

Definizioni ed dimostrazioni di teoremi per il corso di Fondamenti Matematici per l'Informatica

Facchini Luca

A.A. 2023/24

Sommario

In questo documento sono presenti le definizioni e le dimostrazioni dei teoremi richiesti dal Prof. Ghiloni R. per l'esame del corso di Fondamenti Matematici per l'Informatica dell'anno accademico 2023/24.

Indice

I	Ordinamento numeri naturali e seconda forma induzione	3
1	Ordinamento dei numeri naturali	3
2	Seconda forma del principio di induzione	3
II	Teorema dell'esistenza e dell'unicità del quoziente e del resto della divisione euclidea	4
3	Unicità e esistenza del quoziente e del resto della divisione euclidea	4
III	Teorema di esistenza e unicità della rappresentazione in n base ≥ 2	4
4	Esistenza e unicità della rappresentazione in base $b \geq 2$	5
IV	Teorema di esistenza e unicità del massimo comune divisore e del minimo comune multiplo	6
5	Massimo comune divisore	6
6	Minimo comune multiplo	7
V	Teorema fondamentale dell'aritmetica	8
7	Teorema di esistenza e unicità della fattorizzazione in numeri primi	8
VI	Teorema cinese del resto	9
8	Teorema cinese del resto	9

VII	Teorema di Fermat-Eulero e Crittografia RSA	9
9	Teorema di Fermat-Eulero	9
10	Teorema fondamentale della crittografia RSA	10
VIII	Teorema di equivalenza tra la congiungibilità con cammini e la congiungibilità con passeggiate e Teorema la relazione di congiungibilità è una relazione di equivalenza	11
11	Teorema di equivalenza tra la congiungibilità con cammini e la congiungibilità con passeggiate	11
12	La relazione di congiungibilità è una relazione di equivalenza	11
IX	Teorema della relazione fondamentale tra il numero dei lati e i gradi dei vertici di un grafo finito e Lemma delle strette di mano	12
13	Teorema della relazione fondamentale tra il numero dei lati e i gradi dei vertici di un grafo finito	12
14	Lemma delle strette di mano	12
X	Teorema caratterizzante degli alberi finiti	13
15	Teorema caratterizzante degli alberi finiti	13
XI	Teorema di esistenza dell'albero di copertura per i grafi finiti	14
16	Teorema di esistenza dell'albero di copertura per i grafi finiti	15

Parte I

L'ordinamento dei numeri naturali è un buon ordinamento e seconda forma del principio di induzione

1 Ordinamento dei numeri naturali

Teorema I.1. *L'insieme dei numeri naturali \mathbb{N} è un insieme ordinato rispetto alla relazione d'ordine \leq .*

Ipotesi I.1.1. *Sia $A \subseteq \mathbb{N}$.*

Tesi I.1.2. *se $A \subseteq \mathbb{N}$ non ha un minimo allora $A = \emptyset$, dunque \mathbb{N} è un insieme ben ordinato.*

Dimostrazione. Definiamo con B il complementare di A , ($B := A^C = \mathbb{N} \setminus A$), verifichiamo l'ipotesi per induzione di prima forma su B , dunque che $\{0, 1, \dots, n\} \subseteq B \ \forall n \in \mathbb{N} \Rightarrow A = \emptyset$. Assumiamo che \mathbb{N} non sia ben ordinato e che dunque se $A \neq \emptyset$ allora A non ha un minimo.

Base Induttiva : Dunque $0 \notin A$ altrimenti questo ne sarebbe il minimo, dunque $\{0\} \subseteq B$ in quanto B è definito come il complementare di A . ✓

Passo Induttivo : Supponendo ora che $0, 1, \dots, n \in B$, allora $0, 1, \dots, n \notin A$, ciò implica che $n+1 \in A$ questo però lo renderebbe un minimo il che è inammissibile in quanto A non ha un minimo per ipotesi. Dunque $n+1 \in B$, e quindi $\{0, 1, \dots, n, n+1\} \subseteq B$. Il passo induttivo è verificato. ✓ Dunque per induzione di prima forma su B abbiamo che $A = \emptyset$, e quindi \mathbb{N} è un insieme ben ordinato. □

2 Seconda forma del principio di induzione

Teorema I.2. *Seconda forma del principio di induzione:*

Ipotesi I.2.1. *Sia $P(n)$ una serie di proposizioni indicizzata su \mathbb{N} , assumendo che:*

1. $P(0)$ sia vera.
2. $\forall n \in \mathbb{N}$ se $P(0), P(1), \dots, P(n)$ sono vere.

Tesi I.2.2. *Se le ipotesi sono verificate allora $P(n)$ è vera $\forall n \in \mathbb{N}$.*

Dimostrazione. Sia $A := \{n \in \mathbb{N} \mid P(n) \text{ è falsa}\}$, dimostriamo che $A = \emptyset$. Supponendo che $A \neq \emptyset \Rightarrow \exists n \in \mathbb{N} : n = \min(A)$.

Base Induttiva Quindi abbiamo che esiste un minimo su A , per la base induttiva (1) $0 \notin A$ dunque $0 \neq \min(A)$ in quanto $P(0)$ è vera.

