

CRIPTOGRAFIA RSA

Fissiamo $n > 0$. Per ogni $c \in \mathbb{N} \setminus \{0\}$, definiamo la seguente funzione

$$P_c : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*,$$
$$\alpha \longmapsto \alpha^c$$

ovvero $P_c(\alpha) := \alpha^c \quad \forall \alpha \in (\mathbb{Z}/n\mathbb{Z})^*$. Grazie al Lemma 13.4 (2)

(appunti letture precedente), la funzione P_c è BKN-DIFFINITA, ovvero, se $\alpha \neq \beta$ è una classe di congruenza mod n INVERTIBILE (ovvero $\alpha \in (\mathbb{Z}/n\mathbb{Z})^*$), allora anche α^c è INVERTIBILE (ovvero $\alpha^c \in (\mathbb{Z}/n\mathbb{Z})^*$)

TEOREMA 13.7 (PROP. 13.11, p. 36, DISPNSF) (TEOREMI FONDAMENTALI DELLA CRITTOGRAFIA RSA)

Sia $c \in \mathbb{N} \setminus \{0\}$ t.c. $(c, \phi(n)) = 1$ e sia $d \in \mathbb{N} \setminus \{0\}$ un inverso di c modulo $\phi(n)$ (ovvero $d > 0$ e $d \in [c]_{\phi(n)}^{-1}$). Allora

$P_c : (\mathbb{Z}/n\mathbb{Z})^* \xrightarrow{*} (\mathbb{Z}/n\mathbb{Z})^*$ è una funzione invertibile e vale:

$$d \longmapsto \alpha^c$$

$$P_c^{-1} = P_d.$$

DIM. Sia $\alpha \in (\mathbb{Z}/n\mathbb{Z})^*$. Dobbiamo

dimostrare che $P_d(P_c(\alpha)) = \alpha$.

Ricordiamo che, essendo $d \in [c]_{\phi(n)}^{-1}$,

$$(\mathbb{Z}/n\mathbb{Z})^* \xrightleftharpoons[P_d: \beta \mapsto \beta^d]{P_c: \alpha \mapsto \alpha^c} (\mathbb{Z}/n\mathbb{Z})^*$$

$$\begin{aligned} P_d = P_c^{-1} &\Leftrightarrow P_d(P_c(\alpha)) = \alpha \quad \forall \alpha \in (\mathbb{Z}/n\mathbb{Z})^* \\ &\text{e} \\ P_c(P_d(\beta)) &= \beta \quad \forall \beta \in (\mathbb{Z}/n\mathbb{Z})^* \end{aligned}$$

$$cd \equiv 1 \pmod{\phi(n)} \Leftrightarrow \phi(n) \mid cd - 1 \Leftrightarrow \exists K \in \mathbb{Z} \text{ t.c. } \quad \swarrow$$

(1)
$$\boxed{cd = 1 + K\phi(n)} \Leftrightarrow cd - 1 = K\phi(n)$$

per qualche $K \in \mathbb{Z}$

Osserviamo che: $K \frac{\phi(n)}{\phi(n) > 0} = cd - 1 \geq 0 \Rightarrow K \geq 0$ (2)
 $\left. \begin{matrix} c \geq 1 \\ d \geq 1 \end{matrix} \right\} \quad \nearrow$

Grazie al teorema di Fermat-Fulcher (vedi scorse lezioni), $\alpha^{\phi(n)} = [1]_n$.

