Università degli studi di Bari
Aldo Moro
Dipartimento di Matematica

Esercizi di Algebra

Autore:
dott. Maino Luciano
l.maino2@studenti.uniba.it

Introduzione

Il seguente eserciziario sintetizza la mia esperienza da peer-tutor presso l'Università degli studi di Bari. Esso raccoglie gli svolgimenti di alcune tracce d'esame relative all'anno accademico $2018-2019$ *per il corso di Algebra* 1. *Ogni svolgimento è stato revisionato dalla Prof.ssa Margherita Barile (titolare del corso), che ringrazio per la disponibilità e l'aiuto offertomi.*
Vorrei inoltre ringraziare tutti i miei colleghi che hanno partecipato agli incontri e augurare un buon lavoro a tutti coloro che dovranno affrontare l'esame.

Luciano

Indice

Traccia 95

1 Siano date in S_{17} le permutazioni

$$\sigma = (1,2,3,4,5,6)(10,11,12)(13,14,15,16,17),$$

$$\tau = (6,7,8,9)(13,15,14,17,16).$$

(a) Determinare $<\sigma> \cap <\tau>$.

Sia H un sottogruppo di S_{17} a cui appartengono σ e τ.

(b) Provare che H contiene almeno 3 distinti sottogruppi di ordine 3.

(c) Provare che H contiene almeno 2 distinti sottogruppi di ordine 9.

2 Siano n ed m interi maggiori di 1, e sia data l'applicazione

$$\varphi : \mathbb{Z}_{100} \longrightarrow \mathbb{Z}_n \times \mathbb{Z}_m$$

tale che, per ogni $a \in \mathbb{Z}$,

$$\varphi([a]_{100}) = ([a]_n, [a]_m).$$

(a) Determinare tutte le coppie (n,m) per le quali φ è ben definita.

(b) Determinare tutte le coppie (n,m) per le quali φ è surgettiva.

(c) Per $n = 4$, $m = 5$, determinare $\varphi^{-1}([1]_4, [2]_5)$.

3 Sia p un numero primo positivo, e sia $\alpha \in \mathbb{Z}_p$. Sia inoltre

$$f(x) = x^{p^2-1} + x^p + \alpha \in \mathbb{Z}_p[x].$$

Determinare, al variare di p, tutti gli $\alpha \in \mathbb{Z}_p$ tali che $f(x)$ abbia in $\mathbb{Z}_p$ una ed una sola radice.

Svolgimento

1 (a) Si osservi preliminarmente che, essendo $<\sigma> \cap <\tau>$ un sottogruppo di $<\sigma>$, $<\sigma> \cap <\tau>$ è un sottogruppo ciclico, quindi $\exists \alpha\ S_{17}$ t.c. $<\alpha> = <\sigma> \cap <\tau>$.
Poiché $o(\sigma) = mcm(6,3,5) = 30$ e $o(\tau) = mcm(4,5) = 20$, sfruttando il Teorema di Lagrange, $o(\alpha) \mid 20 \ \wedge \ o(\alpha) \mid 30$, da cui

$$o(\alpha) \mid MCD(20,30) = 10.$$

Utilizzando la formula del periodo, si ottiene:

$$10 = o(\tau^k) = \frac{o(\tau)}{MCD(o(\tau),k)} = \frac{20}{MCD(20,k)} \iff MCD(k,20) = 2 \iff$$

$$\iff k \in \{2, 6, 14, 18\}.$$

Si osservi che per ogni $k \in \{2, 6, 14, 18\}$, $k \equiv 2 (mod\, 4)$, da cui $\tau^k(6) = 8$. Ciò mostra che non esiste alcun elemento in comune di periodo 10 tra $< \sigma >$ e $< \tau >$.
Mediante un ragionamento analogo al precedente:

$$o(\sigma^k) = 5 \wedge o(\tau^h) = 5 \iff k \in \{6, 12, 18, 24\} \wedge h \in \{4, 8, 12, 16\}.$$

È utile notare l'equivalenza fra:

- $\exists k \in \{6, 12, 18, 24\},\ h \in \{4, 8, 12, 16\}\ t.c.\ \sigma^k = \tau^h$;
- $\exists\, h \in \{4, 8, 12, 16\}\ t.c.\ \sigma^6 = (13, 14, 15, 16, 17) = \tau^h$.

Infatti:
si supponga che $\exists k \in \{6, 12, 18, 24\},\ h \in \{4, 8, 12, 16\}\ t.c.$ $\sigma^k = \tau^h$. Essendo $< \sigma^k >$ l'unico sottogruppo di ordine 5 di $< \sigma >$ e $o(\sigma^6) = 5$, $\sigma^6 \in < \sigma^k >$.
Poiché $< \sigma^k > = < \tau^h >$, σ^6 è un generatore di $< \tau^h >$. I generatori di $< \tau^h >$ sono: τ^4, τ^8, τ^{12}, τ^{16}, quindi $\sigma^6 = \tau^l$ per un opportuno $l \in \{4, 8, 12, 16\}$.
L'unico valore di $h \in \{4, 8, 12, 16\}$ t.c. $\tau^h(13) = 14$ è 12, ma $\tau^{12}(14) = 16 \neq 15 = \sigma^6(14)$, ciò prova che $o(\alpha) \neq 5$.
Poiché l'unica permutazione di $< \tau >$ avente periodo 2 è $(6, 8)(7, 9)$, $o(\alpha) \neq 2$, da cui $< \sigma > \cap < \tau > = \{id\}$.

(b) Si osservi preliminarmente che:

$$\sigma\tau = (1, 2, 3, 4, 5, 6, 7, 8, 9)(10, 11, 12)(13, 16, 14);$$

$$\tau\sigma = (1, 2, 3, 4, 5, 7, 8, 9, 6)(10, 11, 12)(13, 17, 15).$$

Inoltre $(\sigma\tau)^3 = (1, 4, 7)(2, 5, 8)(3, 6, 9)$, $(\tau\sigma)^3 = (1, 4, 8)(2, 5, 9)(3, 7, 6)$ ed hanno entrambe periodo pari a 3.
Sia H un sottogruppo di S_{17} a cui appartengono σ e τ, allora $\sigma^{10} = (1, 5, 3)(2, 6, 4)(10, 11, 12), (\sigma\tau)^3, (\tau\sigma)^3 \in H$.
Le suddette permutazioni generano tre sottogruppi distinti di ordine 3 e per la struttura delle loro orbite.

(c) Poiché non esiste alcuna permutazione $\alpha \in < \tau\sigma >$ tale che 16 sia un elemento dell'orbita di 13, $< \tau\sigma > \neq < \sigma\tau >$ e ciò esaudisce la richiesta.

2 (a) Si supponga di avere una coppia (n, m) tale che φ sia ben definita. In particolare, considerando $a = 100$ e $b = 0$, si ha che $([a]_n, [a]_m) = ([b]_n, [b]_m)$, ossia $a \equiv b\, (mod\, n)$ e $a \equiv b\, (mod\, m)$, equivalentemente $n | a - b = 100$ e $m | a - b = 100$. Ciò mostra che se φ è ben definita allora $n | 100$ e $m | 100$.
Viceversa, siano $n, m \in \mathbb{Z}$, $n, m > 1$ tali che $n | 100$ e $m | 100$. Si

provi la buona definizione dell'applicazione φ.
Siano $a, b \in \mathbb{Z}$ tali che $[a]_{100} = [b]_{100}$, ossia $100|a-b$. Si osservi che $[a]_n = [b]_n$ in quanto $n|100$, $100|a-b \Rightarrow n|a-b$. Analogamente si mostra che $[a]_m = [b]_m$.
Si può concludere che φ è ben definita se e solo se $n|100 \wedge m|100$.

(b) Sia (n, m) una coppia di interi positivi tali che l'applicazione φ sia surgettiva (e quindi anche ben definita). In particolare $\exists c \in \mathbb{Z}$ tale che $\varphi([c]_{100}) = ([1]_n, [0]_m)$, ossia $n|c-1 \wedge m|c$. Si ponga $d := MCD(n, m)$, allora $d|c-1 \wedge d|c \Rightarrow d|1$. Ciò mostra che n ed m devono essere tra loro coprimi.
Viceversa, si supponga che n, m siano coprimi e verifichino la condizione per la buona definizione di φ. Siano $a, b \in \mathbb{Z}$, allora, per il Teorema cinese del resto, $\exists c \in \mathbb{Z}$ tale che $c \equiv a\,(mod\,n) \wedge c \equiv b\,(mod\,m)$. Ciò mostra che l'applicazione è surgettiva.
Si può concludere che l'applicazione φ è surgettiva se e solo se n, m sono coprimi e verificano la condizione di buona definizione.

