Soluzioni degli esercizi della prova scritta di MD del 9 maggio 2011
Esercizi relativi al II semestre

<u>Es.</u> a) Si provi che dato $[a]_n \in \mathbf{Z}/n\mathbf{Z}$, esiste un intero positivo *r* tale che $([a]_n)^r = ([1]_n)$ in $\mathbf{Z}/n\mathbf{Z}$ se e solo se $[a]_n$ è un elemento invertibile rispetto al prodotto in $\mathbf{Z}/n\mathbf{Z}$

b) Tenendo conto di a) Si calcolino tutte le soluzioni $[x]_{10}$ dell'equazione $([2]_{10}+[x]_{10})^4 = [1]_{10}$ in $\mathbf{Z}/10\mathbf{Z}$.

(Sugg: si ricordino il teorema di Eulero, che si applica se e solo se un elemento di $\mathbf{Z}/n\mathbf{Z}$ è invertibile, con n=10 nel nostro caso, la funzione di Eulero Φ e, per la parte a), un teorema di teoria dei gruppi che abbiamo dimostrato a lezione, applicandolo poi al gruppo degli elementi invertibili di $\mathbf{Z}/n\mathbf{Z}$. In particolare $\Phi(10)$=.........)

<u>Soluzione</u>: a) Gli elementi invertibili di $\mathbf{Z}/n\mathbf{Z}$ formano un gruppo rispetto al prodotto. Per un teorema di teoria dei gruppi visto e dimostrato a lezione, se G è un gruppo con r elementi, allora per ogni $g \in G$ si ha $g^r=1$. In particolare ciò vale per gli elementi invertibili di $\mathbf{Z}/n\mathbf{Z}$. Viceversa da $([a]_n)^r=([1]_n)$ in $\mathbf{Z}/n\mathbf{Z}$, segue che, posto $[b]_n= ([a]_n)^{r-1}$, si ha, per l'ipotesi, $[a]_n[b]_n=[1]_n$ cioè $[b]_n$ è l'inverso di $[a]_n$ in $\mathbf{Z}/n\mathbf{Z}$.

b) Poiché $\Phi(10)=4$, numero degli elementi del gruppo degli elementi invertibili di $\mathbf{Z}/10\mathbf{Z}$, $([2]_{10}+[x]_{10})^4= [1]_{10}$ in $\mathbf{Z}/10\mathbf{Z}$ se e solo se $[2]_{10}+[x]_{10}$ è invertibile in $\mathbf{Z}/10\mathbf{Z}$ e ciò è vero se e solo se $[2+x]_{10}$ è invertibile in $\mathbf{Z}/10\mathbf{Z}$, il che equivale a dire che $2+x$ e 10 sono coprimi. Ciò implica che tutte e sole le soluzioni sono $[x]_{10}=[1]_{10}$, $[5]_{10}$, $[7]_{10}$, $[9]_{10}$.

<u>Es.</u> Si provi che esistono due numeri interi x e y tali che 35x+78y= 253654833.

<u>Soluzione</u>: si ha 35=7·5, 78=2·3·13 e dunque 35 e 78 sono coprimi. L'identità di Bezout ci dice che allora esistono due numeri interi m ed n tali che $1=35m+78n$. Poniamo a=253654833. Allora $a= a\cdot 1= = a\cdot(35m+78n)=35(am)+78(bn)$.
Dunque $x= am$ e $y= bn$ sono i due numeri richiesti.

<u>Es.</u> Si consideri il grafo completo pesato $G=(V,E)$ con 5 vertici a,b,c,d,e, ove il peso dei lati è rappresentato dalla seguente tabella:

	a	*b*	*c*	*d*	*e*
a	-	13	3	9	9
b		-	11	11	13
c			-	9	7
d				-	2
e					-

Si trovi un albero di supporto minimo per G calcolandone il peso totale. Tale albero di supporto minimo è unico?

<u>Soluzione:</u> Applicando l'algoritmo greedy a G, si trova che un albero di supporto minimo per G è dato dall'albero T=(V, $\{\{d,e\},\{e,c\}\{c,a\}\{c,b\}\}$, di peso totale 23. T non è unico poiché anche T'=(V, $\{\{d,e\},\{e,c\}\{c,a\}\{d,b\}\}$ ha peso totale 23.