Segue da:

- $P_d(P_c(\alpha)) = P_d(\alpha^c) = (\alpha^c)^d = \alpha^{cd} \stackrel{(1)}{=} \alpha^{1+K\phi(n)} = \alpha^1 \cdot \alpha^{K\phi(n)} \stackrel{(2)}{=} \alpha \cdot (\alpha^{\phi(n)})^K = \alpha ([1]_n)^K = \alpha [1^K]_n = \alpha [1]_n = \alpha.$
- $P_c(P_d(\beta)) = P_c(\beta^d) = (\beta^d)^c = \beta^{cd} = \dots = \beta. \quad \blacksquare$

Corollario 13.8 Siano $a, c \in \mathbb{Z}$ t.c. $(a, n) = 1$ e $c > 0$. Consideriamo la seguente congruenza in $x \in \mathbb{Z}$:

$$x^c \equiv a \pmod{n}.$$

Sia S l'insieme delle soluzioni delle precedenti congruenze,

ovvero

$$S := \{x \in \mathbb{Z} \mid x^c \equiv a \pmod{n}\}.$$

Allora, se $(c, \phi(n)) = 1$ e $d > 0$ con $d \in [c]_{\phi(n)}$, allora

$$S = [a^d]_n = \{a^d + kn \in \mathbb{Z} \mid k \in \mathbb{Z}\} \subset \mathbb{Z}.$$

DIM. Per dirla $(a, n) = 1$, $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$. Dunque,

$$x^c \equiv a \pmod{n} \iff [x^c]_n = [a]_n \iff [x]_n^c = [a]_n$$

$$x^c \equiv \alpha(-1^n) \Leftrightarrow [x]_n^c = [\alpha]_n \quad (x \in \mathbb{Z})$$

$$(\mathbb{Z}/n\mathbb{Z})^*$$

Sia $x \in S$. Allora $[x]_n^c = [\alpha]_n$

\Updownarrow

$$[x]_n [x]_n^{c-1} = [\alpha]_n$$

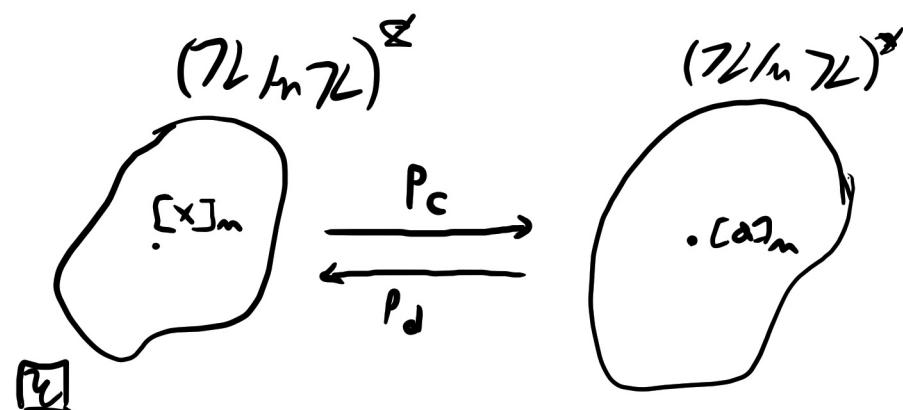
\Updownarrow

$$\underline{[x]_n} \underline{([x]_n^{c-1} [\alpha]_n^{-1})} = [\alpha]_n [\alpha]_n^{-1} = [1]_n$$

