

# Fondamenti di Matematica per Informatica: Schema Esercizi

Aymane Chabbaki

II semestre 2018/2019

## Indice

<b>1</b>	<b>Principio di Induzione</b>	<b>3</b>
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
1.6	Esercizio 5 . . . . .	6
1.7	Esercizio 6 . . . . .	7
<b>2</b>	<b>Massimo Comune Divisore</b>	<b>9</b>
2.1	Esercizio 1 . . . . .	9
2.2	Esercizio 2 . . . . .	9
2.3	Esercizio 3 . . . . .	10
2.4	Esercizio 4 . . . . .	10
<b>3</b>	<b>Teorema Cinese del Resto</b>	<b>11</b>
3.1	Esercizio 1 . . . . .	11
3.2	Esercizio 2 . . . . .	12
3.3	Esercizio 3 . . . . .	13
<b>4</b>	<b>Invertibilità</b>	<b>16</b>
4.1	Esercizio 1 . . . . .	16
4.2	Esercizio 2 . . . . .	17
<b>5</b>	<b>Calcolo della <math>\phi</math></b>	<b>17</b>
5.1	Esercizi . . . . .	17
<b>6</b>	<b>Crittografia RSA</b>	<b>18</b>
6.1	Esercizio 1 . . . . .	18
6.2	Esercizio 2 . . . . .	19
6.3	Esercizio 3 . . . . .	20
<b>7</b>	<b>Grafi</b>	<b>22</b>
7.1	Condizioni necessarie ma non sufficienti per l'esistenza di isomorfismi . . . . .	22
7.2	Ostruzioni all'esistenza di grafi con dato score (condizioni necessarie) . . . . .	22
<b>8</b>	<b>Isomorfismo tra grafi</b>	<b>23</b>
8.1	Esercizio 1 . . . . .	23

<b>9</b>	<b>Score di grafi</b>	<b>25</b>
9.1	Esercizio 1 . . . . .	25
9.2	Esercizio 2 . . . . .	25
9.3	Esercizio 3 . . . . .	25
9.4	Esercizio 4 . . . . .	26
9.5	Esercizio 5 . . . . .	26
9.6	Esercizio 6 . . . . .	27
9.7	Esercizio 7 . . . . .	27
<b>10</b>	<b>Teorema dello score</b>	<b>29</b>
10.1	Enunciato . . . . .	29
<b>11</b>	<b>Teorema dello score: Criterio d'arresto</b>	<b>29</b>
<b>12</b>	<b>Teorema di Eulero</b>	<b>29</b>
<b>13</b>	<b>Osservazioni:</b>	<b>30</b>
13.1	Alberi . . . . .	30
13.2	Forzatura alla sconnessione . . . . .	30
13.3	Forzatura alla connessione . . . . .	30
<b>14</b>	<b>Esercizi Grafi</b>	<b>31</b>
14.1	Esercizio 1 . . . . .	31
14.2	Esercizio 2 . . . . .	31
14.3	Esercizio 3 . . . . .	32
14.4	Esercizio 4 . . . . .	33
14.5	Esercizio 5 . . . . .	34
14.6	Esercizio 6 . . . . .	35
14.7	Esercizio 7 . . . . .	36
14.8	Esercizio 8 . . . . .	37

# 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  $\prod_{k=2}^n \left(1 - \frac{1}{k^2}\right) = \frac{1+n}{2n}$  sia vera 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.

## 1.6 Esercizio 5

Si dimostri per induzione su  $n \in \mathbb{N}$  che  $\forall n \geq 1$  vale  $P(n) := \sum_{k=1}^n \frac{4k^2 + 2k - 1}{(2k+1)!} = 1 - \frac{1}{(2n+1)!}$

SOLUZIONE:

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

$$\frac{4 \cdot 1^2 + 2 \cdot 1 - 1}{(2 \cdot 1 + 1)!} = 1 - \frac{1}{(2 \cdot 1 + 1)!} \iff \frac{4 + 2 - 1}{3!} = 1 - \frac{1}{6} \iff \frac{5}{6} = \frac{5}{6}$$

