

Teoremi richiesti all'Esame di Fondamenti matematici per l'informatica

Matteo Franzil

3 giugno 2018

Indice

I	Buon ordinamento dei numeri naturali e seconda forma del principio di induzione	2
II	Esistenza e unicità della divisione euclidea	2
III	Unicità della rappresentazione di un numero in base arbitraria	4
IV	Esistenza e unicità del Massimo Comune Divisore e del minimo comune multiplo	5
V	Teorema fondamentale dell'aritmetica	7
VI	Teorema cinese del resto	8
VII	Teorema di Fermat-Eulero e crittografia RSA	10
VIII	Teoremi sulla congiungibilità nei grafi	11
IX	Relazione fondamentale nei grafi finiti e lemma delle strette di mano	12
X	Teorema di caratterizzazione degli alberi finiti	13
XI	Teorema di esistenza degli alberi di copertura	14

I Buon ordinamento dei numeri naturali e seconda forma del principio di induzione

Teorema 1 (Buon ordinamento dei numeri naturali). (\mathbb{N}, \leq) è ben ordinato.

Dimostrazione. Supponiamo esista $A \subset \mathbb{N}$ dove $\nexists \min A$. Sia $B := \mathbb{N} \setminus A$. Dimostriamo che $B = \mathbb{N}$ e $A = \emptyset$. Procediamo per induzione di prima forma. Sia $\{0, 1, \dots, n\} \subset B \ \forall n \in \mathbb{N}$, ovvero $P(n) = (\{0, 1, \dots, n\} \subset B)$ è vera $\forall n \in \mathbb{N}$.

$n = 0$

$\{0\} \subset B \Leftrightarrow 0 \in B \Leftrightarrow 0 \notin A$.

Se supponessimo per assurdo che $0 \in A$, allora avremmo che $0 = \min A$. Quindi $0 \notin A$.

$n \geq 1, n \implies n + 1$

Assumiamo che $\{0, 1, \dots, n\} \subset B$ per qualche n .

Proviamo che $\{0, 1, \dots, n, n + 1\} \subset B$.

$n + 1 \in A$? No, perché altrimenti avremmo che $n + 1 = \min A$.

Allora

$$n + 1 \in B \implies B = \mathbb{N}, A = \emptyset$$

■

Teorema 2 (Seconda forma del principio di induzione). Sia una famiglia di proposizioni $\{P(n)\}_{n \in \mathbb{N}}$ indicizzata su $n \in \mathbb{N}$. Supponiamo che

1. $P(0)$ è vera

2. $\forall n > 0, (P(k) \text{ è vera } \forall k < n) \implies P(n) \text{ è vera}$.

Allora $P(n)$ è vera $\forall n \in \mathbb{N}$.

Dimostrazione. Sia $A := \{n \in \mathbb{N} | P(n) \text{ è falsa}\}$, dimostriamo che $A = \emptyset$.

Supponiamo che:

$$A \neq \emptyset \implies \exists n \in \mathbb{N} : n = \min A. \text{ Per la (1), essendo } P(0) \text{ vera, } n \neq 0$$

Inoltre, se $k < n, k \notin A$ in quanto abbiamo che $n = \min A$, ma allora dalla (2) segue che $P(n)$ è vera e che quindi $n \notin A$, che è in contraddizione con quanto asserito all'inizio della dimostrazione. ■

II Esistenza e unicità della divisione euclidea

Teorema 3 (Esistenza e unicità della divisione euclidea). Siano $n, m \in \mathbb{Z}$ con $m \neq 0$.
 $\implies \exists! q, r \in \mathbb{Z} :$

- $n = qm + r$
- $0 \leq r < |m|$

Esistenza. Procediamo per induzione di seconda forma su n .

$n = 0$

Poniamo $q, r = 0$.

$n \geq 1, \forall k < n \implies n$

Supponiamo $n > 0$ e l'asserto vero $\forall k < n$. Dimostriamo che l'asserto vale $\forall n \in \mathbb{N}$.

- Consideriamo innanzitutto il caso $n \geq 0$. Se $n < m$, poniamo $q := 0$ e $r := n$.
- Altrimenti, avremo che $n \geq m$. Sia $k := n - m$.
Applicando la divisione euclidea, otteniamo che:

$$\begin{aligned} \exists q, r \in \mathbb{N} : k = mq + n, \quad 0 \leq k < n, \\ \Leftrightarrow n = k + m = (mq + r) + m = (q + 1)m + r. \end{aligned}$$

- Analizziamo ora il caso opposto, ovvero quando $n < 0$. Se $m > 0$, applicando la procedura di divisione euclidea a $-n > 0, m > 0$, vale:

$$\begin{aligned} \exists q, r \in \mathbb{N} : -n = qm + r, \quad 0 \leq r < |m| \\ \Leftrightarrow n = -qm - r. \end{aligned}$$

Se $r = 0$ abbiamo ~~vinto~~ finito, altrimenti continuiamo per ottenere un resto > 0 . Aggiungendo e togliendo m :

$$\begin{aligned} n &= (-q) - r - m + m \\ &= (-q - 1)m + (m - r) \end{aligned}$$

dove $m - r$ è strettamente positivo per definizione.