$$x \in S \Rightarrow [x]_n \in (\mathbb{Z}/n\mathbb{Z})^*$$

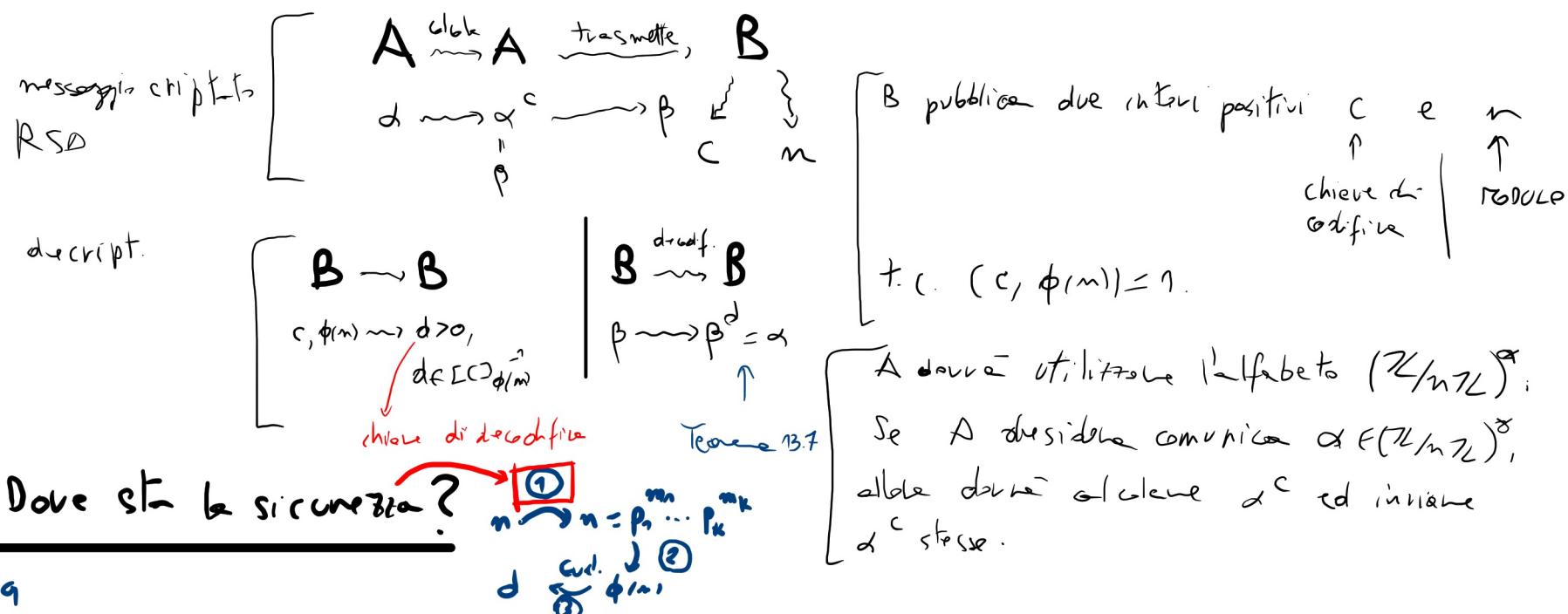
Grazie al teorema precedente, vale:

$$[x]_n = P_d([\alpha]_n) = [\alpha^d]_n \in \mathbb{Z}$$



CRIPTOGRAFIA RSA A CHIAVE PUBBLICA

Supponiamo che A voglia comunicare a B un messaggio via rete mediante la critt. RSA a chiave pubblica.



APPALLO DEL 18/06/2015

ESERCIZIO 3 Determinare le soluzioni delle seguenti congruenze:

$$x^{11} \equiv 35 \pmod{38} \quad (x \in \mathbb{Z})$$

Travare la minima soluzione positiva.

SOLUT. Sia S l'insieme delle soluz. delle congruenze. Calcoliamo S .

1° PASSO: APPLICABILITÀ DEL METODO RSA Dobbiamo verificare le seguenti due proprietà:

$$(1) (35, 38) = 1.$$

$$(2) (11, \phi(38)) = 1.$$

Poiché $35 = 5 \cdot 7$, $\underline{38 = 2 \cdot 19}$ e non ci sono primi comuni nelle due fattORIZZAZIONI; (1) vero.

Vale:

$$\phi(38) = \phi(2 \cdot 19) = \phi(2) \phi(19) = (2-1)(19-1) = 18.$$

Poiché 11 è primo e $11 \nmid 18$, (2) vale.

Segue che si può applicare il metodo RSA (oppure il ~~teorema~~ fondamentale delle congr. RSA) ottenendo

$$S = [35^d]_{38}, \text{ dove } d > 0, d = [11]_{\phi(38)}^{-1}.$$

\uparrow

$$\{35^d + 38k \in \mathbb{Z} \mid k \in \mathbb{Z}\} \subset \mathbb{Z}$$

2° posso) calcolo di d e di S Calcoliamo $d > 0$, $d \in [11]_{\phi(38)}^{-1} = [11]_{18}^{-1}$.

