Svolgimento esame di Fondamenti matematici per l'informatica

Leonardo De Faveri

23 giugno 2021

Esercizio 1) Si dimostri per induzione che, per ogni intero $n \geq 2$, vale:

$$\sum_{k=2}^{n} \frac{k-1}{2^k} = 1 - \frac{n+1}{2^n}$$

Soluzione: Procedo per induzione su $n \geq 2$.

- $n = 2$ (*Base dell'induzione*): dimostro che vale $\sum_{k=2}^{2} \frac{k-1}{2^k} = 1 - \frac{2+1}{2^2}$

  - $\sum_{k=2}^{2} \frac{k-1}{2^k} = \frac{2-1}{2^2} = \frac{1}{4}$
  - $1 - \frac{2+1}{2^2} = 1 - \frac{3}{4} = \frac{1}{4}$

  La base dell'induzione è verificata.

- $n \geq 2 \Rightarrow n+1$ (*Passo induttivo*): ipotizzo che l'uguaglianza sia vera per un qualche $n \geq 2$, cioè che valga:

$$\sum_{k=2}^{n} \frac{k-1}{2^k} = 1 - \frac{n+1}{2^n} \text{ per qualche } n \geq 2 \text{ (Ip. Ind.)}$$

  Dimostro che la stessa uguaglianza vale anche per $n+1$, ovvero dimostro che vale anche:

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

  Vale:

$$\sum_{k=2}^{n+1} \frac{k-1}{2^k} = 1 - \frac{(n+1)+1}{2^{n+1}} \Leftrightarrow \frac{(n+1)-1}{2^{n+1}} + \sum_{k=2}^{n} \frac{k-1}{2^k} = 1 - \frac{n+2}{2^{n+1}}$$

$$\Leftrightarrow \sum_{k=2}^{n} \frac{k-1}{2^k} = 1 - \frac{n+2}{2^{n+1}} - \frac{n}{2^{n+1}} \overset{\text{Ip. Ind.}}{\Longleftrightarrow} 1 - \frac{n+1}{2^n} = 1 - \frac{2n+2}{2^{n+1}}$$

$$\Leftrightarrow \frac{n+1}{2^n} = \frac{2(n+1)}{2^n \cdot 2} \Leftrightarrow \frac{n+1}{2^n} = \frac{n+1}{2^n} \Leftrightarrow 0 = 0$$

  L'identità $0 = 0$ è vera, quindi il passo induttivo risulta verificato, dunque per il teorema d'induzione, l'uguaglianza

$$\sum_{k=2}^{n} \frac{k-1}{2^k} = 1 - \frac{n+1}{2^n}$$

  è vera per ogni intero $n \geq 2$.

Esercizio 2) Si determinino tutte le soluzioni del seguente sistema di congruenze:

$$\begin{cases} x \equiv 45 \pmod{77} \\ x \equiv 59 \pmod{140} \end{cases}$$

Si dimostri inoltre che non esiste alcuna soluzione positiva del suddetto sistema che abbia una cifra pari al posto delle decine.

Soluzione: Sia S l'insieme delle soluzioni.

1^o Passo) *Compatibilità*
Grazie al Teorema cinese del resto so che il sistema di congruenze in questione è compatibile se e solo se $(140, 77)|59 - 45$.
Calcolo $(140, 77)$:

$$\begin{array}{r|l} 140 & 2 \\ 70 & 2 \\ 35 & 2 \\ 7 & 7 \\ 1 & \end{array} \quad \begin{array}{r|l} 77 & 7 \\ 11 & 11 \\ 1 & \end{array}$$