- Sia infine $m < 0$, ovvero $-m > 0$.

$$\begin{aligned} \implies \exists q, r \in \mathbb{Z} : n &= (-m)q + r, \quad 0 \leq r < |m| \\ \Leftrightarrow n &= (-q)m + r \end{aligned}$$

□

Unicità. Supponiamo $\exists n, m \in \mathbb{Z}, m \neq 0; q, q', r, r' \in \mathbb{N}$:

$$\begin{aligned} n &= qm + r, \quad 0 \leq r < |m| \\ n &= q'm + r', \quad 0 \leq r' < |m| \end{aligned}$$

Proviamo che $q = q', r = r'$. Possiamo supporre che $r' > r$. Allora vale:

$qm - q'm = r' - r \Leftrightarrow m(q - q') = r' - r$. Effettuando l'operazione di modulo otteniamo:

$$|m(q - q')| = |r' - r| = r' - r < |m|$$

Affinché la disuguaglianza sia rispettata deve essere $0 \leq |q - q'| < 1$.

Essendo $q, q' \in \mathbb{N}$, concludiamo che $q' - q = 0 \implies q' = q$.

Dall'equazione originale ricaviamo infine che: $mq + r = mq' + r' \implies r' = r$. ■

III Unicità della rappresentazione di un numero in base arbitraria

Teorema 4 (Unicità della rappresentazione di un numero in base $b \geq 2$ arbitraria). *Sia $b \in \mathbb{N}, b \geq 2 \implies \forall n \in \mathbb{N}, \exists!$ rappresentazione di n in base b , ovvero una successione $\{\varepsilon_i\}$ con le seguenti proprietà:*

1. $\{\varepsilon_i\}_{i \in \mathbb{N}}$ è definitivamente nulla dopo qualche $i_0 \in \mathbb{N}$, ovvero $\forall j \geq i_0, \varepsilon_j = 0$.
2. $\varepsilon_i \in I_b = \{0, 1, \dots, b-1\} \forall i \in \mathbb{N}$ (ovvero $0 \leq \varepsilon_i < b$)
3. $\sum_{i \in \mathbb{N}} \varepsilon_i b^i = n$

Inoltre, se esiste un'altra successione $\{\varepsilon'_i\}_{i \in \mathbb{N}}$ allora $\varepsilon_i = \varepsilon'_i \forall i \in \mathbb{N}$.

Esistenza. Procediamo per induzione di seconda forma su n .

$n = 0$

$$n = \sum_{i \in \mathbb{N}} \varepsilon_i b^i = \sum_{i \in \mathbb{N}} 0 b^i = 0_b \forall i \in \mathbb{N}$$

$n \geq 1, \forall k < n \implies n$

Supponiamo $n > 0$ e l'asserto vero $\forall k < n$.

Eseguiamo la divisione euclidea di n con b :

$$n = qb + r, \quad 0 \leq r < |b|$$

Per ipotesi sappiamo che $b \geq 2$, quindi vale $0 < q < qb \leq qb + r = n$.

Per ipotesi induttiva allora esiste una successione $\{\delta_i\}$ che possiede le proprietà (1), (2), (3); inoltre vale:

$$\begin{aligned} n &= \left(\sum \delta_i b^i \right) b + r \\ n &= \left(\sum \delta_i b^{i+1} \right) + r \end{aligned}$$

Sia ora $r = \varepsilon_0$; effettuando un cambio di indice, otteniamo:

$$n = \varepsilon_0 + \sum_{j \geq 1} \delta_{j-1} b^j = \varepsilon_0 + \delta_0 b^1 + \delta_1 b^2 + \dots = \sum_{i \in \mathbb{N}} \varepsilon_i b^i$$

□

Unicità. Procediamo per induzione di seconda forma.

$n = 0$

Se $n = 0$ allora tutti gli addendi della sommatoria saranno nulli $\implies \varepsilon_i = 0 \forall i \in \mathbb{N}$.

$n \geq 1, \forall k < n \implies n$

Sia $n > 0$. Assumiamo l'asserto sia vero $\forall k < n$ e dimostriamo che $P(n)$ è verificata $\forall n \in \mathbb{N}$.
Assumiamo esistano $\{\varepsilon_i\}_{i \in \mathbb{N}}, \{\varepsilon'_i\}_{i' \in \mathbb{N}}$ con le proprietà (1), (2), (3).

Proviamo che $\varepsilon_i = \varepsilon'_i \forall i \in \mathbb{N}$.