Applichiamo l'algoritmo di Euclideo sostituendo $a = 18$ e $b = 11$:

$$18 = 1 \cdot 11 + 7$$

$$11 = 1 \cdot 7 + 4$$

$$7 = 1 \cdot 4 + 3$$

$$4 = 1 \cdot 3 + \boxed{1}$$

$$\cancel{3 = 3 \cdot 1 + 0}$$

$$7 = \underline{18} - \underline{11}$$

$$4 = \underline{11} - \underline{7}$$

$$2 = \underline{\cancel{7}} - \underline{\cancel{4}}$$

$$1 = \underline{4} - \underline{3} = 4 - (7 - 4) = 2 \cdot \cancel{4} - 7 =$$

$$= 2 \cdot (11 - 7) - 7 = 2 \cdot 11 - 3 \cdot 7 =$$

$$= 2 \cdot 11 - 3 \cdot (18 - 11) = 5 \cdot 11 - 3 \cdot 18$$

Vale:

$$1 = (5)11 + (-3)18.$$

Passando al quoziente mdc 18, ottengo

$$\begin{aligned}\langle 1 \rangle_{18} &= \cancel{[5]_{18}} [11]_{18} + \cancel{[-3]_{18}} [18]_{18} = \\ &= \cancel{[5]_{18}} [11]_{18} + \cancel{[-3]_{18}} \cancel{(0)}_{18} = \\ &= \cancel{[5]_{18}} [11]_{18}.\end{aligned}$$

$d > 0,$
 $d \in [11]_{18}^{-1}$

Dunque $[11]_{18}^{-1} = [5]_{18}$. Definisco $d=5$.

Dunque vale.

$$\begin{aligned} S &= [35^5]_{38} = [35]_{38}^5 = [35-38]_{38}^5 = [-3]_{38}^5 = \\ &= [-3]^5 = [-243]_{38} = [-(6 \cdot 38 + 15)]_{38} = \\ &= \cancel{[-6 \cdot 38 - 15]}_{38} = [-15]_{38} = [38-15]_{38} = [23]_{38} \subset \mathbb{Z}. \end{aligned}$$

La minima soluzione positiva delle congruenze è 23.

Appello 21/06/2016

Esercizio 3 Si determinino tutte le soluz. delle seguenti congruenze:

$$x^9 \equiv 49 \pmod{60}$$

Si determini inoltre la massima soluz. negativa.

SOLUT. Sia S l'insieme delle soluzioni della precedente congruenza,
ovvero $S := \{x \in \mathbb{Z} \mid x^9 \equiv 49 \pmod{60}\}$.

1^ PASSO) APPLICABILITÀ DEL METODO RSA

$$x^9 \equiv 49 \pmod{60}$$

Verifichiamo che valgono:

$$(1) (49, 60) = 1.$$

$$(2) (9, \phi(60)) = 1$$

Poi da $49 = 7^2$ e $60 = 2^2 \cdot 3 \cdot 5$, vale (1), ovvero $(49, 60) = 1$.

$$\begin{aligned} \text{Vale: } & \phi(60) = \phi(2^2 \cdot 3 \cdot 5) = \phi(2^2) \phi(3) \phi(5) = (2^2 - 2^1)(3 - 1)(5 - 1) = \\ & = 2 \cdot 2 \cdot 4 = 16 = 2^4, \end{aligned}$$

$$\cdot 9 = 3^2$$

$$\Rightarrow (9, \phi(60)) = (9, 16) = 1$$

Si può dunque applicare il metodo RSA, ottenendo $S = [49^d]_{60}^{c\mathbb{Z}}$ dove $d > 0$, $d \in [9]_{\phi(60)}^{-1} = [9]_{16}^{-1}$.

