

Fondamenti di Matematica per Informatica: Schema Esercizi

Aymane Chabbaki

II semestre 2018/2019

Indice

1	Principio di Induzione	3
1.1	Cosa specificare durante lo sviluppo di un esercizio	3
1.2	Esercizio 1	3
1.3	Esercizio 2	4
1.4	Esercizio 3	5
1.5	Esercizio 4	6
2	Massimo Comune Divisore	7
2.1	Esercizio 1	7
2.2	Esercizio 2	7
2.3	Esercizio 3	8
2.4	Esercizio 4	8
3	Teorema Cinese del Resto	9
3.1	Esercizio 1	9
3.2	Esercizio 2	10
4	Invertibilità	12
4.1	Esercizio 1	12
4.2	Esercizio 2	13
5	Calcolo della ϕ	13
5.1	Esercizi	13
6	Crittografia RSA	14
6.1	Esercizio 1	14
6.2	Esercizio 2	15
7	Grafi	17
7.1	Condizioni necessarie ma non sufficienti per l'esistenza di isomorfismi	17
7.2	Ostruzioni all'esistenza di grafi con dato score (condizioni necessarie)	17
8	Isomorfismo tra grafi	18
8.1	Esercizio 1	18
9	Score di grafi	20
9.1	Esercizio 1	20
9.2	Esercizio 2	20
9.3	Esercizio 3	20
9.4	Esercizio 4	21
9.5	Esercizio 5	21
9.6	Esercizio 6	22

9.7	Esercizio 7	22
10	Teorema dello score	24
10.1	Enunciato	24
10.2	Esercizio 1	24
10.3	Esercizio 2	25
10.4	Esercizio 3	26
10.5	Esercizio 4	27
10.6	Esercizio 5	27

1 Principio di Induzione

1.1 Cosa specificare durante lo sviluppo di un esercizio

- BASE DELL'INDUZIONE
- PASSO INDUTTIVO
- IPOTESI INDUTTIVA

1.2 Esercizio 1

Si dimostri per induzione su $n \in \mathbb{N}$ che $\forall n \geq 1$ $P(n) := \left(\sum_{k=0}^n \frac{5^k}{4^k} = \frac{5^{n+1}}{4^n} - 4 \right)$

SOLUZIONE:

- Osserviamo che vale $n = 1$ (**base dell'induzione**):

$$\begin{aligned} \frac{5^0}{4^0} + \frac{5^1}{4^1} &= \frac{5^{1+1}}{4^1} - 4 \\ 1 + \frac{5}{4} &= \frac{25}{4} - 4 \\ \frac{9}{4} &= \frac{9}{4} \end{aligned}$$

- Dunque $P(0)$ vera.
- $n \implies n + 1$ (**passo induttivo**) con $n \geq 1$.
- Assumo che l'uguaglianza: $\sum_{k=0}^n \frac{5^k}{4^k} = \frac{5^{n+1}}{4^n} - 4$ (**ipotesi induttiva**) sia vera.
- Devo dimostrare che: $\sum_{k=0}^{n+1} \frac{5^k}{4^k} = \frac{5^{(n+1)+1}}{4^{n+1}} - 4$
- Vale:

$$\begin{aligned} \sum_{k=0}^{n+1} \frac{5^k}{4^k} &= \left(\sum_{k=0}^n \frac{5^k}{4^k} \right) + \frac{5^{n+1}}{4^{n+1}} \\ (\text{ipotesi induttiva}) \mapsto &= \left(\frac{5^{n+1}}{4^n} \right) + \frac{5^{n+1}}{4^{n+1}} \\ &= \frac{4 \cdot 5^{n+1} + 5^{n+1}}{4^{n+1}} - 4 \\ &= \frac{5 \cdot 5^{n+1}}{4^{n+1}} - 4 \\ &= \frac{5^{(n+1)+1}}{4^{n+1}} - 4 \end{aligned}$$

- Dunque, visto che $\sum_{k=0}^{n+1} \frac{5^k}{4^k} = \frac{5^{(n+1)+1}}{4^{n+1}} - 4$, abbiamo dimostrato l'uguaglianza.

1.3 Esercizio 2

Si dimostri per induzione su $n \in \mathbb{N}$ che $\forall n \geq 2$ $P(n) := \left(\sum_{k=1}^n \frac{5}{6^k} = 1 - \frac{1}{6^n} \right)$

SOLUZIONE:

- Osserviamo che vale $n = 2$ (**base dell'induzione**):

$$\begin{aligned} \sum_{k=1}^2 \frac{5}{6^k} &= 1 - \frac{1}{6^2} \\ \frac{5}{6} + \frac{5}{6^2} &= 1 - \frac{1}{36} \\ \frac{6 * 5 + 5}{36} &= \frac{36 - 1}{36} \\ \frac{35}{36} &= \frac{35}{36} \end{aligned}$$

- $P(2)$ è vera.

- **1° modo:**

- $n \geq 2, n \implies n + 1$
- Assumiamo $P(n)$ sia verificata per qualche $n \geq 2$ (**ipotesi induttiva**).
- Dimostriamo che $P(n + 1)$ è vera, ovvero $\sum_{k=1}^{n+1} \frac{5}{6^k} = 1 - \frac{1}{6^{n+1}}$ è vera (**passo induttivo**).
- Vale:

$$\begin{aligned} \sum_{k=1}^{n+1} \frac{5}{6^k} &= \left(\sum_{k=1}^n \frac{5}{6^k} \right) + \frac{5}{6^{n+1}} \\ (\text{ipotesi induttiva}) \mapsto &= \left(1 - \frac{1}{6^n} \right) + \frac{5}{6^{n+1}} \\ &= 1 - \frac{1}{6^n} + \frac{5}{6^{n+1}} \\ &= 1 - \left(\frac{1}{6^n} - \frac{5}{6^{n+1}} \right) \\ &= 1 - \left(\frac{6 - 5}{6^{n+1}} \right) \\ &= 1 - \frac{1}{6^{n+1}} \end{aligned}$$

- Dunque, visto che $\sum_{k=1}^{n+1} \frac{5}{6^k} = 1 - \frac{1}{6^{n+1}}$, abbiamo dimostrato l'uguaglianza.

- **2° modo:**

- $n \geq 2, n \implies n + 1$ e assumiamo che valga $\sum_{k=1}^n \frac{5}{6^k} = 1 - \frac{1}{6^n}$ per qualche $n \geq 2$ (**ipotesi induttiva**).
- Devo dimostrare che vale: $\sum_{k=1}^{n+1} \frac{5}{6^k} = 1 - \frac{1}{6^{n+1}}$

– Vale:

$$\begin{aligned}
 \sum_{k=1}^{n+1} \frac{5}{6^k} &= 1 - \frac{1}{6^{n+1}} \iff \\
 \left(\sum_{k=1}^n \frac{5}{6^k} \right) + \frac{5}{6^{n+1}} &= 1 - \frac{1}{6^{n+1}} \iff \\
 1 - \frac{1}{6^n} + \frac{5}{6^{n+1}} &= 1 - \frac{1}{6^{n+1}} \iff \\
 \frac{1}{6^{n+1}} + \frac{5}{6^{n+1}} &= \frac{1}{6^n} \iff \\
 \frac{6}{6^{n+1}} &= \frac{1}{6^n} \iff \\
 \frac{1}{6^n} &= \frac{1}{6^n}
 \end{aligned}$$

- Osserviamo che l'ultima equazione è un'**identità** (sempre vera) e dunque, visto che le operazioni sono delle **successioni di equivalenze**, si può affermare che anche la prima uguaglianza è soddisfatta.