(c) Si osservi preliminarmente che n, m da ipotesi verificano la condizione di surgettività per φ ed inoltre:

$$\varphi^{-1}([1]_4, [2]_5) = \{[c]_{100}\,|c \in \mathbb{Z},\, c \equiv 1\,(mod\,4),\, c \equiv 2\,(mod\,5)\}.$$

Da ciò si evince che è sufficiente trovare tutte le soluzioni del seguente sistema:

$$\begin{cases} x \equiv 1\,(mod\,4) \\ x \equiv 2\,(mod\,5) \end{cases}$$

e considerarne le distinte classi di resto modulo 100.
Utilizzando opportunamente il Teorema cinese del resto si ottiene che le soluzioni sono date da $17+20k$ al variare di $k \in \mathbb{Z}$, da cui:

$$\varphi^{-1}([1]_4, [2]_5) = \{[17]_{100}, [37]_{100}, [57]_{100}, [77]_{100}, [97]_{100}\}.$$

3 Si osservi che se $\alpha = [0]_p$, allora, per ogni p primo positivo, $[0]_p$ e $[p-1]_p$ sono radici di $f(x)$.
Si supponga che $\alpha \neq [0]_p$ e sia $[b]_p$ una radice di $f(x)$ (se esistente e certamente diversa da $[0]_p$), allora:

$$[0]_p = f([b]_p) = [b^{p^2-1}]_p + [b^p]_p + \alpha.$$

Si osservi che $p^2 - 1 = (p-1)(p+1)$, quindi, per il piccolo Teorema di Fermat, $b^{p^2-1} \equiv (b^{p+1})^{p-1} \equiv 1\,(mod\,p)$ e $b^p \equiv b\,(mod\,p)$. Da ciò si evince che:

$$[b]_p = -\alpha - [1]_p.$$

Si supponga che $\alpha \neq [0]_p \wedge \alpha \neq [-1]_p$, allora mediante un calcolo diretto si ha che $f(x)$ ammette come unica radice $-\alpha - [1]_p$, se invece

$\alpha = [-1]_p$ $f(x)$ non ammette radici.
Si noti che, in particolare, per $p = 2$, $f(x)$ o non ammette radici, o ha due radici.

Traccia 96

1 Sia n un intero positivo. Si consideri l'insieme

$$H = \{\sigma \in S_{2n} | \sigma(1) \neq 2\}.$$

(a) Determinare tutti i valori di n per i quali H è un sottogruppo di S_{2n}.

(b) Provare che H contiene un sottogruppo commutativo di S_{2n} avente ordine 2^{n-1}.

(c) Provare che H contiene un sottogruppo di S_{2n} avente ordine $(n!)^2$.

2 Dato un intero n maggiore di 1, si consideri l'applicazione

$$\varphi_n : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$$

tale che, per ogni $\alpha \in \mathbb{Z}_n$, $\varphi_n(\alpha) = \alpha^2$.

(a) Determinare tutti i valori di n per i quali $\varphi_n^{-1}([0]_n) = \{[0]_n\}$.

(b) Determinare tutti i valori di n per i quali φ_n è surgettiva.

3 Sia $f(x) = x^4 + 1 \in \mathbb{Z}[x]$. Dato un primo positivo p, sia $\overline{f}(x) \in \mathbb{Z}_p[x]$ la sua riduzione modulo p.

(a) Per $p = 5$ determinare una fattorizzazione di $\overline{f}(x)$ in $\mathbb{Z}_5[x]$.

(b) Determinare due primi $p > 5$ tali che $\overline{f}(x)$ sia riducibile in $\mathbb{Z}_p[x]$.

Svolgimento

1 (a) Si osservi preliminarmente che se $n = 1$ allora $H = \{id\}$ e quindi è un gruppo.
Sia ora $n \geq 2$ allora $(1, 3, 2) \in H$, ma $(1, 3, 2)^2 = (1, 2, 3) \notin H$, da cui se ne deduce che l'insieme H non è chiuso rispetto all'operazione binaria di S_{2n} ristretta ad H e quindi H non è un sottogruppo di S_{2n}.

(b) Si supponga dapprima che $n = 1$, allora H è un sottogruppo avente ordine $2^{n-1} = 1$.
Sia ora $n \geq 2$, allora, per ogni $i = 1, \ldots, n-1$, si ponga

$$\gamma_i := (2i + 1, 2(i + 1)).$$

Si consideri allora il seguente insieme:

$$L := \{\gamma_1^{i_1} \ldots \gamma_{n-1}^{i_{n-1}} | \, i_1, \ldots, i_{n-1} \in \mathbb{Z}\}.$$

Esso, munito della operazione binaria di S_{2n} opportunamente ristretta, è un gruppo abeliano avente ordine 2^{n-1}, inoltre, per costruzione, $L \subset H$.

(c) Per $n = 1$ l'asserto è ovviamente verificato.
Si supponga che $n \geq 2$, allora si pongano:

$$I_1 := \{2i - 1 | i \in \mathbb{Z}, 1 \leq i \leq n\};$$

$$I_2 := \{2i | i \in \mathbb{Z}, 1 \leq i \leq n\};$$

$$L_1 := \{\sigma \in S_{2n} | \, supp(\sigma) \subset I_1\};$$

$$L_2 := \{\sigma \in S_{2n} | \, supp(\sigma) \subset I_2\}.$$

Gli insiemi L_1, L_2, muniti della operazione binaria di S_{2n} opportunamente ristretta, sono due sottogruppi di S_{2n} aventi ordine $n!$, in quanto isomorfi a S_n.
Si consideri ora:

$$L := \{\alpha\tau | \, \alpha \in L_1, \, \tau \in L_2\}.$$

Esso è un sottogruppo di S_{2n} contenuto in H avente ordine $(n!)^2$.

2 (a) Sia n un intero maggiore di 1. Si osservi preliminarmente che, se n fosse primo, si avrebbe:

$$[a^2]_n = \varphi_n([a]_n) = [0]_n \iff n|a.$$

Si supponga ora che $n = p_1 \cdots p_s$, ove $p_1, \ldots, p_s$ sono primi distinti (Un siffatto intero viene chiamato *square-free integer*).
Sia $[a]_n \in \varphi_n^{-1}([0]_n)$, dunque, essendo $a^2 \equiv 0 (mod \, n)$, si ha che per ogni $i = 1, \ldots, s$ $p_i | a^2$. Sfruttando la primalità dei p_i, si ottiene che per ogni $i = 1, \ldots, s$ $p_i | a$. Da ciò se ne deduce che $mcm(p_1, \ldots, p_s) = p_1 \cdots p_s = n | a$, ossia $[a]_n = [0]_n$.
Ciò mostra che:

$$(\exists p_1, \ldots, p_s \, primi \, distinti \, t.c. \, n = p_1 \cdots p_s) \Rightarrow (\varphi_n^{-1}([0]_n) = \{[0]_n\}).$$

Si provi il viceversa. Sia n tale che $n = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$, ove $\alpha_1 \geq 2$ (È possibile fattorizzare n poiché è maggiore di 1 ed inoltre, a meno di scambiare l'ordine dei p_i, si può supporre $\alpha_1 \geq 2$).
Si ponga $a := p_1^{\alpha_1 - 1} \cdots p_t^{\alpha_t}$. Ovviamente $[a]_n \neq [0]_n$, ma $[a^2]_n = [0]_n$, in quanto $2\alpha_1 - 2 \geq \alpha_1$ e dunque $a^2 = p_1^{2\alpha_1 - 2} \cdots p_t^{2\alpha_t}$ è un multiplo di n. Ma allora $\varphi_n^{-1}([0]_n) \neq \{[0]_n\}$.
Quindi $\varphi_n^{-1}([0]_n) = \{[0]_n\}$ se e solo se n è uno square-free integer.

(b) Si osservi preliminarmente che φ_n è surgettiva se e solo se φ_n è ingettiva e che $\varphi([1]_n) = \varphi_n([-1]_n) = [1]_n$. Se $n > 2$, $[1]_n \neq [-1]_n$ e dunque l'applicazione non è suriettiva per nessun $n > 2$. Mediante un calcolo diretto si ha che per $n = 2$ φ è surgettiva.

3 (a) Si osservi che $x^4 + [1]_5 = x^4 - [4]_5 = (x^2 - [2]_5)(x^2 + [2]_5)$. Mediante un calcolo diretto si ottiene che i due fattori quadratici non ammettono radici e dunque sono irriducibili. Ciò fornisce una fattorizzazione di $\overline{f}(x)$.

(b) Sfruttando il punto (a), si potrebbe pensare di trovare un primo p tale che esista $t \in \mathbb{Z}$ t.c. $p - 1 = t^2$. In tal caso:

$$x^4 + [1]_p = x^4 - [p-1]_p = (x^2 - [t]_p)(x^2 + [t]_p)$$

e quindi $\overline{f}(x)$ è riducibile. Un metodo per trovare due siffatti primi maggiori di 5 è il seguente:
$3^2 + 1 = 10$ che non è primo e quindi lo si scarta;
$4^2 + 1 = 17$ che è primo e quindi è utile per mostrare l'asserto;
$5^2 + 1 = 26$ che non è primo e quindi lo si scarta;
$6^2 + 1 = 37$ che è primo e quindi è utile per mostrare l'asserto.