2° POSSO) CALCOLARE IL S Calcoliamo d, applicando

$$d > 0, d \in [9]_{16}^{-1}$$

l'algoritmo di Euclideo a 9 e 16:

$$\begin{aligned}16 &= 1 \cdot 9 + 7 \\9 &= 1 \cdot 7 + 2 \\7 &= 3 \cdot 2 + \boxed{1} \\2 &= 2 \cdot 1 + 0\end{aligned}$$

$$\begin{aligned}7 &= 16 - 9 \\2 &= 9 - 7 \\1 &= 7 - 3 \cdot 2 = 7 - 3(9 - 7) = 4 \cdot 7 - 3 \cdot 9 = \\&= 4(16 - 9) - 3 \cdot 9 = 4 \cdot 16 - 7 \cdot 9\end{aligned}$$

Vale:

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

$\Downarrow \text{mod } 16$

$$[1]_{16} = [0]_{16} + [-7]_{16} [9]_{16}$$

Dunque,

$$[7]_{16}^{-1} = [-7]_{16}$$

ERRORE GRAVE $S = [49^d]_{60}$

$\frac{1}{[49^{-7}]_{60}}$

$\frac{1}{[49^7]_{60}} \neq 2$

Vale:

$$[7]_{16}^{-1} = [-7]_{16} = [-7 + 16]_{16} = [9]_{16}$$

$$d \neq 0, \quad d \nmid [9]_{16}^{-1}$$

Dunque poniamo $d := 9$

Vale:

$$S = [49^9]_{60} = \{49^9 + 60k\pi \mid k \in \mathbb{Z}\}.$$

Verifica:
 $9 \cdot 9 \equiv 1 \pmod{16}$

$$\begin{aligned} &\Downarrow \\ 81 &\equiv 1 \pmod{16} \\ &\Updownarrow \\ 16 &\mid 81 - 1 = 80 = 5 \cdot 16 \end{aligned}$$

$$[49^9]_{60}^{\text{!}}$$

BRUPIO

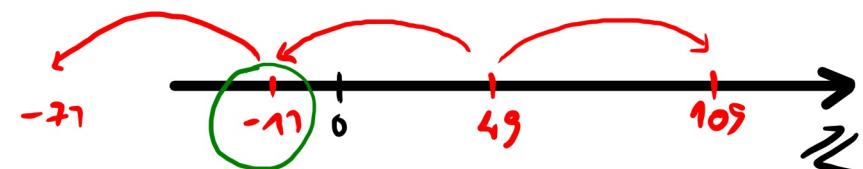
k	rappresentante 49^k mod 60
1	$49^1 = 49$
2	$49^2 = 2401 = 40 \cdot 60 + 1 \equiv 1$



Osserviamo: $49^2 = 2401 = 40 \cdot 60 + 1$, perciò $[49^2]_{60} \stackrel{(n)}{=} [1]_{60}$.

Vale:

$$\begin{aligned} S &= [49^9]_{60} = [49]_{60}^9 = [49]_{60}^{2 \cdot 4 + 1} = ([49]_{60}^2)^4 \cdot [49]_{60}^1 = \\ &= [49^2]_{60}^4 [49]_{60} \stackrel{(n)}{=} [1]_{60}^4 [49]_{60} = [1^4]_{60} [49]_{60} = [1]_{60} [49]_{60} = \\ &= [49]_{60} = \{49 + 60k \in \mathbb{Z} \mid k \in \mathbb{Z}\} \end{aligned}$$



La lessica soluz. negativa è $49 - 60 = -11$.

Grafi (p. 37)

Dato un insieme V , indichiamo con $\binom{V}{2}$ (che si legge " V su 2") l'insieme i cui elementi sono tutti i sottinsiemi di V con 2 elementi (anche detti 2-sottinsiemi di V), ovvero

$$\binom{V}{2} := \{ A \in 2^V \mid |A|=2 \}.$$

Esempi

- Se $V = \emptyset$ oppure se V è un singolo el., allora $\binom{V}{2} = \emptyset$.
- Se $V = \{a, b\}$, allora $\binom{V}{2} = \{V\} = \{\{a, b\}\} \Rightarrow |\binom{V}{2}| = 1$.

