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

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

Algebra 1 – Esame 02.05.13

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

A Sia $\sim$ la relazione su $\mathbb{Z}^{\neq 0} \stackrel{\text{def}}{=} \mathbb{Z} \setminus \{0\}$ definita da $n \sim m$ se $nm > 0$. Sia $f : \mathbb{Z}^{\neq 0} \to \mathbb{Z}_2$ la funzione

$$f(n) = \begin{cases} [0] & n \in \mathbb{N}^+ \\ [1] & n \in \mathbb{N}^- \end{cases}$$

1. Mostrare che $\sim$ è una relazione di equivalenza. | 2 | |

   Evidentemente, dati due interi non nulli n ed m, si ha $n \sim m$ se e solo se n ed m hanno lo stesso segno. Pertanto la relazione è riflessiva, simmetrica e transitiva.

2. Mostrare che f induce una funzione $\bar{f}$ dall'insieme quoziente $\mathbb{Z}^{\neq 0}/\sim$ in $\mathbb{Z}_2$. | 2 | |

   La relazione $\sim$ induce una partizione di $\mathbb{Z}^{\neq 0}$ in due classi di equivalenza, che sono $\mathbb{N}^+$ e $\mathbb{N}^-$. Da questa osservazione segue ovviamente che $\bar{f}$ sia ben definita sull'insieme quoziente.

3. È vero che $\bar{f}$ è bigettiva ? [Sì]

   L'applicazione $\bar{f}$ è suriettiva, da un insieme con due elementi in un insieme con due elementi. Pertanto è anche iniettiva. | 3 | |

B Sia $\mathbb{Z}_{18}^*$ l'insieme degli elementi invertibili di $\mathbb{Z}_{18}$.

1. Si ha che $|\ \mathbb{Z}_{18}^*\ | = [\phi(18) = 6]$ | 3 | |

   Gli elementi invertibili di $\mathbb{Z}_{18}$ *sono classi di resto rappresentate da interi in* $\{0, 1, ..., 17\}$ *coprimi con* 18*. Il loro numero è dato dal valore della funzione* ϕ *di Eulero in* 18*, e si ha* $\phi(18) = \phi(2 \cdot 3^2) = \phi(2) \cdot \phi(3^2) = 1 \cdot (3-1) \cdot 3 = 6$*. (Infatti, i numeri tra* 0 *e* 17 *coprimi con* 18 *sono* $1, 5, 7, 11, 13, 17$*.)*

2. Mostrare che $2 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 2$ per ogni $n \in \mathbb{N}^+$ e trovare il più piccolo $n \in \mathbb{N}^+$ tale che $2 + 2^2 + 2^3 + \cdots + 2^n \equiv_{18} 0$. $n = [6]$ | 3 | |

   Si ha

   $$2^{n+1} - 2 = 2(2^n - 1) = 2(2-1)(1 + 2 + 2^2 + \cdots + 2^{n-1}) = 2 + 2^2 + \cdots + 2^n.$$

   Inoltre, $0 \equiv_{18} 2 + 2^2 + \cdots + 2^n \equiv_{18} 2^{n+1} - 2$ *equivale a* $2^n - 1 \equiv_9 0$*. (Stiamo cercando dunque l'ordine dell'elemento* $[2]$ *in* $\mathbb{Z}_9^*$*.) Si vede facilmente che il più piccolo* $n \in \mathbb{N}^+$ *per cui ciò si verifica è* 6*.*

3. Esiste $n \in \mathbb{N}^+$ tale che $2 + 2^2 + 2^3 + \cdots + 2^n \in \mathbb{Z}_{18}^*$? [No] | 2 | |

   Si fissi un qualunque $n \in \mathbb{N}^+$*. Si ha che* 2 *divide* $2 + 2^2 + 2^3 + \cdots + 2^n$ *in* $\mathbb{Z}$*, quindi l'intero che stiamo considerando non è coprimo con* 18*. Da ciò segue che tale elemento non è invertibile nell'anello* $\mathbb{Z}_{18}$*.*

C Sia $p(X) = X^2+1$ considerato come polinomio in $\mathbb{Z}_5[X]$. Sia $A \stackrel{\text{def}}{=} \mathbb{Z}_5[X]/(p(X))$ l'anello quoziente.

