Università degli Studi Di Bari Aldo Moro
Dipartimento di Matematica

ESERCIZIARIO DI ALGEBRA N.1

Autore:
dott. Antonio De Carlo

Introduzione

Il seguente eserciziario è frutto del lavoro svolto durante l'attività di tutorato da me effettuata e offerta agli studenti del C.d.L. Triennale in Matematica dell'Università degli Studi di Bari Aldo Moro.
Esso si presenta sotto forma di una raccolta di svolgimenti di alcune tracce d'esame proposte, nel corso degli anni, come prove scritte del corso di Algebra N.1, ed è finalizzato ad offrire agli studenti esempi di come i risultati teorici possano essere applicati nelle risoluzioni degli esercizi.
Le soluzioni sono state supervisionate e corrette dalla Prof.ssa Margherita Barile (titolare del corso) a cui va un doveroso ringraziamento.
È altresì importante sottolineare che le soluzioni proposte non rappresentano, spesso, l'unico svolgimento possibile, né tantomeno il migliore in assoluto: sarebbe un ottimo esercizio per i lettori, ove possibile, cercare delle soluzioni alternative e/o migliori.
Qualsiasi risultato teorico citato nel seguito fa capo alla numerazione presente nelle dispense del corso di Algebra N.1 nella versione 2017/2018.
Sia le tracce d'esame degli appelli passati sia le dispense sono scaricabili dalla pagina web della Prof.ssa Barile, disponibile a questo link.

Indice

Come leggere l'eserciziario

L'eserciziario ha una breve sezione introduttiva, che rappresenta un sommario di risultati utili allo svolgimento degli esercizi, in alcuni casi non presenti nelle dispense, in altri lasciati come esercizi all'interno di esse. Ognuno di questi è seguito da una dimostrazione. Nel corso degli esercizi il riferimento a queste proprietà è riportato sotto la dicitura **Proprietà** accompagnata da un numero progressivo che identifica la stessa.
Seguono poi i tre capitoli che racchiudono gli svolgimenti veri e propri degli esercizi, denominati *Esercizi di primo, secondo e terzo tipo*, in base alla suddivisione generalmente proposta nelle tracce d'esame:

- *Esercizi di primo tipo*: sono gli esercizi che compaiono come Esercizio 1 in una traccia d'esame, e riguardano abitualmente i gruppi di permutazioni.

- *Esercizi di secondo tipo*: sono gli esercizi che compaiono come Esercizio 2 in una traccia d'esame, e hanno molto spesso come ambientazione gli anelli $\mathbb{Z}_n$.

- *Esercizi di terzo tipo*: sono gli esercizi che compaiono come Esercizio 3 in una traccia d'esame, e concernono normalmente polinomi a coefficienti in un campo.

Ogni esercizio è indicizzato mediante il numero e la data della traccia da cui proviene, secondo la numerazione riportata qui.

Sommario delle Proprietà importanti

Proprietà sui gruppi

Proprietà 1. *Sia G un gruppo e siano $g_1, g_2 \in G$. Allora il sottinsieme di G formato da tutti i possibili prodotti di un numero finito di potenze di g_1 e di g_2 è un sottogruppo di G, che denoteremo con $H :=< g_1, g_2 >$.*

Dimostrazione. Basta applicare la caratterizzazione dei sottogruppi (Proposizione 2.24). Infatti, è chiaro che H è non vuoto ($g_1 \in H$) e che, se $x, y \in H$, $xy^{-1} \in H$, visto che y^{-1} è ancora un prodotto di potenze dei due elementi citati, e dunque lo è xy^{-1}. □

Proprietà 2. *Sia G un gruppo e sia $\{g_i\}_{i \in I}$ una arbitraria famiglia di elementi di G. Allora l'insieme formato da tutti i possibili prodotti di un numero finito di potenze dei g_i è un sottogruppo di G, che denoteremo con $H =< \{g_i\}_{i \in I} >$.*
In particolare, se K, L sono sottogruppi di G, $< K \cup L >$ è un sottogruppo di G, contentente K, L.

Dimostrazione. Analoga alla precedente. □

Proprietà 3. *Siano $\sigma, \tau \in S_n$ due permutazioni a supporto disgiunto e sia $H =< \sigma, \tau >$. Allora $|H| = o(\sigma)o(\tau)$.*

Dimostrazione. Dal momento che, in base al Lemma 18.18, σ e τ commutano, tutti i possibili prodotti tra le loro potenze possono essere scritti nella forma

$$\sigma^k \tau^l$$

con $0 \leq k < o(\sigma)$ e $0 \leq l < o(\tau)$. È chiaro che se $(k, l) \neq (k', l')$, allora $\sigma^k \tau^l \neq \sigma^{k'} \tau^{l'}$. Infatti, se $\sigma^k \tau^l = \sigma^{k'} \tau^{l'}$ allora $\sigma^{k-k'} = \tau^{l'-l}$. Ma siccome σ e τ hanno supporti disgiunti, questo è vero anche per le loro potenze. Dunque, l'uguaglianza si realizza solo quando le permutazioni a primo e secondo membro sono uguali alla permutazione identica, ossia quando $k = k'$ e $l = l'$.
In particolare, i possibili prodotti sono $o(\sigma)o(\tau)$. □

Proprietà 4. *Siano H, K due sottogruppi di S_n tali che per ogni $\sigma \in H$ e $\tau \in K$ si abbia che σ e τ hanno supporto disgiunto. Allora $L :=< H \cup K >$ ha ordine $|H||K|$.*
In particolare, la Proprietà 3 si estende ad un qualsiasi numero finito di elementi.