1.4 Esercizio 3

Si dimostri per induzione su $n \in \mathbb{N}$ che $\forall n \geq 1$, vale $P(n) := \left(\sum_{k=0}^n 4 \cdot k \cdot 3^k = 3 + 3^{n+1}(2n - 1) \right)$

SOLUZIONE:

- Osserviamo che vale $n = 1$ (**base dell'induzione**):

$$\begin{aligned}
 \sum_{k=0}^1 4 \cdot k \cdot 3^k &= 3 + 3^{1+1}(2 \cdot 1 - 1) \\
 4 \cdot 0 \cdot 3^0 + 4 \cdot 1 \cdot 3^1 &= 3 + 3^2(2 - 1) \\
 12 &= 12
 \end{aligned}$$

- $P(1)$ risulta vera.
- $n \geq 1, n \implies n + 1$
- Assumiamo $P(n)$ vera per qualche $n \geq 1$ (**ipotesi induttiva**).
- Dimostriamo che $P(n + 1)$ è vera, ovvero $\sum_{k=0}^{n+1} 4 \cdot k \cdot 3^k = 3 + 3^{(n+1)+1}(2(n+1) - 1)$
- Vale:

$$\begin{aligned}
 \sum_{k=0}^{n+1} 4 \cdot k \cdot 3^k &= \left(\sum_{k=0}^n 4 \cdot k \cdot 3^k \right) + 4(n+1) \cdot 3^{n+1} \\
 (\text{ipotesi induttiva}) &\mapsto (3 + 3^{n+1} \cdot (2n - 1)) + 4(n+1) \cdot 3^{n+1} \\
 &= 3 + 3^{n+1} \cdot (2n - 1 + 4n + 4) \\
 &= 3 + 3^{n+1} \cdot (6n + 3) \\
 &= 3 + 3^{n+1} \cdot 3(2n + 1)
 \end{aligned}$$

- Dunque, visto che $\sum_{k=0}^{n+1} 4 \cdot k \cdot 3^k = 3 + 3^{n+1} \cdot 3(2n + 1) = 3 + 3^{(n+1)+1} \cdot (2(n+1) - 1)$, abbiamo dimostrato l'uguaglianza.

1.5 Esercizio 4

Si dimostri per induzione su $n \in \mathbb{N}$ che $\forall n \geq 3$ vale $P(n) := \prod_{k=2}^n \left(1 - \frac{1}{k^2}\right) = \frac{1+n}{2n}$

SOLUZIONE:

- Osserviamo che vale $n = 3$ (**base dell'induzione**):

$$\left(1 - \frac{1}{2^2}\right) \left(1 - \frac{1}{3^2}\right) = \frac{1+3}{2 \cdot 3} \iff \left(\frac{3}{4} \cdot \frac{8}{9}\right) = \frac{4}{6} \iff \frac{2}{3} = \frac{2}{3}$$

- $P(3)$ è vera.
- $n \geq 3, n \implies n+1$
- Assumiamo che $\prod_{k=2}^n \left(1 - \frac{1}{k^2}\right) = \frac{1+n}{2n}$ per qualche $n \geq 3$ (**ipotesi induttiva**).
- Proviamo che $\prod_{k=2}^{n+1} \left(1 - \frac{1}{k^2}\right) = \frac{1+(n+1)}{2(n+1)}$ (**passo induttivo**).
- Vale:

$$\begin{aligned} \prod_{k=2}^{n+1} \left(1 - \frac{1}{k^2}\right) &= \frac{1+(n+1)}{2(n+1)} \\ &= \left(\prod_{k=2}^n 1 - \frac{1}{k^2}\right) \cdot \left(1 - \frac{1}{(n+1)^2}\right) \\ (\text{ipotesi induttiva}) \mapsto &= \left(\frac{1+n}{2n}\right) \cdot \left(1 - \frac{1}{(n+1)^2}\right) \\ &= \frac{1+n}{2n} \cdot \frac{(n+1)^2 - 1}{(n+1)^2} \\ &= \frac{n^2 + 2n + 1 - 1}{2n(n+1)} \\ &= \frac{n(n+2)}{2n(n+1)} \\ &= \frac{n+2}{2(n+1)} \\ &= \frac{1+(n+1)}{2(n+1)} \end{aligned}$$

- Dunque, visto che $\prod_{k=2}^{n+1} \left(1 - \frac{1}{k^2}\right) = \frac{1+(n+1)}{2(n+1)}$, abbiamo dimostrato l'uguaglianza.

2 Massimo Comune Divisore

2.1 Esercizio 1

- Calcolo del MCD tra 54 e 39 e calcolo x e y in \mathbb{Z} *tc* :

$$(54, 39) = x \cdot 54 + y \cdot 39$$

- Vale:

$$\begin{aligned} 54 &= 1 \cdot 39 + 15 \\ 39 &= 2 \cdot 15 + 9 \\ 15 &= 1 \cdot 9 + 6 \\ 9 &= 1 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0 \end{aligned} \tag{1}$$

- Ora, da (1) risaliamo i resti:

$$\begin{aligned} 15 &= 54 - 1 \cdot 39 \\ 9 &= 39 - 2 \cdot 15 \\ 6 &= 15 - 1 \cdot 9 \\ 3 &= 9 - 1 \cdot 6 \\ &= 9 - 1(15 - 1 \cdot 9) \\ &= 2 \cdot 9 - 1 \cdot 15 \\ &= 2(39 - 2 \cdot 15) - 1 \cdot 15 \\ &= 2 \cdot 39 - 5 \cdot 15 \\ &= 2 \cdot 39 - 5(54 - 1 \cdot 39) \\ &= 7 \cdot 39 - 5 \cdot 54 \end{aligned}$$

- Dunque si ha che $(54, 39) = 3 = (-5) \cdot 54 + 7 \cdot 39$

2.2 Esercizio 2

- Calcolo del MCD tra 504 e 385 e calcolo x e y in \mathbb{Z} *tc* :

$$(504, 385) = x \cdot 504 + y \cdot 385$$

- Vale:

$$\begin{aligned} 504 &= 1 \cdot 385 + 119 \\ 385 &= 3 \cdot 119 + 28 \\ 119 &= 4 \cdot 28 + 7 \\ 28 &= 4 \cdot 7 + 0 \end{aligned} \tag{2}$$

- Ora, da (2) risaliamo i resti:

$$\begin{aligned} 119 &= 504 - 1 \cdot 385 \\ 28 &= 385 - 3 \cdot 119 \\ 7 &= 119 - 4 \cdot 28 \\ &= 119 - 4(385 - 3 \cdot 119) \\ &= 13 \cdot 119 - 4 \cdot 385 \\ &= 13(504 - 1 \cdot 385) - 4 \cdot 385 \\ &= 13 \cdot 504 - 17 \cdot 385 \end{aligned}$$

- Dunque si ha che $(504, 385) = 7 = 13 \cdot 504 + (-17) \cdot 385$

2.3 Esercizio 3

- Calcolo del MCD tra 48 e 28 e calcolo x e y in \mathbb{Z} *tc* :

$$(48, 28) = x \cdot 48 + y \cdot 28$$

- Vale:

$$\begin{aligned} 48 &= 1 \cdot 28 + 20 \\ 28 &= 1 \cdot 20 + 8 \\ 20 &= 2 \cdot 8 + 4 \\ 8 &= 2 \cdot 4 + 0 \end{aligned} \tag{3}$$

