ALGEBRA 1 — Primo esonero.
SOLUZIONI COMPITO A.
16 Aprile 2011

(1) Determinare la cardinalità dei seguenti insiemi:
- $A = \{(x, y) \in (\mathbb{R} \setminus \mathbb{Q}) \times (\mathbb{R} \setminus \mathbb{Q}) \,|\, x/y \in \mathbb{Q}\}$,
- $B = \{f : \mathbb{N} \to \mathbb{N} \,|\, f$ è invertibile e $f(n) = n$ per n sufficientemente grande$\}$.

Svolgimento. $A \subset (\mathbb{R} \setminus \mathbb{Q}) \times (\mathbb{R} \setminus \mathbb{Q}) \subset \mathbb{R} \times \mathbb{R}$, quindi $|A| \leq |\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$.
D'altronde la seguente applicazione

$$\begin{array}{rccc} \phi: & \mathbb{R} \setminus \mathbb{Q} & \longrightarrow & A \\ & r & \longmapsto & (r, r) \end{array}$$

è iniettiva, dunque $|A| \geq |\mathbb{R} \setminus \mathbb{Q}| = |\mathbb{R}|$. In conclusione $|A| = |\mathbb{R}|$.

Per definizione $B = \cup_{n \in \mathbb{N}} B_n$, dove

$$B_n = \{f : \mathbb{N} \to \mathbb{N} \,|\, f(\{0, \ldots, n\}) = \{0, \ldots, n\}, \;\; f_{|\{0,\ldots,n\}} \text{è invertibile e } f(j) = j \;\; \forall\, j > n\}.$$

Per ogni $n \in \mathbb{N}$, B_n è un insieme finito (essendo $|B_n| = n!$), quindi $|B| \leq |\mathbb{N}|$. Si osservi che non essendo gli insiemi B_n mutuamente disgiunti non si può concludere direttamente che $|B| = |\mathbb{N}|$.
D'altronde, per ogni $n \in \mathbb{N}$, la funzione

$$\begin{array}{rccc} g_n: & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & j & \longmapsto & \begin{cases} n & \text{se } j = 0 \\ 0 & \text{se } j = n \\ j & \text{se } j \neq 0, n \end{cases} \end{array}$$

appartiene a B; dunque, essendo $g_n \neq g_m$ (per $n \neq m$), l'insieme B è infinito, cioè $|B| \geq |\mathbb{N}|$. Abbiamo così provato che $|B| = |\mathbb{N}|$.

(2) Si definisca una relazione sull'insieme delle parti $P(X)$ di un insieme (infinito) X ponendo $A \mathcal{R} B$ se $A \setminus B$ e $B \setminus A$ sono entrambi finiti. Si dica se $\mathcal{R}$ è riflessiva, simmetrica, antisimmetrica, transitiva. *[Ricordiamo che la* differenza insiemistica di due insiemi U e V*, denotata $U \setminus V$, è l'insieme di tutti gli elementi di U che non appartengono a V.]*

Svolgimento.
***Proprietà riflessiva*:** SI
Per ogni $A \in P(X)$, $A \setminus A =$ finito $\Rightarrow \quad A \mathcal{R} A$;
***Proprietà simmetrica*:** SI
Siano $A, B \in P(X)$. Se $A \mathcal{R} B \quad \Rightarrow \quad A \setminus B$ e $B \setminus A$ sono finiti $\Rightarrow \quad B \mathcal{R} A$;
***Proprietà antisimmetrica*:** NO
Sia $x \in X$ e siano $A = \{x\}$ e $B = \emptyset$. Allora $A \setminus B = \{x\}$ e $B \setminus A = \emptyset$ sono entrambi finiti $\Rightarrow \quad A \mathcal{R} B$ e $B \mathcal{R} A$ ma $A \neq B$;
***Proprietà transitiva*:** SI
Siano $A, B, C \in P(X)$. Se $A \mathcal{R} B$ e $B \mathcal{R} C$ allora $A \setminus B$, $B \setminus A$, $B \setminus C$ e $C \setminus B$ sono finiti.

Poiché $A \setminus C \subset (A \setminus B) \cup (B \setminus C)$ e $C \setminus A \subset (C \setminus B) \cup (B \setminus A)$ si ha che anche $A \setminus C$ e $C \setminus A$ sono finiti, quindi $A \mathcal{R} C$.

(3) Si dimostri, per induzione su N, che

$$\sum_{n=1}^{N} \frac{1}{n^2} \leq 2 - \frac{1}{N}. \qquad (P_N)$$

Svolgimento.
N = 1: (P_1) è vera sse $\frac{1}{1} \leq 2 - \frac{1}{1}$ (cioè $1 \leq 1$), quindi (P_1) è vera.
sia $N \geq 2$, supponiamo $(\mathbf{P_{N-1}})$ vera, dimostriamo $(\mathbf{P_N})$ vera:

$$\sum_{n=1}^{N} \frac{1}{n^2} = \sum_{n=1}^{N-1} \frac{1}{n^2} + \frac{1}{N^2} \overset{(P_{N-1})}{\leq} 2 - \frac{1}{N-1} + \frac{1}{N^2};$$

quindi per provare che (P_N) è verificata basta mostrare che $-\frac{1}{N-1} + \frac{1}{N^2} \leq -\frac{1}{N}$. Quest'ultima disuguaglianza si verifica immediatamente in quanto:

$$-\frac{1}{N-1} + \frac{1}{N^2} \leq -\frac{1}{N} \quad \Leftrightarrow \quad \frac{-1}{(N-1)N^2} \leq 0 \text{ che è vera per ogni } N \geq 2.$$