Dimostrazione. Alla luce della Proprietà 2, è evidente che ogni elemento di L si può scrivere nella forma $\sigma\tau$ con $\sigma \in H$ e $\tau \in K$. Inoltre questa rappresentazione è unica, perché se $\sigma\tau = \sigma'\tau'$, allora $\sigma'^{-1}\sigma = \tau'\tau^{-1}$. Ma le permutazioni a primo e secondo membro hanno supporto disgiunto, quindi l'unica possibilità è che siano l'identità, ovvero $\sigma = \sigma'$ e $\tau = \tau'$.
Dunque i possibili prodotti, e quindi gli elementi di L, sono $|H||K|$.
In particolare, un facile procedimento induttivo prova che la Proprietà 3 si estende ad un qualsiasi numero finito di elementi, una volta osservato che $< \sigma_1, \ldots, \sigma_{n-1}, \sigma_n >=< (< \sigma_1 > \cup \cdots \cup < \sigma_{n-1} >) \cup < \sigma_n >>$. □

Proprietà 5. *Sia $\{i_1, \ldots, i_k\} \subset \{1, \ldots, n\}$. Allora l'insieme L degli elementi di S_n che fissano $i_1, \ldots, i_k$ è un sottogruppo di S_n isomorfo s S_{n-k}.*

Dimostrazione. Risulta immediato stabilire che L è un sottogruppo di S_n (per esempio applicando la definizione): infatti, L è non vuoto (id vi appartiene) e prodotti e inversi di elementi che fissano $i_1, \ldots, i_k$, fissano ancora $i_1, \ldots, i_k$.

Sia $X = \{j_1, \ldots, j_{n-k}\}$ il complementare di $\{i_1, \ldots, i_k\}$ in $\{1, \ldots, n\}$. Allora L è identificabile con $S(X)$, che è un insieme di permutazioni su $n-k$ elementi, cioè $Sym(n-k)$ (vedi Definizione 4.3).
Un possibile isomorfismo è dato da

$$\phi : S_{n-k} \to S(X)$$

tale che, per ogni $\sigma \in S_{n-k}$, $\Phi(\sigma)(j_i) = j_{\sigma(i)}$. È un esercizio verificare che Φ è un ben definito isomorfismo di gruppi.

□

Proprietà generali

Sia φ la funzione di Eulero.

Proprietà 6. *Sia $n \geq 1$. In un gruppo ciclico G di ordine n, ci sono esattamente $\varphi(d)$ elementi di periodo d per ogni $d|n$. Non c'è nessun elemento di periodo k se $k \nmid n$.*

Dimostrazione. Sia $d|n$. La Proposizione 17.39 garantisce l'esistenza di un unico sottogruppo ciclico di G di ordine d. Per l'unicità, tutti e soli gli elementi di periodo d di G sono i generatori di questo sottogruppo, che sono $\varphi(d)$ per il Corollario 17.37.
Diversamente, se $k \nmid n$, il Teorema di Lagrange (Teorema 17.19) garantisce che non possano esserci elementi di ordine k. □

Proprietà 7. *[Esercizio 17.43]*

1. *Se $n_1, \ldots, n_s$ sono interi positivi a due a due coprimi, allora*
$$\varphi\left(\prod_{i=1}^{s} n_i\right) = \prod_{i=1}^{s} \varphi(n_i).$$
2. *Siano $p_1, \ldots, p_s$ sono numeri primi a due a due distinti e siano $a_1, \ldots, a_s$ degli interi positivi. Allora*
$$\varphi\left(\prod_{i=1}^{s} p_i^{a_i}\right) = \prod_{i=1}^{s} p_i^{a_i - 1}(p_i - 1).$$

3. *Sia n un intero positivo maggiore di 2. Allora*

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

dove il prodotto è effettuato su tutti i primi p che dividono n.

Dimostrazione.

1. Sia $n = \prod_{i=1}^{s} n_i$. Sappiamo che $\varphi(n) = |\mathcal{U}(\mathbb{Z}_n)|$. In base al Corollario 16.11, con un facile procedimento induttivo, si ha che

$$|\mathcal{U}(\mathbb{Z}_n)| = \prod_{i=1}^{s} |\mathcal{U}(\mathbb{Z}_{n_i})|$$

da cui segue la tesi.

