COGNOME NOME

CORSO DI LAUREA **INF** | **TWM** ANNO DI IMMATRICOLAZIONE

MATRICOLA

SCRITTO DI MATEMATICA DISCRETA, PRIMA PARTE
19 luglio 2011

Il compito è composto da due sezioni. Per superarlo bisogna rispondere in modo corretto ad almeno 8 domande della prima sezione ed ottenere la sufficienza nella seconda sezione. Le risposte sbagliate nella prima sezione influiscono negativamente sul voto complessivo. Compilate subito la parte anagrafica del compito. La durata della prova è di 3 ore.

PRIMA SEZIONE

Nota: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ indicano gli insiemi di numeri naturali, interi, razionali e reali, rispettivamente.

Per ciascuna delle seguenti affermazioni, indicare se è vera o falsa:

1. La funzione $f : \mathbb{N} \to \mathbb{R}$ definita da $f(n) = \sqrt{n}$ è suriettiva. **V** | **F** **F**
2. Esistono numeri complessi non nulli che non hanno inverso moltiplicativo. **V** | **F** **F**
3. La funzione $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \times \mathbb{Z}$ definita da $f(n, m) = (n, -m)$ è suriettiva. **V** | **F** **F**
4. La relazione binaria R definita su $\mathbb{Q}$ da

   $$qRq' \qquad \Leftrightarrow \qquad q - q' \geq 0$$

   è una relazione d'equivalenza. **V** | **F** **F**
5. La relazione d'equivalenza E definita sui numeri interi da

   $$aEb \qquad \Leftrightarrow \qquad 100 \text{ divide } a - b$$

   ha infinite classi d'equivalenza. **V** | **F** **F**
6. Dato un insieme A con n elementi, il numero dei suoi sottoinsiemi è uguale ad n^2. **V** | **F** **F**
7. Se a, b, c sono numeri interi e $MCD(a, b) = MCD(b, c) = 1$ allora MCD(a,c)=1 **V** | **F** **F**
8. L'insieme dei numeri complessi della forma $a + ib$ con $a, b \in \mathbb{Z}$ forma un gruppo rispetto alla somma. **V** | **F** **V**
9. Esistono funzioni biunivoche da $\mathbb{R}$ a $\mathbb{Q}$. **V** | **F** **F**
10. Il numero di strette di mano fra dieci persone è 10×9. **V** | **F** **F**

SECONDA PARTE

1. Dimostrare per induzione che per ogni $n \geq 1$ vale

$$\frac{1}{2^1} + \frac{2}{2^2} + \ldots + \frac{n}{2^n} = 2 - \frac{n+2}{2^n}.$$

La base dell'induzione è verificata in quanto $\frac{1}{2^1} = 2 - \frac{1+2}{2^1}$.

Per il passo induttivo, supponendo che

$$\frac{1}{2^1} + \frac{2}{2^2} + \ldots + \frac{n}{2^n} = 2 - \frac{n+2}{2^n}.$$

dobbiamo dimostrare che

$$\frac{1}{2^1} + \frac{2}{2^2} + \ldots + \frac{n}{2^n} + \frac{n+1}{2^{n+1}} = 2 - \frac{n+3}{2^{n+1}}.$$

Utilizzando l'ipotesi induttiva otteniamo:

$$\frac{1}{2^1} + \frac{2}{2^2} + \ldots + \frac{n}{2^n} + \frac{n+1}{2^{n+1}} = 2 - \frac{n+2}{2^n} + \frac{n+1}{2^{n+1}} = 2 - \frac{2(n+2)}{2^{n+1}} + \frac{n+1}{2^{n+1}} = 2 - \frac{(n+3)}{2^{n+1}}.$$

2. (a) Determinare se il numero 5 ha inverso moltiplicativo modulo 72 e in caso affermativo determinare tale inverso. Rispondere alla stessa domanda per quanto riguarda l'inverso additivo.

