1. L'ordinamento dei numeri naturali è un buon ordinamento e seconda forma del principio d'induzione

Teorema 7.4 (Buon ordinamento). L'ordinamento dei numeri naturali è un buon ordinamento.

Dim. Suppongo che $A \subseteq \mathbb{N}$ non abbia minimo e dimostro che $A = \emptyset$. Sia B il suo complementare, ovvero $B = \mathbb{N} - A$, e dimostro per induzione che

$$\forall n \in \mathbb{N} \ \{0, \dots, n\} \subseteq B$$

$0 \notin A$ poiché altrimenti ne sarebbe il minimo, dunque $\{0\} \subseteq B$. Suppongo ora che $\{0, \dots, n\} \subseteq B$, quindi $0, \dots n \notin A$, ma allora $n+1 \notin A$ altrimenti ne sarebbe il minimo, quindi $\{0, \dots, n+1\} \subseteq B$. Ma allora, $B = \mathbb{N}$ e $A = \emptyset$. ■

Teorema 7.5 (Seconda forma dell'induzione). Sia $\mathcal{P}(n)$ una famiglia di proposizione indicizzate su $\mathbb{N}$ e si supponga che valgano le seguenti:

(i) $\mathcal{P}(0)$ è vera

(ii) $\forall n \in \mathbb{N} \ (\mathcal{P}(k) \text{ vera } \forall k < n) \Rightarrow \mathcal{P}(n)$ vera

allora, $\mathcal{P}(n)$ è vera $\forall n \in \mathbb{N}$.

Dim. Sia $A = \{n \in \mathbb{N} : \mathcal{P}(n) \text{ non è vera}\}$. Suppongo per assurdo che $A \neq \emptyset$, dunque per il Teorema di buon ordinamento, A ha un minimo: $n \coloneqq \min A$. Per l'ipotesi (i), $\mathcal{P}(0)$ è vera, dunque $0 \notin A$. Inoltre, se $k < n$, $k \notin A$ perché n ne è il minimo. Ma allora, $\mathcal{P}(k)$ è vera $\forall k < n$, e quindi per (ii), anche $\mathcal{P}(n)$ è vera, di conseguenza $n \notin A$, contraddicendo il fatto che $n \in A$. ■

2. Esistenza e unicità di quoziente e resto nella divisione euclidea tra numeri interi

Teorema 7.7. Siano $n, m \in \mathbb{Z}$ con $m \neq 0$. Esistono e sono unici $q, r \in \mathbb{Z}$ tali che:

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

Dim. Esistenza. Ipotizzo che $n, m \in \mathbb{N}$ e procedo per induzione su n. Se $n = 0$ basta porre $q = 0$ e $r = 0$. Se invece $0 < n$ e $n < m$ pongo $q = 0$ e $r = n$, altrimenti ipotizzo che la tesi sia vera per ogni $k < n$ e pongo $k = n - m$. Poiché $m \neq 0$, $0 \leq k < n$ e per ipotesi induttiva, vale:

$$\begin{cases} k = mq + r \\ 0 \leq r < m \end{cases}$$

Ma, $n = k + m = (mq + r) + m = m(q+1) + r$.

Siano ora, $n < 0$ e $m > 0$, allora $-n > 0$ e quindi per il caso precedente

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

e dunque, $n = m(-q) - r$. Se $r = 0$ ho finito, se invece $0 < r < m = |m|$ vale $0 < m - r < m = |m|$ e quindi $n = m(-q) - m + (m - r) = m(-q-1) + m - r$.

Infine, se $m < 0$, allora $-m > 0$ e per i due casi precedenti $\exists q, r \in \mathbb{Z}$ tali che $n = (-m)q + r$ con $0 \leq r < -m = |m|$.