2. Grazie al punto 1, le potenze dei primi p_i sono a due a due coprime, e dunque si ha

$$\varphi\left(\prod_{i=1}^{s} p_i^{a_i}\right) = \prod_{i=1}^{s} \varphi(p_i^{a_i}).$$

Determiniamo dunque $\varphi(p^k)$ per un primo p e un intero positivo k.

Vogliamo contare i numeri più piccoli di p^k che sono coprimi con p^k, ovvero con p. Per fare ciò, contiamo invece quelli che non sono coprimi e sottraiamo il numero ottenuto dal totale.

È chiaro che i numeri che cerchiamo sono i multipli di p, cioè

$$p, 2p, 3p, \ldots, p^2, (p+1)p \ldots, p^{k-1}p = p^k,$$

che sono p^{k-1}. Dunque $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$, da cui segue l'enunciato.

3. Consideriamo $n = \prod_{p|n} p^{k_p}$ la fattorizzazione unica di n (in fattori primi positivi). Allora, in base al punto 2, si ha che

$$\varphi(n) = \prod_{p|n} p^{k_p} - p^{k_p - 1} = \prod_{p|n} p^{k_p} \left(1 - \frac{1}{p}\right) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

□

Proprietà 8. *Sia p un primo positivo e k un intero positivo. Allora l'applicazione $a \in \mathbb{Z}_p \mapsto a^{p^k} \in \mathbb{Z}_p$ è un omomorfismo di anelli.*
Inoltre, l'applicazione $f(x) \in \mathbb{Z}_p[x] \mapsto f(x)^{p^k} \in \mathbb{Z}_p[x]$ è un omomorfismo di anelli.

Dimostrazione. Per le proprietà delle potenze, è sufficiente provare l'asserto nel caso in cui $k = 1$.
Siano $a, b \in \mathbb{Z}_p$. Ovviamente $(ab)^p = a^p b^p$. Dunque dobbiamo provare solo che $(a+b)^p = a^p + b^p$. Si ha:

$$\begin{aligned}(a+b)^p &= \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i \\ &= a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i + b^p = a^p + b^p.\end{aligned}$$

Infatti, se $1 \leq i \leq p-1$, si ha che $p | \binom{p}{i}$, visto che

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} = \frac{p(p-1)\dots(p-i+1)}{i!}.$$

Dal momento che $i < p$, si ha che nessun fattore primo di $i!$ divide p, e dunque si ha che $\binom{p}{i} = pl$ per qualche intero positivo l.
La dimostrazione è identica nel caso dell'anello di polinomi, visto che anche in tale anello i multipli p-esimi sono nulli. □

Proprietà sugli omomorfismi di gruppi

La seguente Proprietà vale in ipotesi ben più larghe, ma la enunciamo e dimostriamo solo in un caso particolare, contestualmente ai nostri scopi. Quanto riportato di seguito sarà ben approfondito, comunque, nel corso di Algebra N.2.

Proprietà 9. *Sia $n > 1$ un intero e sia $(G, +)$ un gruppo finito.*
Allora ogni omomorfismo di gruppi $\varphi : \mathbb{Z}_n \to G$ è univocamente determinato assegnando l'immagine di $[1]_n$. Se

$$[1]_n \in \mathbb{Z}_n \mapsto g \in G$$

è tale assegnazione, si deve avere necessariamente che $o(g)|n$.

Dimostrazione. La condizione $o(g)|n$ è necessaria per poter avere un omomorfismo di gruppi. Infatti, se $\varphi : \mathbb{Z}_n \to G$ è un omomorfismo di gruppi tale che $\varphi([1]_n) = g$, si deve avere, se $e \in G$ è l'elemento neutro di G,

$$e = \varphi([0]_n) = \varphi(n \cdot [1]_n) = n \cdot \varphi([1]_n) = n \cdot g$$

e questo è vero, per la Proposizione 17.16, se e solo se $o(g)|n$.
Sotto questa ipotesi, sono automaticamente assegnate le immagini di ogni altro elemento $[a]_n \in \mathbb{Z}_n$ dal momento che si deve avere

$$\varphi([a]_n) = \varphi(a \cdot [1]_n) = a \cdot \varphi([1]_n) = a \cdot g.$$

È un facile esercizio verificare che φ è un omomorfismo di gruppi ben definito, ed è l'unico omomorfismo di gruppi che manda $[1]_n$ in g. □

Con la stessa tecnica è possibile dimostrare anche la seguente Proprietà.