Traccia 97

1 (a) Sia n un intero positivo. Si consideri l'insieme

$$H_n = \{\sigma \in A_n | o(\sigma) \leq 2\}.$$

Determinare tutti i valori di n per i quali H è un sottogruppo di A_n e dire in quali casi non è banale.

(b) Determinare un sottogruppo di A_{12} avente ordine 16.

(c) Determinare un sottogruppo di A_{10} avente ordine 6.

2 Dati gli interi positivi n e m, si consideri l'applicazione

$$\varphi_{n,m} : \mathbb{Z}_{10} \times \mathbb{Z}_{25} :\longrightarrow \mathbb{Z}_5 \times \mathbb{Z}_5$$

tale che, per ogni $a, b \in \mathbb{Z}$, $\varphi_{n,m}([a]_{10}, [b]_{25}) = ([na]_5, [mb]_5)$.

(a) Determinare il numero delle applicazioni $\varphi_{n,m}$ che sono omomorfismi di anelli.

(b) Determinare tutte le coppie (n, m) per le quali $\varphi^{-1}_{n,m}([0]_5, [0]_5)$ ha esattamente 10 elementi.

(c) Determinare tutte le coppie (n, m) per le quali $\varphi_{n,m}$ è surgettiva.

3 Dato un primo positivo p, siano $f(x) = x^{p^2} + x^p - 928$ e $g(x) = x^{2p} + x^2 - 928$, e siano $\overline{f}(x), \overline{g}(x) \in \mathbb{Z}_p[x]$ le loro riduzioni modulo p. Determinare tutti i valori di p per i quali $\overline{f}(x)$ e $\overline{g}(x)$ hanno in $\mathbb{Z}_p$ una radice in comune non nulla.

Svolgimento

1 (a) Si osservino preliminarmente i seguenti casi:
se $n = 1$, ovviamente $H_1 = \{id\}$;
se $n = 2$, $H_2 = A_2 = \{id\}$;
se $n = 3$, A_3 è costituito da due 3−cicli e dalla permutazione identica, quindi $H_3 = \{id\}$;
se $n = 4$, le permutazioni in A_4 hanno struttura ciclica $(1, 1, 1, 1)$, $(3, 1)$ oppure $(2, 2)$. Quelle aventi struttura ciclica $(3, 1)$ hanno periodo 3, quindi H_4 è costituito dalle permutazioni di S_4 aventi struttura ciclica $(1, 1, 1, 1)$ (la permutazione identica) e $(2, 2)$, che sono esattamente 3. Quindi:

$$H_4 = \{id, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}.$$

Per verificare che esso è un gruppo è sufficiente osservare la seguente tabella di composizione:

$\circ$	id	$(1,2)(3,4)$	$(1,3)(2,4)$	$(1,4)(2,3)$
id	id	$(1,2)(3,4)$	$(1,3)(2,4)$	$(1,4)(2,3)$
$(1,2)(3,4)$	$(1,2)(3,4)$	id	$(1,4)(2,3)$	$(1,3)(2,4)$
$(1,3)(2,4)$	$(1,3)(2,4)$	$(1,4)(2,3)$	id	$(1,2)(3,4)$
$(1,4)(2,3)$	$(1,4)(2,3)$	$(1,3)(2,4)$	$(1,2)(3,4)$	id

Sia $n \geq 5$ allora $(1,2)(3,4), (1,2)(4,5) \in H_n$, ma $(1,2)(3,4)(1,2)(4,5) = (3,4,5) \notin H_n$. Ciò mostra che per $n \geq 5$ H_n non è un gruppo.

(b) Si considerino $\gamma_1 := (1,2,3,4)(5,6), \gamma_2 := (7,8,9,10)(11,12) \in A_{12}$ e si ponga:

$$L := \{\gamma_1^h \gamma_2^k | h,k \in \mathbb{Z}\}.$$

Essendo γ_1 e γ_2 a supporto disgiunto si verifica facilmente che L, munito della operazione di composizione, è un sottogruppo di A_{12} di ordine 16.

(c) Si consideri $\gamma := (1,2,3)(4,5)(6,7) \in A_{10}$. Essendo $o(\gamma) = 6$, si ha che $< \gamma >$ è il sottogruppo cercato.

2 (a) Si osservi preliminarmente che, per ogni $n, m \in \mathbb{Z}$, $n, m > 0$, $\varphi_{n,m}$ è ben definita ed è un omomorfismo di gruppi additivi. Restano unicamente da trovare i valori di n, m per i quali $\varphi_{n,m}$ conserva il prodotto.
Siano n, m tali che $\varphi_{n,m}$ è un omomorfismo di anelli. In particolare:

$$([n]_5, [m]_5) = \varphi_{n,m}(([1]_{10}, [1]_{25})) = \varphi_{n,m}(([1]_{10}, [1]_{25})([1]_{10}, [1]_{25})) =$$

$$= ([n]_5, [m]_5)([n]_5, [m]_5) = ([n^2]_5, [m^2]_5).$$

Ossia:
$$\begin{cases} n \equiv n^2 \, (mod\, 5) \\ m \equiv m^2 \, (mod\, 5) \end{cases} \iff \begin{cases} 5|n(n-1) \\ 5|m(m-1) \end{cases} \iff \begin{cases} 5|n \vee 5|(n-1) \\ 5|m \vee 5|(m-1) \end{cases}$$

Viceversa, si supponga che $\begin{cases} 5|n \vee 5|(n-1) \\ 5|m \vee 5|(m-1) \end{cases}$.
Per mostrare $\varphi_{n,m}$ è un omomorfismo di anelli bisogna provare che, per ogni $a, b, c, d \in \mathbb{Z}$, si ha che :

$$([nac]_5, [mbd]_5) = \varphi_{n,m}(([ac]_{10}, [bd]_{25})) = \varphi_{n,m}(([a]_{10}, [b]_{25})([c]_{10}, [d]_{25})) =$$

$$= \varphi_{n,m}(([a]_{10}, [b]_{25}))\varphi_{n,m}(([c]_{10}, [d]_{25})) = ([na]_5, [mb]_5)([nc]_5, [md]_5) =$$
$$= ([n^2ac]_5, [m^2bd]_5).$$

Ossia:
$$\begin{cases} nac \equiv n^2ac \, (mod\, 5) \\ mbd \equiv m^2bd \, (mod\, 5) \end{cases} \iff \begin{cases} 5|n(n-1)ac \\ 5|m(m-1)bd \end{cases}$$

Stante la supposizione, si ha l'asserto.
Ciò dimostra che $\varphi_{n,m}$ è un omomorfismo di anelli se e solo se

$$\begin{cases} 5|n \vee 5|(n-1) \\ 5|m \vee 5|(m-1) \end{cases}$$

e quindi vi sono 4 distinti omomorfismi di anelli:

- se $5|n$ e $5|m$, $\varphi_{n,m}$ è l'omomorfismo nullo;
- se $5|n$ e $5|m-1$, $\varphi_{n,m}$ è l'omomorfismo tale che, per ogni $[a]_n \in \mathbb{Z}_n$,$[b]_m \in \mathbb{Z}_m$, $\varphi([a]_n, [b]_m) = ([0]_5, [b]_5)$;
- se $5|n-1$ e $5|m$, $\varphi_{n,m}$ è l'omomorfismo tale che, per ogni $[a]_n \in \mathbb{Z}_n$,$[b]_m \in \mathbb{Z}_m$, $\varphi([a]_n, [b]_m) = ([a]_5, [0]_5)$;
- se $5|n-1$ e $5|m-1$, $\varphi_{n,m}$ è l'omomorfismo tale che, per ogni $[a]_n \in \mathbb{Z}_n$,$[b]_m \in \mathbb{Z}_m$, $\varphi([a]_n, [b]_m) = ([a]_5, [b]_5)$.

(b) Per ogni $n, m \in \mathbb{Z}$, $n, m > 0$ si definiscano le seguenti applicazioni:

$$\varphi_n^{(1)} : \mathbb{Z}_{10} \longrightarrow \mathbb{Z}_5$$

tale che, per ogni $[a]_{10} \in \mathbb{Z}_{10}$, $\varphi_n^{(1)}([a]_{10}) = [na]_5$;

$$\varphi_m^{(2)} : \mathbb{Z}_{25} \longrightarrow \mathbb{Z}_5$$

tale che, per ogni $[a]_{25} \in \mathbb{Z}_{25}$, $\varphi_m^{(2)}([a]_{25}) = [ma]_5$.
È facile osservare che:

($*$) $\varphi_{n,m}^{-1}([0]_5, [0]_5) = \left(\varphi_n^{(1)}\right)^{-1}([0]_5) \times \left(\varphi_m^{(2)}\right)^{-1}([0]_5)$;

($**$) $\varphi_n^{(1)}$ e $\varphi_m^{(2)}$ sono omomorfismi di gruppi additivi, quindi $Ker\left(\varphi_n^{(1)}\right) = \left(\varphi_n^{(1)}\right)^{-1}([0]_5)$ è un sottogruppo (ciclico) di $\mathbb{Z}_{10}$ e $Ker\left(\varphi_m^{(2)}\right) = \left(\varphi_n^{(2)}\right)^{-1}([0]_5)$ è un sottogruppo (ciclico) di $\mathbb{Z}_{25}$.