Unicità. Sia $n = mq + r = mq' + r'$ con $0 \leq r, r' < |m|$. Ipotizzo $r' \geq r$, quindi vale $m(q - q') = r' - r$ e passando al modulo ottengo $|m| \cdot |q - q'| = |r' - r| = r' - r < |m|$, da cui $0 \leq |q - q'| < 1$ e quindi $|q - q'| = 0$, cioè $q = q'$. A questo punto, da $n = mq + r = mq' + r'$ segue che $r = r'$. ■

3. Rappresentazione dei numeri naturali in una base arbitraria maggiore o uguale a 2

Teorema 8.4 (Rappresentazione dei natural in base arbitraria). Sia $b \in \mathbb{N}$ con $b \geq 2$. Ogni numero $n \in \mathbb{N}$ è rappresentabile in base b, cioè esiste una successione $\{\epsilon_i\}_{i\in\mathbb{N}}$, composta da valori in interi $0 \leq \epsilon_i < b_i$, che sia definitivamente nulla, ovvero per la quale esiste un valore $k \in \mathbb{N}$ per cui $\epsilon_i = 0\ \forall i > k$, e tale che $n = \sum_{i=0}^{+\infty} \epsilon_i b^i$. Inoltre, se esiste un'altra tale successione $\{\epsilon_i'\}_{i\in\mathbb{N}}$, vale $\epsilon_i = \epsilon_i'$ per ogni $i \in \mathbb{N}$.

Dim. Esistenza. Procedo per induzione su n. Se $n = 0$ posso prendere $\epsilon_i = 0$ per ogni $i \in \mathbb{N}$. Se $n > 0$, ipotizzo che la tesi sia vera $\forall k < n$. Considero la divisione euclidea tra n e b, ovvero siano $q, r \in \mathbb{Z}$ tali che

$$\begin{cases} n = bq + r \\ 0 \leq r < b \end{cases}$$

Se $n < b$, valgono $q = 0$ e $r = n$, quindi posso definire una successione $\{\epsilon_i\}_{i\in\mathbb{N}}$ tale per cui $\epsilon_0 = r = n$ e $\epsilon_i = 0\ \forall i > 0$. Se invece $n \geq b$, poiché $b \geq 2$, vale $0 < q < bq \leq bq + r = n$, quindi per ipotesi induttiva esiste una successione definitivamente nulla $\{\delta_i\}_{i\in\mathbb{N}}$, costituita da interi $0 \leq \delta_i < b$ e tale che $q = \sum_{i=0}^{+\infty} \delta_i b^i$. Ma allora:

$$n = bq + r = b\sum_{i=0}^{+\infty} \delta_i b^i + r = \sum_{i=0}^{+\infty} \delta_i b^{i+i} + r = \sum_{i=1}^{+\infty} \delta_{i-1} b^i + r = \sum_{i=0}^{+\infty} \epsilon_i b^i$$

con $\epsilon_0 = r$ e $\epsilon_i = \delta_{i-1}$ per ogni $i \geq 1$. La successione $\{\epsilon_i\}_{i\in\mathbb{N}}$ è definitivamente nulla perché lo è $\{\delta_i\}_{i\in\mathbb{N}}$, inoltre $0 \leq \epsilon_i < b\ \forall i \in \mathbb{N}$.

Unicità. Procedo per induzione su n. Se $n = 0 = \sum_{i=0}^{+\infty} \epsilon_i b^i$, poiché ogni termine $\epsilon_i b^i$ è non negativo e dato che $b \geq 2$, necessariamente $\epsilon_i = 0$ per ogni $i \in \mathbb{N}$. Se $n > 0$, ipotizzo che la tesi sia vera $\forall k < n$. Sia $n = \sum_{i=0}^{+\infty} \epsilon_i b^i = \sum_{i=0}^{+\infty} \epsilon_i' b^i$. Posso scrivere:

$$n = b\sum_{i=1}^{+\infty} \epsilon_i b^i + \epsilon_0 = b\sum_{i=i}^{+\infty} \epsilon_i' b^i + \epsilon_0'$$

Per l'unicità di quoziente e resto nella divisione euclidea tra numeri interi, $\epsilon_0 = \epsilon_0'$ e $q = \sum_{i=1}^{+\infty} \epsilon_i b^i = \sum_{i=1}^{+\infty} \epsilon_i' b^i$, quindi poiché $q < n$, per ipotesi induttiva, si ha che $\epsilon_i = \epsilon_i'\ \forall i \geq 1$. ■

4. Teorema di esistenza e unicità di M.C.D e m.c.m tra due numeri interi non entrambi nulli

Teorema 9.8. Dati due numeri $n, m \in \mathbb{Z}$ non entrambi nulli, esiste il massimo comun divisore tra n e m.