<u>Es.</u> a) Sapendo che un albero finito con n vertici ha n-1 lati, si provi che un albero con almeno 2 vertici ha almeno 2 vertici di grado 1.
b) Si provi che ogni grafo finito con almeno due vertici ha almeno due vertici dello stesso grado (Sugg: Si ricordi il principio del pidgeon-hole).
<u>Soluzione:</u> a) Dalla formula $\sum_{v\in V}\delta(v)=2|E|=2(n-1)$ ove n è il numero dei vertici, in particolare ne segue che la sommatoria a sinistra ha n addendi tutti ≥ 1, dato che un albero non ha vertici isolati e dunque almeno due di tali addendi devono essere uguali ad 1.
b) E' evidente che è sufficiente dimostrare l'asserto per un grafo connesso con almeno due vertici. In tal caso l'applicazione $\delta: V \rightarrow \{1,\ldots,n-1\}$ che ad ogni vertice associa il suo grado, è una applicazione da un insieme con n elementi ad un insieme con n-1 elementi, e dunque non può essere iniettiva.

<u>Es.</u> Si provi che se $G=(V,E)$ è un grafo connesso con n vertici e n lati, $n \geq 3$ allora G possiede uno ed un solo circuito(ciclo)
<u>Soluzione:</u> Dato che ha più di n-1 lati, G non è un albero, G possiede almeno un ciclo (ricordiamo che un grafo connesso senza cicli è un albero). Inoltre, rimuovendo un lato di un ciclo da un grafo connesso, il grafo rimane connesso. Se esistessero due cicli distinti, potrei trovare un lato per ognuno dei due cicli in modo tale che, rimuovendo ambedue tali lati, il grafo rimanga connesso con n-2 lati, impossibile.

<u>Es.</u> Sia $G=(V,E)$ un grafo con numero cromatico $\chi(G)=n$. Ciò, come è noto, equivale a dire che esiste una funzione suriettiva c: $V \rightarrow \{1, \ldots, n\}$ tale che $c(v) \neq c(w)$ se $\{v,w\} \in E$. I sottoinsiemi di V $c^{-1}(i)$ costituiti dalle antiimmagini tramite la funzione c degli elementi di $\{1, \ldots, n\}$ costituiscono una partizione di V che permette di stabilire un ordine in V in modo tale che, applicando l'algoritmo greedy con i vertici in quell'ordine, l'algoritmo fornisce come risultato esattamente $\chi(G)$. Si descriva quale è un tale ordine dei vertici, spiegando perché tale ordine permette all'algoritmo greedy di fornire esattamente il numero cromatico.
<u>Soluzione:</u> Consideriamo i sottoinsiemi di V, che costituiscono una partizione di V, della forma $c^{-1}(i)=\{v_{ij} | j=1,\ldots,n_i=|c^{-1}(i)|\}$ per $i=1,\ldots. \chi(G)=n$. In questo modo ho scelto un ordine qualsiasi per i vertici di $c^{-1}(i)$. Poi ordino tutti i vertici prendendo prima quelli di $c^{-1}(1)$, poi quelli di $c^{-1}(2)$, e così via, fino a n. Utilizzando tale ordine dei vertici l'algoritmo greedy produce il numero cromatico. Basta ricordare il passo generico dell'algoritmo greedy.

<u>Es.</u> Si provi che almeno uno dei due grafi G e $\overline{G}$, il complementare di G, è connesso (Sugg.: se G non è connesso, si considerino le sue componenti connesse, e si sfrutti il fatto che ci sono almeno 2 componenti connesse. Se x e y sono due vertici, e si vuole costruire un cammino da x a y in $\overline{G}$, si consideri prima il caso in cui x e y siano vertici di due componenti connesse distinte di G, e successivamente il caso in cui x e y siano vertici della medesima componente connessa di G, sfruttando il caso precedente).

<u>Soluzione</u>: come indicato nel suggerimento, supponiamo G non connesso e siano x e y due vertici distinti. Se x e y stanno in due componenti connesse distinte di G, essi sono estremi di un lato di $\overline{G}$ per definizione di $\overline{G}$. Altrimenti x e y stanno nella stessa componente connessa di G. Sia z un vertice che sta in una componente connessa di G diversa da quella dove stanno x e y. Allora $\{x,z\}$ e $\{z,y\}$ sono due lati di $\overline{G}$, come nel caso precedente e $\{x,z\}\{z,y\}$ è un cammino da x a y in $\overline{G}$, che pertanto risulta connesso.