Osserviamo che:

$$n = \sum_{i \in \mathbb{N}} \varepsilon_i b^i = \varepsilon_0 + b \left(\sum_{i \geq 1} \varepsilon_i b^{i-1} \right)$$

$$n = \sum_{i \in \mathbb{N}} \varepsilon'_i b^i = \varepsilon'_0 + b \left(\sum_{i \geq 1} \varepsilon'_i b^{i-1} \right)$$

dove $\varepsilon'_0, \varepsilon_0$ sono i resti delle divisioni di n per b . Ma per l'unicità della divisione euclidea vale $\varepsilon'_0 = \varepsilon_0$. Stesso discorso per i quozienti, che inoltre risultano per definizione $\leq n$. Segue, cambiando gli indici della sommatoria:

$$q = \sum_{j \in \mathbb{N}} \varepsilon'_{j+1} b^j = \sum_{j \in \mathbb{N}} \varepsilon_{j+1} b^j < n$$

Come prima si ha $q < n$ e per ipotesi di induzione si ha che $\varepsilon_i = \varepsilon'_i \forall i \geq 1$ ■

IV Esistenza e unicità del Massimo Comune Divisore e del minimo comune multiplo

Teorema 5 (Esistenza e unicità del Massimo Comune Divisore). *Siano $n, m \in \mathbb{N}$ con n, m non entrambi nulli. Diremo che un $d \in \mathbb{N}, d \geq 1$ è Massimo Comune Divisore (M.C.D.) di n, m se:*

1. $d|m \wedge d|n$
2. $c|m \wedge c|n \implies c|d$ per qualche $c \in \mathbb{N}$.

Inoltre, $\exists x, y \in \mathbb{Z} : d = xn + ym$, ovvero d è esprimibile come combinazione lineare con x, y . Se \exists MCD tra n, m , è unico e lo indicheremo con (n, m) .

Unicità. Poniamo $\exists d_1, d_2$ entrambi MCD di n, m . Applicando la proprietà (1) di d_1 e la (2) di d_2 otteniamo:

- (1) $d_1|m \wedge d_1|n$
- (2) dato $c = d_1$, $d_1|m \wedge d_1|n \implies d_1|d_2$

Applicando l'inverso otteniamo che $d_2|d_1 \wedge d_1|d_2 \implies d_1 = \pm d_2$; essendo $d_1, d_2 \in \mathbb{N}$, otteniamo che $d_1 = d_2$. □

Esistenza. Sia $S := \{s \in \mathbb{Z} | s > 0, s = xn + ym \text{ per qualche } x, y \in \mathbb{Z}\}$.

Osserviamo che $S \neq \emptyset$, in quanto $nn + mm > 0, nn + mm \in S$.

Sia $d := \min S$. Vale:

$$d|m \wedge d|n, \quad \exists c \in \mathbb{Z} : (c|m \wedge c|n \implies c|d)$$

Essendo $d \in S, d = xn + ym$ per qualche $x, y \in Z$.

Dalla proprietà 2 si ha che $c|xn + ym$. Dimostriamo che $d|n$. Eseguendo la divisione euclidea tra n, d otteniamo:

$$n = dq + r, \quad 0 \leq r < |d|$$

Proviamo per assurdo che $r = 0$. Se fosse $r > 0$, avremmo che $r \in S$ (quindi risulterebbe che $d \neq \min S$, in quanto $d > r$). Vale:

$$\begin{aligned} r &= n - qd = n - q(xn + ym) \\ &= n - qnx + qmy \\ &= n \underbrace{(1 - qx)}_{x'} + m \underbrace{(qy)}_{y'} \end{aligned}$$

Allora $r \in S$, ma ciò è assurdo. Quindi $r = 0$. ■

Teorema 6 (Esistenza e unicità del minimo comune multiplo). *Siano $n, m \in \mathbb{N}$. Diremo che un $M \in \mathbb{N}$ è minimo comune multiplo di n, m se:*

1. $n|M \wedge m|M$
2. $n|c \wedge m|c \implies M|c$ per qualche $c \in \mathbb{N}$

Se esiste, è unico lo indicheremo come $[n, m]$. Inoltre, se n, m non sono entrambi nulli, vale:

$$[n, m] = \frac{nm}{(n, m)}$$

Se $n, m = 0$, allora $[n, m] = 0$.

Unicità. Supponiamo esistano $M_1, M_2 \in \mathbb{N}$: M_1, M_2 sono entrambi mcm di n, m . Applicando la proprietà (1) di M_1 e la (2) di M_2 otteniamo:

- (1) $n|M_1 \wedge m|M_1$
- (2) con $c = M_1$, $n|M_1 \wedge m|M_1 \implies M_2|M_1$

Invertendo le proprietà si ha che $M_1|M_2 \wedge M_2|M_1 \implies M_2 = \pm M_1$.