Poiché $140 = 2^2 \cdot 5 \cdot 7$ e $77 = 7 \cdot 11$, $(140, 70) = 7$. Dato che $59 - 45 = 14 = 2 \cdot 7$, $(140, 70) = 7|14 = 59 - 45$. Quindi, per il Teorema cinese del resto, il sistema è compatibile, ovvero $S \neq \emptyset$.
Inoltre vale:

$$59 - 45 = 14 = 2 \cdot 7 = 2 \cdot (140, 77)$$

cioè

$$59 - 45 = 2 \cdot (140, 77) \tag{1}$$

2^o Passo) *Calcolo di una soluzione*
Applico l'algoritmo di Euclide con sostituzione a ritroso a 140 e 77:

$$\begin{array}{rcl|rcl} 140 & = & 1 \cdot 77 + 63 & 63 & = & 140 - 1 \cdot 77 \\ 77 & = & 1 \cdot 63 + 14 & 14 & = & 77 - 1 \cdot 63 \\ 63 & = & 4 \cdot 14 + 7 & 7 & = & 63 - 4 \cdot 14 = 63 - 4 \cdot (77 - 1 \cdot 63) \\ & & & & & = 5 \cdot 63 - 4 \cdot 77 \\ & & & & & = 5 \cdot (140 - 1 \cdot 77) - 4 \cdot 77 \\ & & & & & = 5 \cdot 140 - 9 \cdot 77 \\ 14 & = & 2 \cdot 7 + 0 & & & \end{array}$$

Ovvero vale:

$$7 = 5 \cdot 140 + (-9) \cdot 77 \Leftrightarrow (140, 77) = 5 \cdot 140 + (-9) \cdot 77 \tag{2}$$

Grazie a (1) e (2) vale:

$$59 - 45 \overset{(1)}{=} 2 \cdot (140, 77) \overset{(2)}{=} 2 \cdot (5 \cdot 140 + (-9) \cdot 77) = 10. \cdot 140 + (-18) \cdot 77$$

ovvero

$$59 - 45 = 10 \cdot 140 + (-18) \cdot 77 \tag{3}$$

Da (3) deriva che

$$\begin{array}{rcl} 59 - 10 \cdot 140 & = & 45 - 18 \cdot 77 \\ -1341 & = & -1341 \end{array}$$

Di conseguenza $c := -1341$ è una soluzione del sistema.

3^o Passo) *Calcolo di S*

Grazie al Teorema cinese del resto so che l'insieme delle soluzioni S è:

$$S = [c]_{[140,77]} = [-1341]_{[140,77]} \subset \mathbb{Z}$$

Calcolo $[140, 77]$:

$$[140, 77] = \frac{140 \cdot 77}{(140, 77)} = \frac{140 \cdot 77}{7} = 140 \cdot 11 = 1540$$

Dunque:

$$S = [-1341]_{1540} = [-1341 + 1 \cdot 1540]_{1540} = [199]_{1540} \subset \mathbb{Z}$$

Seconda domanda: poiché le soluzioni del sistema sono tutti e soli i valori contenuti in:

$$S = \{199 + k \cdot 1540 \mid k \in \mathbb{Z}\}$$

e, in particolare, le soluzioni positive sono contenute in:

$$S' = \{199 + k \cdot 1540 \mid k \in \mathbb{N}\}$$

ne segue che, siccome la cifra delle decine del valore del modulo, 1540, è 4, quindi è pari, mentre la cifra delle unità è 0, vale che per $k \in \mathbb{N}$ il prodotto $k \cdot 1540$ avrà sempre, come risultato, un valore la cui cifra delle decine sia pari e la cui cifra delle unità sia 0. D'altro canto, la cifra delle decine di 199 è dispari, e poiché la somma tra valori dispari e valori pari restituisce sempre valori dispari, ne deriva che tutte le soluzioni positive del sistema hanno una cifra dispari delle decine e non possono esistere soluzioni positive del sistema la cui cifra delle decine sia pari.

