Matricola: ..... $\mathbf{A}^{\geq 2}$:... $\mathbf{B}^{\geq 3}$:... $\mathbf{C}^{\geq 2}$:... $\mathbf{D}^{\geq 3}$:... Voto: .....

Cognome: ..... Nome: .....

Algebra 1 – Esame 12.06.13

Rispondere alle domande su questo foglio usando gli appositi spazi e giustificando brevemente ma esaurientemente tutte le risposte.

A Sia X un insieme non vuoto e sia $\leq$ una relazione d'ordine totale su X. Consideriamo l'insieme

$$M(X) \stackrel{\text{def}}{=} \{f : X \to X \mid f \text{ monotòna}\}$$

1. Se X è infinito allora $M(X)$ è infinito? Inoltre, se X è finito allora $M(X)$ è finito? [Sì; Sì] | 3 |

   L'insieme delle applicazioni costanti è contenuto in $M(X)$ ed ha ovviamente la stessa cardinalità di X, pertanto se X è infinito anche $M(X)$ lo è. Qualora invece X sia finito, allora l'insieme di tutte le applicazioni di X in sé è finito e pertanto lo è anche $M(X)$.

2. Mostrare che se $f \in M(X)$ è bigettiva allora $f^{-1} \in M(X)$. | 2 |

   Supponiamo che f sia monotona crescente (ovvero, per ogni $x, y \in X$, $x \leq y$ implica $f(x) \leq f(y)$), e siano $x, y \in X$ con $x \leq y$. Se vale $f^{-1}(y) \leq f^{-1}(x)$, allora $y = f(f^{-1}(y)) \leq f(f^{-1}(x)) = x$, da cui $y = x$ e dunque $f^{-1}(y) = f^{-1}(x)$. In ogni caso si ha $f^{-1}(x) \leq f^{-1}(y)$.

3. Consideriamo la relazione d'ordine sull'insieme $M(X)$ definita da $f \leq g$ se $f(x) \leq g(x)$ per ogni $x \in X$. È vero che $(M(X), \leq)$ è totalmente ordinato? [No] | 2 |

   Sia $X = \{0, 1, 2\}$, con l'ordinamento standard indotto da $\mathbb{N}$. Sia f l'identità, e g la funzione che vale ovunque 1. Si vede immediatamente che $f, g \in M(X)$, $f \not\leq g$ e $g \not\leq f$.

B Sia $M \stackrel{\text{def}}{=} \{(x,y) \mid x \in \mathbb{Z}_2, y \in \mathbb{Z}_6\}$. Sia $(x,y) \odot (z,t) \stackrel{\text{def}}{=} (x+z, yt)$ per ogni $(x,y), (z,t) \in M$.

1. Mostrare che M è un monoide e trovare gli elementi invertibili in M. | 3 | |

   Osservando che $(\mathbb{Z}_2, +, [0]_2)$ e $(\mathbb{Z}_6, \cdot, [1]_6)$ sono monoidi, e che l'operazione $\odot$ è definita componente per componente, segue immediatamente che $(M, \odot, ([0]_2, [1]_6))$ è un monoide, i cui elementi invertibili sono le coppie con entrambe le componenti invertibili (quindi, gli elementi (x,y) con $x \in \mathbb{Z}_2$ e $y \in \{[1]_6, [5]_6\}$).

2. Sia $f(n) \stackrel{\text{def}}{=} ([n], [n+1]) \in M$ per $n \in \mathbb{N}$. È vero che $f : \mathbb{N} \to M$ è un omomorfismo da $(\mathbb{N}, +)$ in $(M, \odot)$? [No] | 3 | |

   Si ha $f(1+1) = f(2) = ([0]_2, [3]_6)$, ma $f(1) + f(1) = ([1]_2, [2]_6) \odot ([1]_2, [2]_6) = ([0]_2, [4]_6)$.

3. Esiste un unico omomorfismo f da $(\mathbb{N}, +)$ in $(M, \odot)$ tale che $f(1) \stackrel{\text{def}}{=} ([1], [2])$? [Sì] | 2 | |

   Poichè ogni elemento del monoide $(\mathbb{N}, +, 0)$ si scrive come potenza additiva di 1 (cioè, $n = n \cdot 1$ per ogni $n \in \mathbb{N}$), assegnando ad 1 un valore m preso in un fissato monoide $(M, \cdot, e)$, resta definito un unico omomorfismo di monoidi f da $(\mathbb{N}, +, 0)$ a $(M, \cdot, e)$ (ovvero, $f(n) = m^n$, dove la potenza al secondo membro è effettuata rispetto all'operazione $\cdot$ in M).