Essendo $M_1, M_2 \in \mathbb{N}$, $M_2 = M_1$. □

Esistenza. Supponiamo n, m non entrambi nulli. Osservo che

$$\begin{aligned} (n, m)|n &\Leftrightarrow n = n'(n, m) \text{ per qualche } n' \in \mathbb{Z} \\ (n, m)|m &\Leftrightarrow m = m'(n, m) \text{ per qualche } m' \in \mathbb{Z} \end{aligned}$$

Definisco $M := \frac{nm}{(n, m)}$. Sostituendo si ha che

$$\begin{aligned} \frac{nm}{(n, m)} &= \frac{n'm'(n, m)(n, m)}{(n, m)} = n'm'(n, m) \\ &= (n'(n, m))m' = nm' \\ &= (m'(n, m))n' = mn' \end{aligned}$$

Allora $n|M, m|M$. Sia ora $c \in \mathbb{Z}$. Verifichiamo la (2), ovvero che $n|c \wedge m|c \stackrel{?}{\implies} M|c$.
Vale:

$$\begin{aligned}(n, m)|n, n|c &\implies (n, m)|c \\ (n, m)|m, m|c &\implies (n, m)|c\end{aligned}$$

Allora $c = c'(n, m)$ per qualche $c' \in \mathbb{Z}$.

Sappiamo infine che $(n', m') = 1$; per definizione abbiamo che $n'|c' \wedge m'|c' \implies n'm'|c'$.
Moltiplicando a sinistra a destra si ottiene

$$\underbrace{n'm'(n, m)}_M | \underbrace{c'(n, m)}_c$$

■

V Teorema fondamentale dell'aritmetica

Teorema 7 (Teorema fondamentale dell'aritmetica). *Ogni $n \in \mathbb{N}, n \geq 2$ si può scrivere come prodotto finito di numeri primi:*

$$n = p_1 p_2 p_3 \cdots p_k \quad p_1, p_2, \dots, p_k \in \mathbb{N} \text{ primi eventualmente ripetuti}$$

Tale scrittura è unica a meno di permutazioni. Se

$$n = q_1 q_2 q_3 \cdots q_h \quad q_1, q_2, \dots, q_h \in \mathbb{N} \text{ primi eventualmente ripetuti}$$

Allora $k = h$ ed $\exists \varphi : \{1, 2, \dots, k\} \mapsto \{1, 2, \dots, h\}$, una bigezione (ovvero una permutazione su $\{1, 2, \dots, k\}$) tale che:

$$p_i = q_{\varphi(i)} \quad \forall i \in \{1, 2, \dots, k\}$$

Esistenza. Procediamo per induzione di seconda forma.

$n = 2$

Abbiamo che $2 = 2$.

$n \geq 2, \forall k < n \implies n$

Se n è primo si va al mare abbiamo finito.

Altrimenti possiamo ipotizzare $n = d_1 d_2 : 1 < d_1 < n, 1 < d_2 < n$, dove

$$\begin{aligned}d_1 &= p_1 p_2 p_3 \cdots p_k \\ d_2 &= p'_1 p'_2 p'_3 \cdots p'_k\end{aligned}$$

per ipotesi di induzione. Allora n è fattorizzabile perché prodotto di numeri primi positivi. □

Unicità. Supponiamo che esistano due distinte fattorizzazioni:

$$\begin{aligned} n &= p_1 p_2 p_3 \cdots p_k \\ n &= q_1 q_2 q_3 \cdots q_h \end{aligned}$$

con $h \geq k$. Procediamo per induzione di prima forma.

$k = 1$

Vale $p_1 = n = q_1 q_2 \cdots q_h$ con $h \geq 1$. Dimostriamo che $h = 1$. Ipotizziamo per assurdo che $h \geq 2$; avremmo che $n = q_1 q_2 \cdots q_h$. Sappiamo che essendo p_1 primo, deve necessariamente essere $q_j = 1 \vee q_j = p_1$; tuttavia per ipotesi abbiamo che $q_j > 1 \implies q_j = p_1$. Allora si ha che

$$p_1 = n = q_1 q_2 \cdots q_h \geq q_1 q_2 = p_1^2 > p_1 = n$$

che è un assurdo ($n \not\geq n$). Allora $h = 1$.

$k \geq 2, k \implies k + 1$

Con $k > 1$, assumiamo l'asserto vero per k ($n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_h$ con $h = k$, $p_i = q_i \quad \forall i \in \mathbb{N}$ a meno di permutazioni) e dimostriamolo per $k + 1 = h$. Supponiamo quindi che $p_1 p_2 \cdots p_k p_{k+1} = q_1 q_2 \cdots q_h$ con $h > k + 1$. Abbiamo che $p_{k+1} | n \implies p_{k+1} | q_1 q_2 \cdots q_h$, allora $p_{k+1} | q_h$ per ipotesi; essendo p_{k+1}, q_h primi positivi, vale $p_{k+1} = q_h$. Ma allora

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_{h-1}$$

dove entrambi i membri sono stati divisi per p_{k+1} . Ma allora per ipotesi d'induzione le due fattorizzazioni hanno lo stesso numero d'elementi, ovvero

$$k = h - 1, p_1 = q_1, p_2 = q_2, \cdots p_{k+1} = q_h$$

■

VI Teorema cinese del resto

Teorema 8 (Teorema cinese del resto). *Siano $n, m \in \mathbb{N}; a, b \in \mathbb{Z}$. Consideriamo il seguente sistema di congruenze:*

$$S = \begin{cases} x \in \mathbb{Z} \\ x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{cases} \quad \begin{matrix} (1) \\ (2) \end{matrix}$$

Definiamo $Sol(S) := \{x \in \mathbb{Z} \mid (1), (2) \text{ sono verificate}\}$.