Si supponga di avere n, m tali che la cardinalità di $\varphi_{n,m}^{-1}([0]_5, [0]_5)$ (d'ora in poi si userà il simbolo $|\cdot|$ per indicare la cardinalità di un insieme) sia pari a 10. Si noti che

$$\{[0]_{25}, [5]_{25}, [10]_{25}, [15]_{25}, [20]_{25}\} \subset \left(\varphi_m^{(2)}\right)^{-1}([0]_5)$$

da cui $\left|\left(\varphi_m^{(2)}\right)^{-1}([0]_5)\right| \geq 5$.
Usando la ($**$), si ottiene che $\left|\left(\varphi_n^{(1)}\right)^{-1}([0]_5)\right| \in \{1, 2, 5, 10\}$. Utilizzando la ($*$) e che $\left|\left(\varphi_m^{(2)}\right)^{-1}([0]_5)\right| \geq 5$, si possono escludere i

casi in cui

$$\left|\left(\varphi_n^{(1)}\right)^{-1}([0]_5)\right| = 10 \vee \left|\left(\varphi_n^{(1)}\right)^{-1}([0]_5)\right| = 5.$$

Inoltre $\left|\left(\varphi_n^{(1)}\right)^{-1}([0]_5)\right| \neq 1$, poiché non esiste alcun sottogruppo di ordine 10 in $\mathbb{Z}_{25}$. Ciò mostra che: $\left|\left(\varphi_n^{(1)}\right)^{-1}([0]_5)\right| = 2$, ossia $\left(\varphi_n^{(1)}\right)^{-1}([0]_5) = \{[0]_{10}, [5]_{10}\}$. Ciò avviene se e solo se $5 \not| n$.
Affinché $|\varphi_{n,m}^{-1}([0]_5, [0]_5)| = 10$ si deve avere $\left|\left(\varphi_m^{(2)}\right)^{-1}([0]_5)\right| = 5$, ossia $\left(\varphi_m^{(2)}\right)^{-1}([0]_5) =< [5]_{25} >$. Ciò avviene se e solo se $5 \not| m$.
In conclusione, se $|\varphi_{n,m}^{-1}([0]_5, [0]_5)| = 10$, allora $5 \not| n \wedge 5 \not| m$.
Viceversa, si supponga $5 \not| n \wedge 5 \not| m$, allora, mediante un calcolo diretto, $|\varphi_{n,m}^{-1}([0]_5, [0]_5)| = 10$.

(c) Si osservi che $\varphi_{n,m}$ è surgettiva se e solo se, per ogni $a, b \in \mathbb{Z}$, il sistema: $(*) \begin{cases} nx \equiv a (mod\, 5) \\ my \equiv b (mod\, 5) \end{cases}$ ammette soluzione.
$(*)$ ammette soluzione (per ogni $a, b \in \mathbb{Z}$) se e solo se $5 \not| n \wedge 5 \not| m$

3 Si osservi preliminarmente che $928 = 2^5 \cdot 29$. Sia p un primo positivo, allora $\overline{f}(x), \overline{g}(x) \in \mathbb{Z}_p[x]$ ammettono radice nulla se e solo se $p = 2 \vee p = 29$.
Sia $p = 2$, allora $\overline{f}(x)$ e $\overline{g}(x)$ ammettono $[1]_2$ come radice.
Sia $p = 29$, allora $\overline{f}(x)$ non ammette una radice non nulla. Se per assurdo esistesse $a \in \mathbb{Z}$ tale che $[a]_p$ è radice non nulla di $\overline{f}(x)$, utilizzando il piccolo Teorema di Fermat, $[a]_p + [a]_p = [0]_p$, ossia $2a \equiv 0 (mod\, p)$, da cui si avrebbe che $p|a$,ossia $[a]_p = [0]_p$. Da ciò si deduce che per $p = 29$ non si hanno radici comuni non nulle.
Sia $p \neq 2 \wedge p \neq 29$ un primo positivo. Si supponga che $[a]_p$ sia una radice (certamente non nulla) di $\overline{f}(x)$, allora $[2a]_p = [928]_p$, ossia $[a]_p = [464]_p$, da cui si ottiene che l'unica radice di $\overline{f}(x)$ è $[a]_p = [464]_p$. Utilizzando opportunamente il piccolo Teorema di Fermat, si ha che $[464]_p$ è una radice di $\overline{g}(x)$ se e solo se $[464]_p^2 = [464]_p$, ossia $p|464(464 - 1)$. Avendo supposto che $p \neq 2 \wedge p \neq 29$, si ha che $p|463$. Utilizzando il crivello di Eratostene, si ha che i primi fino a $\lceil \sqrt{463} \rceil = 22$ sono : $2, 3, 5, 7, 11, 13, 17, 19$, ognuno dei quali non divide 463, quindi 463 è primo.
Da ciò si deduce che $\overline{f}(x)$ e $\overline{g}(x)$ hanno in $\mathbb{Z}_p$ una radice in comune non nulla se e solo se $p = 2 \vee p = 463$.

Traccia 98

1 Sia n un intero maggiore di 6. Dato, in S_n, un elemento α di periodo 6, sia $\sigma \in <\alpha>$ tale che $\sigma^3(1) = 2$.

(a) Dire quali sono i possibili valori del periodo di σ.

(b) Per ognuno di tali valori, esibire una coppia (α, σ) corrispondente.

2 Siano n e m interi positivi, e sia data l'applicazione

$$\varphi : \mathbb{Z}_n \longrightarrow \mathbb{Z}_m$$

tale che, per ogni $a \in \mathbb{Z}$, $\varphi([a]_n) = [na]_m$.

(a) Determinare tutte le coppie (n, m) per cui φ è ben definita.

(b) Determinare tutte le coppie (n, m) per cui φ è un omomorfismo di anelli.

(c) Determinare tutte le coppie (n, m) per cui φ è un'applicazione iniettiva.

3 Dato p un numero primo maggiore di 2, si considerino i polinomi

$$f(x) = x^{p^2} + x^p + x - \overline{1} \in \mathbb{Z}_p[x],$$
$$g(x) = x^2 - \overline{2} \in \mathbb{Z}_p[x].$$

(a) Determinare un valore di p tale che $f(x), g(x)$ non siano coprimi.

(b) Determinare un valore di p tale che $f(x), g(x)$ siano coprimi.

Svolgimento

1 (a) Sia $\sigma \in <\alpha>$, quindi, utilizzando il Teorema di Lagrange, si ha che $o(\sigma) \in \{1, 2, 3, 6\}$. Imponendo l'ulteriore condizione che $\sigma^3(1) = 2$, si possono escludere i casi in cui $o(\sigma) = 1$ oppure $o(\sigma) = 3$. Ciò implica che $o(\sigma) \in \{2, 6\}$.

(b)
- <u>**Caso** $o(\sigma) = 2$</u> Si considerino $\alpha := (1, 3, 5, 2, 4, 6)$ e $\sigma = \alpha^3 = (1, 2)(3, 4)(5, 6)$. Essendo $\sigma^3 = \sigma$, si ha $\sigma^3(1) = 2$.
- <u>**Caso** $o(\sigma) = 6$</u> Si consideri $\sigma := \alpha := (1, 3, 5, 2, 4, 6)$. Essendo $\sigma^3 = (1, 2)(3, 4)(5, 6)$, si ha $\sigma^3(1) = 2$.

2 (a) Sia (n, m) una coppia di interi positivi tale che φ sia ben posta. In particolare si deve avere $\varphi([0]_n) = \varphi([n]_n)$, ossia $[0]_m = [n^2]_m$. Ciò mostra che, se φ è ben definita, $m|n^2$.
Viceversa, si supponga che $m|n^2$. Si osservi che, presi $a, b \in \mathbb{Z}$, $\varphi([a]_n) = \varphi([b]_n)$ equivale a richiedere $m|n(a - b)$.
Siano $a, b \in \mathbb{Z}$ tali che $a \equiv b \,(mod\, n)$, ossia $\exists\, q \in \mathbb{Z}$ tale che $nq = (a - b)$. Da ciò si evince che $m|n(a - b) = n^2q$.
Ciò implica che φ è ben definita se e solo se $m|n^2$.