Dim. Sia $S = \{s \in \mathbb{Z} | s > 0, \exists x, y : s = nx + my\}$. Poiché $nn + mm > 0$ (non sono entrambi nulli), $S \neq \emptyset$, dunque per il Teorema di buon ordinamento, S ha minimo: $d \coloneqq nx+my = \min S$.

Dimostro che d è il massimo comun divisore. Se $c|n$ e $c|m$, allora $n = ch$ e $m = ck$, quindi $d = nx + my = chx + xky = c(hx + ky)$, cioè $c|d$.

Resta da dimostrare che $d|n$ e $d|m$. Se considero la divisione euclidea tra n e d ottengo $n = dq + r$ con $0 \leq r < |d|$. Se $r > 0$ potrei scrivere $r = n - dq = n - (nx + my)q = n(1 - xq) + (-m)yq$. Quindi r sarebbe un elemento di S, ma poiché $r < d = \min S$ questo è impossibile, di conseguenza $r = 0$, ovvero $d|n$.

Analogamente si può dimostrare che $d|m$. ■

Proposizione 9.6. Se d e d' sono due massimi comun divisori di n e m, allora $d' = \pm d$.

Dim. Se d è un divisore comune di n e m, poiché d' ne è il massimo comun divisore, si ha che $d|d'$. Invertendo i ruoli di d e d' si ottiene che anche $d'|d$. Poiché $d|d'$ e $d'|d$, $d = hd'$ e $d' = kd$, ma allora $d' = hkd'$, da cui deriva che o $d' = 0$ e quindi $d = 0$, oppure $1 - hk = 0$, ma allora o $h = k = 1$ e quindi $d = d'$, oppure $h = k = -1$ e quindi $d = -d'$. In definitiva, vale che $d' = \pm d$. ■

Teorema 10.4 (Esistenza del m.c.m). Siano $n, m \in \mathbb{Z}$ non entrambi nulli. Esiste il minimo comune multiplo tra di essi.

Dim. Sia $M = \frac{n \cdot m}{(n,m)} = n'm'(n, m)$ con $n = n'(n, m)$ e $m = m'(n, m)$. Chiaramente $M = n \cdot m' = n' \cdot m$, quindi $n|M$ e $m|M$.

Se $n|c$ e $m|c$, $(n, m)|c$ e quindi, posto $c = c'(n, m)$, ho che $n'|c'$ e $m'|c'$. Poiché $n' = \frac{n}{(n,m)}$ e $m' = \frac{m}{(n,m)}$, $(n', m') = \left(\frac{n}{(n,m)}, \frac{m}{(n,m)}\right) = 1$, $n'm'|c'$ e quindi $M = n'm'(n, m)|c'(n, m) = c$. ■

L'unicità si dimostra come per il massimo comun divisore.

5. Teorema fondamentale dell'aritmetica

Teorema 10.5 (Teorema fondamentale dell'aritmetica). Per ogni $n \in \mathbb{Z}$ con $n \geq 2$ esistono numeri primi $p_1, \dots, p_k$ positivi tali che $\prod_{i=1}^{k} p_i = n$. Se anche $q_i, \dots, q_h$ sono numeri primi positivi tali che $\prod_{j=1}^{h} q_j = n$, allora esiste una bigezione $\sigma : \{1, \dots, h\} \to \{1, \dots, k\}$ tale che $q_i = p_{\sigma(i)}$.

In altre parole, ogni numero intero maggiore o uguale a 2 è rappresentabile in modo unico a meno di riordinamento come prodotto di numeri primi positivi.

Dim. Esistenza. Procedo per induzione su n. Se $n = 2$ non devo fare nulla perché 2 è un numero primo. Se $n > 2$, ipotizzo che la tesi sia vera per ogni $d < n$. Se n è primo non c'è nulla da dire, altrimenti esistono sicuramente due numeri $d_1, d_2 \in \mathbb{Z}$ tali che $1 < d_1, d_2 < n$. Per ipotesi induttiva, $d_1 = \prod_{i=1}^{k} p_i$ e $d_2 = \prod_{j=1}^{h} q_j$, quindi poiché $n = d_1 \cdot d_2 = \left(\prod_{i=1}^{k} p_i\right) \cdot \left(\prod_{j=1}^{h} q_j\right)$, ossia è esprimibile come prodotto di numeri primi.