Esercizio 3) Si dica, motivando la risposta, quali dei seguenti vettori

$$d_1 = (0, 0, 1, 2, 2, 3, 4, 5, 7, 8), \;\; d_2 = (1, 1, 2, 2, 2, 3, 3, 3, 4, 5)$$

è lo score di un grafo e, in caso lo sia, si costruisca un tale grafo utilizzando il Teorema dello score. Si dica inoltre se:

(3a) Esiste un tale grafo che sia sconnesso;

(3b) Esiste un tale grafo che sia 2-connesso;

Soluzione: Il vettore d_1 non può essere lo score di un grafo in quanto verifica l'ostruzione 3. Ovvero, il numero di componenti maggiori o uguali a 2 e che non sono le ultime due componenti, $L := 5$, verifica questa disuguaglianza:

$$L = 5 \leq 7 + 8 - 10 = d_{n-1} + d_n - n = 6$$

Di conseguenza, l'ostruzione 3 mi garantisce che non esistono grafi che abbiano d_1 come score. Nessuna delle ostruzioni viste a lezione si applica invece a d_2, dunque d_2 potrebbe essere lo score di un grafo. Poiché la condizione di applicabilità del Teorema dello score è verificata, ovvero vale:

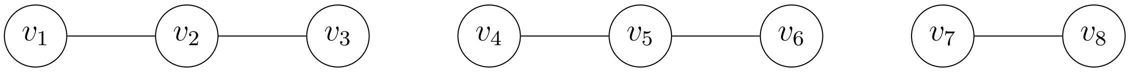
$$d_n = 5 \leq 10 - 1 = n - 1 = 9$$

posso provare ad applicare il suddetto teorema a d_2.

Applico il Teorema delle score:

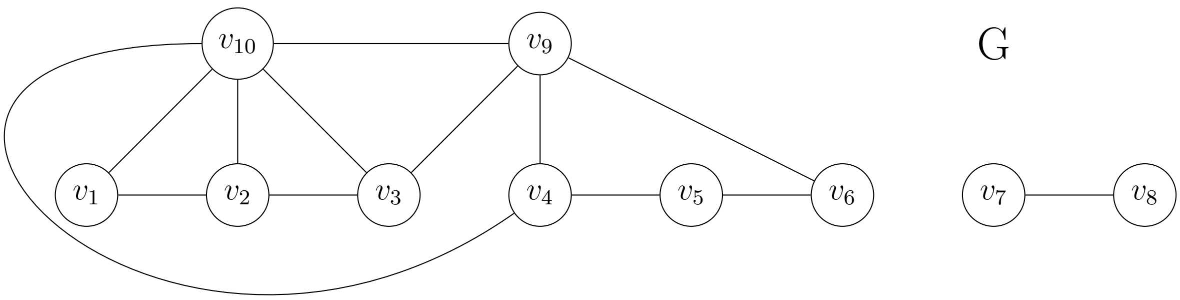
$$
\begin{array}{r|cccccccccc|l}
d_2 & (1, & 1, & 2, & 2, & 2, & 3, & 3, & 3, & 4, & 5) & 5 \leq 10 - 0 = 9 \\
 & (1, & 1, & 2, & 2, & 1, & 2, & 2, & 2, & 3) & = & \\
d_2' & (1, & 1, & 1, & 2, & 2, & 2, & 2, & 2, & 3) & & 3 \leq 9 - 1 = 8 \\
 & (1, & 1, & 1, & 2, & 2, & 1, & 1, & 1) & = & & \\
d_2'' & (1, & 1, & 1, & 1, & 1, & 1, & 2, & 2) & & &
\end{array}
$$

Poiché $d_2'' := (1, 1, 1, 1, 1, 1, 2, 2)$ è lo score del seguente grafo:



grazie al Teorema cinese del resto so che anche d_2 è lo score di un grafo. Costruisco quindi un grafo G con $score(G) = d_2$ utilizzando il Teorema dello score:

$$
\begin{array}{rcccccccccccc}
d_2 & = & (1, & 1, & 2, & 2, & 2, & 3, & 3, & 3, & 4, & 5) \\
 & & & & \downarrow & & & \downarrow & \downarrow & \downarrow & \downarrow & \\
d_2' & = & (1, & 1, & 1, & 2, & 2, & 2, & 2, & 2, & 3) & \\
 & & & & & \downarrow & \downarrow & \downarrow & & & & \\
d_2'' & = & (1, & 1, & 1, & 1, & 1, & 1, & 2, & 2) & &
\end{array}
$$



La risposta alla questione (3a) è Sì, in quanto, il grafo G che ho costruito ha 2 componenti connesse, quindi è sconnesso. Invece, la risposta alla questione (3b) è No, in quanto i grafi 2-connessi non hanno foglie, mentre i grafi con score d_2 ne hanno 2.

