Algebra 1

Proff. P. Piazza, E. Spinelli

Terzo Esame

22 Settembre 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 per quali valori di a e b il seguente sistema ha soluzioni (*non è richiesto di determinarle*)

$$\begin{cases} X \equiv 2a \mod 3 \\ bX \equiv 3 \mod 5 \\ X + 1 \equiv 3 \mod 6 \end{cases}$$

Soluzione: Consideriamo la terza equazione del sistema $X + 1 \equiv_6 3$. L'insieme delle sue soluzioni è dato da $S := \{2 + 6h \,|\, h \in \mathbb{Z}\}$. Imponiamo che un elemento di S sia soluzione anche della prima equazione congruenziale. Questo porta all'equazione (nell'incognita h) $2 + 6h \equiv_3 2a$, ovvero $2 \equiv_3 2a$. Dunque se $a \equiv_3 1$ ogni $y \in S$ è soluzione anche della prima equazione.

Pertanto imponiamo che $2 + 6h$ sia soluzione anche della seconda equazione congruenziale. Questo implica che

$$b(2 + 6h) \equiv_5 3 \quad \iff \quad b(2 + h) \equiv_5 3 \quad \iff \quad bh \equiv_5 3 - 2b.$$

Se $b \not\equiv_5 0$ l'equazione diventa $h \equiv_5 3b^{-1} - 2$ che ha soluzione.

Segue che il sistema in oggetto ammette soluzione quando $a \equiv_3 1$ e $b \not\equiv_5 0$.

Risposta:

a è tale che $\boxed{}$ b è tale che $\boxed{}$

Esercizio 2. Sia p un primo dispari e $\mathbb{Z}_p := \mathbb{Z}/\equiv_p$. Si consideri l'ideale I dell'anello dei polinomi $\mathbb{Z}_p[x]$ generato dal polinomio x^2+1, $I := (x^2+1)_{\mathbb{Z}_p[x]}$, e l'anello quoziente $\mathbb{Z}_p[x]/I$.

(a) Dimostrare che se p **non** è congruo a 1 modulo 4 allora $\mathbb{Z}_p[x]/I$ è un campo.

(b) Sotto le stesse ipotesi di (a) determinare l'ordine del gruppo degli elementi invertibili di $\mathbb{Z}_p[x]/I$.

Soluzione: (a) Per provare l'asserto basterà verificare che, sotto quelle assunzioni per p, il polinomio $f := (x^2+1)$ è irriducibile in $\mathbb{Z}_p[x]$. Ora, essendo f di grado 2, è sufficiente dimostrare che f non ha radici in $\mathbb{Z}_p$. A tal fine, supponiamo, se possibile, che a sia radice di f. Questo implica che $a^2 \equiv_p -1$ e quindi $a^4 \equiv_p 1$. Segue che a è un elemento di ordine 4 in $\mathcal{U}(\mathbb{Z}_p)$, il gruppo degli elementi invertibili di $\mathbb{Z}_p$. Per il Teorema di Lagrange 4 divide $|\mathcal{U}(\mathbb{Z}_p)| = p-1$, ma questo è falso perchè per ipotesi $p \not\equiv_4 1$.
(b) Essendo $\mathbb{Z}_p[x]/I$ un campo

$$|\mathcal{U}(\mathbb{Z}_p[x]/I)| = |\mathbb{Z}_p[x]/I| - 1 = p^2 - 1.$$

Esercizio 3. Sia G un gruppo abeliano e si ponga

$$T(G) := \{x \,|\, x \in G, \quad \exists\, n \in \mathbb{N} \;\; x^n = 1_G\}.$$

(a) Provare che $T(G) \leq G$;

(b) dimostrare che ogni elemento di $G/T(G)$ diverso dall'identità ha ordine infinito.

Soluzione: (a) Osserviamo che $T(G) \neq \emptyset$ in quanto $1_G \in T(G)$. Siano ora $x, y \in T(G)$. Allora esistono $n, m \in \mathbb{N}$ tali che $x^n = 1_G = y^m$. Ora, sfruttando l'abelianità di G, si ha che

$$(xy^{-1})^{nm} = x^{nm}(y^{-1})^{nm} = (x^n)^m(y^{nm})^{-1} = 1_G \cdot ((y^m)^n)^{-1} = 1_G \cdot 1_G = 1_G.$$

Pertanto $xy^{-1} \in T(G)$ e dunque $T(G) \leq G$.

(b) Sia $T(G) \neq xT(G) \in G/T(G)$ ed assumiamo, se possibile, che $xT(G)$ abbia ordine finito, diciamo n. Questo implica che

$$(xT(G))^n = x^nT(G) = T(G),$$

da cui segue che $x^n \in T(G)$. Quindi esiste un intero m tale $(x^n)^m = x^{nm} = 1_G$, ovvero $x \in T(G)$, che è in contraddizione col fatto che $xT(G) \neq T(G)$.

Esercizio 4. Sia G un gruppo abeliano di ordine $m \in \mathbb{N}$ e sia $n \geq 1$ tale che $\mathrm{mcd}(m, n) = 1$. Provare che la funzione

$$f : G \longrightarrow G, \qquad x \longmapsto x^n$$

è un automorfismo di G.

Soluzione: Dall'abelianità di G segue subito che f è un omomorfismo. Poichè G è finito basterà provare quindi che f sia suriettiva. A tal fine sia $y \in G$ e siano $a, b \in \mathbb{Z}$ tali che $am + bn = 1$ (esistono per l'identità di Bezout). Allora

$$y = y^{am+bn} = y^{am}y^{bn} = 1_G \cdot (y^b)^n = f(y^b),$$

che è quanto volevasi provare.

Esercizio 5. Un ideale $H \neq A$ di un anello commutativo A si dice *primario* se per ogni coppia di elementi $(a, b) \in A \times A$ tali che $ab \in H$ e $a \notin H$ esiste un intero positivo n tale che $b^n \in H$, mentre un elemento $a \in A$ è *nilpotente* se esiste $n \geq 1$ tale che $a^n = 0_A$.

Se A è unitario e $A \neq H$ è un ideale di A si provi che H è primario se, e solo se, nell'anello quoziente A/H ogni divisore dello zero è nilpotente.

Soluzione: Assumiamo prima che $A \neq H$ sia un ideale primario di A e sia $x + H \in A/H$ un divisore dello zero non-banale di A/H. Pertanto esiste $y \in A \setminus H$ tale che

$$(x + H)\hat{\cdot}(y + H) = xy + H = H.$$

Da questo segue che $xy \in H$ e, poichè $y \notin H$, esiste $n \geq 1$ tale che $x^n \in H$. Dunque

$$(x + H)^n = x^n + H = H,$$

ovvero $x + H$ è un elemento nilpotente di A/H.

Viceversa, supponiamo che ogni divisore dello zero di A/H sia nilpotente. Vogliamo provare che H è primario. A tal fine, siano $a, b \in A$ tali che $ab \in H$ e $a, b \notin H$ (altrimenti l'asserto è banale). Allora

$$ab + H = (a + H)\hat{\cdot}(b + H) = H.$$

Quindi $b + H$ è un divisore dello zero non-banale di A/H e dunque nilpotente. Pertanto esiste $n \geq 1$ tale che $(b + H)^n = b^n + H = H$, il che implica che $b^n \in H$.