$Sol(S) \neq \emptyset \iff S \text{ è compatibile} \iff (n, m) \mid (a - b)$.

Se S è compatibile, data $c \in \mathbb{Z}$ soluzione particolare di S , vale:

$$Sol(S) = [c]_{[n, m]} = \{c + k[n, m] \in \mathbb{Z} \mid k \in \mathbb{Z}\}$$

Dimostrazione (compatibilità).

(\implies). Supponiamo $Sol(S) \neq \emptyset$. Sia $c \in Sol(S)$. Dimostriamo che valgono (1), (2), ovvero $c \equiv a \pmod{n} \wedge c \equiv b \pmod{m}$. Riscriviamo il sistema di congruenze come:

$$\begin{aligned} c &= a + kn \text{ per qualche } k \in \mathbb{Z} \\ c &= b + hm \text{ per qualche } h \in \mathbb{Z} \end{aligned}$$

Sottraendo membro a membro otteniamo:

$$(a - b) + (kn - hm) = 0 \Leftrightarrow hm - kn = a - b$$

Sappiamo che $(n, m) | n \wedge (n, m) | m \implies (n, m) | (an + bm)$ dove $an + bm$ è una combinazione lineare di n, m con qualche $a, b \in \mathbb{Z}$. Allora $(n, m) | (hm - km) = (a - b)$. \square

(\impliedby). Ora supponiamo $(n, m) | (a - b)$ sia vera, ovvero $a - b = k(n, m)$ per qualche $k \in \mathbb{Z}$. Appliciamo l'Algoritmo di Euclide a ritroso, ottenendo $(n, m) = xn + ym$ per qualche $x, y \in \mathbb{Z}$. Segue che:

$$a - b = kxn + kym \quad \Leftrightarrow \quad \underbrace{a + (-kx)n}_c = \underbrace{b + (ky)m}_c$$

\square

Dimostrazione (insieme delle soluzioni).

Supponiamo infine $Sol(S) \neq \emptyset$, ovvero che il sistema di congruenze è verificato. Sia $c \in Sol(S)$. Dimostriamo che $Sol(S) = [c]_{[n, m]}$ verificando che uno contiene l'altro e viceversa.

(\subset). Sia $c' \in [c]_{[n, m]}$, allora $c' = c + k[n, m]$ per qualche $k \in \mathbb{Z}$. Riscrivo il sistema come

$$S = \begin{cases} [c]_n = [a]_n \\ [c]_m = [b]_m \end{cases}$$

Vale:

$$\begin{aligned} [c']_n &= [c + [n, m]_k]_n \\ &= [c]_n + [k]_n [[n, m]]_n \\ &= [a]_n + [k]_n [0]_n \leftarrow [n, m] \text{ multiplo di } n \end{aligned}$$

Con un procedimento analogo si ottiene $[c']_m = [b]_m$. \square

(\supset). Sia $c \in Sol(S)$. Vale:

$$\begin{aligned} c &= a + hn = b + km \\ c' &= a + h'n = b + k'm \end{aligned}$$

per qualche $h, h', k, k' \in \mathbb{Z}$. Sottraiamo membro a membro:

$$\begin{aligned} c' - c &= (h' - h)n = (k' - k)m \\ \implies n | (c' - c), \quad m | (c' - c) &\implies [n, m] | (c' - c) \\ &\Leftrightarrow c' \equiv c \pmod{[n, m]} \\ &\Leftrightarrow c' \in [c]_{[n, m]} \end{aligned}$$

\blacksquare

VII Teorema di Fermat-Eulero e crittografia RSA

Definizione (Formula di Eulero). Sia $n \in \mathbb{N}, n \geq 2 : n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ con $p_1 \cdots p_k$ primi a due a due distinti. Vale:

$$\begin{aligned}\phi(n) &= \phi(p_1^{m_1}) \phi(p_2^{m_2}) \cdots \phi(p_k^{m_k}) \\ &= (p_1^{m_1} - p_1^{m_1-1})(p_2^{m_2} - p_2^{m_2-1}) \cdots (p_k^{m_k} - p_k^{m_k-1})\end{aligned}$$

Lemma. Siano $\alpha, \beta \in (\mathbb{Z}/n\mathbb{Z})^*$. Allora:

1. $\alpha, \beta \in (\mathbb{Z}/n\mathbb{Z})^*, \quad (\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}$
2. $\alpha^{-1} \in (\mathbb{Z}/n\mathbb{Z})^*, \quad (\alpha^{-1})^{-1} = \alpha$