- Se $V = \{a, b, c\}$, allora $\binom{V}{2} = \{\{a, b\}, \{a, c\}, \{b, c\}\} \Rightarrow |\binom{V}{2}| = 3$.
- Se $V = \{a, b, c, d\}$, allora $\binom{V}{2} = \{\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}\} \Rightarrow |\binom{V}{2}| = 6$.

Valgono le formule seguenti:

$$\left\{ \begin{array}{l} |\binom{V}{2}| = \binom{|V|}{2} = \frac{|V|!}{2!(|V|-2)!} = \frac{|V|(|V|-1)}{2} \\ \text{se } |V| \geq 2 \end{array} \right.$$

$$\boxed{\binom{a}{b} = \frac{a!}{b!(a-b)!}} \quad a \geq b$$

DEF. 14.1 Un grafo G è una coppia (V, E) , dove V è un insieme NON-VUOTO, detto insieme dei vertici di G , e E è un sottoinsieme di $\binom{V}{2}$, detto insieme dei lati di G . Se $G = (V, E)$ è un grafo ed $e = \{v_1, v_2\} \in E$, si dice v_1 e v_2 vertici incidenti su e ed anche che e congiunge v_1 e v_2 .

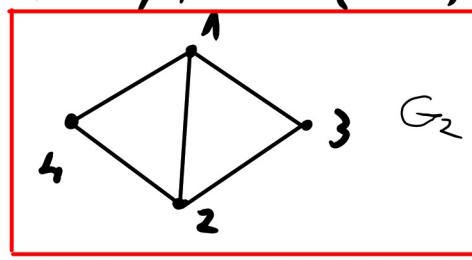
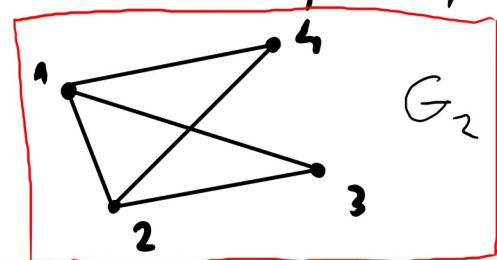
Se G è un grafo, allora $V(G)$ indica l'insieme dei vertici di G e $E(G)$ l'insieme dei lati di G .

ESEMPIO 14.2

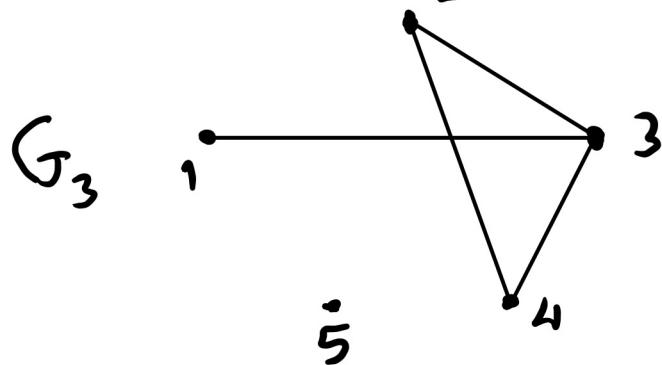
- (1) $G_1 = (V_1, E_1)$, $V_1 = \{1\}$, $E_1 = \emptyset \Rightarrow G_1$ può essere rappresentato con il seguente diagramma:



- (2) Il grafo $G_2 = (V_2, E_2)$, $V_2 = \{1, 2, 3, 4\}$, $E_2 = \{\{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 4\}, \{2, 4\}\}$