Passo Induttivo Inoltre se $k < n$ $k \notin A$ in quanto $n = \min(A)$ e dunque $P(k)$ è vera, a questo punto per il passo induttivo (2) abbiamo che $\forall k < n$ $P(k)$ è vera e dunque $P(n)$ è vera, il che va in contraddizione con la definizione dell'esistenza di un minimo su A . Dunque $A = \emptyset$, e quindi $P(n)$ è vera $\forall n \in \mathbb{N}$. □

Parte II

Teorema dell'esistenza e dell'unicità del quoziente e del resto della divisione euclidea

3 Unicità e esistenza del quoziente e del resto della divisione euclidea

Teorema II.1. *Il quoziente ed il resto della divisione euclidea di un numero naturale n per un numero naturale $m \neq 0$ esistono ed sono unici.*

Ipotesi II.1.1. *Siano $n, m \in \mathbb{N}$ con $b \neq 0$.*

Tesi II.1.2. *Esistono ed sono unici due numeri naturali $q, r \in \mathbb{N}$ tali che $n = mq + r$ con $0 \leq r < b$.*

Dimostrazione.

Esistenza. *Si procede per induzione di seconda forma su n partendo da $n = 0$.*

Base Induttiva. *Per $n = 0$ si ha che $0 = 0 \cdot m + 0$, dunque $q = 0$ e $r = 0$ allora $\forall m \in \mathbb{Z}$ $P(0)$ è verificata.*

Passo Induttivo. *Per $n \geq 1$ si supponga che $\forall k < n$ $P(k)$ sia verificata, e dunque che esistano il quoziente ed il resto di k per m , suddividiamo la dimostrazione in diversi casi:*

- *Se $n < m$ allora $n = m \cdot 0 + n$, dunque $q = 0$ e $r = n$, e quindi $\forall n < m$ $P(n)$ è verificata.*
- *Se $n \geq m$ allora $n = m \cdot 1 + n$, dunque $q = 1$ e $r = 0$, e quindi $\forall n \geq m$ $P(n)$ è verificata.*
- *Se $n < 0$ e $m > 0$ allora applichiamo la divisione euclidea a $-n$ e m dunque $\exists q, r \in \mathbb{N}$ tali che $-n = mq + r$ con $0 \leq r < m$, dunque $n = -mq - r$, e quindi $q = -q$ e $r = -r$, e quindi $\forall n < 0$ $P(n)$ è verificata.*
- *Se $m < 0$ allora $-m > 0$ dunque $\exists q, r \in \mathbb{N}$ tali che $n = -m \cdot q + r$ con $0 \leq r < -m$, dunque $n = m \cdot q - r$, e quindi $q = -q$ e $r = -r$, e quindi $\forall m < 0$ $P(n)$ è verificata.*

Il passo induttivo è verificato, dunque per induzione di seconda forma su n abbiamo che esistono il quoziente ed il resto della divisione euclidea di n per m .

□

Unicità. *Proviamo che $q = q', r = r'$:*

- *Se $r' > r$ a meno di riordinamento, allora vale che: $qm - q'm = r' - r \Leftrightarrow m(q - q') = r' - r$.*
- *Effettuando l'operazione al modulo otteniamo: $|m(q - q')| = |r' - r|$, dunque $|r' - r| < m$, questo è vero se e solo se $0 \leq |q - q'| < 1$,*
- *Questo implica che $q = q'$ in quanto $q, q' \in \mathbb{N}$.*
- *Quindi $mqr = mq' + r' \Rightarrow q = q'$ e $r = r'$.*

■

Parte III

Teorema di esistenza e unicità della rappresentazione in n base ≥ 2

4 Esistenza e unicità della rappresentazione in base $b \geq 2$

Teorema III.1. *Un numero naturale n può essere rappresentato in base $b \geq 2$ in modo unico.*

Ipotesi III.1.1. *Siano $n, b \in \mathbb{N}$ con $b \geq 2$.*

Tesi III.1.2. *Esistono ed sono unici ($\exists!$) una rappresentazione di n in base b , ovvero una successione $\{\varepsilon_i\}$ con le seguenti proprietà:*

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

Inoltre se esiste $\{\varepsilon'_i\}_{i \in \mathbb{N}}$ rappresentazione di n in base b allora $\varepsilon_i = \varepsilon'_i \quad \forall i \in \mathbb{N}$.

Dimostrazione.

Esistenza. *Si procede per induzione di seconda forma su n partendo da $n = 0$.*

Base Induttiva. *Per $n = 0$ si ha che $0 = 0 \cdot b^0$, dunque $\varepsilon_0 = 0$ e quindi $\forall n \in \mathbb{N} P(n)$ è verificata.*

Passo Induttivo. *Per $n \geq 1$ si supponga che $\forall k < n P(k)$ sia verificata, e dunque che esista una rappresentazione di k in base b . Eseguiamo la divisione euclidea di n per b , dunque $\exists q, r \in \mathbb{N}$ tali che $n = b \cdot q + r$ con $0 \leq r < b$, per ipotesi $b \geq 2$ dunque $0 < q < qb \leq qb + r = n$, per ipotesi induttiva è vero che q è rappresentabile come una successione $\{\delta_i\}_{i \in \mathbb{N}}$ con le proprietà (1),(2),(3), inoltre vale che:*

$$n = \left(\sum_{i \in \mathbb{N}} \delta_i b^i \right) b + n \Rightarrow n = \sum_{i \in \mathbb{N}} \delta_i b^{i+1} + r$$

Definiamo: $\epsilon_0 = r$

$$n = \epsilon_0 + \sum_{j \geq 1} \delta_{j-1} b^j = \sum_{i \in \mathbb{N}} \epsilon_i b^i$$