Proprietà 10. *Siano $n_1, n_2, \ldots, n_k$ interi maggiori di 1. Allora ogni omomorfismo di gruppi*

$$\varphi : \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k} \to G$$

è univocamente determinato assegnando l'immagine degli elementi

$$e_1 := ([1]_{n_1}, [0]_{n_2}, \ldots, [0]_{n_k}),$$

$$e_2 := ([0]_{n_1}, [1]_{n_2}, \ldots, [0]_{n_k}),$$

$$\vdots,$$

$$e_k := ([0]_{n_1}, [0]_{n_2}, \ldots, [1]_{n_k}).$$

Per ogni $i = 1, \ldots, k$*, se*

$$e_i \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k} \mapsto g_i \in G$$

è tale assegnazione, si deve avere necessariamente che $o(g_i)|n_i$*.*

Dimostrazione. La dimostrazione è simile a quella della Proprietà 9. Chiaramente, basta provarla nel caso $k = 2$, ed è basata, naturalmente, sul fatto che possiamo scrivere, per ogni $a, b \in \mathbb{Z}$,

$$([a]_{n_1}, [b]_{n_2}) = a \cdot e_1 + b \cdot e_2.$$

□

Esercizi di primo tipo

Esercizio (Traccia N.61, 19 giugno 2015)**.**
Siano date le seguenti permutazioni di S_{11}*:*

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

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

(b) Provare che ogni sottogruppo di S_{11} *contenente* $<\sigma> \cup <\tau>$ *contiene un sottogruppo di ordine* 9*.*

(c) Provare che ad ogni sottogruppo del punto (b) appartiene un elemento di periodo 4.

Svolgimento.

(a) Per la Proposizione 18.26, si ha che $o(\sigma) = 15$ e $o(\tau) = 6$, che coincidono, rispettivamente, con le cardinalità dei sottogruppi ciclici generati da σ e τ. Dunque, visto che $<\sigma> \cap <\tau>$ è un sottogruppo ciclico sia di $<\sigma>$ che di $<\tau>$ (Proposizione 17.35) per il Teorema di Lagrange (17.39) il suo ordine deve dividere sia 15 che 6, e quindi deve dividere 3. Dunque sappiamo che

$$|<\sigma> \cap <\tau>| \in \{1,3\}.$$

Tale sottogruppo è non banale se e solo se contiene un elemento di periodo 3 (che lo genera).

Dalla formula del periodo (Lemma 17.36), si ha che

$$o(\sigma^k) = \frac{15}{MCD(k, 15)},$$

e dunque questo è 3 se e solo se $k = 5$ oppure $k = 10$ (chiaramente, basta considerare esponenti in $\{0, 1, \ldots, 14\}$).

Analogamente, $o(\tau^l) = 3$ se e solo se $l = 2$ o $l = 4$.

Un calcolo esplicito mostra, tuttavia, che né σ^5 né σ^{10} coincidono con τ^2 o τ^4.

Ma allora, nessun elemento di periodo 3 di $< \sigma >$ coincide con alcun elemento di periodo 3 di $< \tau >$. Pertanto l'intersezione non può che essere banale.

(b) Sia H un sottogruppo d S_{11} contenente $< \sigma > \cup < \tau >$.

L'idea fondamentale è quella di ottenere, da opportuni prodotti di potenze di σ e τ (che appartengono a H) due permutazioni di periodo 3 disgiunte, e applicare la Proprietà 3.

Sicuramente, dal punto precedente, sappiamo che σ^5 avrà periodo 3. Infatti,

$$\sigma^5 = (6, 8, 7)(9, 11, 10).$$

Inoltre, anche τ^2 avrà periodo 3. Infatti,

$$\tau^2 = (1, 3, 2)(6, 7, 8)(9, 10, 11).$$

Tuttavia, queste permutazioni non sono disgiunte. Ma, considerando

$$\alpha = \sigma^5\tau^2 = (1, 3, 2),$$

si ha che α e $\beta = \sigma^5$ sono in effetti permutazioni disgiunte contenute in H e di periodo 3.

Ma, allora, l'insieme

$$K := \{\alpha^k\beta^h | h, k \in \mathbb{Z}\}$$

è un sottogruppo di H di ordine $o(\alpha)o(\beta) = 9$.

(c) Sia H un sottogruppo di S_{11} contenente $< \sigma > \cup < \tau >$.

In questo caso basta considerare semplicemente il prodotto di σ e τ. Infatti,

$$\sigma\tau = (1,3,2,4)(6,10)(8,9)(7,11)$$

ha periodo 4, per la Proposizione 18.26.

□

Esercizio (Traccia N.65, 15 gennaio 2016)**.**
Data, in S_{18}, la permutazione

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

sia $G =< \sigma >$.

(a) Detto H l'insieme degli elementi di G aventi periodo dispari, determinare la cardinalità di H e dire se H è un sottogruppo di G.

(b) Determinare un sottogruppo ciclico K di S_{18} avente ordine 9 e tale che $G \cap K$ non sia il sottogruppo banale.

Svolgimento.

(a) In base alla Proposizione 18.26, $o(\sigma) = 60$. Ogni elemento di H è nella forma σ^k per un opportuno $k \in \mathbb{Z}$. Alla luce del Lemma 17.36, si ha che

$$o(\sigma^k) = \frac{60}{\text{MCD}(60,k)}$$

.