1. Mostrare che A non è un campo. | 3 | |

Il polinomio X^2+1 ha una radice ($X = 2$) in $\mathbb{Z}_5$, e non è dunque irriducibile in $\mathbb{Z}_5[X]$. Segue che A non è un campo.

2. Determinare gli zero-divisori di A. | 2 | |

L'anello A è finito (di ordine 25), quindi gli zero-divisori sono esattamente i suoi elementi non invertibili diversi da 0. Gli elementi non invertibili sono tutti e soli quelli contenuti negli ideali propri di A. Determiniamo dunque tali ideali: denotando con $J/(p(X))$ un ideale proprio e non banale di A (equivalentemente, denotando con J un ideale proprio di $\mathbb{Z}_5[X]$ contenente propriamente $(p(X))$), poiché $\mathbb{Z}_5[X]$ è un P.I.D. deve esistere $q(X) \in \mathbb{Z}_5[X]$ tale che $J = (q(X))$; visto che $p(X) \in J$, il polinomio $q(X)$ deve essere un divisore (non invertibile né associato a $p(X)$) di $p(X)$, dunque $q(X) \in \{X+2, X-2\}$ (a meno di associatura). Concludiamo che gli zero-divisori di A sono gli elementi (non nulli) della forma $(p(X)) + f(X)q(X)$, dove $q(X)$ è come sopra, e $f(X)$ varia in $\mathbb{Z}_5[X]$.

3. Determinare gli elementi nilpotenti di A. | 3 | |

Sia $(p(X)) + n(X)$ un elemento nilpotente di A, dunque esiste $m \in \mathbb{N}$ tale che $n(X)^m \in (p(X))$. Ciò significa che $p(X) = X^2+1$ divide $n(X)^m$, pertanto ogni fattore irriducibile di X^2+1 divide $n(X)^m$; ma poiché gli elementi irriducibili di $\mathbb{Z}_5[X]$ sono anche primi, questo implica che ogni fattore irriducibile di $X^2+1 = (X+2)(X-2)$ divide $n(X)$. Concludiamo che X^2+1 divide $n(X)$, pertanto l'unico elemento nilpotente di A è lo zero.

D Si consideri l'anello $A = \mathbb{Z}[i]$ degli interi di Gauss.

1. Mostrare che 61 è un primo di $\mathbb{Z}$ che non è primo in A. | 3 | |

   Essendo 61 *un primo di* $\mathbb{Z}$ *congruo a* 1 *modulo* 4*, esso è somma di due quadrati. In effetti si ha* $61 = 25 + 36$*, da cui* $61 = (5 + 6i) \cdot (5 - 6i)$ *in* A*. Poiché nessuno dei due fattori è invertibile in* A*, concludiamo che* 61 *non è irriducibile in* A*.*

2. Trovare una scomposizione in fattori irriducibili di 61 in A. | 2 | |

   Si ha $61 = (5 + 6i) \cdot (5 - 6i)$*. Poiché la norma di entrambi i fattori è un primo in* $\mathbb{Z}$*, essi sono irriducibili in* A*.*

3. Se l'equazione $x^2 \equiv_p -1$ ha soluzioni allora $p \in \mathbb{Z}$ è primo in A ? [No] | 3 | |

   Sappiamo che esiste $x \in \mathbb{Z}$ *tale che* p *divide* $1 + x^2$*, dunque* p *divide* $(1 + ix) \cdot (1 - ix)$ *in* A*. D'altra parte è evidente che* p *non divide nessuno dei due fattori, visto che non ne divide la parte reale. Concludiamo che* p *non è primo in* A*.*