Unicità. Sia $n = \prod_{i=1}^{k} p_i = \prod_{j=1}^{h} q_j$ e ipotizzo $k \leq h$. Procedo per induzione su k.

Se $k = 1$ allora $n = p_1 = \prod_{j=1}^{h} q_j$, quindi $q_j | p_1$ $\forall j \in \{1, \ldots, h\}$. Ma, poiché p_1 è un numero primo, o $q_j = 1$ o $q_j = p_1$. Siccome, per ipotesi, tutti i q_j sono numeri primi positivi, necessariamente $q_j = p_1$. A questo punto, se $h > 1$ si avrebbe $n = \prod_{j=1}^{h} q_j \geq q_1 \cdot q_2 > q_1 = p_1 = n$ e questo è assurdo, per cui $h = 1$.

Se $k > 1$, ipotizzo che la tesi sia vera per ogni $d < k$. Sicuramente, $p_k | n$, dunque so che esiste un j tale che $q_j | p_k$, ma poiché sia q_j che p_k sono numeri interi positivi, vale $q_j = p_k$. Ma allora, $p_1 \ldots p_{k-1} = q_1 \ldots q_{j-1} \cdot q_{j+1} \ldots q_h$ e, per ipotesi induttiva, le due fattorizzazioni hanno lo stesso numero di elementi, ovvero $k - 1 = h - 1$. Esiste quindi una bigezione $\delta : \{1, \ldots, j-1, j+1, \ldots, h\} \to \{1, \ldots, k-1\}$ tale che $q_i = p_{\delta(i)}$ per ogni i. A questo punto, definendo $\sigma : \{1, \ldots, k\} \to \{1, \ldots, k\}$ come:

$$\sigma(i) = \begin{cases} k & \text{se } i = j \\ \delta(i) & \text{se } i \neq j \end{cases}$$

si ottiene una bigezione tale che $q_i = p_{\sigma(i)}$ per ogni i. ■

6. Teorema cinese del resto

Teorema 12.1 (Teorema cinese del resto). Il sistema di congruenze

$$\begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{cases}$$

ha soluzione se e soltanto se $(n, m) | b - a$. Inoltre, le soluzione sono tutti e soli gli elementi di $[c]_{[n,m]}$.

Dim. Sia c una soluzione del sistema. Esistono $h, k \in \mathbb{Z}$ tali che $c = a + hn = b + km$ e quindi $hn - km = b - a$. Siccome $(n, m)|n$ e $(n, m)|m$ si ha che $(n, m)|hn - km = b - a$. Viceversa, se ipotizzo che $(n, m)|b - a$, esistono $h, k \in \mathbb{Z}$ tali che $hn + km = b - a$, da cui $a + hn = b - km$. Se ora pongo $c = a + hn = b - km$, è evidente che c è una soluzione del sistema.

Sia $S = \{x \in \mathbb{Z} | x \text{ è soluzione del sistema}\}$. Devo dimostrare che se c è una soluzione allora $S = [c]_{[n,m]}$.

Ipotizzo $S \subseteq [c]_{[n,m]}$. Sia $c' \in S$ un'altra soluzione del sistema, allora $c = a + hn = b + km$ e $c' = a + h'n = b + k'm$. Se ora calcolo $c - c'$ ottengo:

$$c - c' = a + hn - (a + h'n) = n(h - h') \Rightarrow n | c - c'$$

$$c - c' = b + km - (b + k'm) = m(k - k') \Rightarrow m | c - c'$$

Ma allora, $[n, m] | c - c'$ ossia $c' \equiv c \pmod{[n, m]}$, ovvero $c' \in [c]_{[n,m]}$.