Dunque, esso è dispari se e solo se $4|\text{MCD}(60,k)$, ossia se e solo se $k \equiv 0 \pmod 4$.

Dunque $H =< \sigma^4 >$ è in effetti un sottogruppo (ciclico) di S_{18}. Il suo ordine coincide con $o(\sigma^4) = 15$.

(b) In base al Teorema di Lagrange (17.19), gli elementi di un gruppo ciclico di ordine 9 possono avere periodo $1, 3$ oppure 9. Ora, visto che $9 \nmid 60$, in G non ci sono elementi di periodo 9, mentre, in base alla Proprietà 6, ci sono esattamente $\varphi(3) = 2$ elementi di periodo 3, ossia σ^{20} e σ^{40}. Questi sono gli unici due candidati a potersi trovare in una intersezione non banale di G con un gruppo ciclico di ordine 9. Si ha, per esempio,

$$\sigma^{20} = (1, 3, 2)(8, 10, 12)(9, 11, 13).$$

Dunque σ^{20} si può ottenere come potenza terza di un 9-ciclo, cioè

$$\alpha = (1, 8, 9, 3, 10, 11, 2, 12, 13).$$

Dunque $K =< \alpha >$ è un sottogruppo ciclico di S_{18} che si interseca con G in $\{id, \sigma^{20}, \sigma^{40}\}$.

□

Esercizio (Traccia N.72, 12 settembre 2016)**.**
Siano date le seguenti permutazioni di S_{18}*:*

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

(a) Determinare l'insieme delle coppie di interi (k, l) *tali che* $\sigma^k = \tau^l$*.*

(b) Dire se l'insieme $H = \{\sigma^n \tau^m | n, m \in \mathbb{Z}\}$ *è un sottogruppo ciclico di* S_{18}*.*

Svolgimento.

(a) Cominciamo con l'osservare che σ, a differenza di τ, non muove gli elementi $15, 16, 17, 18$, così come ogni sua potenza. Dunque, affinché una potenza di τ coincida con una potenza di σ è necessario che le orbite di tali elementi sotto l'azione di tale potenza di τ siano banali.

L'elevamento a potenza deve avere, pertanto, sicuramente l'effetto di "eliminare" il 4-ciclo che muove tali elementi. Dunque $l \equiv 0 \pmod 4$.

Dunque, sotto questa condizione, possiamo sicuramente scrivere

$$\tau^l = (9, 14, 11, 13, 10, 12)^l.$$

Ora, l è sicuramente pari, pertanto ci sono tre possiblità: l può essere congruo a 0,2 oppure 4 modulo 6. Si ha, rispettivamente,

$$\tau^l = (9, 14, 11, 13, 10, 12)^0 = id,$$

$$\tau^l = (9, 14, 11, 13, 10, 12)^2 = (9, 11, 10)(12, 14, 13),$$

$$\tau^l = (9, 14, 11, 13, 10, 12)^4 = (9, 10, 11)(12, 13, 14).$$

Ragioniamo ora in maniera simile su σ, osservando che gli elementi $1, 2, 3, 4, 5, 6, 7, 8$ non sono mossi da τ, e quindi da nessuna sua potenza. Dunque si ha sicuramente $k \equiv 0 \pmod 4$.

Dunque, sotto questa condizione, possiamo sicuramente scrivere

$$\sigma^k = (9, 10, 11)^k (12, 13, 14)^k.$$

Anche in questo caso ci sono tre possibilità: k può essere congruo a $0, 1$ oppure 2 modulo 3. Si ha, rispettivamente,

$$\sigma^k = (9, 10, 11)^0 (12, 13, 14)^0 = id,$$

$$\sigma^k = (9, 10, 11)^1 (12, 13, 14)^1 = (9, 10, 11)(12, 13, 14),$$

$$\sigma^k = (9, 10, 11)^2 (12, 13, 14)^2 = (9, 11, 10)(12, 14, 13).$$

Ora, visto che, per la Proposizione 18.26, $o(\sigma) = o(\tau) = 12$, è sufficiente cercare le coppie (k, l) volute nel prodotto cartesiano

$$\{0, 1, \ldots, 11\} \times \{0, 1, \ldots, 11\}.$$

Dovendo, entrambi gli esponenti, essere multipli di 4, è sufficiente cercare le coppie nel prodotto cartesiano

$$\{0, 4, 8\} \times \{0, 4, 8\}.$$

Un rapido confronto stabilisce che $\sigma^k = \tau^l$ se e solo se:

- $k \equiv 0 \pmod 3 \wedge l \equiv 0 \pmod 6$: cioè per $k = l = 0$.
- $k \equiv 1 \pmod 3 \wedge l \equiv 4 \pmod 6$: cioè per $k = 4$ e $l = 4$.
- $k \equiv 2 \pmod 3 \wedge l \equiv 2 \pmod 6$: cioè per $k = 8$ e $l = 8$.