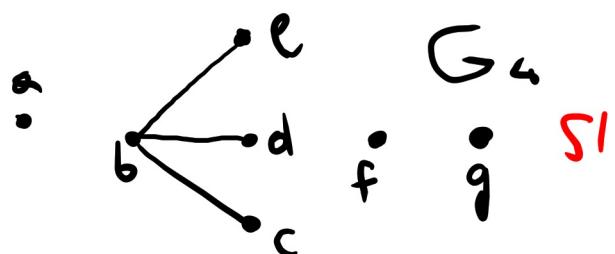


(3) Sia G_3 il seguente grafo

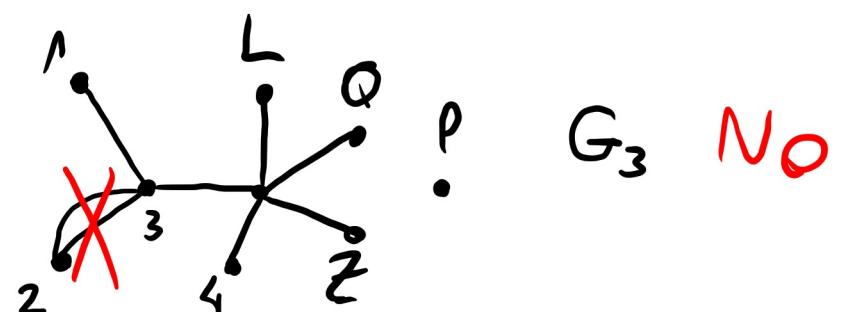


Vale: $V(G_3) = \{1, 2, 3, 4, 5\}$, $E(G_3) = \{\{1, 3\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$

(4) Quale tra i seguenti è un grafo?



SI



?

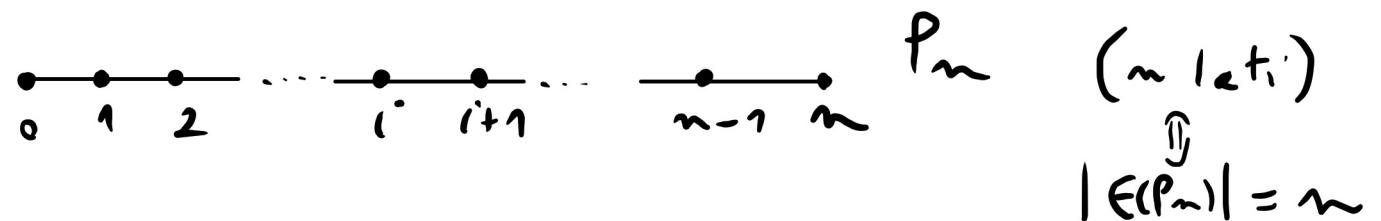
NO

ESEMPI NOTEVOLI 14.3

(a) Per ogni $n \in \mathbb{N}$, definisco il cammino P_n di lunghezza n con il seguente grafo:

$$V(P_n) = \{0, 1, \dots, n\}; E(P_n) := \emptyset \text{ se } n=0,$$

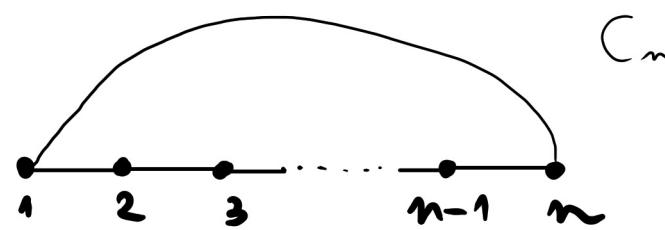
$$E(P_n) := \left\{ \{i, i+1\} \in \binom{V(P_n)}{2} \mid i \in \{0, \dots, n-1\} \right\}$$



(a') P_∞ il cammino infinito, $V(P_\infty) := \mathbb{N}$, $E(P_\infty) = \{\{i, i+1\} \in \binom{\mathbb{N}}{2} \mid i \in \mathbb{N}\}$

