Corso di Laurea in Matematica 2014-2015
compito prova di ALGEBRA I – Soluzioni

Esercizio 1. *Si provi che per ogni* $2 \leq n \in \mathbb{N}$ *vale l'identità:*

$$6 \cdot \sum_{i=2}^{n} \binom{i}{2} = (n-1)n(n+1).$$

Soluzione. Procediamo per induzione su $n \geq 2$. Per $n = 2$ l'identità è soddisfatta, infatti:

$$6 \cdot \sum_{i=2}^{n} \binom{i}{2} = 6\binom{2}{2} = 6 = (2-1)2(2+1).$$

Sia $n \geq 3$ e assumiamo la proprietà vera per $n-1$. Allora per l'ipotesi induttiva

$$6 \cdot \sum_{i=2}^{n} \binom{i}{2} = 6\binom{n}{2} + 6 \cdot \sum_{i=2}^{n-1} \binom{i}{2} = \binom{n}{2} + (n-2)(n-1)n,$$

quindi

$$6 \cdot \sum_{i=2}^{n} \binom{i}{2} = 3n(n-1) + (n-2)(n-1)n = (n-1)n(n+1).$$

Per il principio di induzione, l'identità vale per ogni $n \geq 2$.

Esercizio 2. *Sull'insieme* $A = \mathbb{N}^{\mathbb{N}} = \{f \mid f : \mathbb{N} \to \mathbb{N}\}$ *si definisca la relazione* ω *ponendo, per ogni* $f, g \in A$, $f\omega g$ *se*

$$\{f(0), \ldots, f(n)\} = \{g(0), \ldots, g(n)\} \text{ per ogni } n \in \mathbb{N}$$

1. *Si provi che* ω *è una relazione d'equivalenza su* A.
2. *Si provi che* $[f]_\omega = \{f\}$ *se* f *è iniettiva.*
3. *Dire se il porre, per* $f \in A$, $[f]_\omega \mapsto f(2)$ *fornisce una buona definizione di un'applicazione* $A/\omega \to \mathbb{N}$.

$*$ *Si provi che se* $2 \leq |Im(f)| < \infty$ *allora* $[f]_\omega$ *contiene infiniti elementi.*

Soluzione. 1. Questa dimostrazione è banale e non sto a scriverla.

2. Siano $f, g \in A$, con f iniettiva e $f\omega g$. Supponiamo, per assurdo, $f \neq g$. llora, per il l'assioma del buon ordine, esiste un minimo $n \in \mathbb{N}$ tale che $f(n) \neq g(n)$. Poiché $f\omega g$, $f(0) = g(0)$; dunque $n \geq 1$ e, per la scelta di n, $f(i) = g(i)$ per ogni $0 \leq i \leq n-1$. Ora, dato che $f\omega g$, si ha per

definizione $\{f(0),\dots,f(n)\}=\{g(0),\dots,g(n)\}$; quindi, poiché $g(n)\neq f(n)$, $f(n)\in\{g(0),\dots,g(n-1)\}$, ovvero, per qualche $0\leq i\leq n-1$,

$$f(n)=g(i)=f(i)$$

contro l'ipotesi che f sia iniettiva. Questo prova che se f è iniettiva allora $[f]_\omega=\{f\}$.

3. NO. Consideriamo, infatti, le funzioni $f,g:\mathbb{N}\to\mathbb{N}$ definite da,

$$f(n)=\begin{cases}0 & \text{se } x=0\\ 1 & \text{se } x=1\\ 0 & \text{se } x\geq 2\end{cases}\qquad g(n)=\begin{cases}0 & \text{se } x=0\\ 1 & \text{se } x=1\\ 1 & \text{se } x\geq 2\end{cases}$$

Allora, come si verifica dalla definizione di ω, $f\omega g$ e dunque $[f]_\omega=[g]_\omega$, ma $f(2)=0\neq 1=g(2)$.

$*$. Sia $f\in A$ con $2\leq|Im(f)|<\infty$. Poiché $I:=Im(f)$ è finita, esiste $t\in N$ tale che $I=\{f(0),f(1),\dots,f(t)\}$; poniamo $J=\mathbb{N}\setminus\{0,\dots,t\}$. Sia g una qualsiasi applicazione $J\to I$, e definiamo $\bar g:\mathbb{N}\to\mathbb{N}$ ponendo, per ogni $n\in\mathbb{N}$

$$\bar g(n)=\begin{cases}f(n) & \text{se } 0\leq n\leq t\\ g(n) & \text{se } n\geq t+1\end{cases}$$

Osserviamo che $Im(\bar g)=Im(f)=I$. Sia $n\in\mathbb{N}$; se $n\leq k$ allora, per definizione, $\{f(0),\dots,f(n)\}=\{\bar g(0),\dots,\bar g(n)\}$; se $n\geq k+1$ allora

$$I=Im(\bar g)\supseteq\{\bar g(0),\dots,\bar g(n)\}\supseteq\{\bar g(0),\dots,\bar g(t)\}=\{f(0),\dots,f(t)\}=I,$$

dunque $\{\bar g(0),\dots,\bar g(n)\}=I=\{f(0),\dots,f(n)\}$. In conclusione, $\bar g\omega f$ e dunque $\bar g\in[f]_\omega$. Poiché $|I|\geq 2$, l'insieme delle funzioni $I^J=\{g\mid g:J\to I\}$ è infinito e pertanto $[f]_\omega$ contiene infiniti elementi.