- Ora, da (3) risaliamo i resti:

$$\begin{aligned} 20 &= 48 - 1 \cdot 28 \\ 8 &= 28 - 1 \cdot 20 \\ 4 &= 20 - 2 \cdot 8 \\ &= 20 - 2 \cdot (28 - 1 \cdot 20) \\ &= 3 \cdot 20 - 2 \cdot 28 \\ &= 3 \cdot (48 - 1 \cdot 28) - 2 \cdot 28 \\ &= 3 \cdot 48 - 5 \cdot 28 \end{aligned}$$

- Dunque si ha che $(48, 28) = 4 = 3 \cdot 48 + (-5) \cdot 28$

2.4 Esercizio 4

- Calcolo del MCD tra 52 e 28 e calcolo x e y in \mathbb{Z} *tc* :

$$(52, 28) = x \cdot 52 + y \cdot 28$$

- Vale:

$$\begin{aligned} 52 &= 1 \cdot 28 + 24 \\ 28 &= 1 \cdot 24 + 4 \\ 24 &= 6 \cdot 4 + 0 \end{aligned} \tag{4}$$

- Ora, da (4) risaliamo i resti:

$$\begin{aligned} 24 &= 52 - 1 \cdot 28 \\ 4 &= 28 - 1 \cdot 24 \\ &= 28 - 1 \cdot (52 - 1 \cdot 28) \\ &= 2 \cdot 28 - 1 \cdot 52 \end{aligned}$$

- Dunque si ha che $(52, 28) = 4 = 2 \cdot 28 + (-1) \cdot 52$

3 Teorema Cinese del Resto

3.1 Esercizio 1

- Si determinino tutte le soluzioni di:

$$\begin{cases} x \equiv 33 \pmod{77} \\ x \equiv -2 \pmod{56} \end{cases}$$

- SOLUZIONE:

1. COMPATIBILITÀ:

- Grazie al **Teorema Cinese del Resto**, il sistema è **compatibile**, ovvero il suo insieme Sol delle soluzioni non è vuoto, se e soltanto se $(77, 56) \mid 33 - (-2)$, ovvero $(77, 56) \mid 35$
- Vale:

$$77 = 7 \cdot 11$$

$$56 = 2^3 \cdot 7$$

- $(77, 56) = 7 \mid 35$ è valido, quindi $Sol \neq \emptyset$ e vale:

$$(77, 56) \cdot 5 = 33 - (-2) \quad (1)$$

2. ALGORITMO DI EUCLIDE:

- Calcolo di una soluzione c del sistema, via algoritmo di Euclide.
- Eseguiamo l' **algoritmo di Euclide** per $(77, 56)$:

$$77 = 1 \cdot 56 + 21$$

$$56 = 2 \cdot 21 + 7$$

$$21 = 1 \cdot 14 + 7$$

$$14 = 2 \cdot 7 + 0$$

- Risaliamo i resti e calcoliamo x e y :

$$21 = 77 - 1 \cdot 56$$

$$14 = 56 - 2 \cdot 21$$

$$7 = 21 - 1 \cdot 14$$

$$= 21 - 1(56 - 2 \cdot 21)$$

$$= 3 \cdot 21 - 1 \cdot 56$$

$$= 3(77 - 1 \cdot 56) - 1 \cdot 56$$

$$= 3 \cdot 77 - 4 \cdot 56$$

- Dunque $(77, 56) = 7 = 3 \cdot 77 - 4 \cdot 56 \quad (2)$

- Dalla **(1)** e dalla **(2)** segue che:

$$5(3 \cdot 77 - 4 \cdot 56) = 33 - (-2)$$

$$15 \cdot 77 + (-20) \cdot 56 = 33 + (-2)$$

$$33 + (-15) \cdot 77 = -2 + (-20) \cdot 56$$

- $c := -1122 = -1122 \in Sol$

3. SOLUZIONE COMPLETA:

- Grazie al Teorema Cinese del Resto, vale:
- $Sol = [-1122]_{[77,56]}$
- Vale: $[77, 56] = \frac{77 \cdot 56}{(77, 56)} = 11 \cdot 56 = 616$
- Dunque:

$$\begin{aligned} Sol &= [-1122]_{616} = [110]_{616} \subset \mathbb{Z} \\ &= [110]_{616} = (110 + 616 \cdot k \in \mathbb{Z}) \end{aligned}$$

3.2 Esercizio 2

- Risolvere:

$$(S) = \begin{cases} x \equiv 112 \pmod{72} \\ x \equiv 4 \pmod{330} \end{cases}$$

- SOLUZIONE:

- Osservo che $112 \equiv 40 \pmod{72}$. Dunque il sistema (S) è equivalente al seguente:

$$\begin{cases} x \equiv 40 \pmod{72} \\ x \equiv 4 \pmod{330} \end{cases}$$

1. COMPATIBILITÀ

- * Ricordiamo che, grazie al Teorema Cinese del Resto, il sistema S è compatibile ($Sol(S) \neq \emptyset$) $\iff (72, 330) \mid 40 - 4 \iff (72, 330) \mid 36$
- * Vale:

$$72 = 2^3 \cdot 3^2$$

$$330 = 2 \cdot 3 \cdot 5 \cdot 11$$

$$\implies (72, 330) = 2 \cdot 3 = 6$$

- * $(72, 330) \mid 36 \iff 6 \mid 36$ (visto che 6 divide 36, il sistema (S) è compatibile).
- * Dunque: $40 - 4 = 6 \cdot 6 = 6(72, 330)$ **(1)**

2. EUCLIDE

- * Vale:

$$330 = 4 \cdot 72 + 42$$

$$72 = 1 \cdot 42 + 30$$

$$42 = 1 \cdot 30 + 12$$

$$30 = 2 \cdot 12 + 6$$

$$12 = 2 - 6 + 0$$

* Ora risaliamo i resti:

$$\begin{aligned}
 42 &= 330 - 4 \cdot 72 \\
 30 &= 72 - 1 \cdot 42 \\
 12 &= 42 - 1 \cdot 30 \\
 6 &= 30 - 2 \cdot 12 \\
 &= 30 - 2(42 - 1 \cdot 30) \\
 &= 3 \cdot 30 - 2 \cdot 42 \\
 &= 3(72 - 1 \cdot 42) - 2 \cdot 42 \\
 &= 3 \cdot 72 - 5 \cdot 42 \\
 &= 3 \cdot 72 - 5(330 - 4 \cdot 72) \\
 &= 23 \cdot 72 - 5 \cdot 330
 \end{aligned}$$

* Dunque $(72, 330) = (-5) \cdot 330 + 23 \cdot 72$ **(2)**

3. CALCOLO DELLA SOLUZIONE C

* Dalla **(1)** e **(2)**, segue:

$$\begin{aligned}
 40 - 4 &= 6((-5) \cdot 330 + 23 \cdot 72) \\
 40 - 4 &= (-30) \cdot 330 + (138) \cdot 72
 \end{aligned}$$