(b) Si osservi preliminarmente che, per ogni coppia (n, m) che rende φ ben definita, si ha che la già citata applicazione è un omomorfismo di gruppi additivi.
Sia (m, n) una coppia che rende φ un omomorfismo di anelli. In particolare:

$$[n]_m = \varphi([1]_n) = \varphi([1]_n[1]_n) = \varphi([1]_n)\varphi([1]_n) =$$

$$= [n]_m[n]_m = [n^2]_m.$$

Affinché sia ben definita, si deve avere anche $m|n^2$, da cui si ottiene che $m|n$.
Viceversa si supponga che $m|n$. Bisogna provare che, per ogni $a, b \in \mathbb{Z}$,

$$[nab]_m = \varphi([a]_m[b]_m) = \varphi([a]_m)\varphi([b]_m) = [n^2ab]_m.$$

Quindi, stante l'ipotesi che $m|n$, si ha l'asserto.
In definitiva φ è un omomorfismo di anelli se e solo se $m|n$.

(c) Sia (n, m) un coppia di interi tale che φ sia ingettiva. Si osservi che, essendo $\varphi([0]_n) = \varphi([m]_n)$, si ha $[0]_n = [m]_n$, ossia $n|m$. Si dimostri che $m = n^2$.
Se $n = 1$, allora $m = 1$, in quanto $m|n^2$ e quindi si ha l'asserto.
Sia $n > 1$, allora $m > 1$ in quanto $n|m$. Utilizzando il Teorema di fattorizzazione unica su n, m, $\exists p_1, \ldots, p_s$ primi positivi a due a due distinti, $q_1, \ldots, q_t$ primi positivi a due a due distinti e $\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_t \in \mathbb{N}^*$ tali che $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ e $m = q_1^{\beta_1} \cdots q_t^{\beta_t}$. Si ha che, per ogni $i \in \{1, \ldots, s\}$, $p_i|m$ poiché $n|m$, quindi $\{p_1, \ldots, p_s\} \subset \{q_1, \ldots, q_t\}$. Inoltre, per ogni $i \in \{1, \ldots, t\}$, $q_i|n$ poiché $m|n^2$, da cui $\{p_1, \ldots, p_s\} \supset \{q_1, \ldots, q_t\}$. Ciò prova che $\{p_1, \ldots, p_s\} = \{q_1, \ldots, q_t\}$ e quindi $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ e $m = p_1^{\beta_1} \cdots p_s^{\beta_s}$. Resta da provare che, per ogni $i \in \{1, \ldots, s\}$, $\beta_i = 2\alpha_i$. Si osservi che, per ogni $i \in \{1, \ldots, s\}$, $\alpha_i \leq \beta_i \leq 2\alpha_i$ in quanto $m|n^2$ e $n|m$. Se per assurdo esistesse $\bar{i} \in \{1, \ldots, s\}$ tale che $\beta_{\bar{i}} < 2\alpha_{\bar{i}}$, si ponga $\gamma := \beta_{\bar{i}} - \alpha_{\bar{i}}$.
Si ha che: $m|p_1^{2\alpha_1} \cdots p_{\bar{i}}^{\beta_{\bar{i}}} \ldots p_s^{2\alpha_s} = n \cdot p_1^{\alpha_1} \cdots p_{\bar{i}}^{\gamma} \cdots p_s^{\alpha_s}$, ossia $\varphi([p_1^{\alpha_1} \cdots p_{\bar{i}}^{\gamma} \cdots p_s^{\alpha_s}]_n) = \varphi([0]_n)$.
Essendo φ ingettiva si ha che $n|p_1^{\alpha_1} \cdots p_{\bar{i}}^{\gamma} \cdots p_s^{\alpha_s}$, ma ciò è assurdo in quanto $p_{\bar{i}}^{\alpha_{\bar{i}}} \not| p_{\bar{i}}^{\gamma}$ essendo $\gamma < \alpha_{\bar{i}}$. Ciò implica che $m = n^2$.
Viceversa si supponga che $m = n^2$. Siano $a, b \in \mathbb{Z}$ tali che $\varphi([a]_n) = \varphi([b]_n)$, ossia $n^2|n(a - b)$, allora $n|(a - b)$, ossia $[a]_n = [b]_n$. Ciò mostra che φ è ingettiva.
Quindi φ è ingettiva se e solo se $m = n^2$.

3 (a) Una maniera per poter trovare un fattore comune ad $f(x)$ e $g(x)$ può essere quella di cercare un primo p tale che i due polinomi abbiano una radice comune.

Sia p un primo maggiore di 2. Si supponga che esista $a \in \mathbb{Z}$ tale che $f([a]_p) = 0$. Utilizzando opportunamente il piccolo Teorema di Fermat, si ha $3[a]_p = [1]_p$. Si supponga che $p \neq 3$, allora $[a]_p = [3]_p^{-1}$. Bisogna cercare ora un primo (maggiore di 3) tale che $g([3]_p^{-1}) = [0]_p$, equivalentemente $[3]_p^{-2} = [2]_p \iff [1]_p = [18]_p$. Un siffatto primo è proprio 17.

Osservazione È possibile trovare un $a \in \mathbb{Z}$ tale che $0 \leq a \leq 16$, $[a]_{17} = [3]_{17}^{-1}$ nella seguente maniera:

Si osservi che $3, 17$ sono coprimi quindi, per il Lemma di Bézout, esistono $s, t \in \mathbb{Z}$ tali che $3 \cdot s + 17 \cdot t = 1$. Ciò mostra che $[s]_{17} = [3]_{17}^{-1}$, poiché $[3]_{17}[s]_{17} = [1]_{17}$. Per determinare i coefficienti di Bézout non resta che applicare l'algoritmo delle divisioni successive come segue:

$$17 = 3 \cdot 5 + 2$$

$$3 = 2 \cdot 1 + 1$$

$$2 = 1 \cdot 2$$

Da cui $2 = 17 - 3 \cdot 5$ e quindi $1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (17 - 3 \cdot 5) = -1 \cdot 17 + 6 \cdot 3$. In definitiva $[3]_{17}^{-1} = [6]_{17}$.

(b) Un' idea per trovare un primo tale che i due polinomi siano coprimi può essere quella di trovarne uno per il quale $g(x)$ ha due radici che non annullano $f(x)$.

Si osservi che per $p = 3$ e $p = 5$ $g(x)$ non ammette radici. Per $p = 7$ si ha che $g([3]_7) = g([4]_7) = [0]_7$, mentre $f([3]_7) = [1]_7$ e $f([4]_7) = [4]_7$.

Traccia 99

1 Data in S_{18} la permutazione:

$$\alpha = (1,2,3,4)(5,6,7)(8,9,10,11)(12,13,14)(15,16)(17,18)$$

per ogni $\sigma \in S_{18}$ si consideri l'insieme $H(\sigma) = \{\tau \in <\alpha> | \sigma\tau = \tau\sigma\}$.
Si determini $H(\sigma)$ per

(a) $\sigma = (1,9,4,8,3,11,2,10)$;

(b) $\sigma = (5,6,7)(12,14,13)$;

(c) $\sigma = (15,17)(16,18)(1,4,3,2)$.

2 Dato un un intero $n > 1$, si considerino le applicazioni

$$\varphi_n : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{2n}$$

tale che, per ogni $[a]_n \in \mathbb{Z}_n$, $\varphi_n([a]_n) = [a^2]_{2n}$

$$\psi_n : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{4n}$$

tale che, per ogni $[a]_n \in \mathbb{Z}_n$, $\psi_n([a]_n) = [a^4]_{4n}$.

(a) Determinare tutti i valori di n per i quali φ_n è ben definita.

(b) Determinare tutti i valori di n per i quali ψ_n è ben definita.

(c) Determinare $\psi_{40}^{-1}([0]_{160})$.

3 Sia p un primo nella forma $2^{2^N} + 1$, ove N è un opportuno intero.
Provare che il polinomio $f(x) = x^{3p} + x^{2p} + x^p + \overline{1} \in \mathbb{Z}_p[x]$ si decompone nel prodotto di fattori lineari.

Svolgimento

1 Si osservi preliminarmente che, per ogni σ, $H(\sigma)$ è un sottogruppo di α, infatti:
$H(\sigma)$ è non vuoto in quanto $id \in H(\sigma)$. Siano $\gamma_1, \gamma_2 \in H(\sigma)$, allora $\gamma_1\gamma_2^{-1} \in H(\sigma)$ poiché

$$\gamma_1\gamma_2^{-1}\sigma = \gamma_1\sigma\gamma_2^{-1} = \sigma\gamma_1\gamma_2^{-1}.$$

Inoltre $H(\sigma) \subset <\alpha>$. Quindi, se $\alpha \in H(\sigma)$, $<\alpha> \subset H(\sigma)$, da cui $H(\sigma) = <\alpha>$.

(a) Si verifichi preliminarmente che $\alpha \in H(\sigma)$, ossia $\alpha\sigma = \sigma\alpha$. Sebbene si possa effettuare un calcolo diretto, di seguito verrà utilizzato un metodo basato sul "buon senso". Si osservi che $(5,6,7)(12,13,14)(15,16)(16,17)$ è a supporto disgiunto con σ, quindi:

$$\alpha\sigma = \sigma\alpha \iff (1,2,3,4)(8,9,10,11)\sigma = \sigma(1,2,3,4)(8,9,10,11)$$

poiché permutazioni a supporto disgiunto commutano. Inoltre $(1,2,3,4)(8,9,10,11) = \sigma^6$, da cui $\sigma^6\sigma = \sigma^7 = \sigma\sigma^6$. Per l'osservazione precedente, $H(\sigma) =< \alpha >$.