Dunque, tutte e sole le coppie in $\mathbb{Z} \times \mathbb{Z}$ cercate sono

$$\{(12k, 12l), (4 + 12k, 4 + 12l), (8 + 12k, 8 + 12l) | k, l \in \mathbb{Z}\}.$$

(b) Un possibile svolgimento di questo esercizio si sviluppa attraverso uno studio delle strutture cicliche, mostrando che, in effetti, nessun elemento di S_{18} può avere struttura ciclica tale che, per due suoi opportuni elevamenti a potenza, si ottengano permutazioni con struttura ciclica simile a quelle di σ e τ (ossia due elementi di H), provando che il gruppo non può essere ciclico. Tuttavia, l'elevato numero di elementi su cui il gruppo agisce (18), implica un alto numero di casi da trattare, con il rischio dimenticare qualcuno di questi, lasciando l'esercizio incompleto.

In effetti, è possibile trovare una via più semplice.

Innanzitutto, come è immediato verificare σ e τ commutano (pur non essendo permutazioni disgiunte!). Dunque, per la Proprietà 1, H è effettivamente un sottogruppo (abeliano) di S_{18} (infatti, stante la commutatività, ogni prodotto di potenze di σ e τ è della forma $\sigma^n \tau^m$). Dunque, dal momento che $\sigma, \tau \in H$, per il Teorema di Lagrange (17.19), $12 || H|$.

Ma allora, se H fosse ciclico, per la Proposizione 17.39, esisterebbe un unico sottogruppo (ciclico) di H avente ordine 12. Ma, chiaramente,

ce ne sono due distinti, ossia $< \sigma >$ e $< \tau >$. Infatti, se non fossero distinti, la loro intersezione avrebbe ancora ordine 12. Tuttavia, nel punto (a), abbiamo di fatto mostrato che tale intersezione ha ordine 3.

Dunque H non è ciclico.

□

Esercizio (Traccia N.80, 21 giugno 2017)**.**
Sia data la seguente permutazione di S_{13}*:*

$$\sigma = (1, 2, 3, 4)(5, 6, 7, 8).$$

(a) Determinare tutte le strutture cicliche delle permutazioni α *di* S_{13} *tali che* $\alpha^6 = \sigma$*.*

(b) Dimostrare che σ *non appartiene ad alcun sottogruppo ciclico di* S_{13} *avente ordine 60.*

(c) Determinare un sottogruppo di S_{13} *di ordine 1920 a cui appartiene* σ*.*

Svolgimento.

(a) La permutazione data ha struttura ciclica $(4, 4, 1, 1, 1, 1, 1)$. Al fine di determinare tutte le possibili strutture cicliche di permutazioni la cui sesta potenza sia σ, studiamo l'effetto dell'elevamento alla sesta sui cicli di tutte le lunghezze possibili.

- Gli 1-cicli, i 2-cicli, i 3-cicli e i 6-cicli vengono "eliminati".
- I 5-cicli, i 7-cicli, gli 11-cicli e i 13-cicli vengono lasciati inalterati (nel senso che rimangono, rispettivamente, 5,7,11,13-cicli).
- I 4-cicli si spezzano in due 2-cicli.
- Gli 8-cicli si spezzano in due 4-cicli.
- I 9-cicli si spezzano in tre 3-cicli.
- I 10-cicli si spezzano in due 5-cicli.

– I 12-cicli si spezzano in sei 2-cicli.

Dunque, è evidente che l'unica possibilità per avere due 4-cicli è che α abbia un 8-ciclo. A questo punto, il problema si riduce soltanto a determinare quali strutture cicliche che coinvolgono i restanti 5 elementi siano compatibili con il problema dato, ovvero che "spariscano" quando elevati alla sesta potenza, andando a formare i restanti cinque 1-cicli.

Consideriamo le possibili partizioni di 5. Ce ne sono sette e sono:

(5)
(4,1)
(3,2)
(3,1,1)
(2,2,1)
(2,1,1,1)
(1,1,1,1,1).

Dalla nostra analisi precedente, risulta evidente che le prime due non vanno bene, mentre le restanti sì.

Dunque, le strutture cicliche che cerchiamo sono:

(8,3,2)
(8,3,1,1)
(8,2,2,1)
(8,2,1,1,1)
(8,1,1,1,1,1).

(b) In base alla Proposizione 18.26, un gruppo ciclico di ordine $60 = 2^2 \cdot 3 \cdot 5$ in S_{13} può essere generato solo da una permutazione di struttura ciclica (5,4,3,1). Perché non ci sono altre possibilità?

Affinché il minimo comune multiplo delle lunghezze dei cicli della decomposizione in cicli disgiunti del generatore sia 60, la decomposizione deve coinvolgere un 5 ciclo o un 10 ciclo. Nel secondo caso, però, "rimane spazio" solo per permutazioni su 3 elementi di struttura ciclica (3),

(2,1), (1,1,1), nessuna delle quali permette di ottenere 60 come minimo comune multiplo.

