Algebra 1

Proff. E. Spinelli

Primo Esonero - Compito B

22 Aprile 2016

Nome e Cognome: ____________________

Numero di Matricola: ____________________

Esercizio	Punti totali	Punteggio
1	6	
2	6	
3	6	
4	6	
5	6	
Totale	30	

ATTENZIONE:
- I COMPITI DISORDINATI O POCO LEGGIBILI NON SARANNO NEANCHE CORRETTI
- **GIUSTIFICATE LE VOSTRE ARGOMENTAZIONI**
- SCRIVETE LE RISPOSTE NEGLI APPOSITI RIQUADRI
- I FOGLI DI BRUTTA NON SARANNO ACCETTATI
- TUTTI I DISPOSITIVI ELETTRONICI (CALCOLATRICI, SMARTPHONES, TABLETS, TELEFONINI ETC ...) DEVONO ESSERE SPENTI E IN BORSA
- NON SONO AMMESSI LIBRI O APPUNTI.

Esercizio 1. Determinare la cardinalità dei seguenti insiemi:

(a) $S := \{\alpha \mid \alpha \in \mathbb{R}\,,\ \alpha = 11^n 13^m \text{ per qualche } m, n \in \mathbb{N}\}$

(b) $T := \{n \mid n \in \mathbb{R}\,,\ n = x^3 \text{ per qualche } x \in \mathbb{Z}\}$

(c) $U := \{(x, y) \mid (x, y) \in \mathbb{R}^2\,,\ x^2 - y^2 \in \mathbb{Q}\}$

(d) $V := \mathcal{P}_{\text{fin}}(\mathbb{P})$, dove $\mathcal{P}_{\text{fin}}(\mathbb{P})$ denota le parti finite dell'insieme $\mathbb{P}$ dei numeri primi.

Soluzione: (a) Osserviamo subito che $S \subseteq \mathbb{N}$. Inoltre, per il Teorema fondamentale dell'Aritmetica, la funzione

$$f : \mathbb{N} \times \mathbb{N} \longrightarrow S, \qquad (n, m) \longmapsto 11^n 13^m$$

è iniettiva. Pertanto $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}| \leq |S| \leq |\mathbb{N}|$. Dunque S è numerabile.

(b) Ovviamente $T \subseteq \mathbb{Z}$, quindi $|T| \leq |\mathbb{Z}| = |\mathbb{N}|$. Inoltre la funzione reale di variabile reale $y = k^3$ è biettiva. Pertanto la sua restrizione a $\mathbb{Z}$ è iniettiva. Dunque $|\mathbb{Z}| \leq |T|$ e pertanto T è numerabile.

(c) Vale che $U \subseteq \mathbb{R} \times \mathbb{R}$ e quindi $|U| \leq |\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$. Ora l'insieme $H := \{(x, x) \mid x \in \mathbb{R}\}$ è contenuto in U ed è equipotente a $\mathbb{R}$. Ne segue che $|\mathbb{R}| = |H| \leq |U|$ e dunque U ha la potenza del continuo.

(d) Consideriamo la funzione

$$g : \mathbb{N} \setminus \{0, 1\} \longrightarrow V, \qquad n \longmapsto \{p_1, \ldots, p_t\}$$

dove $p_1, \ldots, p_t$ sono i numeri primi distinti che compaiono nella decomposizione in fattori primi di n. La funzione g è chiaramente suriettiva, quindi $|V| \leq |\mathbb{N} \setminus \{0, 1\}| = |\mathbb{N}|$.

Ma $\mathbb{P}$ è un insieme numerabile, quindi $\{\{p\} \mid p \in \mathbb{P}\}$ è un sottinsieme di V infinito. Pertanto V è numerabile.

Risposta:

(a) Card(S)= $\boxed{|\mathbb{N}|}$ (b) Card(T)= $\boxed{|\mathbb{N}|}$ (c) Card(U)= $\boxed{|\mathbb{R}|}$ (d) Card (V)= $\boxed{|\mathbb{N}|}$

Esercizio 2.

(a) Per ogni $n \in \mathbb{N}$, $n \geq 1$, determinare $\mathrm{mcd}(n, n^2 - n)$.

