ciascun lato.
  - Si ottiene quindi che il primo membro può essere riscritto come:

$$\sum_{j=1}^{k} \left(\sum_{i=1}^{n} m_{i,j} \right) = 2k$$

- Mentre il secondo membro ha il seguente significato:
  - $\sum_{j=1}^{k} m_{i,j}$ è la somma dei numeri su una colonna, posto fisso i per via della sommatoria che precede questa.
  - $\sum_{i=1}^{n} \left(\sum_{j=1}^{k} m_{i,j} \right)$ risulta essere la somma dei valori ottenuti sommando i valori di ciascuna colonna.
  - Ma la prima sommatoria non è altro che la sommatoria di 1 se un lato entra o esce da un determianto i-esimo vertice, o 0 se ciò non accade.
  - Questa somma non è altro che il numero di lati che incontrano tale vertice.
  - Si può quindi scrivere il primo membro in questo modo:

$$\sum_{i=1}^{n} (deg_G(v_i))$$

- Dunque si ha che:

$$\begin{aligned}
\sum_{j=1}^{k}\left(\sum_{i=1}^{n} m_{i,j}\right) &= \sum_{i=1}^{n}\left(\sum_{j=1}^{k} m_{i,j}\right) \\
\sum_{j=1}^{k} 2 &= \sum_{i=1}^{n} deg_G(v_i) \\
2k &= \sum_{i=1}^{n} deg_G(v_i) \\
2\,|E| &= \sum_{i=1}^{n} deg_G(v_i)
\end{aligned}$$

- *C.V.D*

4.4 Lemma delle strette di mano

ENUNCIATO:

- In un grafo **finito**, il **numero di vertici** con **grado dispari** è **pari**.

DIMOSTRAZIONE:

- $G = (V, E)$ finito:

$$\begin{aligned}
\underbrace{2\,|E|}_{\text{pari}} &= \sum_{v\in V} deg_G(v) \\
&= \underbrace{\sum_{v\in V} deg_G(v)}_{deg_G(v)\text{ pari}} + \underbrace{\sum_{v\in V} deg_G(v)}_{deg_G(v)\text{ dispari}} \qquad (1) \\
\text{numero pari} &= \text{numero pari} \implies \text{numero pari}
\end{aligned}$$

4.5 Teorema di caratterizzazione degli alberi finiti

ENUNCIATO:

- Sia $T = (V, E)$ un grafo **finito**, ovvero $|V|$ è finita.
- Le seguenti affermazioni sono equivalenti:
  1. T è un **albero**.
  2. T è **connesso** e vale la seguente **formula di Eulero**:

$$|V| - 1 = |E| = \frac{1}{2}\sum_{v\in V} deg_T(v)$$

ENUNCIATO:

- 1. $\implies$ 2.
  * T è un albero, dunque T è connesso per definizione di albero.
  * Dobbiamo provare la formula di Eulero.
  * Procediamo per induzione (1° forma) sul numero di vertici di T:

· **Base dell'induzione**: $|V(T)| = 1$, questo implica che $|E(T)| = 0$, dunque:

$$\begin{gathered} |V| - 1 = |E| \\ 1 - 1 = 0 \end{gathered} \tag{2}$$

· La base dell'induzione è verificata.
· $|V(T)| \implies |V(T)|$ con $|V(T)| \geq 2$ (**passo induttivo**).
· Sia T un albero (finito) con almeno 2 vertici ($|V(T)| \geq 2$), allora T possiede almeno 2 foglie (Lemma 20.4).
· Sia v una tale foglia.
· Poichè $T - v$ è ancora un albero, per **ipotesi induttiva**, $T - v$ soddisfa la formula di Eulero, cioè:

$$\begin{gathered} \underbrace{|V(T-v)|}_{V(T)-1} - 1 = \underbrace{|E(T-v)|}_{|E(T)-1|} \\ |V(T)| - 2 = |E(T)| - 1 \\ |V(T)| - 1 = |E(T)| \end{gathered} \tag{3}$$

∗ La prima implicazione è stata dimostrata.