Infine, suppongo $[c]_{[n,m]} \subseteq S$. Sia $c' \in [c]_{[n,m]}$, ovvero $c' = c + h[n, m]$. Poiché $c \equiv a \pmod{n}$ e $h[n, m] \equiv 0 \pmod{n}$, $c' = c + h[n, m] \equiv a \pmod{n}$. In modo analogo si dimostra che $c' \equiv b \pmod{m}$ e che quindi $c' \in S$. ■

7. Teorema di Fermat-Eulero e crittografia RSA

Teorema 13.9. Sia $n > 0$. Per ogni $\alpha \in (\mathbb{Z}/_{n\mathbb{Z}})^*$, vale:

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

o, equivalentemente, $\forall \alpha \in \mathbb{Z}$ *t.c.* $(\alpha, n) = 1$, vale:

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

Dim. Sia $\alpha \in (\mathbb{Z}/_{n\mathbb{Z}})^*$. Considero la seguente funzione:

$$L_\alpha : (\mathbb{Z}/_{n\mathbb{Z}})^* \to (\mathbb{Z}/_{n\mathbb{Z}})^*$$

definita in modo che $L_\alpha(\beta) \mapsto \alpha\beta \ \forall \beta \in (\mathbb{Z}/_{n\mathbb{Z}})^*$. Poiché l'insieme $(\mathbb{Z}/_{n\mathbb{Z}})^*$ è finito e coincide sia col dominio che col codominio, se riesco a dimostrare che L_α è iniettiva, sarà anche suriettiva.

Dimostro quindi l'iniettività. Siano $\beta_1, \beta_2 \in (\mathbb{Z}/_{n\mathbb{Z}})^*$ *t.c.* $L_\alpha(\beta_1) = L_\alpha(\beta_2)$. Provo che $\beta_1 = \beta_2$. Vale:

$$L_\alpha(\beta_1) = L_\alpha(\beta_2) \Leftrightarrow \alpha\beta_1 = \alpha\beta_2 \Rightarrow \alpha^{-1}\alpha\beta_1 = \alpha^{-1}\alpha\beta_2 \Rightarrow [1]_n\beta_1 = [1]_n\beta_2 \Rightarrow \beta_1 = \beta_2$$

Dunque, L_α è iniettiva e suriettiva, ovvero è una bigezione.

Passo ora alla dimostrazione del teorema. Sia $k := \Phi(n)$ e $(\mathbb{Z}/_{n\mathbb{Z}})^* = \{\beta_1, \dots, \beta_k\}$, allora gli elementi $L_\alpha(\beta_1), \dots, L_\alpha(\beta_k)$ sono tutti e soli gli elementi di $(\mathbb{Z}/_{n\mathbb{Z}})^*$, a meno di riordinamento. Poiché il prodotto in $(\mathbb{Z}/_{n\mathbb{Z}})^*$ è commutativo, vale:

$$\prod_{i=i}^{k} \beta_i = \prod_{i=1}^{k} L_\alpha(\beta_i) = \prod_{i=1}^{k} \alpha\beta_i = \alpha^k \prod_{i=1}^{k} \beta_i \text{ in } (\mathbb{Z}/_{n\mathbb{Z}})^*$$

Sia $(\mathbb{Z}/_{n\mathbb{Z}})^* \ni \gamma := \prod_{i=1}^{k} \beta_i$, segue che:

$$\gamma = \alpha^k\gamma \Rightarrow \gamma^{-1} \cdot \gamma = \alpha^k\gamma \cdot \gamma^{-1} \Rightarrow [1]_n = \alpha^k$$

Se $\alpha \in \mathbb{Z}$ con $(\alpha, n) = 1$, allora $[\alpha]_n \in (\mathbb{Z}/_{n\mathbb{Z}})^*$ e per la precedente segue che:

$$[\alpha]_n^{\Phi(n)} = [1]_n \Rightarrow [\alpha^{\Phi(n)}]_n = [1]_n \Leftrightarrow \alpha^{\Phi(n)} \equiv 1 \pmod{n}$$