Domanda di teoria Si enunci e si dimostri il Teorema di Fermat-Eulero e si dica come viene utilizzato nella crittografia RSA.

Enunciato Teorema di Fermat-Eulero: Sia $n \in \mathbb{N}$ con $n > 0$. $\forall \alpha \in (\mathbb{Z}/n\mathbb{Z})^*$, vale:

$$\alpha^{\Phi(n)} = [1]_n \text{ in } (\mathbb{Z}/n\mathbb{Z})^*$$

o, equivalentemente, $\forall \alpha \in \mathbb{Z}$ *t.c.* $(\alpha, n) = 1$, vale:

$$\alpha^{\Phi(n)} \equiv 1 \pmod n$$

Dim. Sia $\alpha \in (\mathbb{Z}/n\mathbb{Z})^*$. Si consideri la funzione:

$$L_\alpha : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*$$

tale che $L_\alpha(\beta) \mapsto \alpha \cdot \beta \ \forall \beta \in (\mathbb{Z}/n\mathbb{Z})^*$. Poiché dominio e codominio di L_α coincidono entrambi con $(\mathbb{Z}/n\mathbb{Z})^*$ che è un insieme finito, se riesco a dimostrare che L_α è una funzione iniettiva, allora varrà anche la suriettività. Dimostro l'iniettività di L_α. Siano $\beta_1, \beta_2 \in (\mathbb{Z}/n\mathbb{Z})^*$ tali che $L_\alpha(\beta_1) = L_\alpha(\beta_2)$. Provo che $\beta_1 = \beta_2$. Vale:

$$L_\alpha(\beta_1) = L_\alpha(\beta_2) \Leftrightarrow \alpha \cdot \beta_1 = \alpha \cdot \beta_2$$

poiché $\alpha \in (\mathbb{Z}/n\mathbb{Z})^*$, α è invertibile, ovvero esiste $\alpha^{-1} \in (\mathbb{Z}/n\mathbb{Z})^*$ tale che $\alpha \cdot \alpha^{-1} = [1]_n$. Dunque vale:

$$\alpha \cdot \beta_1 = \alpha \cdot \beta_2 \Leftrightarrow \alpha^{-1} \cdot \alpha \cdot \beta_1 = \beta_2 \cdot \alpha \cdot \alpha^{-1} \Leftrightarrow [1]_n \cdot \beta_1 = [1]_n \cdot \beta_2 \Leftrightarrow \beta_1 = \beta_2$$

Quindi, L_α è una funzione iniettiva e suriettiva, dunque è una bigezione.

Passo alla dimostrazione del teorema vero e proprio. Sia $n \in \mathbb{Z}$ con $n > 0$ e sia $k := \Phi(n)$. Se $(\mathbb{Z}/n\mathbb{Z})^* = \{\beta_1, \dots, \beta_k\}$, poiché L_α è una bigezione, i valori $L_\alpha(\beta_1), \dots, L_\alpha(\beta_k)$ sono tutti e soli gli elementi di $(\mathbb{Z}/n\mathbb{Z})^*$ eventualmente riordinati. Per la commutatività del prodotto in $(\mathbb{Z}/n\mathbb{Z})^*$ vale:

$$\prod_{i=1}^{k} \beta_i = \prod_{i=1}^{k} L_\alpha(\beta_1) = \prod_{i=1}^{k} \alpha \cdot \beta_i = \alpha^k \cdot \prod_{i=1}^{k} \beta_i$$