- $P(1)$  è vera.
- $n \geq 1, n \implies n+1$  (**passo induttivo**).
- Assumiamo che  $\sum_{k=1}^n \frac{4k^2+2k-1}{(2k+1)!} = 1 - \frac{1}{(2n+1)!}$  sia vera per qualche  $n \geq 1$  (**ipotesi induttiva**).
- Dobbiamo provare che  $\sum_{k=1}^{n+1} \frac{4k^2+2k-1}{(2k+1)!} = 1 - \frac{1}{(2(n+1)+1)!}$
- Vale:

$$\begin{aligned}
\sum_{k=1}^n \frac{4k^2+2k-1}{(2k+1)!} &= 1 - \frac{1}{(2n+1)!} \\
&= \left( \sum_{k=1}^n \frac{4k^2+2k-1}{(2k+1)!} \right) + \left( \frac{4(n+1)^2+2(n+1)-1}{(2(n+1)+1)!} \right) \\
(\text{ipotesi induttiva}) \mapsto &= \left( 1 - \frac{1}{(2n+1)!} \right) + \left( \frac{4(n^2+2n+1)+2n+2-1}{(2n+3)!} \right) \\
&= 1 - \frac{1}{(2n+1)!} + \frac{4n^2+10n+5}{(2n+3)!} \\
&= 1 - \frac{1}{(2n+1)!} + \frac{4n^2+10n+5}{(2n+3)(2n+2)(2n+1)!} \\
&= 1 - \left[ \frac{(2n+3)(2n+2) - (4n^2+10n+5)}{(2n+3)(2n+2)(2n+1)!} \right] \\
&= 1 - \left[ \frac{4n^2+10n+6-4n^2-10n-5}{(2n+3)(2n+2)(2n+1)!} \right] \\
&= 1 - \frac{1}{(2n+3)!} \\
&= 1 - \frac{1}{(2(n+1)+1)!}
\end{aligned}$$

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

## 1.7 Esercizio 6

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

SOLUZIONE:

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

$$\frac{3}{(2 \cdot 1 + 1)(2 \cdot 1 + 3)} = \frac{1}{2 \cdot 1 + 3} \iff \frac{3}{(2+1)(2+3)} = \frac{1}{2+3} \iff \frac{3}{15} = \frac{1}{5} \iff \frac{1}{3} = \frac{1}{5}$$

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

- Dobbiamo provare che  $\sum_{k=1}^{n+1} \frac{3}{(2k+1)(2k+3)} = 1 - \frac{n+1}{(2(n+1)+3)}$

- Vale:

$$\begin{aligned}
 \frac{3}{(2k+1)(2k+3)} &= \frac{n+1}{(2(n+1)+3)} \\
 &= \left( \sum_{k=1}^n \frac{3}{(2k+1)(2k+3)} \right) + \left( \frac{3}{(2(n+1)+1)(2(n+1)+3)} \right) \\
 \text{(ipotesi induttiva)} \mapsto &= \left( \frac{n}{(2n+3)} \right) + \left( \frac{3}{(2n+3)(2n+5)} \right) \\
 &= \frac{2n^2 + 5n + 3}{(2n+3)(2n+5)} \\
 &= \frac{(n+1)(2n+3)}{(2n+3)(2n+5)} \\
 &= \frac{n+1}{2n+5} \\
 &= \frac{n+1}{(2(n+1)+3)}
 \end{aligned}$$

- Dunque, visto che  $\sum_{k=1}^{n+1} \frac{3}{(2k+1)(2k+3)} = 1 - \frac{n+1}{(2(n+1)+3)}$ , 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  $(77, 56)$ :

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

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

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

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

- 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:

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

## 3.3 Esercizio 3

- Determinare tutte le soluzioni di:

$$(S) = \begin{cases} x \equiv -7 \pmod{21} \\ x \equiv 41 \pmod{81} \end{cases}$$

e dire se esiste una soluzione divisibile per 14.

