ALGEBRA I: QUARTA ESERCITAZIONE
13 aprile 2011 Soluzione degli esercizi

Esercizio 1. Sia n un intero, $\phi(n)$ il valore della sua funzione di Eulero.
Dimostrare che $\phi(n) = \frac{n}{3}$ se e solo se $n = 2^h 3^k$, $h, k \geq 1$.

Soluzione. Sia $n = 2^h 3^k$ con $h, k \geq 1$. Allora $\phi(n) = \phi(2^h)\phi(3^k) = 2^{h-1}3^{k-1}2 = 2^h 3^{k-1}$, che è proprio $\frac{n}{3}$.

Viceversa, se $n = p_1^{a_1} \dots p_r^{a_r}$ è la fattorizzazione di n in primi, allora, imponendo che $3\phi(n) = p_1^{a_1} \dots p_r^{a_r}$, otteniamo $3(p_1 - 1) \dots (p_r - 1) = p_1 \dots p_r$, quindi necessariamente uno dei primi è 3, da cui $3 \cdot 2(p_2 - 1) \dots (p_r - 1) = 3p_2 \dots p_r$. Quindi c'è un altro primo $p_2 = 2$ e gli altri non ci sono, ovvero $s = 2$ ed n è della forma cercata. □

Esercizio 2. Dimostrare che ogni numero primo $p \neq 2, 3, 5$ divide $\underbrace{11..1}_{p-1}$.

(*Suggerimento: applicare il piccolo teorema di Fermat con un opportuno $a \in \mathbb{N}$, tale che $(a, p) = 1$ per ogni primo $p \neq 2, 3, 5$*)

Soluzione. Sia p un numero primo diverso da $2, 3$ e 5. Dunque $(10, p) = 1$, quindi applicando il piccolo Teorema di Fermat otteniamo:

$$10^{p-1} \equiv 1 \mod p.$$

Quindi $10^{p-1} - 1 \equiv 0 \mod p$, cioè $\underbrace{99..9}_{p-1} \equiv 0 \mod p$. Questo implica che $p | \underbrace{99..9}_{p-1}$, ma, essendo $\underbrace{99..9}_{p-1} = 9 \cdot \underbrace{11..1}_{p-1}$ ed essendo p primo, $p|9$ o $p|\underbrace{11..1}_{p-1}$.
Siccome per ipotesi $p \neq 3$, allora $p \not| 9$, quindi si ha $p|\underbrace{11..1}_{p-1}$. □

Esercizio 3. Trovare tutte le soluzioni intere del sistema

$$\begin{cases} X \equiv 1472^{3453} \mod 20 \\ X \equiv 219^{45} \mod 23. \end{cases}$$

Soluzione. Iniziamo portando il sistema ad una forma più ragionevole. Per quanto riguarda la seconda equazione, 219 è primo con 23 e più precisamente abbiamo $219 \equiv 12 \mod 23$. Poichè $\phi(23) = 22$, otteniamo

$$219^{45} \equiv 12^{2 \cdot 22 + 1} \equiv 12 \mod 23.$$

La seconda equazione è quindi equivalente a $x \equiv 12 \mod 23$.

Per calcolare 1472^{3453}, osserviamo innanzitutto che 1472 non è primo con 20. Possiamo calcolare il risultato riducendo modulo 4 e modulo 5, e poi ricomponendo facendo uso del teorema cinese del resto. Poichè 1472 è pari, la potenza 1472^{3453} è sicuramente multipla di 4. Invece, ricordando che $\phi(5) = 4$, si ha: $1472^{3453} \equiv 2^{863 \cdot 4 + 1} \equiv 2 \mod 5$, pertanto

$$\begin{cases} 1472^{3453} \equiv 0 \mod 4 \\ 1472^{3453} \equiv 2 \mod 5 \end{cases}$$

e di conseguenza $X \equiv 12 \mod 20$. Il sistema da risolvere è, in conclusione:

$$\begin{cases} X \equiv 12 \mod 20 \\ X \equiv 12 \mod 23 \end{cases}$$

e a questo punto possiamo concludere, anche senza fare i conti, che $X \equiv 12 \mod 460$. □

Esercizio 4. Osserviamo che, per ogni $m \in \mathbb{N}^*$, $\mathbb{Z}_m \setminus \{\bar{0}\} = \mathcal{U}(\mathbb{Z}_m) \cup \{\text{divisori dello zero di } \mathbb{Z}_m\}$. Mostrare con almeno due esempi che, se $(A, +, \cdot)$ è un anello, l'inclusione

$$A \setminus \{0\} \supset \mathcal{U}(A) \cup \{\text{divisori dello zero di } A\}.$$

può essere stretta.