Esercizio 3. *Su $A=\mathbb{N}^*\times\mathbb{N}^*$ (dove $\mathbb{N}^*=\mathbb{N}\setminus\{0\}$) si definisca la relazione $\preceq$ ponendo, per ogni $(a,b),(c,d)\in A$,*

$$(a,b)\preceq(c,d)\quad\text{se}\quad(a,b)=(c,d)\ \text{ oppure }\begin{cases}a\leq c\\ a\leq d-b\end{cases}$$

1. *Si provi che $\preceq$ è una relazione d'ordine su A; si dica se è totale.*
2. *Si determinino gli elementi minimali di $(A,\preceq)$; si dica se c'è un minimo.*
3. *Si determini, se esiste, l'estremo superiore di $\{(2,3),(3,2)\}$.*

Soluzione. 1. La proprietà riflessiva di $\preceq$ è data per definizione.
Per l'antisimmetria, consideriamo $(a,b),(c,d)\in A$ tali che $(a,b)\preceq(c,d)$

e $(a,b) \preceq (c,d)$, e supponiamo, per assurdo $(a,b) \neq (c,d)$. Allora, per definizione di $\preceq$,

$$\begin{cases} a \leq c \\ a \leq d-b \end{cases} \qquad \text{e} \qquad \begin{cases} c \leq a \\ c \leq b-d \end{cases}$$

da cui segue subito $a = c$; di conseguenza $d - b \geq a = c \leq b - d$, che è un assurdo perché $a = c > 0$. Quindi $(a,b) = (c,d)$ è $\preceq$ è antisimmetrica.
Provare la transitività è semplice; siano $(a,b),(c,d),(e,f) \in A$ tali che $(a,b) \preceq (c,d)$ e $(c,d) \preceq (e,f)$; se $(a,b) = (b,c)$, o $(c,d) = (e,f)$, allora $(a,b) \preceq (e,f)$ è ovvia; possiamo dunque assumere che le tre coppie $(a,b),(c,d),(e,f)$ siano a due a due distinte; quindi che

$$\begin{cases} a \leq c \\ a \leq d-b \end{cases} \qquad \text{e} \qquad \begin{cases} c \leq e \\ c \leq f-d \end{cases}$$

quindi $a \leq e$, e

$$f - b = (f - d) + (d - b) \geq c + a \geq a$$

Dunque $(a,b) \preceq (e,f)$. Pertanto $(A, \preceq)$ è un insieme parzialmente ordinato. Non è totalmente ordinato perché, ad esempio $(2,1) \not\preceq (2,2)$ e $(2,2) \not\preceq (2,3)$.

2. Sia $(a,b) \in A$. Se $b \geq 2$ allora $(a,b) \neq (1,1) \in A$ e $(1,1) \preceq (a,b)$. Questa osservazione mostra che se (a,b) è minimale allora $b = 1$; esaminiamo quindi questo caso. Sia $(c,d) \in A$ tale che $(c,d) \preceq (a,1)$; se $(c,d) \neq (a,1)$ allora, in particolare, $1 \leq c \leq 1 - d$, che è assurdo dato che $d \geq 1$; dunque $(c,d) = (a,1)$. In conclusione l'insieme degli elementi minimali di $(A, \preceq)$ è $\{(a,1) \mid a \in \mathbb{N}^*\}$; e siccome ci sono almeno due elementi minimali distinti, non c'è un minimo.

3. Cominciamo con il trovare - se ce ne sono - i maggioranti di $\{(2,3),(3,2)\}$. Sia quindi $(a,b) \in A$ con $(2,3) \preceq (a,b)$ e $(3,2) \preceq (a,b)$. Poiché $(2,3) \not\preceq (3,2)$ e $(3,2) \not\preceq (2,3)$, $(a,b) \notin \{(2,3),(3,2)\}$, e dunque

$$\begin{cases} 2 \leq a \\ 2 \leq b-3 \end{cases} \qquad \text{e} \qquad \begin{cases} 3 \leq a \\ 3 \leq b-2 \end{cases}$$

Quindi, l'insieme dei maggioranti di $\{(2,3),(3,2)\}$ è

$$\mathcal{M} = \{(a,b) \in A \mid a \geq 3,\ b \geq 5\}.$$

Ragionando come nel punto precedente, si verifica facilmente che $(3,5)$ è un elemento minimale di $\mathcal{M}$, ma che non è il minimo dato che, ad esempio, $(3,5) \not\preceq (4,5)$. Quindi $\mathcal{M}$ non ha minimo e dunque non esiste l'estremo superiore di $\{(2,3),(3,2)\}$.