Se $(\mathbb{Z}/n\mathbb{Z})^* \ni \gamma := \prod_{i=1}^{k} \beta_i$, vale che:

$$\gamma = \alpha^k \cdot \gamma \Leftrightarrow \gamma^{-1} \cdot \gamma = \alpha^k \cdot \gamma \cdot \gamma^{-1} \Leftrightarrow [1]_n = \alpha^k \cdot [1]_n \Leftrightarrow [1]_n = \alpha^k$$

Ora, se $\alpha \in \mathbb{Z}$, vale anche che:

$$[\alpha]_n^{\Phi(n)} = [1]_n \Rightarrow [\alpha^{\Phi(n)}]_n \Leftrightarrow \alpha^{\Phi(n)} \equiv 1 \pmod n$$

La tesi del teorema è quindi verificata. ■

Il Teorema di Fermat-Eulero viene usato per dimostrare il Teorema fondamentale della crittografia RSA.

Enunciato Teorema fondamentale della crittografia RSA: Siano $n, c \in \mathbb{N} \backslash 0$. Se $(c, \Phi(n)) = 1$ e $d > 0$ con $d \in [c]_{\Phi(n)}^{-1}$, allora la funzione $P_c : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*$, tale per cui $P_c(\beta) \mapsto \beta^c \ \forall \beta \in (\mathbb{Z}/n\mathbb{Z})^*$, è una funzione invertibile e vale:

$$(P_c)^{-1} = P_d$$

con $P_d : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*$ e tale che $P_d(\beta) = \beta^d \ \forall \beta \in (\mathbb{Z}/n\mathbb{Z})^*$.

Dim. Sia $\alpha \in (\mathbb{Z}/n\mathbb{Z})^*$. Devo dimostrare che $P_d\left(P_c(\alpha)\right) = \alpha$. Poiché $d \in [c]^{-1}_{\Phi(n)}$, vale:

$$c \cdot d \equiv 1 \pmod{n} \Leftrightarrow \Phi(n)|c \cdot d - 1 \Leftrightarrow \exists k \in \mathbb{Z}\ t.c.\ k \cdot \Phi(n) = c \cdot d - 1 \Leftrightarrow k \cdot \Phi(n) + 1 = c \cdot d$$

Osservo che, $k \cdot \Phi(n) = c \cdot d - 1$, ma per ipotesi $c, d > 0$, dunque $c \cdot d - 1 \geq 0$, inoltre $\Phi(n) > 0$, quindi anche $k \geq 0$. Per il Teorema di Fermat-Eulero $\alpha^k = [1]_n$, quindi vale:

$$P_d\left(P_c(\alpha)\right) = P_d\left(\alpha^c\right) = \left(\alpha^c\right)^d = \alpha^{c \cdot d} = \alpha^{1+k\cdot\Phi(n)} = \alpha \cdot \alpha^{k\cdot\Phi(n)} = \alpha \cdot \left(\alpha^{\Phi(n)}\right)^k = \alpha \cdot \left([1]_n\right)^k = \alpha$$

Dunque la tesi del teorema è dimostrata. ■

Il teorema appena dimostrato consente di utilizzare il metodo della crittografia RSA per crittografare e decriptare messaggi. Il metodo RSA funziona come segue:

Siano α il messaggio da trasmettere, M e D mittente e destinatario. Il valore c, detto chiave pubblica e noto a tutti, è utilizzato soltanto per crittografare i messaggi da M a D. Soltanto D conosce il valore d, detto chiave privata, necessario per decriptare tali messaggi. Al momento dell'invio M calcola $P_c(\alpha)$ e ne trasmette il risultato. D riceve $P_c(\alpha)$ e calcola $P_d\left(P_c(\alpha)\right)$.

Grazie al Teorema fondamentale della crittografia RSA, $P_d\left(P_c(\alpha)\right) = \alpha$, per cui D può leggere il messaggio.