Dimostrazione. Vale:

1. $(\alpha\beta)(\beta^{-1}\alpha^{-1}) = \alpha(\beta\beta^{-1})\alpha^{-1} = \alpha[1]_n\alpha^{-1} = \alpha\alpha^{-1} = [1]_n$
2. $(\alpha)(\alpha^{-1}) = [1]_n$

□

Teorema 9 (Teorema di Fermat-Eulero). Sia $n > 0$. $\forall [a]_n \in (\mathbb{Z}/n\mathbb{Z})^*$, vale:

$$[a]_n^{\phi(n)} = [1]_n$$

Equivalentemente:

$$a^{\phi(n)} \equiv 1 \pmod{n}, \quad \forall a \in \mathbb{Z}, \text{ con } (a, n) = 1$$

Dimostrazione. Definiamo:

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

L_α è ben definita per il lemma precedente. Proviamo che L_α è una bigezione. Mostriamo che è iniettiva (la surgettività è dimostrata perché gli insiemi di partenza e arrivo coincidono, conseguenza del Lemma dei Cassetti). Supponiamo $\exists \beta_1, \beta_2 \in (\mathbb{Z}/n\mathbb{Z})^*$:

$$\begin{aligned}\alpha\beta_1 &= L_\alpha(\beta_1) = L_\alpha(\beta_2) = \alpha\beta_2 \\ \implies \beta_1 &= (\alpha^{-1}\alpha)\beta_1 = (\alpha^{-1})(\alpha\beta_1) = (\alpha^{-1})(\alpha\beta_2) = \beta_2\end{aligned}$$

Sia ora $\{\beta_1, \beta_2, \dots, \beta_k\} \in (\mathbb{Z}/n\mathbb{Z})^*$ con $k = \phi(n)$. Applicando L_α si ottiene

$$\{\alpha\beta_1, \alpha\beta_2, \dots, \alpha\beta_k\} = \alpha^k(\beta_1, \beta_2, \dots, \beta_k)$$

Allora L_α non è altro che una permutazione, per cui possiamo scrivere:

$$(\beta_1, \beta_2, \dots, \beta_k) = \alpha^k(\beta_1, \beta_2, \dots, \beta_k)$$

Moltiplicando a destra e a sinistra per $\{\beta_k^{-1}, \beta_{k-1}^{-1}, \dots, \beta_1^{-1}\}$ si ottiene:

$$\alpha^k = 1$$

■

Definizione. Siano $n > 0, m > 0$. Definiamo:

$$\begin{aligned} P_m : (\mathbb{Z}/n\mathbb{Z})^* &\longrightarrow (\mathbb{Z}/n\mathbb{Z})^* \\ \alpha &\longmapsto \alpha^m \end{aligned}$$

ovvero $P_m(\alpha) := \alpha^m \quad \forall \alpha \in (\mathbb{Z}/n\mathbb{Z})^*$. P_m è ben definita grazie al Lemma precedente.

Teorema 10 (Teorema fondamentale della crittografia RSA). Sia $c > 0 : (c, \phi(n)) \leq 1$ con n fissato; $d > 0 : d \in [c]_{\phi(n)}^{-1}$.

Allora la funzione P_c (analogo a P_m nella seguente definizione) è invertibile e la sua inversa è $P_c^{-1} = P_d$.

Dimostrazione. Sia $\alpha \in (\mathbb{Z}/n\mathbb{Z})^*$. Osserviamo che

$$\begin{aligned} [d]_{\phi(n)}[c]_{\phi(n)} &= [dc]_{\phi(n)} = [1]_{\phi(n)} \\ \Leftrightarrow dc &\equiv 1 \pmod{\phi(n)} \\ \Leftrightarrow dc &= 1 + k\phi(n) \quad \text{per qualche } k \in \mathbb{Z} \end{aligned}$$

Applicando contemporaneamente P_c e P_d otteniamo che

$$P_d(P_c(\alpha)) = (\alpha^c)^d = \alpha^{cd} = \alpha^{1+k\phi(n)} = \alpha(\alpha^{\phi(n)})^k$$

Per il Teorema di Fermat-Eulero ciò è equivalente a $\alpha \cdot 1^k = \alpha$. Allo stesso modo dimostro che $P_c(P_d(\beta)) = \beta$. ■

VIII Teoremi sulla congiungibilità nei grafi

Teorema 11 (Teorema di equivalenza tra la congiungibilità con cammini e congiungibilità con passeggiate). Siano $G = (V, E)$; $v, w \in V(G)$. Allora v, w sono congiungibili tramite cammini se e solo se sono congiungibili tramite passeggiate.

Dimostrazione.

(\Rightarrow). Banale. Il cammino è una passeggiata per definizione.