* Ovvero:

$$\begin{aligned}
 40 + (-138) \cdot 72 &= 4 + (-30) \cdot 330 \\
 -9896 &= -9896
 \end{aligned}$$

$$\implies c := -9896 \in \text{Sol}(S)$$

4. SOLUZIONE COMPLETA (CALCOLO DEL $\text{Sol}(S)$)

* Grazie al Teorema Cinese del Resto si ha:

$$\text{Sol}(S) = [-9896]_{[72, 330]} \subset \mathbb{Z}$$

$$* \text{ Segue che } [72, 330] = \frac{72 \cdot 330}{(72, 330)} = \frac{72 \cdot 330}{6} = 3960$$

* Dunque:

$$\begin{aligned}
 \text{Sol}(S) &= [-9896]_{[3960]} = [1984]_{[3960]} \\
 &= \{1984 + 3960 \cdot k \mid k \in \mathbb{Z}\}
 \end{aligned}$$

4 Invertibilità

4.1 Esercizio 1

1. $[12]_{30}$ è invertibile? Cioè $[12]_{30} \in (\mathbb{Z}/n\mathbb{Z})^*$

- $n = 30, a = 12$
- $(12, 30) = 6 \neq 1 \implies \nexists [x]_{30} \text{ t.c. } [12]_{30} * [x]_{30} = [1]_{30}$

2. $[11]_{30}$ è invertibile? Cioè $[11]_{30} \in (\mathbb{Z}/n\mathbb{Z})^*$

- $n = 30, b = 11$
- $(11, 30) = 1 \implies \exists [11]_{30}^{-1} \in (\mathbb{Z}/n\mathbb{Z})^*$
- Appliciamo Euclide:

$$30 = 2 \cdot 11 + 8$$

$$11 = 1 \cdot 8 + 3$$

$$8 = 2 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 - 1 + 0$$

- Risaliamo i resti:

$$8 = 30 - 2 \cdot 11$$

$$3 = 11 - 1 \cdot 8$$

$$2 = 8 - 2 \cdot 3$$

$$1 = 3 - 1 \cdot 2$$

$$= 3 - 1(8 - 2 \cdot 3)$$

$$= 3 \cdot 3 - 1 \cdot 8$$

$$= 3(11 - 1 \cdot 8) - 1 \cdot 8$$

$$= 3 \cdot 11 - 4 \cdot 8$$

$$= 3 \cdot 11 - 4(30 - 2 \cdot 11)$$

$$= 11 \cdot 11 - 4 \cdot 30$$

- Dunque:

$$1 = (11) \cdot 11 + (-4) \cdot 30$$

$$[1]_{30} = [11]_{30} \cdot [11]_{30} + [-4]_{30} \cdot [30]_{30}$$

- Passando a (mod 30) si ha che:

$$[1]_{30} = [11]_{30} \cdot [11]_{30}$$

- $[11]_{30}^{-1} = [11]_{30}$

4.2 Esercizio 2

1. $[48]_{20}$ è invertibile? Cioè $[48]_{20} \in (\mathbb{Z}/n\mathbb{Z})^*$

- $n = 20, b = 48$
- $(48, 20) = 4 \neq 1 \implies \nexists [x]_{20} \text{ t.c. } [48]_{20} * [x]_{20} = [1]_{20}$

2. $[3]_{20}$ è invertibile? Cioè $[3]_{20} \in (\mathbb{Z}/n\mathbb{Z})^*$

- $n = 20, a = 3$
- $(3, 20) = 1 \implies \exists [3]_{20}^{-1} \in (\mathbb{Z}/n\mathbb{Z})^*$
- Applichiamo Euclide:

$$20 = 6 * 3 + 2$$

$$3 = 2 * 1 + 1$$

$$2 = 2 - 1 + 0$$

- Risaliamo i resti:

$$2 = 20 - 6 \cdot 3$$

$$1 = 3 - 2 \cdot 1$$

$$= 3 - (20 - 6 \cdot 3)$$

$$= 7 \cdot 3 - 20$$

- Dunque:

$$1 = (7) \cdot 3 + (-1) \cdot 20$$

$$[1]_{20} = [3]_{20} \cdot [7]_{20} + [-1]_{20} \cdot [20]_{20}$$

- Passando a (mod 20) si ha che:

$$[1]_{20} = [3]_{20} \cdot [7]_{20}$$

- $[3]_{20}^{-1} = [7]_{20}$

5 Calcolo della ϕ

5.1 Esercizi

1. $\phi(21) = \phi(3 \cdot 7) = (3 - 1)(7 - 1) = 12$

2. $\phi(35) = \phi(5 \cdot 7) = (5 - 1)(7 - 1) = 24$

3. $\phi(10) = \phi(2 \cdot 5) = (2 - 1)(5 - 1) = 4$

4. $\phi(16) = \phi(2^4) = 2^4 - 2^3 = 8$

5. $\phi(81) = \phi(3^4) = 3^4 - 3^3 = 54$

6. $\phi(24) = \phi(2^3 \cdot 3) = \phi(2^3) \cdot \phi(3) = (2^3 - 2^2)(3 - 1) = 8$

7. $\phi(108) = \phi(2^2 \cdot 3^3) = \phi(2^2) \cdot \phi(3^3) = (2^2 - 2^1)(3^3 - 3^2) = 36$

6 Crittografia RSA

6.1 Esercizio 1

- Risolvere: $x^7 \equiv 2 \pmod{35}$

- SOLUZIONE:

1. Applicabilità del Teorema della crittografia RSA

- Dobbiamo verificare che:
 - (a) $(2, 35) = 1$ (questo è vero in quanto 2 è un numero primo e 35 non è un numero pari)
 - (b) $(7, \phi(35)) = 1$
 - * $\phi(35) = \phi(5) \cdot \phi(7) = (5-1)(7-1) = 24$
 - * Vale che $(7, \phi(35)) = (7, 24) = 1$ (in quanto 7 è un numero primo che non divide 24)
- Grazie al Teorema fondamentale della crittografia RSA vale:

$$\begin{aligned} Sol &= [2^d]_{35} \subset \mathbb{Z} \\ &= \{2^d + k \cdot 35 \in \mathbb{Z} \mid k \in \mathbb{Z}\} \end{aligned}$$

$$* \text{ Dove } d > 0, d \in [7]_{\phi(35)}^{-1} = [7]_{\phi(35)}^{-1} = [7]_{24}^{-1}$$

2. Calcolo della soluzione d ($d > 0, d \in [7]_{24}^{-1}$)

- Calcoliamo $[7]_{24}^{-1}$ via Euclide:

$$\begin{aligned} 24 &= 3 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1 \\ 3 &= 3 - 1 + 0 \end{aligned}$$

- Risaliamo i resti:

$$\begin{aligned} 3 &= 24 - 3 \cdot 7 \\ 1 &= 7 - 2 \cdot 3 \\ &= 7 - 2(24 - 3 \cdot 7) \\ &= 7 \cdot 7 - 2 \cdot 24 \end{aligned}$$

- Dunque:

$$1 = 7 \cdot 7 + (-2) \cdot 24$$

$$[1]_{24} = [7]_{24} \cdot [7]_{24} + [-2]_{24} \cdot [24]_{24}$$

- Passando a $(\text{mod } 24)$ si ha che:

$$[1]_{24} = [7]_{24} \cdot [7]_{24}$$

- $[7]_{24}^{-1} = [7]_{24}$, con $d = 7$

- Segue che:

$$\begin{aligned} Sol &= [2^d]_{35} = [2^7]_{35} \\ &= [2^5]_{35} \cdot [2^2]_{35} \\ &= [32]_{35} \cdot [4]_{35} \\ &= [-3]_{35} \cdot [4]_{35} \\ &= [-12]_{35} \\ &= [23]_{35} \end{aligned}$$