– 2. $\implies$ 1.

∗ Sia T un grafo finito, connesso che soddisfa la formula di Eulero, cioè vale la 2.
∗ Dobbiamo provare che T è un albero.
∗ Procediamo per induzione su $|V(T)|$:

· **Base dell'induzione**:

$$|V(T)| = 1, \text{ dunque } T \text{ è un albero.}$$

· Base dell'induzione dimostata.
· $|V(T)| \geq 2$, $|V(T)| - 2 \implies |V(T)|$ (**ipotesi induttiva**).
· Dimostriamo che T ha almeno una foglia.
· Supponiamo che ciò sia falso. Poichè T è connesso, il $deg_T(v) \geq 2\ \forall v \in V(T)$ dunque:

$$\begin{gathered} |V(T)| - 1 = |E(T)| \\ 2\,|V(T)| - 2 = 2\,|E(T)| = \sum_{v \in V} deg_T(v) \geq \sum_{v \in V} 2 = 2\,|V(T)| \\ \implies 2\,|V(T)| - 2 \geq 2\,|V(T)| \text{ che è assurdo.} \end{gathered} \tag{4}$$

· Abbiamo appena dimostrato che T ha **almeno una foglia**.
· Sia dunque v una foglia di T.
· Osservo che $T - v$ è **connesso**.
· Ricordiamo che:

$$|V(T) - 1| = |E(T)| \iff (|V(T)| - 1) - 1 = |E(T)| - 1 \iff |V(T - v)| - 1 = |E(T - v)|$$

· Per ipotesi induttiva $T - v$ è un albero ($T - v$ è connesso e soddisfa la formula di Eulero).
· Supponiamo che c sia un ciclo di T che passa per i vertici v e w.
· $T - v$ creerebbe un ciclo, ma visto che $T - v$ per ipotesi è un albero, questo implica che non ha cicli, dunque anche T non ha cicli. $\implies$ T è un albero.

∗ La seconda implicazione è stata dimostrata.

– Visto che sia la prima che la seconda implicazione sono state dimostrate, abbiamo finito la dimostrazione del teorema.

4.6 Teorema esistenza alberi di copertura

ENUNCIATO:

- Ogni grafo **finito** e **connesso ammette un albero di copertura**.

DIMOSTRAZIONE:

- Sia G un grafo finito e connesso.
- Scriviamo $G = (V, E)$.
- Consideriamo:

$$\mathbb{C} := \{C \,|\, C \text{ è un sottografo conneso di } G \text{ tale che } V(C) = V(G)\}$$

- Osserviamo che $\mathbb{C} \neq \varnothing$ in quanto $G \in \mathbb{C}$.
- Definiamo:

$$A := \{|E(C)| \in \mathbb{N} \,|\, C \in \mathbb{C}\} \neq \varnothing \text{ in quanto } |E(G)| \in \mathbb{A}$$

- Grazie al **teorema di buon ordinamento** $(\mathbb{N}, \leq)$ $\exists\, \overline{C} \in \mathbb{C}$ tale che:

$$|E(\overline{C})| \leq |E(C)| \quad \forall\, C \in \mathbb{C}$$

- Poichè $\overline{C} \in \mathbb{C}$ vale che $V(\overline{C}) = V(G)$.
- Dunque per dimostrare che $\bar{C}$ è un albero di copertura di G è sufficiente verificare che $\bar{C}$ è un albero.
- Se $\overline{C}$ non fosse un albero, ciò significherebbe che contiene almeno un ciclo, visto che $\overline{C}$ è connesso ma non è un albero.
- Se togliessi un lato da $\overline{C}$, quello che ottengo è un grafo connesso senza cicli.
- Ma visto che, togliendo un alto, la minimalità del numero di lati di $\overline{C}$ viene a mancare, cioè $|E(\overline{C} - e)| \leq |E(\overline{C})|$, ma questo è **assurdo** perchè $|E(\overline{C}|$ è il minor numero di lati, definito per costruzione.
- Dunque $\overline{C}$ è un albero e in particolare è un **albero di copertura**.