□

Unicità. *Procediamo per induzione di seconda forma su n da $n = 0$*

Base Induttiva. *Per $n = 0$ $\epsilon_i = 0 \quad \forall i \in \mathbb{N}$, dunque questa è l'unica rappresentazione di 0 in base b .*

Passo Induttivo. *Assumendo che esistano $\{\epsilon_i\}_{i \in \mathbb{N}} \quad \{\epsilon'_i\}_{i \in \mathbb{N}}$ con le proprietà (1),(2),(3), proviamo che $\epsilon_i = \epsilon'_i \quad \forall i \in \mathbb{N}$. Dalla dimostrazione precedente osserviamo:*

$$\begin{aligned} n &= \sum_{i \in \mathbb{N}} \epsilon_i b^i = \sum_{i \in \mathbb{N}} \epsilon'_i b^i \\ \Rightarrow \epsilon_0 + b \left(\sum_{i \geq 1} \epsilon_i b^{i-1} \right) &= \epsilon'_0 + b \left(\sum_{i \geq 1} \epsilon'_i b^{i-1} \right) \end{aligned}$$

Dove ϵ_0 e ϵ'_0 sono i resti della divisione euclidea di n per b , e quindi in quanto questi uguali in entrambi i casi per il teorema dell'unicità del quoziente e del resto questi sono uguali. Inoltre dato che $\sum_{i \geq 1} \epsilon_i b^{i-1} = \sum_{i \geq 1} \epsilon'_i b^{i-1}$ per ipotesi, in quanto questi sono $< n$ allora la loro rappresentazione è unica dunque $\forall i > 1 \quad \epsilon_i = \epsilon'_i$, unendo i due risultati otteniamo che $\epsilon_i = \epsilon'_i \quad \forall i \in \mathbb{N}$. Il passo induttivo è stato fatto e l'unicità della rappresentazione è stata dimostrata.

■

Parte IV

Teorema di esistenza e unicità del massimo comune divisore e del minimo comune multiplo

5 Massimo comune divisore

Teorema IV.1.

Ipotesi IV.1.1. Siano $n, m \in \mathbb{Z}$ con n, m non entrambi nulli.

Tesi IV.1.2. Esiste $\exists d$ che è MCD di n, m se:

1. $d|n$ e $d|m$.
2. se $c|n$ e $c|m$ allora $\Rightarrow c|d$.

Inoltre: Se \exists M.C.D tra n, m allora questo è unico e lo indichiamo con (n, m) .

Lemma IV.1.3.

$$\exists x, y \in \mathbb{Z} : d = nx + my$$

Ovvero d è esprimibile come combinazione lineare di n e m .

Dimostrazione.

Unicità. Supponendo che $\exists d_1, d_2 \in \mathbb{N}$ che rispettino (1) e (2). Applichiamo allora queste ottenendo:

- (1) $d_1|n \wedge d_1|m$
- (2) $c = d_1 \mid d_1|n \wedge d_1|m \Rightarrow d_1|d_2$

applicando l'inverso si ottiene che $d_2|d_1$, dunque $d_1 = \pm d_2$, ma dato che $d_1, d_2 \in \mathbb{N}$ allora $d_1 = d_2$, e quindi il M.C.D è unico. □

Esistenza. Sia $S := \{nx + my \mid x, y \in \mathbb{Z}\}$, definito come l'insieme delle combinazioni lineari di n e m , questo insieme è non vuoto in quanto $nn + mm > 0 \in S$. Esiste dunque un minimo elemento in S , chiamiamolo $d = \min S$, vale che:

$$\begin{aligned} d|n \wedge d|m \\ \exists c \in \mathbb{Z} : c|n \wedge c|m \Rightarrow c|d \end{aligned}$$

in quanto $d \in S$. Dalla proprietà (2) si deduce

$$c|xm + ym$$

Si prova ora che $d|n$ tramite la divisione euclidea di n per d , ottenendo dunque $n = qd + r$, ponendo per assurdo che $r > 0$ allora $r \in S$ e quindi $d \neq \min S$ in quanto $r < d$, assumendo che sia vero:

$$\begin{aligned} r &= n - qd = n - q(xd + ym) = \\ &= n - qnx - qmy = \\ &= n(1 - qn) + m(-qy) \in S \end{aligned}$$

dunque è verificato che il resto della divisione euclidea è in S , e quindi che il $\min S \neq d$ ma per definizione $d := \min S$, il che è un assurdo e quindi $r = 0$ il che dimostra che $d|n$, analogamente si dimostra che $d|m$.

■

6 Minimo comune multiplo

Teorema IV.2.

Ipotesi IV.2.1. Siano $n, m \in \mathbb{Z}$

Tesi IV.2.2. $\exists! M \in \mathbb{N}$ che è m.c.m di n e m , se:

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

Inoltre: Se \exists m.c.m tra n e m allora questo è unico e lo indichiamo con $[n, m]$, e vale se n, m non sono entrambi nulli vale che: $[n, m] = \frac{n \cdot m}{(n, m)}$, altrimenti $[n, m] = 0$.

Dimostrazione.