- Quindi:

$$\begin{aligned} Sol &= [23]_{35} \\ &= \{23 + k \cdot 35 \in \mathbb{Z} \mid k \in \mathbb{Z}\} \end{aligned}$$

6.2 Esercizio 2

- Determinare tutte le soluzioni di $x^9 \equiv 49 \pmod{60}$ e se ne determini la massima soluzione negativa.
- SOLUZIONE:

1. Applicabilità del Teorema della crittografia RSA

- Dobbiamo verificare che:
 - (a) $(49, 60) = 1$ (questo è vero in quanto non ci sono primi comuni)
 - (b) $(9, \phi(60)) = 1$
 - * $\phi(60) = \phi(2^2) \cdot \phi(3) \cdot \phi(5) = (2^2 - 2^1)(3 - 1)(5 - 1) = 16$
 - * Vale che $(9, \phi(60)) = (9, 16) = 1$ (in quanto non ci sono primi comuni)
- Grazie al Teorema fondamentale della crittografia RSA vale:

$$Sol = [49^d]_{60} \subset \mathbb{Z}$$

$$d > 0, d \in [9]_{\phi(60)}^{-1} = [9]_{16}^{-1}$$

2. Calcolo di Sol:

- Prima calcolo $d > 0, d \in [9]_{16}^{-1}$ per mezzo dell'algoritmo di Euclide:

$$16 = 1 \cdot 9 + 7$$

$$9 = 1 \cdot 7 + 2$$

$$7 = 3 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

- Risaliamo i resti:

$$7 = 16 - 1 \cdot 9$$

$$2 = 9 - 1 \cdot 7$$

$$1 = 7 - 3 \cdot 2$$

$$= 7 - 3 \cdot 2$$

$$= 7 - 3(9 - 1 \cdot 7)$$

$$= 4 \cdot 7 - 3 \cdot 9$$

$$= 4(16 - 1 \cdot 9) - 3 \cdot 9$$

$$= 4 \cdot 16 - 7 \cdot 9$$

- Dunque:

$$1 = 4 \cdot 16 + (-7) \cdot 9$$

$$[1]_{16} = [4]_{16} \cdot [16]_{16} + [-7]_{16} \cdot [9]_{16}$$

- Passando a (mod 16) si ha che:

$$[1]_{16} = [-7]_{16} \cdot [9]_{16}$$

- Dunque: $[9]_{16}^{-1} = [9]_{16}$ con $d = 9$ e:

$$Sol = [49]_{60}^9 = [7^2]_{60}^9 = [7^{18}]_{60} \subset \mathbb{Z}$$

- Dopo aver studiato l'orbita segue che:

$$\begin{aligned} Sol &= [7^{(4 \cdot 4 + 2)}]_{60} \\ &= [7^4]_{60}^4 \cdot [7]_{60}^2 \\ &= [1]_{60}^4 \cdot [7^2]_{60} \\ &= [1]_{60}^4 \cdot [49]_{60} \\ &= [49]_{60} \end{aligned}$$

- Quindi:

$$\begin{aligned}Sol &= [49]_{60} \\ &= \{49 + k \cdot 60 \in \mathbb{Z} | k \in \mathbb{Z}\}\end{aligned}$$

- La massima soluzione negativa è: -11 (data da $49 - 60$).

7 Grafi

7.1 Condizioni necessarie ma non sufficienti per l'esistenza di isomorfismi

- Alcune condizioni necessarie (**ma non sufficienti**) per l'esistenza di isomorfismi, ovvero se G e G' sono grafi **finiti** ed **isomorfi** allora:
 1. $|V(G)| = |V(G')|$
 2. $|E(G)| = |E(G')|$
 3. $score(G) = score(G')$ in forma canonica
 4. $\#c.c$ di $G = \#c.c$ di G'
 5. G 2-connesso $\iff G'$ 2-connesso
 6. G hamiltoniano $\iff G'$ hamiltoniano
 7. $\#(\{3, \dots, n\}\text{-cicli di } G) = \#(\{3, \dots, n\}\text{-cicli di } G')$
- Queste condizioni vengono utilizzate per **escludere a priori** grafi che non sono isomorfi.
- Basta che una di queste condizioni necessarie venga a mancare affinché i grafi non siano isomorfi.
- Bisogna ricordare però che queste condizioni sono **necessarie ma non sufficienti** per l'esistenza di isomorfismi, dunque se 2 grafi passano tutte le verifiche (basta arrivare fino alla costruzione n. 6), **nulla si può dire** e per verificare se i grafi sono isomorfi bisogna passare a verifica diretta.
- Quando si passa a **verifica diretta di un isomorfismo** è prassi gestire prima i vertici con **grado massimo (minimo)** o che compaiono una **sola volta**, così da ridurre i casi da gestire.

7.2 Ostruzioni all'esistenza di grafi con dato score (condizioni necessarie)

1. OSTRUZIONE 1:

- Se G è un grafo finito con score $d = (d_1, \dots, d_n)$ con $d_1 \leq d_2 \leq \dots, \leq d_n$, allora:

$$d_n \leq n - 1$$

OSTRUZIONE 2:

- Se G è un grafo finito con score $d = (d_1, \dots, d_n)$, per il **lemma delle strette di mano**, il **numero di vertici** di G di **grado dispari** deve essere **pari**.

OSTRUZIONE 3:

- Se $d = (d_1, d_2, \dots, d_{n-k+1}, d_{n-k+2}, \dots, d_{n-1}, d_n) = (d_1, d_2, \dots, d_{n-k}, \underbrace{n-1, \dots, n-1}_{k\text{-volte}})$ fosse lo score di un grafo G , allora:

$$k \leq d_1$$

OSTRUZIONE 4:

- Sia G un grafo finito con score canonico $d = (d_1, \dots, d_{n-1}, d_n)$ e siano $u, v \in V(G)$ tale che:

$$deg_G(u) = d_n - 1$$

$$deg_G(v) = d_n$$

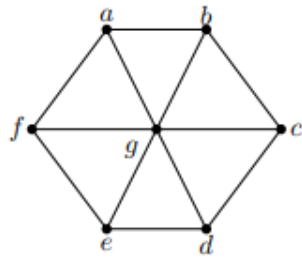
- Allora:

$$|\{w \in V(G) \setminus \{u, v\} \mid deg_G(w) \geq 2\}| \geq d_{n-1} + d_n - n$$

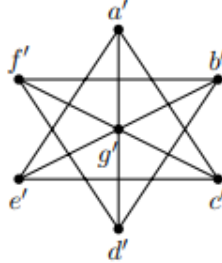
8 Isomorfismo tra grafi

8.1 Esercizio 1

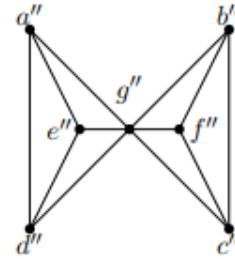
- Stabilire l'esistenza o meno di isomorfismi tra i seguenti grafi:



Grafo G_{25}



Grafo G_{26}

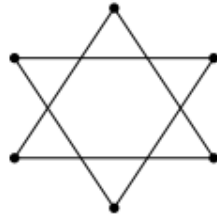


Grafo G_{27}

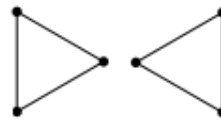
- Alcune condizioni necessarie:

1. $|V(G_{25})| = |V(G_{26})| = |V(G_{27})| = 7$ (NULLA SI PUÒ DIRE)
2. $|E(G)| = |E(G')| = |E(G_{27})| = 12$ (NULLA SI PUÒ DIRE)
3. SCORE:

$$\left. \begin{aligned} score(G_{25}) &= (3, 3, 3, 3, 3, 3, 6) \\ score(G_{26}) &= (3, 3, 3, 3, 3, 3, 6) \\ score(G_{27}) &= (3, 3, 3, 3, 3, 3, 6) \end{aligned} \right\} \text{ NULLA SI PUÒ DIRE}$$
4. G_{25} , G_{26} e G_{27} sono connessi.
5. G_{25} è 2-connesso in quanto hamiltoniano, essendo $\{a, b, c, d, e, f, g, a\}$ un suo ciclo hamiltoniano.
 G_{26} non è 2-connesso in quanto $G_{26} - g'$ è un grafo con 2 c.c.
 G_{27} non è 2-connesso in quanto $G_{27} - g''$ è un grafo con 2 c.c.



(a) $G_{26} - g'$



(b) $G_{27} - g''$

Dunque:

$$G_{25} \not\cong G_{26}$$

$$G_{25} \not\cong G_{27}$$

6. G_{26} e G_{27} non sono 2-connessi e dunque neanche hamiltoniani (NULLA SI PUÒ DIRE).
7. Calcolare $\#(\{3, \dots, n\}\text{-cicli di } G)$ in generale è complicato e non porta a niente.

- Le costruzioni passano tutte le verifiche dunque NULLA SI PUÒ DIRE. Si passa a verifica diretta dell'isomorfismo tra G_{26} e G_{27} :

– Costruiamo un isomorfismo $f : G_{26} \longrightarrow G_{27}$

$$\begin{array}{ccc}
 V_{26} & \xrightarrow{f} & V_{27} \\
 a' & \longmapsto & a'' \\
 b' & \longmapsto & b'' \\
 c' & \longmapsto & c'' \\
 d' & \longmapsto & d'' \\
 e' & \longmapsto & e'' \\
 f' & \longmapsto & f'' \\
 g' & \longmapsto & g''
 \end{array}$$

- Osservo che f è **iniettiva** (i vertici elencati nella colonna di destra sono a 2 a 2 distinti).
- Inoltre f è **surgettiva** (nella colonna a destra compaiono tutti i vertici di G_{27}).
- Dunque f è una **bigezione**.
- Verifico se si tratta di un **morfismo** con f^{-1} morfismo:

$$\begin{array}{ccc}
 E(G_{26}) & \xrightarrow{f'} & \left(\frac{V(G_{27})}{2} \right) \\
 \{a', e'\} & \longmapsto & \{f'', c''\} \in E(G_{27}) \\
 \{a', g'\} & \longmapsto & \{f'', g''\} \in E(G_{27}) \\
 \{a', c'\} & \longmapsto & \{f'', b''\} \in E(G_{27}) \\
 \{e', g'\} & \longmapsto & \{c'', g''\} \in E(G_{27}) \\
 \{e', c'\} & \longmapsto & \{c'', b''\} \in E(G_{27}) \\
 \{c', g'\} & \longmapsto & \{b'', g''\} \in E(G_{27}) \\
 \{f', d'\} & \longmapsto & \{a'', d''\} \in E(G_{27}) \\
 \{f', b'\} & \longmapsto & \{a'', e''\} \in E(G_{27}) \\
 \{f', g'\} & \longmapsto & \{e'', g''\} \in E(G_{27}) \\
 \{b', d'\} & \longmapsto & \{e'', d''\} \in E(G_{27}) \\
 \{b', g'\} & \longmapsto & \{e'', g''\} \in E(G_{27}) \\
 \{d', g'\} & \longmapsto & \{d'', g''\} \in E(G_{27})
 \end{array}$$

- Se avessi trovato un lato che non appartiene a $E(G_{27})$ avrei dovuto rifare tutto, cambiando la funzione f che ho definito in precedenza.
- Poichè i 2-sottoinsiemi di $V(G_{27})$ che compaiono nella colonna di destra sono lati di G_{27} , segue che f è un **morfismo**.
- Poichè nella colonna di destra compaiono tutti i lati di G_{27} , f è un **isomorfismo**.
- In conclusione: $G_{26} \simeq G_{27}$

9 Score di grafi

9.1 Esercizio 1

- Dire se $d = (1, 1, 2, 4, 5, 6, 7)$ è lo score di un grafo.

$$n = 7$$

$$d_n = 7$$

$$d_n \leq n - 1 \iff 7 \leq 7 - 1$$

$$\iff 7 \leq 6$$

- La prima ostruzione non è rispettata, dunque non esiste alcun grafo con score d .

9.2 Esercizio 2

- Dire se $d = (1, 1, 1, 1, 5, 6, 7, 8)$ è lo score di un grafo.

$$n = 8$$

$$d_n = 8$$

$$d_n \leq n - 1 \iff 8 \leq 8 - 1$$

$$\iff 8 \leq 7$$

- La prima ostruzione non è rispettata, dunque non esiste alcun grafo con score d .

9.3 Esercizio 3

- Dire se $d = (0, 1, 2, 4, 4, 4, 4, 8, 8, 9)$ è lo score di un grafo.
- Supponiamo che esista un grafo finito G con $score(G) = d$
- Allora $n := |V(G)| = 10$ e il grado massimo di uno dei suoi vertici è $d_n = 9$
- Deve valere:

$$d_n \leq n - 1 \iff 9 \leq 10 - 1$$

$$\iff 9 \leq 9$$

- La prima ostruzione è valida, **ma nulla si può dire**.
- Supponiamo che d sia uno score di un grafo, allora anche $d' = (1, 2, 4, 4, 4, 4, 8, 8, 9)$ sarebbe lo score di un grado (quello precedente con il **vertice isolato rimosso**).
- Allora vale:

$$d_n \leq n - 1 \iff 9 \leq 9 - 1$$

$$\iff 9 \leq 8$$

- La prima ostruzione non è rispettata, dunque non esiste alcun grafo con score d' , dunque neanche con d .

9.4 Esercizio 4

- Dire se $d = (1, 1, 2, 2, 2, 3, 4, 5, 5, 7)$ è lo score di un grafo.
- Supponiamo che esista un grafo finito G con $score(G) = d$
- Allora $n := |V(G)| = 10$ e il grado massimo di uno dei suoi vertici è $d_n = 7$
- Deve valere:

$$\begin{aligned}d_n \leq n - 1 &\iff 7 \leq 10 - 1 \\ &\iff 7 \leq 9\end{aligned}$$

- La prima ostruzione è valida, **ma nulla si può dire**.
- Per il lemma delle strette di mano, il numero di vertici dispari deve essere pari:

$$\begin{aligned}|V(G) \text{ pari} | &= 4 \\ |V(G) \text{ dispari} | &= 3\end{aligned}$$

- Il lemma delle strette di mano (ostruzione $n.2$) non è rispettato, dunque non esiste alcun grafo con score d .