Dunque dobbiamo avere un 5-ciclo. Il passo successivo è osservare che ci deve essere per forza o un 3-ciclo o un 6-ciclo (per ottenere il fattore 3). Come prima, il 6-ciclo non permette di ottenere il minimo comune multiplo uguale a 60.

Infine, con le stesse argomentazioni, si vede che solo con un ulteriore 4-ciclo è possibile raggiungere 60 come minimo comune multiplo. A questo punto "resta spazio" solo per un 1-ciclo. Dunque l'unica struttura ciclica possibile è (5,4,3,1).

A questo punto, è facile vedere che nessuna potenza di una permutazione con tale struttura ciclica dà come risultato una permutazione con struttura ciclica (4,4,1,1,1,1,1), visto che non è mai possibile ottenere due 4-cicli.

(c) In base alla Proprietà 1 e alla Proprietà 3,

$$H = \{(1,2,3,4)^h(5,6,7,8)^k | h,k \in \mathbb{Z}\}$$

è un sottogruppo di S_{13} di ordine $4 \cdot 4 = 16$.

Ovviamente $\sigma \in H$.

Ora, alla luce della Proprietà 5, l'insieme delle permutazioni che fissano 1,2,3,4,5,6,7,8 è un sottogruppo di S_{13} isomorfo a S_5, e ha quindi 120 elementi. Sia K tale sottogruppo.

Inoltre, ogni permutazione di K è disgiunta da ogni permutazione di H. Pertanto, in base alla Proprietà 2 e alla Proprietà 4,

$$H = \{\alpha^h\beta^k | \alpha \in H, \beta \in K, h,k \in \mathbb{Z}\}$$

è un sottogruppo di S_{13} di ordine $16 \cdot 120 = 1920$, a cui σ appartiene.

□

Esercizio (Traccia N.81, 5 luglio 2017)**.**
Sia data la seguente permutazione di S_{10} :

$$\sigma = (1,2,3,4,5)(6,7,8)(9,10).$$

Determinare i seguenti insiemi e dire quali sono sottogruppi di S_{10}*:*

(a) $H = \{\alpha \in < \sigma > | \alpha(\{3,5\}) = \{3,5\}\}$

(b) $H = \{\alpha \in < \sigma > | \alpha(\{1,9\}) = \{1,9\}\}$

(c) $H = \{\alpha \in < \sigma > | \alpha(\{7,8,9,10\}) = \{7,8,9,10\}\}$

Svolgimento. Calcoliamo il periodo di σ. In base alla Proposizione 18.26 si ha $o(\sigma) = 30$.
Ora, l'esercizio richiede di determinare le potenze di σ che fissino certi insiemi di indici. Un elemento che viene fissato da un ciclo viene fissato da ogni sua potenza. Di conseguenza, dobbiamo concentrarci solo sui cicli che coinvolgono (ovvero che non fissano) gli elementi degli insiemi dati.

(a) Dobbiamo concentrarci solo sul ciclo $\tau = (1,2,3,4,5)$, perché è l'unico che non fissa 3 e 5. Determiniamo le potenze di τ che fissano l'insieme $\{3,5\}$, ovvero che fissano 3 e 5 oppure li scambiano (si ricordi che ogni permutazione è una trasformazione bigettiva).

L'unica possibilità affinché 3 e 5 vengano scambiati è che nella decomposizione di una certa potenza di τ compaia il 2-ciclo $(3,5)$. Ma questo non è mai possibile perché la lunghezza di τ è 5, e una potenza di un 5-ciclo non si decompone mai non banalmente. Dunque l'unica possibilità è che 3 e 5 siano fissati da una potenza di τ, ovvero è considerare $\tau^0 = id$. In altri termini, $\alpha = \sigma^k \in H$ se e solo se l'effetto dell'elevamento a potenza è quello di far "scomparire" il 5-ciclo: dunque

$$H = \{id, \sigma^5, \sigma^{10}, \sigma^{15}, \sigma^{20}, \sigma^{25}\} = < \sigma^5 >$$

è un sottogruppo.

(b) In questo frangente, occorre concentrarci sul 5-ciclo e sul 2-ciclo. Anche in questa situazione, è ovvio che 1 e 9 non possano mai venire scambiati da una potenza di σ, visto che sono mossi da cicli disgiunti. Dunque, anche in questo caso l'unica possibilità è che vengano fissati singolarmente. Dobbiamo pertanto prendere le potenze di σ che "eliminano" il 5-ciclo e il 2-ciclo, ovvero le potenze multiple di 10. Si ha:

$$K = \{id, \sigma^{10}, \sigma^{20}\} =< \sigma^{10} >,$$

che è un sottogruppo.