(\Leftarrow). Supponiamo esista una passeggiata P che congiunge v, w . Sia \mathcal{P} l'insieme di tutte le passeggiate che congiungono v, w . Osserviamo che $\mathcal{P} \neq \emptyset$ ($P \in \mathcal{P}$).

Sia $A := \underbrace{\{\mathcal{L}(\bar{P}) \in \mathbb{N} \mid \bar{P} \in \mathcal{P}\}}_{\text{lati di } \bar{P}}$. Abbiamo che $A \neq \emptyset$, infatti $\mathcal{L}(P) \in A$.

Grazie al teorema del buon ordinamento (\mathbb{N}, \leq) , vale:

$$\exists \min A = m \implies \exists P_0 \in \mathcal{P} : \mathcal{L}(P_0) = m \leq \mathcal{L}(\bar{P}), \quad \forall \bar{P} \in \mathcal{P}$$

ovvero esiste $\min A$, quindi esiste una passeggiata \mathcal{P} con il minimo numero di lati.

Proviamo ora che P_0 è un cammino in G . Vale:

$$P_0 = (v_0, v_1, \dots, v_n) \quad v = v_0, \quad w = v_n$$

Poniamo per assurdo che P_0 non sia un cammino, ovvero $\exists i, j \in \{0, 1, \dots, n\} : i < j, v_i = v_j$. Definiamo $P_1 := (v_0, v_1, \dots, v_{i-1}, v_i, v_j, v_{j+1}, \dots, v_n) \in \mathcal{P}$ (ovvero P_0 alla quale sono stati tolti tutti i vertici tra i e j). Vale:

$$\mathcal{L}(P_1) = \mathcal{L}(P_0) - (j - i) = m - (j - i) < m$$

Ma ciò è assurdo in quanto P_0 è già per definizione un cammino con il minimo numero di lati. ■

Teorema 12 (La relazione di congiungibilità è una relazione di equivalenza). *Dato $G = (V, \epsilon)$ la relazione di congiungibilità in G su V è una relazione di equivalenza su V :*

1. (riflessività) $u \sim u$ $\forall u \in V$
2. (simmetria) $(u \sim v) \implies (v \sim u)$ $\forall v, u \in V$
3. (transitività) $(u \sim v) \wedge (v \sim w) \implies (u \sim w)$ $\forall v, u, w \in V$

Indicheremo la relazione d'equivalenza con \sim .

Dimostrazione. Siano $u, v, w \in V$, \sim la relazione d'equivalenza. Vale:

1. è vera in quanto (u) è un cammino che congiunge u a u .
2. è vera in quanto se $u \sim v$ esiste una passeggiata $P = (v_0, \dots, v_n)$ tale che $u = v_0$ e $v = v_n$. Ma allora $P' = (v_n, v_{n-1}, \dots, v_0)$ è una passeggiata, dove vertici consecutivi in P lo sono anche in P' (anche se in ordine inverso).
3. è vera in quanto se $u \sim v$ e $v \sim w$ allora esistono due passeggiate $P_1 = (v_0, \dots, v_n), P_2 = (u_0, \dots, u_m)$ dove $u = v_0, v = v_n = u_0, w = u_m$. Possiamo definire una terza passeggiata $P_3 = (v_0, \dots, v_n, u_1, \dots, u_m)$ costruita come unione delle precedenti; P_3 è una passeggiata in quanto vertici consecutivi in P_3 lo sono o in P_1 o in P_2 , e i primi e ultimi vertici della passeggiata sono rispettivamente u e w . ■

IX Relazione fondamentale nei grafi finiti e lemma delle strette di mano

Teorema 13 (Relazione fondamentale tra $|\epsilon(G)|$ e $\deg(G_i)$ in un grafo finito). *Sia $G = (V, \epsilon)$ un grafo finito. Vale:*

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

Dimostrazione. Siano v_1, v_2, \dots, v_n i vertici di G , e_1, e_2, \dots, e_k i lati di G (dove $k := |\epsilon|$). Sia

$$M_{ij} := \begin{cases} 0 & v_i \notin \epsilon_j \\ 1 & v_i \in \epsilon_j \end{cases} \quad \begin{matrix} \forall i \in \{1, 2, \dots, n\} \\ \forall j \in \{1, 2, \dots, k\} \end{matrix}$$

dove i rappresenta l'indice sul numero dei vertici e j l'indice sul numero dei lati. Vale, grazie alla proprietà commutativa delle somme:

$$(1) \sum_{i=1}^n \sum_{j=1}^k m_{ij} = \sum_{j=1}^k \sum_{i=1}^n m_{ij} \quad (2)$$

dove (1) rappresenta una somma di sommatorie con un vertice i fissato; in ciascuna somma, si somma 1 se un lato contiene il vertice fissato, 0 se ciò non accade. Ma ciò non è altro che il grado del dato vertice; (2) invece somma k volte una sommatoria con un lato j fissato, dove viene sommato 1 tante volte quante un vertice appartiene a un dato lato, ovvero 2. Infine vale:

$$\sum_{v \in V} \deg(v) = 2k$$

■

Teorema 14 (Lemma delle strette di mano). *In un grafo $G = (V, \epsilon)$ finito il numero di vertici di grado dispari è pari.*