9.5 Esercizio 5

- Dire se $d = (1, 2, 3, 4, 5, 6, 7, 8, 8)$ è lo score di un grafo.
- Supponiamo che esista un grafo finito G con $score(G) = d$
- Allora $n := |V(G)| = 9$ e il grado massimo di uno dei suoi vertici è $d_n = 8$
- Deve valere:

$$\begin{aligned}d_n \leq n - 1 &\iff 8 \leq 9 - 1 \\ &\iff 8 \leq 8\end{aligned}$$

- La prima ostruzione è valida, **ma nulla si può dire**.
- Per il lemma delle strette di mano, il numero di vertici dispari deve essere pari:

$$\begin{aligned}|V(G) \text{ pari} | &= 4 \\ |V(G) \text{ dispari} | &= 4\end{aligned}$$

- La seconda ostruzione è rispettata, **ma nulla si può dire**.
- Siamo nelle ipotesi della terza ostruzione, cioè lo score termina con termini che valgono $n - 1$, ma deve valere anche $k < d_1$, cioè il numero di termini che valgono $n - 1$ deve essere minore del primo termine dello score.
- Vale:

$$\begin{aligned}k &< d_1 \\ 2 &< 1\end{aligned}$$

- La terza ostruzione non è rispettata, dunque non esiste alcun grafo con score d .

9.6 Esercizio 6

- Dire se $d = (2, 2, 3, 3, 3, 3, 4, 4, 11, 11, 11)$ è lo score di un grafo.
- Supponiamo che esista un grafo finito G con $score(G) = d$
- Allora $n := |V(G)| = 12$ e il grado massimo di uno dei suoi vertici è $d_n = 11$
- Deve valere:

$$\begin{aligned}d_n \leq n - 1 &\iff 11 \leq 12 - 1 \\ &\iff 11 \leq 11\end{aligned}$$

- La prima ostruzione è valida, **ma nulla si può dire**.
- Per il lemma delle strette di mano, il numero di vertici dispari deve essere pari:

$$\begin{aligned}|V(G) \text{ pari} | &= 4 \\ |V(G) \text{ dispari} | &= 8\end{aligned}$$

- La seconda ostruzione è rispettata, **ma nulla si può dire**.
- Siamo nelle ipotesi della terza ostruzione, cioè lo score termina con termini che valgono $n - 1$, ma deve vale anche $k < d_1$, cioè il numero di termini che valgono $n - 1$ deve essere minore del primo termine dello score.
- Vale:

$$\begin{aligned}k &< d_1 \\ 3 &< 2\end{aligned}$$

- La terza ostruzione non è rispettata, dunque non esiste alcun grafo con score d .

9.7 Esercizio 7

- Dire se $d = (1, 1, 2, 2, 2, 2, 2, 2, 3, 4, 4, 12, 13)$ è lo score di un grafo.
- Supponiamo che esista un grafo finito G con $score(G) = d$
- Allora $n := |V(G)| = 14$ e il grado massimo di uno dei suoi vertici è $d_n = 13$
- Deve valere:

$$\begin{aligned}d_n \leq n - 1 &\iff 13 \leq 14 - 1 \\ &\iff 13 \leq 13\end{aligned}$$

- La prima ostruzione è valida, **ma nulla si può dire**.
- Per il lemma delle strette di mano, il numero di vertici dispari deve essere pari:

$$\begin{aligned}|V(G) \text{ pari} | &= 10 \\ |V(G) \text{ dispari} | &= 4\end{aligned}$$

- La seconda ostruzione è rispettata, **ma nulla si può dire**.
- Non siamo nelle ipotesi della terza ostruzione, perchè lo score termina con un solo termine che vale $n - 1$, dunque visto che "ex falso quodlibet", cioè "dal falso segue qualsiasi cosa", la terza ostruzione è rispettata.

- Verifichiamo la quarta ostruzione, cioè "il numero di entrate di d (eccetto le ultime due) maggiori o uguali a 2" deve essere maggiore di $d_{n-1} + d_n - n$
- Dunque:

$$|(2, 2, 2, 2, 2, 2, 3, 4, 4, 12, 13)| \geq 12 + 13 - 14$$

$$10 \geq 11$$

- La quarta ostruzione non è rispettata, dunque non esiste alcun grafo con score d .

10 Teorema dello score

10.1 Enunciato

- Sia $n \geq 2$ e sia $d = (d_1, d_2, \dots, d_n) \in \mathbb{N}^n$ tale che $0 \leq d_1 \leq \dots \leq d_n \leq n-1$
- Definiamo il seguente vettore $d' = (d'_1, d'_2, \dots, d'_{n-1}) \in \mathbb{N}^{n-1}$

$$d'_i := \begin{cases} d_i & i < n - d_n \\ d_i - 1 & i \geq n - d_n \end{cases} \quad (5)$$

- Allora d è lo score di un grafo se e soltanto se lo è d' .
- Se tutto degenera e va a 0, allora d' è lo score di un grafo, e di conseguenza anche d è lo score di un grafo.
- Per semplicità nei calcoli, quando le entrate dell' i -esimo score sono tutte minori o uguali a 2 ci si può fermare.

10.2 Esercizio 1

- Dire se $d = (2, 2, 3, 3, 3, 3, 4, 4, 11, 11, 11)$ è lo score di un grafo.
- Supponiamo che esista un grafo finito G con $score(G) = d$
- Allora $n := |V(G)| = 12$ e il grado massimo di uno dei suoi vertici è $d_n = 11$
- Deve valere:

$$\begin{aligned} d_n \leq n - 1 &\iff 11 \leq 12 - 1 \\ &\iff 11 \leq 11 \end{aligned}$$

- La prima ostruzione è valida, **ma nulla si può dire**.
- Per il lemma delle strette di mano, il numero di vertici dispari deve essere pari:

$$\begin{aligned} |V(G) \text{ pari}| &= 4 \\ |V(G) \text{ dispari}| &= 8 \end{aligned}$$

- La seconda ostruzione è rispettata, **ma nulla si può dire**.
- Siamo nelle ipotesi della terza ostruzione, cioè lo score termina con termini che valgono $n-1$, ma deve valere anche $k < d_1$, cioè il numero di termini che valgono $n-1$ deve essere minore del primo termine dello score.
- Vale:

$$\begin{aligned} k &< d_1 \\ 3 &< 2 \end{aligned}$$

- La terza ostruzione non è rispettata, dunque non esiste alcun grafo con score d .

10.3 Esercizio 2

- Dire se $d = (2, 2, 2, 2, 3, 3, 5, 5, 8, 8)$ è lo score di un grafo.
- Supponiamo che esista un grafo finito G con $score(G) = d$
- Allora $n := |V(G)| = 10$ e il grado massimo di uno dei suoi vertici è $d_n = 8$
- Deve valere:

$$\begin{aligned} d_n \leq n - 1 &\iff 8 \leq 10 - 1 \\ &\iff 8 \leq 9 \end{aligned}$$

- La prima ostruzione è valida, **ma nulla si può dire**.
- Per il lemma delle strette di mano, il numero di vertici dispari deve essere pari:

$$\begin{aligned} |V(G) \text{ pari}| &= 6 \\ |V(G) \text{ dispari}| &= 4 \end{aligned}$$

- La seconda ostruzione è rispettata, **ma nulla si può dire**.
- La terza ostruzione è verificata.
- Verifichiamo la quarta ostruzione, cioè "il numero di entrate di d (eccetto le ultime due) maggiori o uguali a 2" deve essere maggiore di $d_{n-1} + d_n - n$
- Dunque:

$$\begin{aligned} |(2, 2, 2, 2, 3, 3, 5, 5, 8, 8)| &\geq 8 + 8 - 10 \\ 8 &\geq 6 \end{aligned}$$