- SOLUZIONE:

#### 1. COMPATIBILITÀ

- Ricordiamo che, grazie al Teorema Cinese del Resto, il sistema  $S$  è compatibile ( $\text{Sol}(S) \neq \emptyset$ )  
 $\iff (21, 81) \mid 41 - (-7) \iff (21, 81) \mid 48$

– Vale:

$$21 = 3 \cdot 7$$

$$81 = 3^4$$

$$\implies (21, 81) = 3$$

–  $(21, 81) \mid 48 \iff 3 \mid 48 = 3 \cdot 16$  (visto che 3 divide 36, il sistema  $(S)$  è compatibile).

– Dunque:  $41 - (-7) = 16 \cdot (21, 81)$  **(1)**

## 2. CALCOLO DI UNA SOLUZIONE:

– Applico l'algoritmo di Euclide a 21 e 81:

$$81 = 3 \cdot 21 + 18$$

$$21 = 1 \cdot 18 + 3$$

$$~~18 = 6 \cdot 3 + 0~~$$

– Ora risaliamo i resti:

$$18 = 81 - 3 \cdot 21$$

$$3 = 21 - 1 \cdot 18$$

$$= 21 - (81 - 3 \cdot 21)$$

$$= 4 \cdot 21 - 81$$

– Dunque  $(21, 81) = 3 = 4 \cdot 21 - 81$  **(2)**

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

$$41 - (-7) = 16 \cdot (21, 81)$$

$$41 - (-7) = 16(4 \cdot 21 - 81)$$

$$= 64 \cdot 21 - 16 \cdot 81$$

$$41 + 16 \cdot 16 \cdot 81 = -7 + 64 \cdot 21$$

$$1337 = 1337$$

–  $c := 1337 \in Sol$

## 3. CALCOLO DELLA SOLUZIONE GENERALE (CALCOLO DEL $Sol(S)$ )

– Grazie al Teorema Cinese del Resto si ha:

$$Sol(S) = [1337]_{[21, 81]} \subset \mathbb{Z}$$

– Segue che  $[21, 81] = \frac{21 \cdot 81}{(21, 81)} = \frac{21 \cdot 81}{3} = 567$

– Dunque:

$$\begin{aligned} Sol(S) &= [1337]_{[567]} = [203]_{[567]} \\ &= \{203 + 567 \cdot k \in \mathbb{Z} \mid k \in \mathbb{Z}\} \end{aligned}$$

- Esiste un  $x \in Sol(S)$  tale che  $14 \mid x$  ?

### 1. METODO 1:

– Grazie al teorema cinese del resto, l'esistenza di  $x \in Sol(S)$  tale che  $14 \mid x$  è equivalente alla compatibilità del seguente sistema:

$$\begin{cases} x \equiv 200 \pmod{567} \\ x \equiv 0 \pmod{14} \end{cases}$$

- Tale sistema è compatibile se e soltanto se:

$$(567, 14) \mid 203 - 0 \iff 7 \mid 203$$

- Visto che  $7 \mid 203$  è vero, il sistema risulta compatibile, quindi ammette soluzione.
- Dunque esiste una soluzione divisibile per 14.

## 2. METODO 2:

- $x = 203 + k \cdot 567$

$$\begin{aligned} [203 + k \cdot 567]_{14} &= [203]_{14} + [k]_{14} \cdot [567]_{14} \\ &= [203]_{14} + [k]_{14} \cdot [7]_{14} \\ &= [7 + k \cdot 7]_{14} \\ &= [14]_{14} \quad \text{con } k = 1 \\ &= [0]_{14} \end{aligned}$$

- Si ne esiste almeno una e corrisponde, ad esempio, a  $k = 1$ .

## 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  $[3]_{20} \in (\mathbb{Z}/n\mathbb{Z})^*$

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

### 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  $(\text{mod } 16)$  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:

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

- 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  $49 - 60$ ).