■

Teorema fondamentale della crittografia RSA. Sia $c \in \mathbb{N}\backslash\{0\}$ *t.c.* $(c, \Phi(n)) = 1$ e sia $d \in [c]^{-1}_{\Phi(n)}$ con $d > 0$. Allora, la funzione P_c, che eleva il suo argomento alla potenza c, è una funzione invertibile e vale:

$$(P_c)^{-1} = P_d$$

Dim. Sia $\alpha \in (\mathbb{Z}/_{n\mathbb{Z}})^*$. Devo dimostrare che $P_d(P_c(\alpha)) = \alpha$. Ricordo che, poiché $d \in [c]^{-1}_{\Phi(n)}$, vale:

$$c \cdot d \equiv 1 \pmod{\Phi(n)} \Leftrightarrow \Phi(n) | c \cdot d - 1 \Leftrightarrow \exists k \in \mathbb{Z} \textit{ t.c. } c \cdot d - 1 = k \cdot \Phi(n) \Leftrightarrow c \cdot d = 1 + k \cdot \Phi(n)$$

Osservo che, $k \cdot \Phi(n) = c \cdot d - 1$ e, siccome per ipotesi $c, d \geq 1$, $c \cdot d - 1 \geq 0$, inoltre $\Phi(n) > 0$, dunque anche $k \geq 0$. Per il Teorema 13.9 vale $\alpha^{\Phi(n)} = [1]_n$, quindi segue che:

$$P_d(P_c(\alpha)) = P_d(\alpha^c) = (\alpha^c)^d = \alpha^{c \cdot d} = \alpha^{1 + k \cdot \Phi(n)} = \alpha^1 \cdot \alpha^{k \cdot \Phi(n)} = \alpha \cdot (\alpha^{\Phi(n)})^k = \alpha \cdot ([1]_n)^k = \alpha$$

■

8. Teorema di equivalenza tra la congiungibilità con cammini e la congiungibilità con passeggiate; la relazione di congiungibilità è una relazione di equivalenza

Proposizione 15.8. Sia G un grafo e siano $u, v \in V(G)$ suoi vertici, allora u e v sono congiungibili mediante cammino se e solo se lo sono mediante una passeggiata.

Dim. Dato che un cammino è anche una passeggiata, se due vertici sono congiungibili mediante un cammino lo sono anche mediante una passeggiata.

Viceversa, suppongo che tra due vertici $u, v \in V(G)$ esista una passeggiata. Definisco i seguenti insiemi:

$$\mathcal{P} = \{P \mid P \text{ è una passeggiata tra } u \text{ e } v\} \; A = \{l(P) | P \in \mathcal{P}\}$$

Poiché i vertici u e v sono congiungibili per passeggiata, $\mathcal{P} \neq \emptyset$ e quindi anche $A \neq \emptyset$. Ma allora, per il Teorema di buon ordinamento, A possiede un minimo, ovvero esiste una passeggiata P_0 da u a v che ha lunghezza minima, nel senso che:

$$l(P_0) \leq l(P) \; \forall P \in \mathcal{P}$$

Dimostro che P_0 è un cammino. Sia $P_0 = \{v_0, \ldots, v_n\}$. Se per assurdo P_0 non fosse un cammino, esisterebbero $i, j \in \{0, \ldots, n\}$ con $i < j$ tali che $v_i = v_j$. Si consideri quindi, $P_1 = \{v_0, \ldots, v_i, v_{j+1}, \ldots, v_n\}$. P_1 è una passeggiata dato che lo è anche P_0, cioè vale:

$$\{v_h, v_{h+1}\} \in E(G) \; \forall 0 \leq h < n$$

e poiché $v_i = v_j$, $\{v_i, v_{i+1}\} = \{v_j, v_{j+1}\} \in E(G)$. Dato che, $v_0 = u$ e $v_n = v$, P_1 congiunge u a v, ovvero $P_1 \in \mathcal{P}$, ma siccome $l(P_1) = l(P_0) - (j - i) < l(P_0)$, ciò contraddice la minimalità di P_0. È stato quindi assurdo supporre che P_0 non fosse un cammino. ■

Proposizione 15.9. La relazione di congiungibilità è una relazione di equivalenza.

Dim. Sia G un grafo. Indico con $\sim$ la relazione di congiungibilità, ovvero se $u, v \in V(G)$, $u \sim v$ se e solo se u è congiungibile a v. Devo dimostrare che per $\sim$ valgono le proprietà riflessiva, simmetrica e transitiva.