(b) Per ogni $n \in \mathbb{N}$ tale che 11 non divida n verificare che $n^{10} - 10^{2n} \equiv_{11} 0$.

Soluzione: (a) Ovviamente n divide n e $n^2 - n$. Inoltre ogni divisore comune di n e $n^2 - n$ è al più n. Pertanto $\mathrm{mcd}(n, n^2 - n) = n$.

(b) Poichè 11 non divide n, $\mathrm{mcd}(11, n) = 1$. Per Fermat, $n^{\phi(11)} = n^{10} \equiv_{11} 1$.
Ora $10 \equiv_{11} -1$ e quindi $(10^2)^n \equiv_{11} ((-1)^2)^n \equiv_{11} 1$.
Pertanto $n^{10} - 10^{2n} \equiv_{11} 1 - 1 \equiv_{11} 0$.

Risposta:

(a) $\mathrm{mcd}(n, n^2 - n) = \boxed{n}$

Esercizio 3. Sia $\mathbb{N}^* := \mathbb{N} \setminus \{0\}$ e si consideri su $\mathbb{N}^* \times \mathbb{N}^*$ la seguente relazione ρ:

$$(x, y)\, \rho\, (x', y') \iff (x + y) \operatorname{mcd}(x', y') = (x' + y') \operatorname{mcd}(x, y).$$

(a) Verificare che ρ è una relazione di equivalenza su $\mathbb{N}^* \times \mathbb{N}^*$.

(b) Dimostrare che $\mathbb{N}^* \times \mathbb{N}^*/\rho$ è equipotente a $A := \{n \,|\, n \in \mathbb{N},\ n \geq 2\}$ determinando una biezione $\bar{f} : \mathbb{N}^* \times \mathbb{N}^*/\rho \to A$.

Soluzione: Consideriamo la funzione

$$f : \mathbb{N}^* \times \mathbb{N}^* \longrightarrow \mathbb{N}^*, \qquad (x, y) \longmapsto \frac{x + y}{\operatorname{mcd}(x, y)}.$$

Proviamo che $f(\mathbb{N}^* \times \mathbb{N}^*) \subseteq A$. Infatti, supponiamo che esista $(x, y) \in \mathbb{N}^* \times \mathbb{N}^*$ tale che $f(x, y) = 1$. Allora $x + y = \operatorname{mcd}(x, y) \leq x < x + y$, il che è una contraddizione.

Proviamo ora che l'equivalenza data mediante l'uguaglianza delle immagini ρ_f coincide con ρ. A tal fine, siano $(x, y), (x', y') \in \mathbb{N}^* \times \mathbb{N}^*$. Vale che

$$\begin{aligned} (x, y)\, \rho_f\, (x', y') &\iff \frac{x + y}{\operatorname{mcd}(x, y)} = \frac{x' + y'}{\operatorname{mcd}(x', y')} \iff (x + y) \operatorname{mcd}(x', y') = (x' + y') \operatorname{mcd}(x, y) \\ &\iff (x, y)\, \rho\, (x', y'). \end{aligned}$$

Essendo ρ_f una relazione d'equivalenza, abbiamo provato che ρ è una relazione d'equivalenza.

Per il Teorema fondamentale delle applicazioni si ha che $\mathbb{N}^* \times \mathbb{N}^*/\rho = \mathbb{N}^* \times \mathbb{N}^*/\rho_f$ è equipotente a $f(\mathbb{N}^* \times \mathbb{N}^*)$. A questo punto, basta provare che $f(\mathbb{N}^* \times \mathbb{N}^*) = A$. Consideriamo allora $n \in A$. L'elemento $(n^2 - n, n) \in \mathbb{N}^* \times \mathbb{N}^*$ e

$$f(n^2 - n, n) = \frac{n^2 - n + n}{\operatorname{mcd}(n^2 - n, n)} = n.$$

Ancora per il Teorema fondamentale e la sua dimostrazione la funzione $\bar{f}$ è la seguente:

$$\bar{f} : \mathbb{N}^* \times \mathbb{N}^*/\rho \longrightarrow A, \qquad [(x, y)]_\rho \longmapsto f(x, y).$$

Risposta:

Esercizio 4.