Unicità. Supponiamo che esistano $M_1, M_2 \in \mathbb{N}$ che rispettino (1) e (2), applicando queste otteniamo:

- (1) $M_1|n \wedge M_1|m$
- (2) $c = M_1 \mid c|n \wedge c|m \Rightarrow M_1|c$

applicando l'inverso si ottiene che $M_2|c$, dunque $M_1 = \pm M_2$, ma dato che $M_1, M_2 \in \mathbb{N}$ allora $M_1 = M_2$, e quindi il m.c.m è unico. \square

Esistenza. Supponendo che n, m non sono entrambi nulli, altrimenti $[n, m] \exists := 0$ allora:

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

Definendo $M := \frac{n \cdot m}{(n, m)}$ e sostituendo n, m otteniamo che:

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

ma per la proprietà associativa della moltiplicazione, e per la definizione precedente di n', m' otteniamo che:

$$M = \begin{cases} (n'(n, m))m' &= nm' \\ (m'(n, m))n' &= n'm \end{cases} \Rightarrow n'm = nm'$$

quindi la proprietà (1) è verificata perchè $n|M$ e $m|M$. Per verificare la proprietà (2) controlliamo che per $c \in \mathbb{Z}$ vale che $n|c \wedge m|c \Rightarrow M|c$?

$$\begin{aligned} (n, m)|n, n|c &\Rightarrow (n, m)|c \\ (n, m)|m, m|c &\Rightarrow (n, m)|c \Rightarrow c = c'(n, m) \end{aligned}$$

Inoltre per definizione di $n', m' \Rightarrow (n', m') = 1$, dunque $n'|c' \wedge m'|c' \Rightarrow n'm'|c'$, moltiplicando l'equazione per (n, m) otteniamo: $n'm'(n, m)|c'(c, m) \Rightarrow M|c$, dunque la proprietà (2) è verificata e l'esistenza dimostrata. \blacksquare

Parte V

Teorema fondamentale dell'aritmetica

7 Teorema di esistenza e unicità della fattorizzazione in numeri primi

Teorema V.1.

Ipotesi V.1.1. Sia un numero $n \in \mathbb{Z}, n \geq 2$.

Tesi V.1.2. Esistono numeri primi $p_1, p_2, \dots, p_k > 0$ tali che $n = p_1 \cdot p_2 \cdot \dots \cdot p_k$. Se anche q_1, q_2, \dots, q_l sono numeri primi tali che $n = q_1 \cdot q_2 \cdot \dots \cdot q_l$ allora esiste una bigezione $\delta: \{1, 2, \dots, l\} \rightarrow \{1, 2, \dots, k\}$ tale che $q_i = p_{\delta(i)}$.

Dimostrazione.

Esistenza. Si procede per induzione di 2° forma shiftata su n , partendo da $n = 2$. Se $n = 2$ è scrivibile come prodotto di numeri primi e ogni numero $k < n$ è scrivibile come prodotto di numeri primi allora n è scrivibile come prodotto di numeri primi.

Base Induttiva. Per $n = 2$ si ha che $2 = 2$, dunque 2 è scrivibile come prodotto di numeri primi.

Passo Induttivo. Per $n > 2$ si supponga che $\forall k < n$ $P(k)$ sia verificata, e dunque che k sia scrivibile come prodotto di numeri primi, la dimostrazione si suddivide in due casi:

- Se n è primo allora n è scrivibile come prodotto di numeri primi.
- Se n non è primo allora esistono almeno due numeri d_1, d_2 tali che $1 < d_1, d_2 < n$ $n = d_1 \cdot d_2$. Per ipotesi induttiva in quanto $d_1, d_2 < n$ allora d_1, d_2 sono scrivibili come prodotto di numeri primi: $d_1 = p_1 \cdot p_2 \cdot \dots \cdot p_k$ e $d_2 = q_1 \cdot q_2 \cdot \dots \cdot q_l$, dunque $n = p_1 \cdot p_2 \cdot \dots \cdot p_k \cdot q_1 \cdot q_2 \cdot \dots \cdot q_l$, e quindi n è scrivibile come prodotto di numeri primi.

Il passo induttivo è verificato, dunque per induzione di 2° forma shiftata su n abbiamo che n è scrivibile come prodotto di numeri primi. \square

Unicità. Siano $n = p_1 \cdot p_2 \cdot \dots \cdot p_k = q_1 \cdot q_2 \cdot \dots \cdot q_h$ con p_i, q_j numeri primi, inoltre si supponga che per $k \leq h$. Si procede per induzione di seconda forma shiftata su k da $k = 1$.

Base Induttiva. Per $k = 1$ si ha che $n = p_1 = q_1 \cdot q_2 \cdot \dots \cdot q_h$ dunque $q_j | p_1 \forall i \in \{1, 2, \dots, h\}$, il che è possibile ma $\Leftrightarrow q_j = \pm 1 \vee q_j = \pm p_1$, in quanto però abbiamo definito per ipotesi che $q_j > 1$ allora l'unica possibilità è che $q_j = p_1$, ma se $h > 1$ allora $q_j = p_1 \quad \forall j \in \{1, 2, \dots, h\}$, che comporta che se $h > k \Rightarrow n = q_1 \cdot \dots \cdot q_h \geq q_1 q_2 \Rightarrow p_1^2 > p_1$ in quanto $p_1 > 1$, il che è un assurdo, dunque $h = k = 1$, e quindi $n = p_1 = q_1$.