### 6.3 Esercizio 3

- Determinare tutte le soluzioni di  $x^5 \equiv 49 \pmod{171}$  e se ne determini la massima soluzione negativa.
- SOLUZIONE:

#### 1. Applicabilità del Teorema della crittografia RSA

- Dobbiamo verificare che:
  - (a)  $(49, 171) = 1$  (vero in quanto nella fattorizzazione di 41 e 171 non sono presenti numeri primi comuni).
  - (b)  $(5, \phi(171)) = 1$ 
    - \*  $\phi(60) = \phi(3^2) \cdot \phi(19) = (3^2 - 3^1)(18) = 108$
    - \* Vale che  $(5, \phi(171)) = (5, 108) = 1$  (visto che 5 è un numero primo e non divide 108)
- Possiamo dunque applicare il teorema fondamentale della crittografia RSA, ottenendo:

$$\begin{aligned} Sol &= [49^d]_{171} \subset \mathbb{Z} \\ d > 0, d &\in [5]_{\phi(171)}^{-1} = [5]_{108}^{-1} \end{aligned}$$

#### 2. Calcolo del Sol:

- Appliciamo l'algoritmo di Euclide a  $(108, 5)$ :

$$\begin{aligned} 108 &= 21 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

- Risaliamo i resti:

$$\begin{aligned} 3 &= 108 - 21 \cdot 5 \\ 2 &= 5 - 1 \cdot 3 \\ 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1(5 - 1 \cdot 3) \\ &= 2 \cdot 3 - 1 \cdot 5 \\ &= 2(108 - 21 \cdot 5) - 1 \cdot 5 \\ &= 2 \cdot 108 - 43 \cdot 5 \end{aligned}$$

- Dunque:

$$\begin{aligned} 1 &= 2 \cdot 108 + (-43) \cdot 5 \\ [1]_{108} &= [2]_{108} \cdot [108]_{108} + [-43]_{108} \cdot [5]_{108} \end{aligned}$$

- Passando a  $(\text{mod } 108)$  si ha che:

$$[1]_{108} = [-43]_{108} \cdot [5]_{108}$$

- Dunque:  $[5]_{108}^{-1} = [-43 + 108]_{108} = [65]_{108}$  con  $d = 65$  e:

$$Sol = [49]_{171}^{65} = [7^2]_{108}^{65} = [7^{130}]_{108} \subset \mathbb{Z}$$

- Dopo aver studiato l'orbita segue che:

$$\begin{aligned}
Sol &= [7^{130}]_{171} \\
&= [7^{(3 \cdot 43 + 1)}]_{171} \\
&= [(7^3)^{43} \cdot 7^1]_{171} \\
&= [7^3]_{171}^{43} \cdot [7^1]_{171} \\
&= [1]_{171}^{43} \cdot [7]_{171} \\
&= [1^{43}]_{171} \cdot [7]_{171} \\
&= [1]_{171} \cdot [7]_{171} \\
&= [7]_{171}
\end{aligned}$$

- Quindi:

$$\begin{aligned}
Sol &= [7]_{171} \\
&= \{7 + k \cdot 171 \in \mathbb{Z} | k \in \mathbb{Z}\}
\end{aligned}$$

- Esiste un  $k \in Sol$  tale che la somma del numero ottenuto faccia 12 ( $\exists k \geq 0$  *tc.* la somma delle cifre del numero  $\{7 + 171 \cdot k\}$  faccia 12)?

- Se esistesse, il numero sarebbe multiplo di 3:

$$[0]_3 = [7 + k \cdot 171]_3 = [7]_3 + [171]_3 \cdot [k]_3 = [1]_3 + [0]_3 \cdot [k]_3 = [1]_3$$

- Qualunque essa sia la soluzione della mia congruenza, se viene divisa per 3, ottengo sempre un resto di 1.
- Dunque, non può esserci una soluzione divisibile per 3 la cui somma delle cifre faccia 12.

## 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:

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

$$deg_G(v) = d_n$$

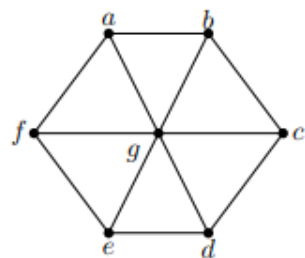
- Allora:

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

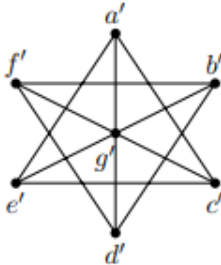
## 8 Isomorfismo tra grafi

### 8.1 Esercizio 1

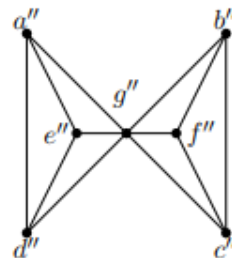
- Stabilire l'esistenza o meno di isomorfismi tra i seguenti grafi:



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:

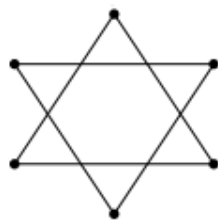
$$\left. \begin{aligned} score(G_{25}) &= (3, 3, 3, 3, 3, 3, 6) \\ score(G_{26}) &= (3, 3, 3, 3, 3, 3, 6) \\ score(G_{27}) &= (3, 3, 3, 3, 3, 3, 6) \end{aligned} \right\} \text{NULLA SI PUÒ DIRE}$$

4.  $G_{25}$ ,  $G_{26}$  e  $G_{27}$  sono connessi.

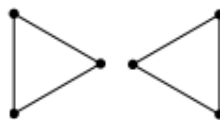
5.  $G_{25}$  è 2-connesso in quanto hamiltoniano, essendo  $\{a, b, c, d, e, f, g, a\}$  un suo ciclo hamiltoniano.

$G_{26}$  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:

$$\begin{array}{ccc}
 E(G_{26}) & \xrightarrow{f^{-1}} & \left( \frac{V(G_{27})}{2} \right) \\
 \{a', e'\} & \longmapsto & \{f'', c''\} \in E(G_{27}) \\
 \{a', g'\} & \longmapsto & \{f'', g''\} \in E(G_{27}) \\
 \{a', c'\} & \longmapsto & \{f'', b''\} \in E(G_{27}) \\
 \{e', g'\} & \longmapsto & \{c'', g''\} \in E(G_{27}) \\
 \{e', c'\} & \longmapsto & \{c'', b''\} \in E(G_{27}) \\
 \{c', g'\} & \longmapsto & \{b'', g''\} \in E(G_{27}) \\
 \{f', d'\} & \longmapsto & \{a'', d''\} \in E(G_{27}) \\
 \{f', b'\} & \longmapsto & \{a'', e''\} \in E(G_{27}) \\
 \{f', g'\} & \longmapsto & \{e'', g''\} \in E(G_{27}) \\
 \{b', d'\} & \longmapsto & \{e'', d''\} \in E(G_{27}) \\
 \{b', g'\} & \longmapsto & \{e'', g''\} \in E(G_{27}) \\
 \{d', g'\} & \longmapsto & \{d'', g''\} \in E(G_{27})
 \end{array}$$

- 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 grafo (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  $\text{score}(G) = d$
- 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  $\text{score}(G) = d$
- 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  $d' = (d'_1, d'_2, \dots, d'_{n-1}) \in \mathbb{N}^{n-1}$

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

- 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.

## 11 Teorema dello score: Criterio d'arresto

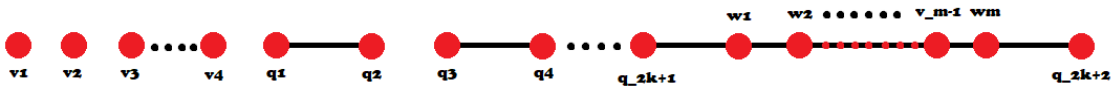
- Sia  $d = (d_1, \dots, d_n) \in \mathbb{N}$  tale che  $0 \leq d_1 \leq \dots \leq d_n \leq 2$ .
- Supponiamo che  $d$  soddisfi il lemma delle strette di mano, cioè il numero di volte che compare 1 è pari.
- Allora valgono:

#### 1. Non compare 1:

- $d = (0, 0, 0, \dots, 0)$  è lo score di un grafo con vertici isolati.
- $d = (0, 0, 0, \dots, 2)$  non è lo score di un grafo; l'ultimo vertice prevede due lati ma tutti gli altri vertici sono isolati.
- $d = (0, 0, 0, \dots, 2, 2)$  non è lo score di un grafo.
- $d = (0, 0, 0, \dots, \underbrace{2, 2, \dots, 2}_{m\text{-volte}})$  è lo score di un grafo.