- La quarta ostruzione è rispettata, **ma nulla si può dire**.
- Le ostruzioni non forniscono informazioni, applico quindi il **teorema dello score**:

<i>Score</i>	<i>Dati</i>
$d = (2, 2, 2, 2, 3, 3, 5, 5, 8, 8)$	$n = 10$ $d_n = 8 \leq 10 - 1$
$d' = (2, 1, 1, 1, 2, 2, 4, 4, 7)$ $= (1, 1, 1, 2, 2, 2, 4, 4, 7)$	$n = 9$ $d_n = 7 \leq 9 - 1$
$d'' = (1, 0, 0, 1, 1, 1, 3, 3)$ $= (0, 0, 1, 1, 1, 1, 3, 3)$	$n = 8$ $d_n = 3 \leq 8 - 1$
$d''' = (0, 0, 1, 1, 0, 0, 2)$ $= (0, 0, 0, 0, 1, 1, 2)$	Entrate minori o uguali a 2

- Poichè d''' è lo score del seguente grafo G''' :



- Dunque, grazie al teorema dello score anche d è lo score di un grafo G .

10.4 Esercizio 3

- Dire se $d = (2, 2, 2, 2, 3, 3, 5, 6)$ è lo score di un grafo.
- Supponiamo che esista un grafo finito G con $score(G) = d$
- Allora $n := |V(G)| = 9$ e il grado massimo di uno dei suoi vertici è $d_n = 6$
- Deve valere:

$$\begin{aligned} d_n \leq n - 1 &\iff 6 \leq 9 - 1 \\ &\iff 6 \leq 8 \end{aligned}$$

- La prima ostruzione è valida, **ma nulla si può dire**.
- Per il lemma delle strette di mano, il numero di vertici dispari deve essere pari:

$$\begin{aligned} |V(G) \text{ pari}| &= 5 \\ |V(G) \text{ dispari}| &= 4 \end{aligned}$$

- La seconda ostruzione è rispettata, **ma nulla si può dire**.
- La terza ostruzione è verificata, in quanto lo score termina con 6 e non con $n - 1 = 9 - 1 = 8$
- Verifichiamo la quarta ostruzione, cioè "il numero di entrate di d (eccetto le ultime due) maggiori o uguali a 2" deve essere maggiore di $d_{n-1} + d_n - n$
- Dunque:

$$\begin{aligned} |(2, 2, 2, 2, 3, 3, 5, 6)| &\geq 5 + 6 - 9 \\ 7 &\geq 2 \end{aligned}$$

- La quarta ostruzione è rispettata, **ma nulla si può dire**.
- Le ostruzioni non forniscono informazioni, applico quindi il **teorema dello score**:

<i>Score</i>	<i>Dati</i>
$d = (2, 2, 2, 2, 3, 3, 5, 6)$	$n = 9$ $d_n = 6 \leq 9 - 1$
$d' = (2, 2, 1, 1, 2, 2, 2, 4)$ $= (1, 1, 2, 2, 2, 2, 2, 4)$	$n = 8$ $d_n = 4 \leq 8 - 1$
$d'' = (1, 1, 2, 1, 1, 1, 1)$ $= (1, 1, 1, 1, 1, 1, 2)$	Entrate minori o uguali a 2

- Poichè d''' è lo score del seguente grafo G''' :



- Dunque, grazie al teorema dello score anche d è lo score di un grafo G .
- Costruiamo un grafo (procedura a ritroso) con score d utilizzando il teorema dello score:

10.5 Esercizio 4

- Dire se $d = (3, 3, 3, 3, 4, 4, 4, 4, 4, 13, 13, 13, 13)$ è lo score di un grafo.
- Supponiamo che esista un grafo finito G con $score(G) = d$
- Allora $n := |V(G)| = 14$ e il grado massimo di uno dei suoi vertici è $d_n = 13$
- Deve valere:

$$\begin{aligned} d_n \leq n - 1 &\iff 13 \leq 14 - 1 \\ &\iff 13 \leq 13 \end{aligned}$$

- La prima ostruzione è valida, **ma nulla si può dire**.
- Per il lemma delle strette di mano, il numero di vertici dispari deve essere pari:

$$\begin{aligned} |V(G) \text{ pari}| &= 6 \\ |V(G) \text{ dispari}| &= 8 \end{aligned}$$

- La seconda ostruzione è rispettata, **ma nulla si può dire**.
- Se d fosse lo score di un grado, per la terza ostruzione sarebbero previsti 4 vertici di grado $13 = n - 1$ (dove $n = 14$ è il numero di vertici) che dovrebbero essere collegati a tutti gli altri vertici.
- Dunque il grado minimo previsto dovrebbe essere maggiore o uguale a 4, che è assurdo visto che il grado minimo dello score d è 3.
- La terza ostruzione non è rispettata, dunque non esiste un grafo con score d .

10.6 Esercizio 5

- Dire se $d = (1, 1, 1, 1, 1, 1, 1, 1, 1, 4, 4, 4)$
- Supponiamo che esista un grafo finito G con $score(G) = d$
- Allora $n := |V(G)| = 13$ e il grado massimo di uno dei suoi vertici è $d_n = 4$
- Deve valere:

$$\begin{aligned} d_n \leq n - 1 &\iff 4 \leq 13 - 1 \\ &\iff 4 \leq 12 \end{aligned}$$

- La prima ostruzione è valida, **ma nulla si può dire**.
- Per il lemma delle strette di mano, il numero di vertici dispari deve essere pari:

$$\begin{aligned} |V(G) \text{ pari}| &= 3 \\ |V(G) \text{ dispari}| &= 10 \end{aligned}$$

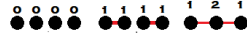
- La seconda ostruzione è rispettata, **ma nulla si può dire**.
- La terza ostruzione è verificata, in quanto non è possibile controllarla.
- Verifichiamo la quarta ostruzione, cioè "il numero di entrate di d (eccetto le ultime due) maggiori o uguali a 2" deve essere maggiore di $d_{n-1} + d_n - n$
- Dunque:

$$\begin{aligned} |(1, 1, 1, 1, 1, 1, 1, 1, 1, 4, 4, 4)| &\geq 4 + 4 - 13 \\ 1 &\geq -5 \end{aligned}$$

- La quarta ostruzione è rispettata, **ma nulla si può dire**.
- Le ostruzioni non forniscono informazioni, applico quindi il **teorema dello score** a d_2 :

<i>Score</i>	<i>Dati</i>
$d = (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 4, 4, 4)$	$n = 13$ $d_n = 4 \leq 13 - 1$
$d' = (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 3, 3)$ $= (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 3, 3)$	$n = 12$ $d_n = 3 \leq 12 - 1$
$d'' = (0, 0, 1, 1, 1, 1, 1, 0, 0, 2)$ $= (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 2)$	Entrate minori o uguali a 2

- Poichè d'' è lo score del seguente grafo G''' :



- Grazie al teorema dello score anche d_2 è lo score di un grafo G_2 .
- Costruiamo un grafo (procedura a ritroso) con score d utilizzando il teorema dello score:

$$\begin{aligned}
 d_2 &= (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 4, 4, 4) \\
 d'_2 &= (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 3, 3) \\
 d''_2 &= (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 2)
 \end{aligned}$$