Passo Induttivo. Sia ora $k > 1$ allora $p_k | n = q_1 \cdot \dots \cdot q_h$ dunque in quanto q_1, \dots, q_h sono primi \exists almeno un $p_k | q_j$ allora $p_k = q_j$ in quanto come detto precedentemente p_k, q_k primi > 1 . Seguendo la divisione euclidea $p_1 \cdot \dots \cdot p_{k-1} = q_1 \cdot \dots \cdot q_{j-1} \cdot q_{j+1} \cdot \dots \cdot q_h$, questi sono numeri $< n$ per ipotesi induttiva dunque hanno lo stesso numero di elementi: $k - 1 = h - 1$ e che esiste una bigezione $\delta: \{1, 2, \dots, h - 1\} \rightarrow \{1, 2, \dots, k - 1\}$, possiamo ora definire una bigezione $\sigma: \{1, 2, \dots, h\} \rightarrow \{1, 2, \dots, k\}$ tale che:

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

dunque è stata definita una bigezione tale che $q_i = p_{\sigma(i)} \quad \forall i \in \{1, 2, \dots, h\}$.

Il passo induttivo è verificato, dunque per induzione di seconda forma shiftata su k abbiamo che se n è scrivibile come prodotto di numeri primi allora questa è unica a meno di riordinamento in quanto esiste una bigezione tra gli indici delle sequenze di numeri primi.

■

Parte VI

Teorema cinese del resto

8 Teorema cinese del resto

Teorema VI.1.

Ipotesi VI.1.1. Siano $a, b, n, m \in \mathbb{Z}$ tali che $n, m > 0$ e sia il seguente sistema di congruenze:

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

Tesi VI.1.2. Il sistema ha soluzione se e solo se $(n, m) | b - a$, inoltre se c è una soluzione allora gli elementi di $[c]_{[n, m]}$ sono tutte e sole le soluzioni del sistema (le soluzioni in \mathbb{Z} sono: $c + k[n, m] \in \mathbb{Z} \quad k \in \mathbb{Z}$).

Dimostrazione. Sia c una soluzione allora esistono $h, k \in \mathbb{Z}$ tali che $c = a + hn = b + km$ in quanto $x \equiv a \pmod{n}$ e $x \equiv b \pmod{m} \Rightarrow [x]_n = [a]_n \Rightarrow x = a + kn$, e $x = b + km$, dunque $a + kn = b + km \Rightarrow a - b = kn - km \Rightarrow a - b = k(n - m) \Rightarrow (n, m) | a - b$. Da prima possiamo dire che $a - b = hn + km$ e che quindi $a - hm = b + kn = c$. Si noti come c risolvi entrambe le equazioni. Sia ora $S := \{x \in \mathbb{Z} \mid x \text{ risolve il sistema}\}$ "l'insieme di tutte le soluzioni", bisogna provare che se $c \in S$ allora $S = [c]_{[n, m]}$ e inoltre cse c' è una soluzione allora $c' \in [c]_{[n, m]}$. Quindi $c = a + hn = b + km \quad c' = a + h'n = b + k'm$, dunque $c - c' = h - h'n = k - k'm$, e quindi $c - c' = h - h'n = k - k'm$, dunque sottraendo c a c' si ottiene che: $c - c' = \cancel{a} + hn - \cancel{a} - h'n = (h - h')n$ e $c - c' = \cancel{b} + km - \cancel{b} - k'm = (k - k')m$, dunque $n | c - c'$ e $m | c - c'$. Allora $[n, m] | c - c'$, e $c' \equiv c \pmod{[n, m]}$, dunque $c' \in S$.

■

Parte VII

Teorema di Fermat-Eulero e Crittografia RSA

9 Teorema di Fermat-Eulero

Teorema VII.1. Sia $n \in \mathbb{N} \quad n \geq 2$. Allora $n = p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_k^{m_k}$ con p_i numeri primi a due a due distinti, allora vale che $\phi(n) = \phi(p_1^{m_1}) \cdot \phi(p_2^{m_2}) \cdot \dots \cdot \phi(p_k^{m_k})$, in quanto p_i è primo allora $\Rightarrow (p_1^m - p_1^{m-1}) \cdot (p_2^m - p_2^{m-1}) \cdot \dots \cdot (p_k^m - p_k^{m-1})$.

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

- $(\alpha\beta)^{-1} = \alpha^{-1}\beta^{-1}$
- $(\alpha^{-1})^{-1} = \alpha$

Dimostrazione. Verifichiamo che la moltiplicazione tra le classi α, β moltiplicata per le inverse esiste in quanto $\alpha, \beta \in (\mathbb{Z}/n\mathbb{Z})^*$, questa risulterà la classe di $[1]_n$ dunque che $(\alpha\beta)(\beta^{-1}\alpha^{-1}) = [1]_n$.

- $(\alpha\beta)(\alpha^{-1}\beta^{-1}) = \alpha(\beta\beta^{-1})\alpha^{-1}$ per la proprietà distributiva e associativa del prodotto in $(\mathbb{Z}/n\mathbb{Z})^*$, dunque $(\alpha(\beta\beta^{-1})\alpha^{-1} = \alpha[1]_n\alpha^{-1} = \alpha\alpha^{-1} = [1]_n$, dunque $(\alpha\beta)^{-1} = \alpha^{-1}\beta^{-1} \checkmark$.
- $(\alpha^{-1})^{-1}\alpha^{-1} = \alpha^{-1}(\alpha^{-1})^{-1} = [1]_n$, dunque $(\alpha^{-1})^{-1} = \alpha$.

□

Il teorema di Fermat-Eulero enuncia:

Ipotesi VII.1.1. Sia $n > 0$.