(i) *Riflessività*: se $v \in V(G)$, $\{v\}$ è un cammino che congiunge v a v e dunque $v \sim v$

(ii) *Simmetria*: se $v, w \in V(G)$ con $v \sim w$, esiste un cammino $(v_0, \ldots, v_n)$ con $v_0 = v$ e $v_n = w$ che congiunge v a w. Allora, invertendo l'ordine dei vertici si ottiene $(v_n, \ldots, v_0)$ che è un cammino da w a v, ovvero $w \sim v$

(iii) *Transitività*: se $v, w, z \in V(G)$ con $v \sim w$ e $w \sim z$, esistono due passeggiate $P_1 = (v_0, \ldots, v_n)$ e $P_2 = (w_0, \ldots, w_m)$ con $v_0 = v$, $v_n = w_0 = w$ e $w_m = z$. Sia $Q = (v_0, \ldots, v_n, w_1, \ldots, w_m)$. Poiché $v_n = w_0$, $\{w_0, w_1\} = \{v_n, w_1\} \in E(G)$ e quindi Q è una passeggiata. Dato che $v_0 = v$ e $w_m = z$, Q è una passeggiata da v a z, ovvero $v \sim z$

■

9. Relazione fondamentale dei grafi finiti e Lemma delle strette di mano

Proposizione 17.2. Se $G = (V, E)$ è un grafo finito, allora:

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

Dim. Siano $V = \{v_1, \dots, v_n\}$ e $E = \{e_1, \dots, e_k\}$. Per ogni $i \in \{1, \dots, n\}$ e $j \in \{1, \dots, k\}$, definisco il numero $m_{i,j} = 0, 1$ come:

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

Vale:

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

Per ogni $i \in \{1, \dots, n\}$, vale:

$$\sum_{j=1}^{k} m_{i,j} = |\{j \in \{1, \dots, k\} | v_i \in e_j\}| = \deg_G(v) \Rightarrow \sum_{i=1}^{n} \left(\sum_{j=1}^{k} m_{i,j} \right) = \sum_{i=1}^{n} \deg_G(v) \qquad (1)$$

Per ogni $j \in \{1, \dots, k\}$, vale:

$$\sum_{i=1}^{n} m_{i,j} = |\{i \in \{1, \dots, n\} | v_i \in e_j\}| = 2 \Rightarrow \sum_{j=1}^{k} \left(\sum_{i=1}^{n} m_{i,j} \right) = \sum_{j=1}^{k} 2 = 2|E| \qquad (2)$$

Poiché (1)=(2), $\sum_{i=1}^{n} \deg_G(v) = 2|E|$. ■

Corollario 17.6 (Lemma delle strette di mano). In un grafo finito il numero di vertici di grado dispari è sempre pari.

Dim. Sia $G = (V, E)$ un grafo finito. Definisco P e D come segue:

$$P = \{v \in V | \deg_G(v) \text{ è pari}\}; \; D = \{v \in V | \deg_G(v) \text{ è dispari}\}$$

Vale:

$$\sum_{v \in P} \deg_G(v) + \sum_{v \in D} \deg_D(v) = \sum_{v \in V} \deg_G(v) \underset{\text{Relaz. fondamentale}}{=} 2|E|$$

$$\Rightarrow \sum_{v \in D} \deg_G(v) = 2|E| - \sum_{v \in P} \deg_G(v)$$

Poiché al termine destro ci sono solo quantità pari, anche il termine sinistro deve esserlo, ma $\sum_{v \in D} \deg_G(v)$ è pari se e soltanto se $|D|$ è pari. ■

10. Teorema di caratterizzazione degli alberi finiti mediante la formula di Eulero

Teorema 20.6. Sia $T = (V, E)$ un grafo finito. Sono fatti equivalenti:

(i) T è un albero

(ii) T è connesso e vale la seguente formula di Eulero:

$$|V| - 1 = |E|$$

Dim. $(i) \Rightarrow (ii)$. Procedo per induzione su $|V(T)|$. Se $|V(T)| = 1$ la tesi è vera. Suppongo $|V(T)| \geq 2$ e sia $v \in V(T)$ una foglia. Ora, $T - v$ è un albero e $|V(T - v)| = |V(T)| - 1$. Per ipotesi induttiva, vale:

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

Dato che $\deg_T(v) = 1$, $|E(T - v)| = |E(T)| - 1$ e quindi la tesi è verificata.