Soluzione. Un esempio è $(\mathbb{Z}, +, \cdot)$, infatti in $\mathbb{Z}$ non ci sono divisori dello zero, mentre gli elementi invertibili in $\mathbb{Z}$ sono solo ± 1. Quindi

$$\mathcal{U}(\mathbb{Z}) \cup \{\text{divisori dello zero di } \mathbb{Z}\} = \{\pm 1\} \subsetneq \mathbb{Z}.$$

Un altro esempio è l'anello $(\mathcal{M}_{2,2}(\mathbb{Z}), +, \cdot)$, delle matrici 2×2 a entrate in $\mathbb{Z}$. Infatti la matrice diagonale $M := \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \in \mathcal{M}_{2,2}(\mathbb{Z})$ è invertibile in $\mathcal{M}_{2,2}(\mathbb{R})$ e il suo inverso (che è unico in $\mathcal{M}_{2,2}(\mathbb{R})$) è $N := \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$. Ma $N \notin \mathcal{M}_{2,2}(\mathbb{Z})$, quindi M non è invertibile in $\mathcal{M}_{2,2}(\mathbb{Z})$. D'altronde, essendo $\det(M) = 4 \neq 0$, per ogni matrice $B \neq 0$ $M \cdot B \neq 0$; quindi M non è un divisore dello zero. Abbiamo così dimostrato che

$$\mathcal{U}(\mathcal{M}_{2,2}(\mathbb{Z})) \cup \{\text{divisori dello zero di } \mathcal{M}_{2,2}(\mathbb{Z})\} \subsetneq \mathcal{M}_{2,2}(\mathbb{Z}). \qquad \square$$

Esercizio 5. Si consideri l'applicazione

$$\begin{array}{rccc} g: & \mathbb{Z}^2 & \longrightarrow & \mathbb{Z} \\ & (a,b) & \longmapsto & 8a + 6b. \end{array}$$

i. Dire se g è iniettiva e/o suriettiva.

ii. Determinare $Im(g)$.

iii. Determinare $g^{-1}(5)$ e $g^{-1}(6)$ e le rispettive cardinalità.

Soluzione. *i.* La funzione g non è iniettiva: si ha, ad esempio, $g(-3,4) = g(-9,12) = 0$.
La funzione g non è neanche suriettiva: si ha ad esempio $f^{-1}(1) = \emptyset$, infatti $8a + 6b$ è sempre multplo di $2 (= MCD(8,6))$, e dunque non possono esistere $a, b \in \mathbb{Z}$ tali che $8a + 6b = 1$.
ii. L'equazione $8a + 6b = c$ ha soluzioni se e solo se c è un multiplo di $MCD(8,6) = 2$. Dunque

$$Im(g) \stackrel{def}{=} g(\mathbb{Z}^2) = 2\mathbb{Z} = \{2k : k \in \mathbb{Z}\}.$$

iii. Poichè 5 non è multiplo di 2, si ha $g^{-1}(5) = \emptyset$, quindi $|g^{-1}(5)| = 0$.
Invece determinare $g^{-1}(6)$ vuol dire risolvere l'equazione

$$8a + 6b = 6.$$

Questa è equivalente a $4a + 3b = 3$. Una soluzione particolare è $(a,b) = (0,1)$ (se non la si trova a occhio, si deve risolvere l'equazione diofantea). Per determinare tutte le soluzioni, basta sommare a questa la generica soluzione dell'equazione omogenea associata $4a + 3b = 0$, cioè $4a = -3b$. Le soluzioni di questa sono $(a,b) = (3k, -4k)$, con $k \in \mathbb{Z}$.
Dunque

$$g^{-1}(6) = \{(3k, 1 - 4k) \,|\, k \in \mathbb{Z}\}.$$

Osserviamo che $g^{-1}(6) \subset \mathbb{Z}^2$ (con $|\mathbb{Z}^2| = |\mathbb{N}|$) e che $g^{-1}(6)$ è infinito, quindi possiamo dedurre che $|g^{-1}(6)| = |\mathbb{N}|$.

Esercizio 6. Verificare che l'insieme delle funzioni reali di variabile reale ha cardinalità superiore a quella del continuo.

Soluzione. Per il Teorema di Cantor $|\mathbb{R}| < |\mathcal{P}(\mathbb{R})| = |\{0,1\}^{\mathbb{R}}|$. Inoltre, essendo $\{0,1\} \subset \mathbb{R}$, ogni elemento di $\{0,1\}^{\mathbb{R}}$ (cioè ogni funzione da $\mathbb{R}$ in $\{0,1\}$) appartiene anche ad X, quindi $\{0,1\}^{\mathbb{R}} \subset X$. Abbiamo così dimostrato che $|\{0,1\}^{\mathbb{R}}| \leq |X|$, quindi $|X| > |\mathbb{R}|$. $\square$