#### 2. Supponiamo che 1 compaia $2k + 2$ volte per qualche $k > 0$ :

$$d = (\underbrace{0, \dots, 0}_n, \underbrace{1, 1, \dots, 1}_{2k+2}, \underbrace{2, 2, \dots, 2}_m)$$



## 12 Teorema di Eulero

ENUNCIATO:

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

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

## 13 Osservazioni:

### 13.1 Alberi

- Sia  $d = (d_1, d_2, \dots, d_n) \in \mathbb{N}^n$  tale che  $1 \leq d_1 \leq d_2 \leq \dots \leq d_n$  tale che:

$$n - 1 = \frac{1}{2} \sum_{i=1}^n d_i$$

allora **esiste almeno un albero** con tale score.

- Se un grafo  $G$  ammette almeno un **albero di copertura**, allora  $G$  è **connesso**.

### 13.2 Forzatura alla sconnessione

- Se  $G = (V, E)$  è un grafo finito tale che  $|E| < |V| - 1$ , allora  $G$  è **sconnesso**.
- Sia  $d = (d_1, d_2, \dots, d_n) \in \mathbb{N}^n$  tale:

$$\frac{1}{2} \left( \sum_{i=1}^n d_i \right)$$

allora **ogni** grafo (se esiste) con score  $d$  è **connesso**.

### 13.3 Forzatura alla connessione

- Sia  $G = (V, E)$  un grafo finito con score  $d = (d_1, \dots, d_n)$  in forma canonica.  
Se  $d_1, d_2, \dots \geq n - d_n - 1$ , allora tutti i grafi con score  $d$  sono connessi.
- Sia  $d = (d_1, \dots, d_n) \in \mathbb{N}^n$  tale che:
  - $d_1 \leq d_2 \leq \dots \leq d_n$
  - $d_1 \geq n - d_n - 1$
- Allora ogni grado (se esiste) con score  $d$  è **connesso**.

Se la **disuguaglianza per la connessione** (o per la **sconnessione**) non funziona, cioè risulta **falsa**, allora **nulla si può dire** in merito alla connessione di un grafo con tale score.

## 14 Esercizi Grafi

### 14.1 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  $d$ .

### 14.2 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:

$$|(2, 2, 2, 2, 3, 3, 5, 5, 8, 8)| \geq 8 + 8 - 10$$

$$8 \geq 6$$

- 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  $G$ .

### 14.3 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:

$$d_n \leq n - 1 \iff 6 \leq 9 - 1$$

$$\iff 6 \leq 8$$

- 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:

$$|V(G) \text{ pari}| = 5$$

$$|V(G) \text{ dispari}| = 4$$

- 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: **(DA FARE GRAFO)**

#### 14.4 Esercizio 4

- Dire se  $d = (3, 3, 3, 3, 4, 4, 4, 4, 4, 4, 13, 13, 13, 13)$  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 grafo, 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  $d$ .

## 14.5 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  $d_2$ :

Score	Dati
$d = (1, 1, 1, 1, 1, 1, 1, 1, 1, 4, 4, 4)$	$n = 13$ $d_n = 4 \leq 13 - 1$
$d' = (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 3, 3)$ $= (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 3, 3)$	$n = 12$ $d_n = 3 \leq 12 - 1$
$d'' = (0, 0, 1, 1, 1, 1, 1, 0, 0, 2)$ $= (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 2)$	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: **(DA FARE GRAFO)**



## 14.6 Esercizio 6

- Quale dei seguenti vettori è lo score di un albero?

1.  $d_1 = (0, 1, 1, 3, 3, 3, 3, 4, 4)$
2.  $d_2 = (1, 2, 2, 2, 3, 3, 4, 4, 5)$
3.  $d_3 = (2, 2, 2, 2, 3, 3, 3, 4, 4, 7)$
4.  $d_4 = (1, 1, 1, 1, 1, 2, 2, 3, 4)$
5.  $d_5 = (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 3, 6, 6, 7)$

- SOLUZIONE:

1.  $d_1$  non è uno score di un albero, in quanto, sarebbe presente un **vertice isolato** e dunque il grafo con tale score risulterebbe sconnesso.
2.  $d_2$  non è lo score di un albero, in quanto, un grafo con score  $d_2$  avrebbe 9 vertici e se fosse un albero dovrebbero essere presenti almeno 2 foglie (vertici di grado 1).