Tesi VII.1.2. allora $\forall [\alpha]_n \in (\mathbb{Z}/n\mathbb{Z})^* \Rightarrow [\alpha]^{\phi(n)} = [1]_n$. Notare come le classi prese in considerazione sono invertibili.

Dimostrazione. Definiamo la funzione $L_\alpha : (\mathbb{Z}/n\mathbb{Z})^* \rightarrow (\mathbb{Z}/n\mathbb{Z})^*$ definita come $\beta \rightarrow \alpha\beta$. La presente è ben definita per il lemma appena dimostrato, questa funzione è bigettiva, dimostriamo l'iniettività in quanto la surgettività ne sarà una conseguenza in quanto l'insieme di partenza e di arrivo sono uguali (vedi lemma casseti). Supponiamo dunque, per assurdo, $\exists \beta_1, \beta_2 \in (\mathbb{Z}/n\mathbb{Z})^*$ tali che $L_\alpha(\beta_1) = L_\alpha(\beta_2) \Rightarrow \alpha\beta_1 = \alpha\beta_2 \rightarrow \beta_1 = (\alpha\alpha^{-1})\beta_1 = (\alpha^{-1})(\alpha\beta_1) \Leftrightarrow (\alpha^{-1})(\alpha\beta_2) = (\alpha^{-1}\alpha)\beta_2 = \beta_2$, dunque $\beta_1 = \beta_2$, e quindi L_α è iniettiva. Avendo dimostrato la bigettività di L_α possiamo dire che $L_\alpha(\beta_1) \dots L_\alpha(\beta_k) = \alpha\beta_1 \dots \alpha\beta_k$ inoltre essendo il prodotto su $(\mathbb{Z}/n\mathbb{Z})^*$ associativo possiamo dire che il precedente è $= \alpha^k(\beta_1 \dots \beta_k)$, in quanto β_1, \dots, β_k sono tutti e i soli elementi in $(\mathbb{Z}/n\mathbb{Z})^*$ allora $\beta_1 \dots \beta_k = \alpha^k(\beta_1 \dots \beta_k)$ moltiplicando a sinistra e destra per $\beta_1^{-1} \dots \beta_k^{-1}$ otteniamo che $[1]_n = \alpha^k$, in quanto come dimostrato k è in numero di classi in $(\mathbb{Z}/n\mathbb{Z})^*$ e dunque $k = \phi(n) \Rightarrow [1]_n = \alpha^{\phi(n)} \quad \forall \alpha \in (\mathbb{Z}/n\mathbb{Z})^*$.

■

10 Teorema fondamentale della crittografia RSA

Teorema VII.2.

Ipotesi VII.2.1. Sia $c > 0$ tale che: $(c, \phi(n)) = 1$ con n fissato > 0 e $d > 0 : d \in [c]_{\phi(n)}^{-1}$.

Tesi VII.2.2. Allora P_c è invertibile, e la sua inversa è $P_c^{-1} = P_d$ dunque che $[d]_{\phi(n)}[c]_{\phi(n)} = [1]_{\phi(n)}$.

Dimostrazione. Questo è equivalente a dire che: $cd \equiv 1 \pmod{\phi(n)} \Rightarrow \exists k \in \mathbb{Z} : cd = 1 + k\phi(n)$, applicando ora P_c, P_d su una α classe otteniamo: $P_d(P_c(\alpha)) = (\alpha^c)^d = \alpha^{cd} = \alpha^{1+k\phi(n)} = \alpha\alpha^{k\phi(n)} = \alpha$, il che è verificato per le proprietà delle potenze e del prodotto in $(\mathbb{Z}/n\mathbb{Z})^*$ e in quanto $\alpha^{\phi(n)} = 1$ per il teorema di eulero. Quindi questo dimostra che $P_d(P_c(\alpha)) = \alpha$, equivalentemente $[c]_{\phi(n)}[d]_{\phi(n)} = [1]_{\phi(n)}$ il che significa che P_c è invertibile e che la sua inversa è P_d .

■

Parte VIII

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

11 Teorema di equivalenza tra la congiungibilità con cammini e la congiungibilità con passeggiate

Teorema VIII.1.

Ipotesi VIII.1.1. *Supponendo di avere $G = (V, E)$ un grafo e $u, v \in V$ due vertici di G .*

Tesi VIII.1.2. *Allora u è congiungibile con v in G per cammini se e solo \Leftrightarrow se u è congiungibile con v in G per passeggiate.*

Dimostrazione.

\Rightarrow Banale, in quanto un cammino è una particolare passeggiata per definizione.

\Leftarrow Supponiamo che u, v siano congiungibili in G per passeggiate, allora definitmo: $\mathcal{P} := \{P \mid P \text{ è una passeggiata da } u \text{ a } v\}$ L'insieme delle passeggiate da u a v in G . $\mathcal{A} := \{n \in \mathbb{N} \mid \exists P \in \mathcal{P} : L(P) = n\}$ L'insieme delle lunghezze delle passeggiate da u a v in G . In quanto $\mathcal{A} \subseteq \mathbb{N}$ allora grazie al teorema del buon ordinamento di \mathbb{N} allora:

$$\begin{aligned} \exists! \min(\mathcal{A}) &\Leftrightarrow \exists P_0 \in \mathcal{P} : L(P_0) = \min(\mathcal{A}) = m \\ &\Rightarrow L(P_0) \leq L(P) \quad \forall P \in \mathcal{P} \end{aligned}$$