(b) Precedendo come in (a):

$$\alpha\sigma = \sigma\alpha \iff (5,6,7)(12,14,13)\sigma = \sigma(5,6,7)(12,14,13).$$

Osservando che $(12,14,13) = (12,13,14)^2$ si ottiene $(5,6,7)(12,14,13)\sigma = \sigma(5,6,7)(12,13,14)$, da cui $H(\sigma) =< \alpha >$.

(c) Si vuole nuovamente provare che $\alpha\sigma = \sigma\alpha$. Essendo $(1,2,3,4)^3 = (1,4,3,2)$, è sufficiente mostrare che $(15,16)(17,18)(15,17)(16,18) = (15,17)(16,18)(15,16)(17,18)$.
Mediante un calcolo diretto si prova quanto richiesto e quindi $H(\sigma) =< \alpha >$.

2 (a) Si supponga che n sia un intero positivo tale che φ_n è ben definita. In particolare, essendo $[0]_n = [n]_n$,

$$[0]_{2n} = \varphi_n([0]_n) = \varphi_n([n]_n) = [n^2]_{2n}.$$

Ciò mostra che, se φ_n è ben definita, si ha $2n|n^2$, ossia n è pari.
Viceversa, si supponga che $2|n$. Siano $a, b \in \mathbb{Z}$ tali che $a \equiv b \,(mod\ n)$.
Si osservi che $2|(a+b)$, in quanto $2|n$, per transitività $2|(a-b)$ e quindi $2|(a-b+2b)$.
Verificare la buona definizione di φ_n equivale a mostrare che, sotto le presenti ipotesi, $\varphi_n([a]_n) = \varphi_n([b]_n)$, ossia $2n|(a^2-b^2)$.
Essendo $a^2 - b^2 = (a-b)(a+b)$, $2n|(a-b)(a+b)$, in quanto $2|(a+b)$ e $n|(a-b)$.
Ciò implica che φ_n è ben definita se e solo se n è pari.

(b) Si supponga che n sia un intero positivo tale che ψ_n è ben definita. In particolare, essendo $[0]_n = [n]_n$,

$$[0]_{4n} = \psi_n([0]_n) = \psi_n([n]_n) = [n^4]_{4n}.$$

Si osservi che se $4n|n^4$, $4|n^3$ ed in particolare $2|n$. Ciò mostra che, se ψ_n è ben definita, si ha che n è pari.
Viceversa, si supponga che $2|n$. Siano $a, b \in \mathbb{Z}$ tali che $a \equiv b \,(mod\ n)$.
Si osservi che:

- $a^4 - b^4 = (a^2 - b^2)(a^2 + b^2) = (a - b)(a + b)(a^2 + b^2)$;
- per il ragionamento precedente $2|(a + b)$;
- $2|(a^2 + b^2)$, in quanto $2|(a^2 - b^2)$.

Verificare la buona definizione di ψ_n equivale a mostrare che, sotto le presenti ipotesi, $\psi_n([a]_n) = \psi_n([b]_n)$, ossia $4n|(a^4 - b^4)$.
L'asserto discende dalle osservazioni fatte.
Ciò conclude che ψ_n è ben definita se e solo se n è pari.

(c) Sia $a \in \mathbb{Z}$, allora
$$2^5|a^4 \iff 4|a.$$
Infatti, si supponga che $2^5|a^4$. In particolare $2|a$ e quindi:
$$a \equiv 0\,(mod\,4) \vee a \equiv 2\,(mod\,4).$$
Se, per assurdo, $a \equiv 2\,(mod\,4)$ esisterebbe $q \in \mathbb{Z}$ t.c. $a = 2(2q+1)$, da cui $2^5|2^4(2q + 1)^4$ e quindi $2|(2q + 1)^4$.
Si supponga che $4|a$, allora $2^5|a^4$.
Sia $a \in \mathbb{Z}$, allora
$$2^5 \cdot 5 = 160|a^4 \iff \begin{cases} a^4 \equiv 0\,(mod\ 2^5) \\ a^4 \equiv 0\,(mod\ 5) \end{cases} \iff$$
$$\iff \begin{cases} a \equiv 0\,(mod\ 4) \\ a \equiv 0\,(mod\ 5) \end{cases}$$
Quindi
$$160|a^4 \iff a \in \{20k \mid k \in \mathbb{Z}\}.$$
Si osservi che $\psi_{40}^{-1}([0]_{160}) = \{[a]_{40} | \, a^4 \equiv 0\,(mod\ 160)\}$, quindi, per quanto appena mostrato, $\psi_{40}^{-1}([0]_{160}) = \{[0]_{40}, [20]_{40}\}$.

3 Sia p un primo nella forma $p = 2^{2^N} + 1$. Essendo $f(x)$ un polinomio a coefficienti in $\mathbb{Z}_p$, $f(x) = (x^3 + x^2 + x + \overline{1})^p$. Inoltre $x^3 + x^2 + x + \overline{1} = (x + \overline{1})(x^2 + \overline{1})$.
Da ciò si evince che $f(x)$ si decompone nel prodotto di fattori lineari se e solo se il polinomio $x^2 + \overline{1} \in \mathbb{Z}_p[x]$ ammette radici.
Si supponga di avere $\alpha \in \mathbb{Z}_p$ una radice. Essa verifica la seguente identità: $\alpha^2 = -\overline{1}$, da cui $\alpha^4 = \overline{1}$.
Ciò mostra che $o(\alpha)|4$. Ma $o(\alpha)$ non può essere 1 o 2, altrimenti non si avrebbe $\alpha^2 = -\overline{1}$, quindi $o(\alpha) = 4$.
Viceversa, prendendo un elemento di periodo 4, il suo quadrato ha periodo 2 e quindi è uguale a $-\overline{1}$.
L'esercizio viene risolto nel momento in cui si riesce a determinare l'esistenza di un elemento di periodo 4 in $\mathbb{Z}_p^*$. Essendo p un primo nella forma $p = 2^{2^N} + 1$ per un opportuno $N \in \mathbb{Z}$, si ha che $|\mathbb{Z}_p^*| =$

$p-1=2^{2^N}$. Si osservi che, per ogni $N>0$, $4|2^{2^N}$. Essendo $\mathbb{Z}_p^*$ un gruppo ciclico, esiste un unico sottogruppo (ciclico) di ordine 4 in $\mathbb{Z}_p^*$. I due generatori di questo sottogruppo sono le radici del polinomio in causa.
Il caso in cui $N=0$, ossia $p=2$, lo si può giustificare osservando che $x^2+\overline{1}=(x+\overline{1})^2$.

Traccia 100

(1) (a) Provare che in S_{17} il numero degli elementi di periodo 210 è $\frac{17!}{210}$.

(b) Provare che in S_{13} , il numero dei sottogruppi ciclici di ordine 13 è 11!.

(c) Provare che in S_{12} il numero degli elementi di periodo 9 è $\frac{12!}{18}$.

(2) (a) Per ogni intero a sia $\varphi(a) = a^5 - a^4 + a^3 - a^2 + a - 1$. Sia, inoltre, N un intero positivo. Determinare tutti i valori di a per i quali 2^N divide $\varphi(a)$.

(b) Dire se l'applicazione $\psi : \mathbb{Z} \to \mathbb{Z}_3$, tale che, per ogni $a \in \mathbb{Z}$, si ha che $\psi(a) := \left[\sum_{i=1}^{103} a^i\right]_3$, è un omomorfismo di anelli.

(3) Dato un numero primo positivo p, sia $f(x) = x^5 + x^4 + x^3 + x^2 + x + \overline{1} \in \mathbb{Z}_p[x]$.

(a) Determinare tutti i valori di p per i quali il numero delle radici di $f(x)$ in $\mathbb{Z}_p$ è pari.

(b) Provare che per nessun valore di p il polinomio $f(x)$ possiede in $\mathbb{Z}_p[x]$ un fattore di irriducibile di grado 3.