Poiché $MCD(5, 72) = 1$, il numero 5 ha inverso moltiplicativo modulo 72 e possiamo trovare questo inverso utilizzando l'algoritmo di Euclide:
$72 = 14 \times 5 + 2$;
$5 = 2 \times 2 + 1$;

L'ultimo resto non nullo è 1 e $1 = 5 - 2 \times 2 = 5 - 2 \times (72 - 14 \times 5) = 29 \times 5 - 2 \times 72$.

L'inverso moltiplicativo di 5 è quindi 29, modulo 72.

L'inverso additivo di 5 modulo 72 è $72 - 5 = 67$

(b) Trovare la chiave privata del codice RSA che ha per modulo il numero $m = 91$ e per chiave pubblica il numero 5.

Poiché $91 = 7 \times 13$ è prodotto di due primi, si ha $\phi(m) = 6 \times 12 = 72$. La chiave privata t è l'inverso di 5 modulo 72, che abbiamo calcolato nell'esercizio precedente: $t = 29$.

3. Trovare la forma trigonometrica del numero complesso

$$\frac{i}{1-i}$$

Per prima cosa possiamo notare che

$$\frac{i}{1-i} = \frac{i}{1-i} \times \frac{1+i}{1+i} = \frac{-1+i}{2} = \frac{1}{2}(i-1).$$

Il modulo di questo numero complesso è $|\frac{1}{2}(i-1)| = \frac{1}{2}|i-1| = \frac{\sqrt{2}}{2}$, mentre l'argomento è lo stesso di $(i-1)$ e cioè $\frac{3}{4}\pi$. La forma trigonometrica richiesta è quindi

$$\frac{\sqrt{2}}{2}(cos(\frac{3}{4}\pi) + isen(\frac{3}{4}\pi)).$$

4. Sia A l'insieme delle funzioni f con dominio e codominio uguale all'insieme dei numeri naturali. Si consideri la seguente relazione binaria E sull'insieme A

$$fEg \quad \Leftrightarrow \quad f(0)+f(1)=g(0)+g(1).$$

(a) Provare che E è una relazione di equivalenza.

E è riflessiva: se $f \in A$ abbiamo fEf poiché $f(0)+f(1)=f(0)+f(1)$.
E è simmetrica : se $f,g \in A$ e fEg allora $f(0)+f(1)=g(0)+g(1)$ e quindi anche $g(0)+g(1)=f(0)+f(1)$. Ne segue gEf.
E è transitiva : se $f,g,h \in A$ e fEg, gEh allora $f(0)+f(1)=g(0)+g(1)$ e $g(0)+g(1)=h(0)+h(1)$. Ne segue $f(0)+f(1)=h(0)+h(1)$ e quindi fEh.

(b) Determinare la classe d'equivalenza della funzione $f : \mathbb{N} \to \mathbb{N}$ definita da $f(n)=n+1$. Descrivere almeno tre elementi diversi in questa classe.

$$[f]_E=\{g \in A : fEg\}=\{g \in A : f(0)+f(1)=g(0)=g(1)\}=\{g \in A : 1+2=g(0)+g(1)\}=$$

$$=\{g \in A : g(0)+g(1)=3\}.$$

Inoltre siano g,h le funzioni definite da $g(0)=1, g(1)=2$ e $g(n)=3$, per ogni $n \geq 3$ e $h(0)=1, h(1)=2$ e $h(n)=4$, per ogni $n \geq 3$. Le funzioni f,g,h e appartengono alla classe di equivalenza della funzione f.

(c) Stabilire se l'insieme

$$X=\{f : \ f \text{ è una funzione costante}\}$$

è un insieme di rappresentanti per le classi d'equivalenza di E su A, giustificando adeguatamente la risposta.

L'insieme X non è un insieme di rappresentanti. Infatti se $f \in X$ allora $f(0)-f(1)=0$ e due elementi qualsiasi di X sono in relazione tramite E: l'insieme X è quindi contenuto in una singola classe di E su A. Visto che E ha più di una classe d'equivalenza, l'insieme X non può essere un insieme di rappresentanti per le classi di E su A.