Esercizio 4. *Siano $a,b,c \in \mathbb{Z}$. Si provi che*

$$(b,c) = 1 \Rightarrow (a,bc) = (a,b)(a,c).$$

SOLUZIONE. Poniamo $d_1 = (a, b)$, $d_2 = (a, c)$ e $d = (a, bc)$. Poiché b e c sono coprimi, anche d_1 e d_2 lo sono, cioè $(d_1, d_2) = 1$. Quindi il m.c.m. di d_1 e d_2 è il loro prodotto, e dunque $d_1 d_2 | a$; siccome, chiaramente, $d_1 d_2 | bc$ si deduce che $d_1 d_2 | d$.
Ora, $(d, b) = d_1$ [infatti d_1 è divisore comune di b e d, dunque $d_1 | (b, d)$, mentre $(b, d) | d_1$ dato che $(b, d) | b$ per definizione e (b, d) divide a dato che divide d, che è a sua volta un divisore di a]. Similmente $(d, c) = d_2$. Poiché $d | bc$ si conclude che $d | d_1 d_2$, il che completa la dimostrazione che $d = d_1 d_2$.

Esercizio 5. *Si trovino le soluzioni intere della congruenza:*

$$(x^{123} + x^{321})^2 \equiv 555x \pmod{35}.$$

SOLUZIONE. Poiché $35 = 5 \cdot 7$, per il Teorema Cinese dei resti, un numero $x \in \mathbb{Z}$ soddisfa la congruenza data se e solo se soddisfa il sistema

$$\begin{cases} (x^{123} + x^{321})^2 \equiv 555x \pmod{5} \\ (x^{123} + x^{321})^2 \equiv 555x \pmod{7} \end{cases} \tag{1}$$

Consideriamo la prima congruenza. Essa è chiaramente soddisfatta se $5 | x$ (ovvero se $x \equiv 0 \pmod{5}$); se $5 \nmid x$, applicando il piccolo Teorema di Fermat si ha

$$x^{123} = (x^4)^{30} x^3 \equiv x^3 \pmod{5} \quad \text{e} \quad x^{321} = (x^4)^{80} x^1 \equiv x \pmod{5}$$

la prima congruenza equivale quindi a $(x^3 + x)^2 \equiv 555x \equiv 0 \pmod{5}$ (per $5 \nmid x$), ovvero (applicando ancora Fermat):

$$x^6 + 2x^4 + x^2 \equiv 2x^2 + 2 \equiv 2(x^2 + 1) \equiv 0 \pmod{5}$$

e cioè:

$$x^2 \equiv -1 \pmod{5} \tag{2}$$

le cui soluzioni si ricavano direttamente, e sono $x \equiv 2, 3 \pmod{5}$. Concludendo, le soluzioni della prima congruenza del sistema (1) sono tutti gli $x \in \mathbb{Z}$ tali che

$$x \equiv 0, 2, 3 \pmod{5} \tag{3}$$

Per la seconda congruenza, vediamo che ogni $x \in \mathbb{Z}$ tale che $7 | x$ è una soluzione; se $7 \nmid x$, applicando Fermat

$$x^{123} = (x^6)^{20} x^3 \equiv x^3 \pmod{7} \quad \text{e} \quad x^{321} = (x^6)^{53} x^3 \equiv x^3 \pmod{7}$$

quindi (applicando ancora Fermat),

$$(x^{123} + x^{321})^2 \equiv (x^3 + x^3)^2 \equiv 4x^6 \equiv 4 \pmod{7};$$

dunque, tenendo conto che $555 \equiv 2 (\text{mod } 7)$, la seconda congruenza (per $7 \not| x$) equivale a

$$4 \equiv 2x \pmod 7 \tag{4}$$

le cui soluzioni sono $x \equiv 2 \pmod 7$. Pertanto, le soluzioni della seconda congruenza del sistema (1) sono tutti gli $x \in \mathbb{Z}$ tali che

$$x \equiv 0, 2 \pmod 7 \tag{5}$$

Per determinare le soluzioni del sistema si risolvono, col Teorema Cinese dei resti, separatamente i vari casi (sono sei) dati dalla (3) e dalla (5): Il primo caso

$$\begin{cases} x \equiv 0 \pmod 5 \\ x \equiv 0 \pmod 7 \end{cases}$$

ha come soluzioni $x \equiv 0 \pmod{35}$. Per gli altri casi

$$\begin{cases} x \equiv 0 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases} \quad \Leftrightarrow \quad x \equiv 30 \pmod{35}$$

$$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 0 \pmod 7 \end{cases} \quad \Leftrightarrow \quad x \equiv 7 \pmod{35}$$

$$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases} \quad \Leftrightarrow \quad x \equiv 2 \pmod{35}$$

$$\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 0 \pmod 7 \end{cases} \quad \Leftrightarrow \quad x \equiv 28 \pmod{35}$$

$$\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases} \quad \Leftrightarrow \quad x \equiv 23 \pmod{35}$$

In conclusione, le soluzioni della congruenza sono tutti gli $x \in \mathbb{Z}$ tali che

$$x \equiv 0, 2, 7, 18, 23, 28, 30 \pmod{35}.$$