Dimostrazione. Sia $G = (V, \epsilon)$. Vale, grazie alla relazione fondamentale tra lati e gradi di un grafo:

$$\begin{aligned} 2|\epsilon| &= \sum_{v \in V} \deg(v) \\ 2|\epsilon| &= \underbrace{\sum_{v \in V} \deg(v)}_{\deg(v) \text{ pari}} + \underbrace{\sum_{v \in V} \deg(v)}_{\deg(v) \text{ dispari}} \\ 2|\epsilon| - \underbrace{\sum_{v \in V} \deg(v)}_{\deg(v) \text{ pari}} &= \underbrace{\sum_{v \in V} \deg(v)}_{\deg(v) \text{ dispari}} \end{aligned}$$

Allora la somma dei vertici con grado dispari deve essere pari perché differenza di un numero pari e una somma di numeri pari. ■

X Teorema di caratterizzazione degli alberi finiti

Teorema 15 (Teorema di caratterizzazione degli alberi finiti mediante la formula di Eulero). *Sia $T = (V, \epsilon)$ un grafo finito. Le seguenti affermazioni sono equivalenti:*

1. T è un albero
2. $\forall v, v' \in V, \exists!$ cammino da v in v'
3. T è connesso e $\forall e \in \epsilon, T - e := (V, \epsilon \setminus \{e\})$ è sconnesso
4. T non ha cicli e $\forall e \in \binom{V}{2} \setminus \epsilon, T + e := (V, \epsilon \cup \{e\})$ ha almeno un ciclo

5. T è connesso e $|V| - 1 = |\epsilon|$.

Dimostrazione.

$(1 \implies 5)$. Procediamo per induzione su $|V(T)|$.

$$|V(T)| = 1$$

Vale $|\epsilon(T)| = 0 = |V(T)| - 1$.

$$|V(T)| \geq 2, |V(T)| - 1 \implies |V(T)|$$

Sia T un qualsiasi albero con $|V(T)| \geq 2$. Dimostriamo che vale la proprietà (5). Essendo T un albero, \exists almeno una foglia $v \in T$. Consideriamo ora $T - v$: è ancora un albero, dove

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

$$|\epsilon(T - v)| = |\epsilon(T)| - 1$$

Vale, per ipotesi induttiva:

$$|V(T - v)| - 1 = |\epsilon(T - v)|,$$

$$|V(T)| - 1 - 1 = |\epsilon(T)| - 1$$

□

$(1 \Leftarrow 5)$. Procediamo per induzione su $|V(T)|$.

$$|V(T)| = 1$$

Un grafo con 1 vertice e 0 lati è un albero per definizione.

$$|V(T)| \geq 2, |V(T)| - 1 \implies |V(T)|$$

Sia T un grafo connesso che soddisfa la formula di Eulero. Supponiamo per assurdo che T non abbia foglie, ovvero che $\deg(v) \geq 2 \forall v \in V(T)$. Allora

$$\begin{aligned} |V(T)| - 1 &= \frac{1}{2} \sum_{v \in V} \deg(v) \\ 2 |V(T)| - 2 &= \sum_{v \in V} \deg(v) \geq 2 |V(T)| \end{aligned}$$

che è un assurdo. Allora T ha almeno una foglia. Se consideriamo $v \in V(T)$ foglia, $T - v$ è ancora connesso e vale Eulero. Allora per ipotesi induttiva $T - v$ è un albero $\implies T$ è un albero. ■

XI Teorema di esistenza degli alberi di copertura

Teorema 16 (Teorema di esistenza degli alberi di copertura per un grafo finito). *Ogni grafo connesso ammette almeno un albero di copertura.*

Dimostrazione. Determiniamo

$$\mathcal{T} := \{T \mid T \text{ è un sottografo di } G, T \text{ è un albero}\}$$

Sia $\bar{T} \in \mathcal{T} : |V(\bar{T})| \geq |V(T)| \quad \forall T \in \bar{\mathcal{T}}$.

Osservo che $\bar{T} \neq \emptyset$ in quanto se $v \in V(G)$ allora $(v, \emptyset) \in \mathcal{T}$. Proviamo che $V(\bar{T}) = V(G)$ ovvero che \bar{T} è un albero di copertura.

Usando la connessione di G , è possibile determinare un vertice $w \in V(G) \setminus V(\bar{T})$ e un vertice $u \in V(\bar{T})$ tali che $\{u, w\} \in E(G)$. Ma allora possiamo definire

$$\bar{\bar{T}} \in \mathcal{T}, \quad \bar{\bar{T}} := (V(\bar{T}) \cup \{w\}, E(\bar{T}) \cup \{u, w\})$$

che è chiaramente un albero, ma che va in contraddizione con la massimalità dei vertici di \bar{T} . ■