(4) Decidere, giustificando la risposta, se le seguenti affermazioni siano vere o false:
(i). Se $d \in \mathbb{Z}$ è della forma $ha + kb$, con $a, b, h, k \in \mathbb{Z}$, allora $d = \mathrm{MCD}(a, b)$.
(ii). Se $a, b, c, d \in \mathbb{Z}$, allora $\mathrm{MCD}(ab, cd) = \mathrm{MCD}(a, c)\,\mathrm{MCD}(b, d)$.
(iii). $x^4 + y^4 = (x + y)^4$ per ogni scelta di $x, y \in \mathbb{Z}/(4)$ (che è la stessa cosa di $\mathbb{Z}_4$).
(iv). L'unione di due relazioni di equivalenza è ancora una relazione di equivalenza. *[Abbiamo utilizzato qui la seguente definizione. Se ρ e σ sono relazioni sull'insieme X, la loro* unione *è la relazione $\mathcal{R}$ definita da*

$$a \mathcal{R} b \Leftrightarrow \textit{ almeno una tra } a\rho b \textit{ e } a\sigma b \textit{ è vera}.$$

Equivalentemente, l'unione di due relazioni è definita dal sottoinsieme di $X \times X$ dato dall'unione dei sottoinsiemi che definiscono ρ e σ.]

Svolgimento.
(i). FALSA. Controesempio: $a = b = k = 1$, $h = 2 \Rightarrow d = 3$ mentre $\mathrm{MCD}(a, b) = 1$.
(ii). FALSA. Controesempio: $a = 2$, $b = 6$, $c = 4$, $d = 3 \Rightarrow \mathrm{MCD}(ab, cd) = 12$ mentre $\mathrm{MCD}(a, c)\,\mathrm{MCD}(b, d) = 2 \cdot 3 = 6$.
(iii). FALSA. Controesempio: $x = y = \bar{1} \Rightarrow x^4 + y^4 = \bar{2}$ mentre $(x + y)^4 = 0$ in $\mathbb{Z}_4$.
(iv). FALSA. Controesempio: sia $U = \{\text{esseri umani}\}$ e definiamo su U le seguenti relazioni di equivalenza ρ e σ:
per $a, b \in U$

$$a \,\rho\, b \quad \Leftrightarrow \quad a \text{ e } b \text{ sono nati nello stesso secolo,}$$
$$a \,\sigma\, b \quad \Leftrightarrow \quad a \text{ e } b \text{ sono dello stesso sesso.}$$

La relazione unione $\mathcal{R}$ non è transitiva in quanto

$$\text{Francesca De Marchis} \quad \mathcal{R} \quad \text{Jacopo Gandini} \quad \text{(essendo FDM } \rho \text{ JG)}$$
$$\text{Jacopo Gandini} \quad \mathcal{R} \quad \text{Albert Einstein} \quad \text{(essendo JG } \sigma \text{ AE)}$$

mentre

$$\text{Francesca De Marchis } \mathcal{R} \text{ Albert Einstein} \quad \text{(in quanto FDM } \not\rho \text{ AE e FDM } \not\sigma \text{ AE)}$$

(5) Si trovino tutte le soluzioni intere del sistema di congruenze lineari

$$\begin{cases} x \equiv & 13^{190} & \mod 35 \\ 4x \equiv & 8 & \mod 6 \end{cases}$$

Svolgimento. Applicando il teorema cinema dei resti nella seconda formulazione alla prima equazione ($35 = 5 \cdot 7$, $\mathrm{MCD}(5,7) = 1$) e semplificando la seconda equazione, il sistema risulta equivalente al seguente:

$$(*) \qquad \begin{cases} x \equiv & 13^{190} & \mod 5 \\ x \equiv & 13^{190} & \mod 7 \\ 2x \equiv & 4 & \mod 3. \end{cases}$$

La prima equazione di $(*)$ si può semplificare nel seguente modo:

$$\begin{aligned} x &\equiv 3^{190} && \mod 5 && \text{(essendo } 13 \equiv 3 \mod 5) \\ x &\equiv 3^{\varphi(5)\cdot 47+2} && \mod 5 && \text{(essendo } \varphi(5) = 4) \\ x &\equiv 3^2 && \mod 5 && \text{(per il teorema di Eulero-Fermat)} \\ x &\equiv 4 && \mod 5 && \text{(essendo } 3^2 \equiv 4 \mod 5) \end{aligned}$$

La seconda equazione di $(*)$, osservando che $13 \equiv 1 \mod 7$, equivale a $x \equiv (-1)^{190} \mod 7$ e cioè a

$$x \equiv 1 \mod 7$$

Infine la terza equazione di $(*)$, essendo $2 \cdot 2 \equiv 1 \mod 4$ ed essendo $8 \equiv 2 \mod 3$, si può riscrivere come

$$x \equiv 2 \mod 3$$

Il sistema da risolvere è in conclusione

$$(\#) \qquad \begin{cases} x \equiv & 4 & \mod 5 \\ x \equiv & 1 & \mod 7 \\ x \equiv & 2 & \mod 3. \end{cases}$$

Una soluzione del sistema $(\#)$ (che è un sistema cinese in forma normale) è 29, quindi l'insieme delle soluzioni è

$$S = \{29 + 105z \mid z \in \mathbb{Z}\}$$

dove $105 = 3 \cdot 5 \cdot 7$.