(2) Per ogni $n \in \mathbb{N}$ con $n \geq 3$, il ciclo C_n di lunghezza n è definito ponendo:

$$V(C_n) = \{1, 2, \dots, n\}, E(C_n) := \left\{ \{i, i+1\} \in \binom{V(C_n)}{2} \mid i \in \{1, \dots, n-1\} \cup \{1, n\} \right\}$$



C_n

(n bti)



$$|E(C_n)| = n.$$

(3) Per ogni $n \in \mathbb{N}$, $n \geq 1$, il grafo completo su n vertici, denotato con K_n , è definito ponendo:

$$V(K_n) := \{1, 2, \dots, n\}, E(K_n) := \binom{V(K_n)}{2}$$

$K_1 : |$

$K_2 : |$

$K_3 : |$

$K_4 : |$

Sottografi e sottografi indotti

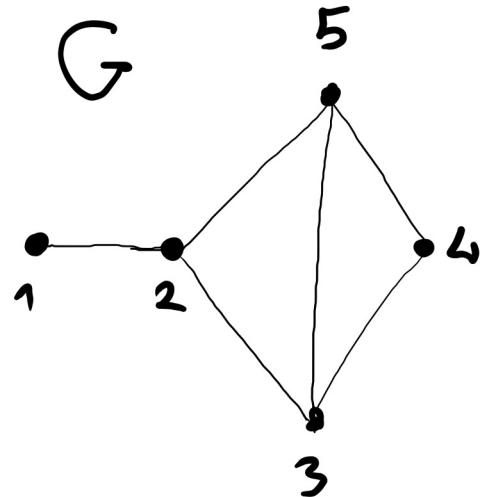
Def. 14.4 Siano $G = (V, E)$ e $G' = (V', E')$ due grafici. Diciamo che G' è un sottografo di G se $V' \subset V$ e $E' \subset E$.

Se G' è un sottografo di G e vale

$$E' = \{e \in E \mid e = \{v_1, v_2\}, v_1 \in V', v_2 \in V'\}$$

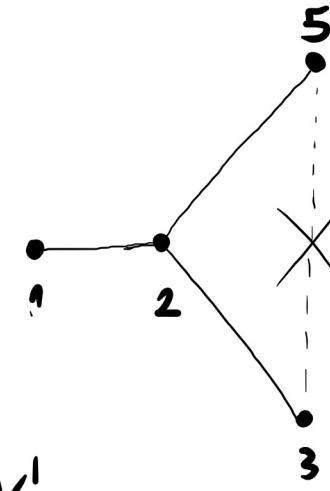
allora G' si dice sottografo di G indotto da V' , e si indica con il simbolo $G[V']$.

ESEMPIO 14.5 Consideriamo i seguenti grafici G e G' :



$$V(G) = \{1, 2, 3, 4, 5\}$$

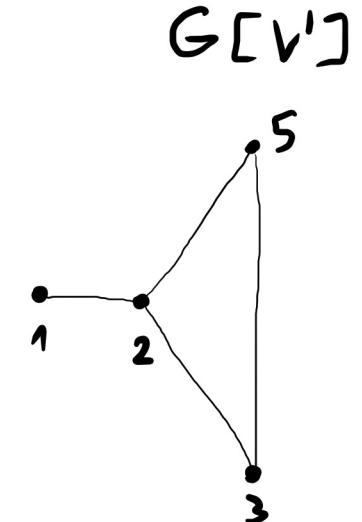
$$E(G) = \{\{1, 2\}, \{2, 3\}, \{2, 5\}, \{3, 4\}, \{3, 5\}, \{4, 5\}\}$$



$$V(G') = \{1, 2, 3, 5\} \subset V(G)$$

$$E(G') = \{\{1, 2\}, \{2, 3\}, \{2, 5\}\} \subset E(G)$$

G'
non è
un
grafo
indatto



\Rightarrow
 G'
è un
sottografo
di G