Dunque esiste un minimo dell'insieme \mathcal{A} . Dimostriamo ora per assurdo che P_0 sia un cammino da u a v :
Assumendo che P_0 non sia un cammino da u a v : $P_0 = \{v_0, \dots, v_{i-1}, v_i, v_{i+1}, \dots, v_{j-1}, v_j, v_{j+1}, \dots, v_k\}$, dunque $\exists i, j \in \{0, 1, \dots, k\}$ tali che $v_i = v_j$, possiamo definire una passeggiata P_1 tale che $P_1 := \{u = v_0, \dots, v_{i-1}, v_i = v_j, v_{j+1}, \dots, v_k = v\}$, dunque $L(P_1) = L(P_0) - (j - i)$, in quanto $j - i \geq 1$ allora $L(P_1) < L(P_0)$, il che lo renderebbe un minimo, ma questo è un assurdo in quanto va contro la definizione di P_0 come minimo, dunque per assurdo P_0 è un cammino da u a v . ■

12 La relazione di congiungibilità è una relazione di equivalenza

Teorema VIII.2.

Ipotesi VIII.2.1. *Dato $G = (V, E)$ un grafo,*

Tesi VIII.2.2. *La relazione di congiungibilità in G su V è una relazione di equivalenza su V dunque:*

1. *Riflessiva:* $u \sim u \quad \forall u \in V$
2. *Simmetrica:* $u \sim v \Rightarrow v \sim u \quad \forall u, v \in V$
3. *Transitiva:* $u \sim v \wedge v \sim w \Rightarrow u \sim w \quad \forall u, v, w \in V$

Dimostrazione.

1. È verificabile in quanto la passeggiata $P = (u)$ è una passeggiata da u a u .
2. È verificabile in quanto se esiste una passeggiata $P = (u = v_0, v_1, \dots, v_k = v)$ possiamo definire un'altra passeggiata $P' = (v = v_k, v_{k-1}, \dots, v_0 = u)$ detta "inversa" che è una passeggiata da v a u .
3. Supponendo ora che esistano le passeggiate $P_0 = (u = u_0, u_1, \dots, u_k = v)$ e $P_1 = (v = v_0, v_1, \dots, v_h = w)$ allora possiamo definire una passeggiata $P_2 = (u = v_0, v_1, \dots, v_h = w)$ che è una passeggiata da u a w .

■

Parte IX

Teorema della relazione fondamentale tra il numero dei lati e i gradi dei vertici di un grafo finito e Lemma delle strette di mano

13 Teorema della relazione fondamentale tra il numero dei lati e i gradi dei vertici di un grafo finito

Teorema IX.1.

Ipotesi IX.1.1. Sia $G = (V, E)$ un grafo finito.

Tesi IX.1.2. Allora vale $2|E| = \sum_{v \in V} \deg_G(v)$

Dimostrazione. Sia $V = \{v_1, \dots, v_n\}$ i vertici di G e $E = \{e_1, \dots, e_k\}$ i lati di G con $k := |E|$. Sia ora:

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

ovvero la matrice di adiacenza del grafo G . Allora:

$$(1) \quad \sum_{j=1}^k \left(\sum_{i=1}^n M_{ij} \right) = \sum_{i=1}^n \left(\overbrace{|\{e \in E \mid v_i \in e\}|}^{\text{def. } \deg_G(v)} \right) = \sum_{i=1}^n \deg_G(v_i)$$

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

quindi per la proprietà commutativa della somma possiamo dire che:

$$\sum_{i=1}^n \sum_{j=1}^k m_{ij} = \sum_{j=1}^k \sum_{i=1}^n m_{ij} \stackrel{(1)}{=} \sum_{i=1}^n \deg_G(v_i) \stackrel{(2)}{=} 2|E|$$

■

14 Lemma delle strette di mano

Teorema IX.2.

Ipotesi IX.2.1. Sia $G = (V, E)$ un grafo finito.

Tesi IX.2.2. *Il numero di vertici con grado dispari è pari.*

Dimostrazione. Definiamo $D := \{v \in V \mid 2 \nmid \deg_G(v)\}$ l'insieme dei vertici con grado dispari e $P := \{v \in V \mid 2 \mid \deg_G(v)\}$ l'insieme dei vertici con grado pari $\Rightarrow P \cap D = \emptyset \wedge P \cup D = V$. Grazie alla relazione fondamentale dei grafi finiti:

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

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

In quanto $\deg_G(v) \forall v \in P$ è pari allora $\sum_{v \in P} \deg_G(v)$ è pari in quanto somma di numeri pari, inoltre $2|E|$ è pari in quanto qualsiasi numero moltiplicato per un numero pari è pari. Allora $\sum_{v \in D} \deg_G(v)$ è pari perchè è sottrazione di pari, ma in quanto $\deg_G(v) \forall v \in D$ è dispari allora la somma di questi è pari \Leftrightarrow il numero di vertici con grado dispari è pari. ■

Parte X

Teorema caratterizzante degli alberi finiti

15 Teorema caratterizzante degli alberi finiti

Teorema X.1.

Ipotesi X.1.1. *Sia $T = (V, E)$ un grafo finito*

Tesi X.1.2. *Allora le seguenti affermazioni sono equipotenti:*

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

Dimostrazione.

1 \Rightarrow 5) Si procede per induzione di prima forma su $|V(T)|$ partendo da $|V(T)| = 1$.