$(ii) \Rightarrow (i)$. Devo dimostrare che T non ha cicli. Procedo per induzione su $|V(T)|$. Se $|V(T)| = 1$ la tesi è vera. Suppongo $|V(T)| \geq 2$. Dimostro che T ha una foglia. Dalla Relazione fondamentale dei grafi finiti, ottengo:

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

Dato che T è connesso ed ha almeno due lati, non possono esistere vertici di grado 0, dunque, se non esistessero foglie, ogni $v \in V(T)$ dovrebbe avere $\deg_T(v) \geq 2$, ma questo genererebbe un assurdo perché varrebbe $2|V(T)| - 2 \geq 2|V(T)|$. Pertanto, almeno un vertice deve essere di grado 1. Sia quindi $v \in V(T)$ una foglia e si consideri il grafo $T - v$.

Dato che T è connesso e $\deg_T(v) = 1$, anche $T - v$ è connesso. Inoltre, poiché $|V(T - v)| = |V(T)| - 1$ e $|E(T - v)| = |E(T)| - 1$, si ha che $|V(T - v)| - 1 = |E(T - v)|$. Per ipotesi induttiva $T - v$ è un albero, ma allora T non ha cicli in quanto i vertici di un ciclo hanno tutti grado almeno 2 e quindi un ciclo in T non potrebbe passare per v, ossia sarebbe contenuto in $T - v$ contraddicendo il fatto che $T - v$ è un albero. ∎

11. Teorema di esistenza dell'albero di copertura per i grafi connessi finiti

Teorema 21.3. Si G un grafo connesso finito. Allora, G ha un albero di copertura.

Dim (Prima dimostrazione)**.** Si consideri l'insieme

$$\mathcal{T} = \{T | T \text{ è un sottografo di } G \text{ e } T \text{ è un albero}\}$$

$\mathcal{T} \neq \emptyset$, poiché se $v \in V(G)$, $\{\{v\}, \emptyset\} \in \mathcal{T}$. Dato che G è finito, esiste $\bar{T} \in \mathcal{T}$ con massimo numero di vertici, ossia tale che:

$$|V(T)| \leq |V(\bar{T})| \ \forall T \in \mathcal{T}$$

Devo dimostrare che $|V(\bar{T})| = |V(G)|$. Suppongo che esista $v \in V(G) \backslash V(\bar{T})$, allora, sfruttando la connessione di G, posso determinare due vertici $w \in V(G) \backslash V(\bar{T})$ e $u \in V(\bar{T})$ tali che $\{u, w\} \in E(G)$. Ma allora, $T' = (V(\bar{T}) \cup \{w\}, E(\bar{T}) \cup \{u, w\})$ è sia un sottografo di G che un albero. Quindi $T' \in \mathcal{T}$, ma poiché $|V(T')| = |V(\bar{T})| + 1$, viene contraddetta la massimalità di $\bar{T}$. ∎

Dim (Seconda dimostrazione)**.** Si consideri l'insieme

$$\mathcal{C} = \{C | C \text{ è un sottografo connesso di } G \text{ e } V(C) = V(G)\}$$

$\mathcal{C} \neq \emptyset$ dato che $G \in \mathcal{C}$. Poiché G è finito, esiste un grafo $\bar{C} \in \mathcal{C}$ con il minor numero di lati, ovvero:

$$|E(\bar{C})| \leq |E(C)| \ \forall C \in \mathbb{C}$$

Devo dimostrare che $\bar{C}$ è un albero. Se non lo fosse, per la proprietà (3) del Teorema di caratterizzazione degli alberi finiti, esisterebbe un lato $e \in E(\bar{C})$ tale che $\bar{C} - e$ è connesso. Ma, $V(\bar{C} - e) = V(C) = V(G)$, quindi $C \in \mathcal{C}$ e poiché, $|E(\bar{C} - e)| = |E(\bar{C}) - 1| = E(C)$, la minimalità di $\bar{C}$ viene contraddetta. ■