C Sia $p(X) = X^5 - 2X^4 + 5X^3 - 3X^2 + 2X - 7$.

1. Fattorizzare $p(X)$ in $\mathbb{Z}_2[X]$. | 3 | |

   Il polinomio $p(X)$ in $\mathbb{Z}_2[X]$ diventa $X^5 + X^3 + X^2 + 1 = X^3(X^2 + 1) + X^2 + 1 =$

   $$= (X^3 + 1)(X^2 + 1) = (X + 1)(X^2 + X + 1)(X + 1)^2 = (X + 1)^3(X^2 + X + 1),$$

   con l'ultimo fattore irriducibile poiché privo di radici in $\mathbb{Z}_2$.

2. È sufficiente che $p(X)$ non abbia radici in $\mathbb{Z}_3$ per concludere che l'anello quoziente $\mathbb{Z}_3[X]/(p(X))$ è un campo ? [No] | 2 | |

   Il polinomio ha grado maggiore di 3, dunque potrebbe spezzarsi pur non avendo radici.

3. Se $\mathbb{Z}_3[X]/(p(X))$ è un campo è vero che $p(X)$ è irriducibile in $\mathbb{Z}[X]$? [Sì] | 3 | |

   Supponiamo che $p(X)$ si spezzi come $a(X)b(X)$, con $a(X)$ e $b(X)$ polinomi in $\mathbb{Z}[X]$ entrambi diversi da ± 1 (dunque entrambi non costanti, visto che $p(X)$ è monico). Se, per $f(X) \in \mathbb{Z}[X]$, denotiamo con $\overline{f}(X)$ il polinomio in $\mathbb{Z}_3[X]$ ottenuto riducendo modulo 3 i coefficienti di $f(X)$, avremmo allora la fattorizzazione $\overline{p}(X) = \overline{a}(X)\overline{b}(X)$ in $\mathbb{Z}_3[X]$, il che implica (possiamo supporre) $\overline{a}(X) = \pm[1]_3$, visto che per per ipotesi $\overline{p}(X)$ è irriducibile in $\mathbb{Z}_3[X]$. Ma allora il coefficiente direttore di $a(x)$, quindi anche di $p(X)$, sarebbe un multiplo di 3, il che non è.

D Si consideri il sistema di congruenze $S : \begin{cases} 8x \equiv_5 3 \\ 8x \equiv_7 3 \\ 8x \equiv_{11} 3 \end{cases}$

1. Mostrare che il sistema S è equivalente al sistema $S' : \begin{cases} x \equiv_5 1 \\ x \equiv_7 3 \\ x \equiv_{11} -1 \end{cases}$ | 3 |

   Tenendo conto del fatto che $8 \equiv_5 3$, $8 \equiv_7 1$ *e* $8 \equiv_{11} -3$ *(e del fatto che* 3 *è invertibile sia modulo* 5 *che modulo* 11*), segue immediatamente ciò che si vuole.*

2. Il sistema è anche equivalente all'equazione $8x \equiv_{385} 3$? [Sì] | 2 |

   Si ha che $8x - 3$ *è divisibile per* $385 = 5 \cdot 7 \cdot 11$ *se e solo se è divisibile per ciascuno dei fattori primi* $5, 7, 11$.

3. La più piccola soluzione positiva del sistema S è [241] | 3 |

   Dalla prima congruenza si ricava $x = 5h + 1$ *che, sostituendo nella seconda, dà* $h \equiv_7 -1$, *ovvero* $h = 7k - 1$ *e quindi* $x = 5(7k-1)+1 = 35k-4$. *Sostituendo nella terza congruenza, si ottiene ora* $2k \equiv_{11} 3$, *da cui* $k \equiv_{11} -4$ *e quindi* $k = 11w - 4$. *A questo punto si ottiene* $x = 35(11w - 4) - 4 = 385w - 144$, *dunque* -144 *è l'unica soluzione del sistema (modulo* 385*). Si vede ora immediatamente che la più piccola soluzione positiva è* 241.