Base Induttiva ($|V(T)| = 1$). In questo caso $T = (\{v\}, \emptyset)$ è un albero in quanto un singolo vertice, e $|E| = 0, |V| = 1 \Rightarrow |E| = |V| - 1 = 0$. ✓

Passo Induttivo ($|V(T)| \geq 2 \mid V(T) - 1 \Rightarrow$). In quanto $|V(T)| \geq 2$ allora per il "Lemma delle foglie" questo ha almeno due foglie, sia dunque v una di queste, allora: il grafo $T - v$ è un albero per il lemma sopracitato. Vale che $|V(T - v)| = |V(T)| - 1$, e $|E(T - v)| = |E(T)| - 1$, in quanto v è una foglia (e quindi $\deg_T(v) = 1$) allora:

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

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

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

il che è verificato in quanto $T - v$ è un albero e $|V(T - v)| = |V(T)| - 1$, dunque T è connesso e $|E| = |V| - 1$.

□

1 \Leftarrow 5) Si procede per induzione di prima forma su $|V(T)|$ partendo da $|V(T)| = 1$.

Base Induttiva ($|V(T)| = 1$). Per $|V(T)| = 1$ abbiamo che $T = (\{v\}, \emptyset)$ verifica $|E| = |V| - 1 = 0$ ed è un albero in quanto è un singolo vertice.

Passo Induttivo ($|V(T)| \geq 2 \quad |V(T)| - 1 \implies |V(T)|$). Sia T un grafo connesso che verifica la formula di Eulero $|E| = |V| - 1$ con $|V(T)|$. Sapendo che T è connesso si dimostra per assurdo come questo abbia almeno una foglia:

Dimostrazione. Supponiamo per assurdo che T non abbia foglie, quindi $\forall v \in V(T) \quad \deg_T(v) \geq 2$, inoltre sappiamo per ipotesi che l'equazione di eulero è verificata, dunque:

$$\begin{aligned} 2|E| &= \sum_{v \in V(T)} \deg_T(v) \\ 2(|V| - 1) &= \sum_{v \in V(T)} \deg_T(v) \\ 2|V| - 2 &= \sum_{v \in V(T)} \deg_T(v) \geq 2|V| \\ -2 &\geq 0 \end{aligned}$$

questo significa che se T non avesse foglie allora T non sarebbe connesso, il che è un assurdo, dunque T ha almeno una foglia. □

Prendiamo in considerazione ora una foglia $v \in V(T)$, allora $T - v$ è un grafo connesso in quanto T è connesso e v ne è una sua foglia, vale inoltre che:

$$\begin{aligned} |V(T - v)| &= |V(T)| - 1 \\ |E(T - v)| &= |E(T)| - 1 \\ |V(T - v)| - 1 &= |E(T - v)| \\ |V(T)| - 1 - 1 &= |E(T)| - 1 \\ |V(T)| - 2 &= |E(T)| - 1 \\ |V(T)| - 1 &= |E(T)| \end{aligned}$$

il che conferma l'ipotesi induttiva, dunque T è un albero in quanto connesso e $T - v$ è un albero per ipotesi induttiva, □

Verifichiamo inoltre che T sia un albero, prendiamo per assurdo che \exists un ciclo c in T , ogni vettore $v_i \in c$ ha $\deg_T(v_i) \geq 2$ altrimenti questo non potrebbe essere un ciclo, ma in quanto v è una foglia allora c è anche un ciclo in $T - v$, il che va contro l'ipotesi induttiva, dunque T è un albero. □

Dunque in conclusione possiamo dire che il passo induttivo è stato fatto e che se il grafo T è connesso e $|E| = |V| - 1$ allora T è un albero. ■

Parte XI

Teorema di esistenza dell'albero di copertura per i grafi finiti

16 Teorema di esistenza dell'albero di copertura per i grafi finiti

Teorema XI.1.

Ipotesi XI.1.1. *Sia $G = (V, E)$ un grafo finito connesso.*

Tesi XI.1.2. *G ammette almeno un albero di copertura.*

Dimostrazione. Definiamo il seguente insieme: $e := \{c : c \text{ è un sottografo connesso di } G \wedge V(c) = V(G)\}$ in quanto $G \in e$ allora $\Rightarrow E \neq \emptyset$. Definiamo inoltre $S := \{n \in \mathbb{N} : n = |E(C)| \text{ per qualche } c \in e\}$ l'insieme delle cardinalità degli insiemi di lati dei sottografi connessi di G , anche questo non è vuoto ($S \neq \emptyset$) in quanto $|E(G)| \in S$, in quanto G è un sottografo connesso di G . Dato che l'insieme $S \subseteq \mathbb{N} \wedge S \neq \emptyset$ allora per il teorema del buon ordinamento di \mathbb{N} S ha un minimo, definiamo questo minimo: $\exists \bar{C} \in e : \min(S) = |V(\bar{C})|$. Per costruzione $V(\bar{C}) = V(G)$, dimostriamo dunque per assurdo che \bar{C} è un albero: Se \bar{C} non fosse un albero allora $\exists e \in E(\bar{C}) : \bar{C} - e$ è connesso, dunque $|E(\bar{C} - e)| = |E(\bar{C})| - 1$, in quanto $\bar{C} - e := (V(\bar{C}), E(\bar{C} \setminus \{e\}))$, questo però comporta che $|E(\bar{C} - e)| < |E(\bar{C})|$ il che è un assurdo in quanto va contro la definizione di \bar{C} come sottografo con $|E(\bar{C})| = \min(S)$, dunque \bar{C} è un albero. ■