– Inoltre usando la formula di Eulero si ha:

$$\begin{aligned}
 n &= 9 \\
 |E| &= \frac{1}{2}(1 + 2 + 2 + 2 + 3 + 3 + 4 + 4 + 5) \\
 &= \frac{1}{2}(26) \\
 &= 13
 \end{aligned}$$

– Deve valere:

$$n - 1 = |E| \iff 9 - 1 = 13 \iff 8 = 13$$

– Visto che quest' ultima affermazione è falsa, **la formula di Eulero non è soddisfatta** e dunque non esiste un albero con score  $d_2$ .

3.  $d_3$  non è uno score di un albero per **assenza di foglie**.

4. Verifichiamo la formula di Eulero per  $d_4$ :

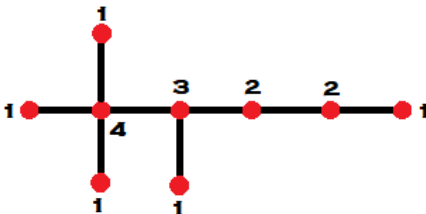
–  $n = 9$

$$|E| = \frac{1}{2}(1, 1, 1, 1, 1, 2, 2, 3, 4) = \frac{1}{2}(16) = 8$$

– Vale:

$$n - 1 = |E| \iff 9 - 1 = 8 \iff 8 = 8$$

– Osservo che  $d_4$  non ha entrate nulle (vertici isolati) e che vale la formula di Eulero; dunque l'albero con score  $d_4$  può essere costruito nel seguente modo:



5. Verifichiamo la formula di Eulero per  $d_5$ :

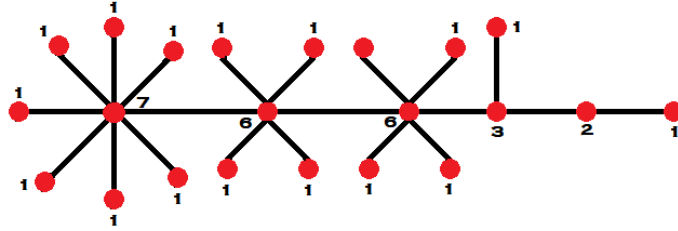
–  $n = 21$

–  $|E| = \frac{1}{2}(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 3, 6, 6, 7) = \frac{1}{2}(40) = 20$

– Vale:

$$n - 1 = |E| \iff 21 - 1 = 20 \iff 20 = 20$$

– Osservo che  $d_5$  non ha entrate nulle (vertici isolati) e che vale la formula di Eulero; dunque l'albero con score  $d_5$  può essere costruito nel seguente modo:



## 14.7 Esercizio 7

• Dise se esiste un grafo connesso con il seguente score:

1.  $d_1 = (1, 1, 1, 1, 1, 1, 2, 2)$

– Vale:

$$\frac{1}{2} \left( \sum_{i=1}^n d_{1i} \right) < n - 1$$

$$\frac{1}{2} (6 \cdot 1 + 2 + 2) < 8 - 1$$

$$\frac{1}{2} (10) < 7$$

$$5 < 7$$

– Tutti i grafi che hanno  $d_1$  come score sono sconnessi, dunque non esiste un grafo connesso con score  $d_1$ .

2.  $d_2 = (1, 1, 2, 2, 2)$

– Vale:

$$\frac{1}{2} \left( \sum_{i=1}^n d_{2i} \right) < n - 1$$

$$\frac{1}{2} (2 \cdot 1 + 3 \cdot 2) < 5 - 1$$

$$\frac{1}{2} (8) < 4$$

$$4 < 7$$

– **Nulla si può dire**, la condizione (necessaria ma non sufficiente) non è verificata.