Svolgimento

1 (a) Si osservi preliminarmente che $210 = 2\cdot 3\cdot 5\cdot 7$, quindi un elemento in S_{17} ha periodo 210 se e solo se la sua struttura ciclica è data da $(7, 5, 3, 2)$. Da ciò si evince che è sufficiente contare tutti gli elementi aventi struttura ciclica $(7, 5, 3, 2)$.
Si osservi che il numero di $7-$cicli in S_{17} è dato da $\frac{1}{7}\frac{17!}{10!}$. Si può pensare che, una volta fissato un $7-$ciclo, bisogna considerare le permutazioni sui restanti 10 elementi lasciati fissi dal $7-$ciclo come elementi di S_{10}. Quindi tutte le possibili permutazioni di S_{17} aventi struttura ciclica $(7, 5, 1, 1, 1, 1, 1)$ sono $\frac{1}{7}\frac{17!}{10!}\cdot\frac{1}{5}\frac{10!}{5!}$. Procedendo in questa maniera si ottiene che tutte le possibili permutazioni di S_{17} aventi struttura ciclica $(7, 5, 3, 2)$ sono:

$$\frac{1}{7}\frac{17!}{10!}\cdot\frac{1}{5}\frac{10!}{5!}\cdot\frac{1}{3}\frac{5!}{2!}\cdot\frac{1}{2}\frac{2!}{0!} = \frac{17!}{2\cdot 3\cdot 5\cdot 7} = \frac{17!}{210}$$

(b) Si osservi preliminarmente che il numero di $13-$cicli in S_{13} è dato da: $\frac{1}{13}\frac{13!}{1} = 12!$. Inoltre ogni gruppo ciclico di ordine 13 ha $\varphi(13) = 12$ generatori. Da ciò si evince che il numero di sottogruppi ciclici aventi ordine 13 è dato dal numero di tutti i possibili $13-$cicli fratto il numero di $13-$cicli che sono generatori dello stesso gruppo ciclico, ossia:

$$\frac{12!}{\varphi(13)} = 11!$$

(c) In S_{12} un elemento ha periodo 9 se e solo se ha struttura ciclica $(9,1,1,1)$ oppure $(9,3)$. Quindi, per contare tutti gli elementi di periodo 9, è sufficiente contare gli elementi aventi struttura ciclica $(9,1,1,1)$, quelli aventi struttura ciclica $(9,3)$ e poi sommarli.
Mediante un ragionamento analogo a quello in (a) si ha che il numero di permutazioni aventi struttura ciclica $(9,3)$ è dato da $\frac{1}{9}\frac{12!}{3!}\cdot\frac{1}{3}\frac{3!}{0!}=\frac{12!}{27}$
Il numero di $9-$cicli in S_{13} è dato da $\frac{1}{9}\frac{12!}{3!}=\frac{12!}{54}$.
Da ciò si evince che $\frac{12!}{27}+\frac{12!}{54}=\frac{12!}{18}$.

2 (a) Si osservi preliminarmente che, per ogni intero a,

$$\varphi(a)=(a^4+a^2+1)(a-1).$$

Si supponga di avere un a intero tale che $2^N|\varphi(a)$. È facile osservare che $MCD(a^4+a^2+1,2^N)=1$. Se per assurdo $MCD(a^4+a^2+1,2^N)\neq 1$, allora $2|a^4+a^2+1$, ma ciò è assurdo. Ciò mostra che $2^N|(a-1)$.
Viceversa, si supponga di avere un intero a tale che $2^N|(a-1)$. Allora $2^N|\varphi(a)$.
Ciò mostra che $2^N|\varphi(a)$ se e solo se $a\equiv 1\,(mod\ 2^N)$.

(b) Si osservi preliminarmente che:

- $\psi(0)=[0]_3$;
- $\psi(1)=[1]_3$;
- $\sum_{i=1}^{103}2^i=\frac{1-2^{104}}{1-2}-1=2^{104}-2$;
- $\psi(2)=[2]_3^{104}-[2]_3=[2]_3$;
- siano $a,b\in\mathbb{Z}$ tali che $a\equiv b\,(mod\ 3)$, allora $\psi(a)=\psi(b)$.

Ne consegue che, per ogni $a\in\mathbb{Z}$, $\psi(a)=[a]_3$, da cui si ottiene che ψ è un omomorfismo di anelli.

3 (a) Sia $p=2$, allora $f(x)$ ammette come unica radice $[1]_2$.
Sia p un primo positivo maggiore di 2. Si ponga $g(x):=f(x)(x-\overline{1})=x^6-\overline{1}$.
Se $6|p-1$ esiste $\alpha\in\mathbb{Z}_p^*$ tale che $o(\alpha)=6$. In questo caso ogni elemento di $<\alpha>$ è radice di $g(x)$, quindi $g(x)=\prod_{i=0}^{5}(x-\alpha^i)$, da cui $f(x)=\prod_{i=1}^{5}(x-\alpha^i)$ e quindi $f(x)$ ammette esattamente 5 radici distinte.
Si supponga che $6\not|p-1$. Si osservi che $g(x)=x^6-\overline{1}=(x^3-\overline{1})(x^3+\overline{1})$.
Se $p=3$ segue immediatamente che $f(x)$ ammette come radice unicamente $[1]_3$ e $[-1]_3$.
Sia $p>3$. Essendo $[-1]_p$ radice di $x^3+\overline{1}$, si ha che $x+\overline{1}$ divide (x^3+1). Eseguendo la divisione tra polinomi si ha che $x^3+\overline{1}=$

$(x+\overline{1})(x^2-x+\overline{1})$.
Mediante un ragionamento analogo su $x^3-\overline{1}$ si ottiene che $x^3-\overline{1} = (x-\overline{1})(x^2+x+\overline{1})$.
Da ciò deriva che:

$$f(x) = (x+\overline{1})(x^2-x+\overline{1})(x^2+x+\overline{1}).$$

Si pongano:

$$h_1(x) := x^2 - x + \overline{1}$$
$$h_2(x) := x^2 + x + \overline{1}$$

Viene verificata una delle seguenti condizioni:

(i) $h_1(x)$ e $h_2(x)$ sono entrambi irriducibili;
(ii) uno solo tra $h_1(x)$ e $h_2(x)$ è irriducibile;
(iii) $h_1(x)$ e $h_2(x)$ sono entrambi riducibili.

Nel caso (i) $f(x)$ ammette un'unica radice.
Nel caso (ii) $f(x)$ ammette esattamente 3 radici distinte, in quanto, uno tra $h_1(x)$ e $h_2(x)$ è riducibile e si decompone in fattori lineari. Essendo $p > 3$, $-\overline{1}$ non è radice né di $h_1(x)$ né di $h_2(x)$ ed inoltre né $h_1(x)$ né $h_2(x)$ ha una radice multipla altrimenti avrebbe una forma del tipo

$$(x-\alpha)^2 = x^2 + \alpha^2 - 2\alpha x.$$

In particolare $\alpha^2 = \overline{1}$, ossia $\alpha = \overline{1}$ oppure $\alpha = -\overline{1}$, ma ciò è assurdo in quanto non sono radici né di $h_1(x)$ né di $h_2(x)$.
Si supponga di essere nel caso (iii). Si osservi che $MCD(h_1(x), h_2(x)) = 1$, in quanto se, per assurdo, non lo fosse esisterebbe $\alpha \in \mathbb{Z}_p$ tale che $x-\alpha$ dividerebbe sia $h_1(x)$ sia $h_2(x)$. In particolare $(x-\alpha)|h_1(x) - h_2(x)$, ossia $(x-\alpha)|\overline{-2}x$, da cui $\alpha = [0]_p$. Ciò implica che $[0]_p$ è radice di $h_1(x)$ e di $h_2(x)$.
Essendo $MCD(h_1(x), h_2(x)) = 1$, $h_1(x)$ e $h_2(x)$ non ammettono radici comuni e, per quanto detto in precedenza, $-\overline{1}$ non è radice né di $h_1(x)$ né di $h_2(x)$. Inoltre né $h_1(x)$ né $h_2(x)$ ammette una radice doppia, quindi $f(x)$ ammette 5 radici distinte.
Volendo concludere è possibile affermare $f(x)$ ammette un numero di radici pari se e solo se $p = 3$.

(a alternativo) Sia p un primo positivo e si osservi che $[-1]_p$ è radice di $f(x)$. Da ciò deriva che $f(x) = (x+\overline{1})(x^4+x^2+\overline{1})$. Si ponga

$$h(x) := x^4 + x^2 + \overline{1}.$$

Se $\alpha \in \mathbb{Z}_p^*$ è una radice di $h(x)$ allora anche $-\alpha$ è una radice di $h(x)$. In particolare, se $p \neq 2$, $\alpha \neq -\alpha$ e quindi $h(x)$ ammette un

numero pari di radici. Se $p > 2$ allora $f(x)$ ammette un numero pari di radici se e solo se $-\overline{1}$ è radice di $h(x)$, ossia, se e solo se $p = 3$.
Nel caso $p = 2$, $\overline{1}$ è l'unica radice di $f(x)$.

(b) Discende da quanto detto nel punto (a).

Traccia 101

(1) Dato un intero $n \geq 2$, sia $\sigma \in S_n$.

  (a) Provare che, per ogni $\alpha \in S_n$, $Supp\left(\alpha\sigma\alpha^{-1}\right) = \alpha(Supp(\sigma))$.

  (b) Provare che $o\left(\alpha\sigma\alpha^{-1}\right) = o(\sigma)$.

  (c) Determinare la cardinalità dell'insieme $C = \left\{\alpha(1,2)\alpha^{-1} | \alpha \in S_n\right\}$.

(2) (a) Dati due numeri primi positivi distinti p e q, provare che

$$p^{\varphi(pq)} \equiv p^{q-1}\,(mod\,pq).$$

  (b) Dato un numero primo positivo p, determinare, al variare di p, il resto della divisione euclidea di $p^{2p(p-1)}$ per $6p^2$.