(a). Semplificando il sistema attraverso l'utilizzo di metodi elementari, determinare per quali $a, b \in \mathbb{Z}$ esso ammette soluzioni:

$$\begin{cases} aX \equiv 4 \mod 7 \\ 7^{290715}X \equiv b \mod 14 \end{cases}$$

(b). Determinare le soluzioni del sistema

$$\begin{cases} 3^{330033030303033003030}X \equiv 4 \mod 7 \\ 7X - 21 \equiv 7 \mod 14 \end{cases}$$

Soluzione: (a) Osserviamo subito che, per ogni $n \geq 1$, $7^n \equiv_{14} 7$ (si procede per induzione osservando che $7^2 = 49 \equiv_{14} 7$). Pertanto la seconda equazione diventa $7X \equiv_{14} b$ che ha soluzione quando $\operatorname{mcd}(7, 14) = 7$ divide b. In tal caso l'equazione si riduce a $X \equiv_2 b'$.

Essendo $\operatorname{mcd}(2, 7) = 1$, il sistema ammette soluzioni quando la prima equazione ammette soluzioni, ovvero quando $\operatorname{mcd}(a, 7)$ divide 4. Essendo 7 un numero primo, questo implica che a deve essere coprimo con 7.

In conclusione il sistema ha soluzione quando $b \in \mathbb{Z}7$ e a è coprimo con 7.

(b) Osserviamo che $3^3 = 27 \equiv_7 -1$. Dunque la prima equazione del sistema è $X \equiv_7 4$, mentre la seconda è $X \equiv_2 0$. Per il Teorema cinese dei resti, l'insieme delle soluzioni è dunque $[4]_{\equiv_{14}}$.

Risposta:

(a) Il sistema ammette soluzioni per: | |
|---|

Esercizio 5. Sia G un gruppo, $f : G \to G$ un endomomorfismo di G e H un sottogruppo di G.

(a) Verificare che, per ogni $a, b \in G$ se $ab = ba$, allora $a^{-1}b = ba^{-1}$.

(b) Verificare che
$$K := \{x \,|\, x \in G,\ f(xh) = f(hx)\ \forall h \in H\}$$
è un sottogruppo di G.

(c) *Facoltativo.* Dire se vale che se H è normale in G allora K è normale in G.

Soluzione: (a) Siano $a, b \in G$ tali che $ab = ba$. Allora $b = a^{-1}ab = a^{-1}ba$. Dunque $ba^{-1} = a^{-1}baa^{-1} = a^{-1}b$.

(b) K è non vuoto poichè $1_G \in K$ (infatti $f(1_G h) = f(h) = f(h1_G)$ per ogni $h \in H$).

Siano ora $x, y \in K$ e $h \in H$. Voglio provare che $xy^{-1} \in K$, ovvero $f(xy^{-1}h) = f(hxy^{-1})$. Poichè f è un omomorfismo,
$$f(xy^{-1}h) = f(x)f(y^{-1}h) = f(x)f(y^{-1})f(h) = f(x)f(y)^{-1}f(h).$$
Essendo $y \in K$, $f(y)f(h) = f(h)f(y)$ e, per (a), anche $f(y)^{-1}$ commuta con $f(h)$. Pertanto, sfruttando che anche $x \in K$, si ha
$$f(xy^{-1}h) = f(x)f(h)f(y)^{-1} = f(x)f(h)f(y^{-1}) = f(xh)f(y^{-1}) = f(hx)f(y^{-1}) = f(hxy^{-1}).$$

(c) Siano $x \in K$, $h \in H$ e $g \in G$. Voglio provare che K è normale in G, ovvero $f(g^{-1}xgh) = f(hg^{-1}xg)$. A tal fine,
$$f(g^{-1}xgh) = f(g^{-1}xghg^{-1}g) = f(g^{-1}x(ghg^{-1})g).$$
Ma $ghg^{-1} \in H$ dato che H è normale in G. Dunque
$$f(g^{-1}xgh) = f(g^{-1})f(ghg^{-1})f(x)f(g) = f(hg^{-1}xg).$$