## 14.8 Esercizio 8

- $d_1 = (2, 3, 4, 4, 5, 5, 5, 6, 7, 7)$
- $d_2 = (1, 2, 3, 3, 3, 3, 4, 8, 8, 9)$
- Esiste un grafo con score  $d_1$  e/o  $d_2$ . Se esiste, costruirlo con il Teorema dello score.
- Costruire inoltre un grafo con tale score tale che:
  - Sia hamiltoniano.
  - Sia connesso.
  - Sia un albero.
- Studiamo  $d_1$ :
  - Sono previsti  $n = 10$  vertici.
  - Ostruzione 1:  $7 \leq 9$ , NPSD
  - Ostruzione 2: LSM 6 è pari, NPSD
  - Ostruzione 3:  $\emptyset$ , NPSD
  - Ostruzione 4:  $8 \geq 4$ , NPSD
  - Tutte le istruzioni sono verificate, dunque passo all'applicazione del teorema dello score a  $d_1$ :

<i>Score</i>	<i>Dati</i>
$d = (2, 3, 4, 4, 5, 5, 5, 6, 7, 7)$	$n = 10$ $d_n = 7 \leq 10 - 1$
$d' = (2, 3, 3, 3, 4, 4, 4, 5, 6)$	$n = 9$ $d_n = 6 \leq 9 - 1$
$d'' = (2, 3, 2, 2, 3, 3, 3, 4)$ $= (2, 2, 2, 3, 3, 3, 3, 4)$	$n = 8$ $d_n = 4 \leq 8 - 1$
$d''' = (2, 2, 2, 2, 2, 2, 2)$	Entrate minori o uguali a 2

- Poichè  $d'''$  è lo score del seguente grafo  $G'''$ :
- Grazie al teorema dello score, anche  $d_1$  è lo score di un grafo  $G_1$ .
- Appliciamo la costruzione "a ritroso" implicata dal teorema dello score: **(DA FARE GRAFO)**
- Il grafo  $G_1$  ha score  $d_1$ .
- Osserviamo che:  $(v_{10}, v_9, v_8, v_7, v_1, v_2, v_3, v_4, v_5, v_8, v_9, v_{10})$  è un ciclo hamiltoniano del grafo  $G_1$  che abbiamo appena costruito. Dunque  $G_1$  è un grafo hamiltoniano con score  $d_1$ .
- Osservo che:
  - \*  $d_1 = (D_1, \dots, D_n)$  con  $(D_1 \leq D_2 \leq \dots \leq D_n)$
  - \*  $D_1 \geq n - D_n - 1$  cioè  $2 \geq 10 - 7 - 1 \implies 2 \geq 2$
  - \* Osservo che il grado minimo previsto 2 è maggiore o uguale a  $10 - 7 - 1$ ; dunque ogni grafo con score  $d_1$  è sconnesso.
- Non esiste un albero con score  $d_1$  per assenza di foglie ( $n = 10 \geq 2$ ).
- Studiamo  $d_2$ :
  - Sono previsti  $n = 10$  vertici.
  - Ostruzione 1:  $9 \leq 9$ , NPSD

- Ostruzione 2: LSM 6 è pari, NPSD
- Ostruzione 3:  $\emptyset$ , NPSD
- Ostruzione 4:  $7 \geq 7$ , NPSD
- Tutte le istruzioni sono verificate, dunque passo all'applicazione del teorema dello score a  $d_1$ :

<i>Score</i>	<i>Dati</i>
$d = (1, 2, 3, 3, 3, 3, 4, 8, 8, 9)$	$n = 10$ $d_n = 9 \leq 10 - 1$
$d' = (0, 1, 2, 2, 2, 2, 3, 7, 7)$	$n = 9$ $d_n = 7 \leq 9 - 1$
$d'' = (0, 0, 1, 1, 1, 1, 2, 6)$	$n = 8$ $d_n = 6 \leq 8 - 1$
$d''' = (0, -1, 0, 0, 0, 0, 1)$	Entrata negativa.

- $d'''$  non è lo score di un grafo avendo una componente negativa.
- Grazie al teorema dello score, anche  $d_2$  non è lo score di un grafo.