(3) Sia p un numero primo positivo.

  (a) Determinare, al variare di p, tutte le radici in $\mathbb{Z}_p$ del polinomio

$$f(x) = x^{(p!)^2} + x^{p!} + \overline{1} \in \mathbb{Z}_p[x].$$

  (b) Determinare, al variare di p, tutte le radici in $\mathbb{Z}_p$ del polinomio

$$g(x) = x^{\left(p^5\right)!} + x^{\left(p^4\right)!} + x^{\left(p^3\right)!} + x^{\left(p^2\right)!} + x^{p!} + \overline{1} \in \mathbb{Z}_p[x].$$

Svolgimento

1 (a) Siano $n \in \mathbb{Z}$, $n \geq 2$, $\alpha, \sigma \in S_n$. Si ponga $X = \{1, \ldots, n\}$ e si ricordi che:

$$Supp\left(\alpha\sigma\alpha^{-1}\right) = \left\{x \in X |\, \alpha\sigma\alpha^{-1}(x) \neq x\right\},$$

$$\alpha(Supp(\sigma)) = \{\alpha(x) |\, x \in X,\, \sigma(x) \neq x\}.$$

Sia $x \in Supp\left(\alpha\sigma\alpha^{-1}\right)$, allora $\sigma(\alpha^{-1}(x)) \neq \alpha^{-1}(x)$. Da ciò deriva che $\alpha^{-1}(x) \in Supp(\sigma)$, da cui si ottiene che $x \in \alpha(Supp(\sigma))$. Ciò mostra che $Supp\left(\alpha\sigma\alpha^{-1}\right) \subset \alpha(Supp(\sigma))$.

Si supponga ora che $y \in \alpha(Supp(\sigma))$, allora $\exists x \in X$ tale che $\alpha(x) = y$ e $\sigma(x) \neq x$, ossia $\sigma(\alpha^{-1}(y)) \neq \alpha^{-1}(y)$, equivalentemente $\alpha(\sigma(\alpha^{-1}(y))) \neq y$. Da quanto detto segue che $Supp\left(\alpha\sigma\alpha^{-1}\right) \supset \alpha(Supp(\sigma))$.

Dalle considerazioni fatte segue l'asserto.

(b) Siano $n \in \mathbb{Z}$, $n \geq 2$, $\alpha \in S_n$. Si consideri la seguente applicazione $\varphi_\alpha : S_n \to S_n$ tale che, per ogni $\sigma \in S_n$, $\varphi_\alpha(\sigma) = \alpha\sigma\alpha^{-1}$. È facile verificare che φ_α è un isomorfismo con inverso $\varphi_{\alpha^{-1}}$.

Sapendo che ogni isomorfismo manda un elemento in un altro avente lo stesso periodo, si ha l'asserto.

(c) Per il punto (b) si ha che ogni elemento di C ha periodo 2. Inoltre, per il punto (a), per ogni $\alpha \in S_n$, $Supp(\alpha(1,2)\alpha^{-1}) = \{\alpha(1), \alpha(2)\}$. Ciò mostra C è dato dall'insieme di tutti i $2-$cicli, che sono esattamente $\frac{1}{2}\frac{n!}{(n-2)!}$.

2 (a) Siano p e q due primi distinti. Si osservi che:

$$pq|(p^{(p-1)(q-1)} - p^{q-1}) \iff \begin{cases} p|(p^{(p-1)(q-1)} - p^{q-1}) \\ q|(p^{(p-1)(q-1)} - p^{q-1}) \end{cases} \iff$$

$$\iff q|(p^{(p-1)(q-1)} - p^{q-1}).$$

Per il piccolo Teorema di Fermat si ha che $p^{q-1} \equiv 1\,(mod\ q)$, da cui $p^{(q-1)(p-1)} \equiv p^{q-1}\,(mod\ q)$, ossia $q|(p^{(p-1)(q-1)} - p^{q-1})$.

(b) La determinazione del resto della divisione euclidea prevede due casi distiniti: p non è coprimo con 6 (ossia $p = 2$ oppure $p = 3$), p è coprimo con 6 (ossia $p > 3$).
Si supponga che $p = 2$, allora bisogna trovare il resto della divisione euclidea di $2^4 = 16$ per 24. In questo caso il resto è proprio dato da 16.
Si supponga che $p = 3$, allora bisogna trovare il resto della divisione euclidea di 3^{12} per 54, ossia bisogna trovare $x \in \mathbb{Z}$, $0 \le x < 54$ tale che $3^{12} \equiv x\,(mod\ 54)$. Quanto detto equivale a risolvere

$$\begin{cases} x \equiv 3^{12}\,(mod\ 2) \\ x \equiv 3^{12}\,(mod\ 27) \end{cases} \iff \begin{cases} x \equiv 1\,(mod\ 2) \\ x \equiv 0\,(mod\ 27) \end{cases}$$

La soluzione cercata è proprio $x = 27$.
Si supponga che $p > 3$, analogamente a quanto detto nel caso $p = 3$, bisogna trovare $x \in \mathbb{Z}$, $0 \le x < 6p^2$ tale che $p^{2p(p-1)} \equiv x\,(mod\ 6p^2)$. Sfruttando la coprimalità di 6 e p^2, il problema è equivalente a risolvere:

$$\begin{cases} x \equiv p^{2p(p-1)}\,(mod\ 6) \\ x \equiv p^{2p(p-1)}\,(mod\ p^2) \end{cases} \iff \begin{cases} x \equiv p^{2p(p-1)}\,(mod\ 2) & (*) \\ x \equiv p^{2p(p-1)}\,(mod\ 3) & (**) \\ x \equiv p^{2p(p-1)}\,(mod\ p^2) & (***) \end{cases}$$

La $(*)$ è equivalente a $x \equiv 1\,(mod\ 2)$, in quanto p è dispari.
La $(**)$ è equivalente a $x \equiv 1\,(mod\ 3)$, in quanto p è coprimo con 3 e, utilizzando il piccolo Teorema di Fermat, $p^2 \equiv 1\,(mod\ 3)$.
La $(***)$ è equivalente a $x \equiv 0\,(mod\ p^2)$, in quanto $p^{2p(p-1)}$ è un multiplo di p^2.
L'asserto equivale quindi a risolvere:

$$\begin{cases} x \equiv 1\,(mod\ 2) \\ x \equiv 1\,(mod\ 3) \\ x \equiv 0\,(mod\ p^2) \end{cases} \iff \begin{cases} x \equiv 1\,(mod\ 6) \\ x \equiv 0\,(mod\ p^2) \end{cases}$$

Essendo p coprimo con 6, per il piccolo Teorema di Fermat, $p^2 \equiv 1\,(mod\ 6)$, quindi il resto cercato è p^2.

3 (a) Sia p un primo positivo. Sia (se esistente) $[a]_p$ una radice di $f(x)$. In particolare $[a]_p \neq [0]_p$, ossia $p \not| a$.
Essendo $[a]_p$ una radice, $[0]_p = [a]_p^{p!^2} + [a]_p^{p!} + [1]_p = [a^{p-1}]_p^{p!p(p-2)!} + [a^{p-1}]_p^{p(p-2)!} + [1]_p$, applicando opportunamente il piccolo Teorema di Fermat, $[3]_p = [0]_p$.
Ciò mostra che $f(x)$ ammette radici se e solo se $p = 3$. Se $p = 3$, mediante un calcolo diretto, le radici di $f(x)$ sono esattamente $[1]_3$ e $[2]_3$.

(b) Sia p un primo positivo. Sia (se esistente) $[a]_p$ una radice di $g(x)$. In particolare $[a]_p \neq [0]_p$, ossia $p \not| a$.
Essendo $[a]_p$ una radice,

$$[0]_p = [a]_p^{(p^5)!} + [a]_p^{(p^4)!} + [a]_p^{(p^3)!} + [a]_p^{(p^2)!} + [a]_p^{p!} + [1]_p =$$

$$= [a^{p-1}]_p^{\left(\left(\prod_{i=p}^{p^5}\right)(p-2)!\right)} + [a^{p-1}]_p^{\left(\left(\prod_{i=p}^{p^4}\right)(p-2)!\right)} + [a^{p-1}]_p^{\left(\left(\prod_{i=p}^{p^3}\right)(p-2)!\right)} +$$

$$+ [a^{p-1}]_p^{\left(\left(\prod_{i=p}^{p^2}\right)(p-2)!\right)} + [a^{p-1}]_p^{p(p-2)!} + [1]_p$$

applicando opportunamente il piccolo Teorema di Fermat,
$[6]_p = [0]_p$.
Ciò mostra che $g(x)$ ammette radici se e solo se $p = 2$ oppure $p = 3$. Se $p = 2$, l'unica radice di $g(x)$ è $[1]_2$, mentre, se $p = 3$, le radici sono esattamente $[1]_3$ e $[2]_3$.