(c) In questo caso dobbiamo guardare al 3-ciclo e al 2-ciclo. Ancora una volta, certamente, non è possibile che 7,8 si scambino con 9,10. Dunque vogliamo che 7,8 si scambino tra loro o che vengano fissati, e che 9,8 si scambino tra loro o vengano fissati (e questo avviene sempre, quindi non dobbiamo preoccuparci del 2-ciclo). Visto che 7,8 appartengono ad un 3-ciclo, come nel punto (a) non è mai possibile scambiarli per nessuna potenza di σ ma è solo possibile fissarli. Dunque, alla luce di quanto detto, dobbiamo prendere le potenze di σ in cui "sparisce" il 3-ciclo, ovvero i multipli di 3. Per questo motivo si ha

$$L = \{id, \sigma^3, \sigma^6, \ldots, \sigma^{27}\} =< \sigma^3 >,$$

che è ancora un sottogruppo.

□

Esercizio (Traccia N.82, 11 settembre 2017)**.**
Sia data la permutazione

$$\sigma = (1,2)(3,4,5,6)(7,8,9)(10,11,12,13,14) \in S_{14}.$$

(a) Determinare l'insieme $H = \{\alpha \in < \sigma > | o(\alpha)$ *è dispari*$\}$ *e dire se è un sottogruppo di* S_{14}*.*

(b) *Determinare l'insieme* $K = \{\alpha \in < \sigma > | \alpha^4 = id\}$ *e dire se è un sottogruppo si* S_{14}.

(c) *Determinare la cardinalità dell'insieme* $L = \{\alpha \in < \sigma > | 5 \text{ } divide \text{ } o(\alpha)\}$.

Svolgimento.

(a) Calcoliamo il periodo di σ. In base alla Proposizione 18.26 si ha $o(\sigma) = 60$.

Se $\alpha \in H$, l'ordine di $\alpha \in < \sigma >$ è quindi un divisore dispari di 60 (Teorema di Lagrange,17.19). Dunque, essendo $60 = 2^2 \cdot 3 \cdot 5$, si ha che

$$o(\alpha) \in \{1, 3, 5, 15\}.$$

Si tratta allora di prendere $\alpha = \sigma^k$, in maniera tale che l'effetto dell'elevamento a potenza sia quello di "rimuovere" i cicli di lunghezza pari, ovvero il 2-ciclo e il 4-ciclo, dopodiché il risultato discende ancora dalla Proposizione 18.26. Infatti, nella decomposizione in cicli digiunti di α non compariranno più cicli di lunghezza pari, visto che le potenze del 3-ciclo e del 5-ciclo sono o la permutazione identica, oppure ancora rispettivamente un 3-ciclo e un 5-ciclo. Dunque il minimo comune multiplo delle lunghezze dei cicli non sarà multiplo di 2.

Dunque

$$H = \{\sigma^{4k} | k \in \mathbb{Z}\} = < \sigma^4 >$$

che è un sottogruppo di S_{14}.

(b) Sia $\alpha = \sigma^k \in K$. Allora si ha $\sigma^{4k} = id$. Ora, osservando che un elevamento a potenza quarta non "eliminerebbe" il 3-ciclo e il 5-ciclo, affinché la situazione riportata si verifichi bisognerà già partire da una situazione in cui questi due tipi di cicli non appaiono. La potenza quarta, in seguito, "elimina" anche eventuali 2-cicli e 4-cicli, quindi non dobbiamo preoccuparcene.

Affinché il 3-ciclo e il 5-ciclo spariscano in seguito all'elevamento a potenza, ci serve che $15|k$. Dunque

$$K = \{id, \sigma^{15}, \sigma^{30}, \sigma^{45}\} =< \sigma^{15} >$$

che è un sottogruppo di S_{14}.

(c) Si tratta di determinare il numero di elementi di periodo multiplo di 5 e divisore di 60 (Teorema di Lagrange,17.19). Dunque, se $\alpha \in L$, si ha

$$o(\alpha) \in \{5, 10, 15, 20, 30, 60\}.$$

In base alla Proprietà 6, per ogni d divisore di 60 ci sono esattamente $\varphi(d)$ elementi di periodo d. Usando le proprietà della funzione di Eulero (Proprietà 7), si calcola quindi che

$$\begin{aligned} |L| &= \varphi(5) + \varphi(10) + \varphi(15) + \varphi(20) + \varphi(30) + \varphi(60) \\ &= \varphi(5)(1 + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(2)\varphi(3) + \varphi(3)\varphi(4)) \\ &= 4(1 + 1 + 2 + 2 + 2 + 4) = 48. \end{aligned}$$

□

Esercizio (Traccia N.83, 25 settembre 2017)**.**
Sia data la permutazione

$$\sigma = (1, 2, 3, 4)(5, 6, 7) \in S_{11}.$$

(a) Provare che l'insieme $H = \{\alpha \in S_{11} | \alpha\sigma = \sigma\alpha\}$ *ha almeno 288 elementi.*

(b) Provare che H *contiene un sottogruppo commutativo di 48 elementi.*

(c) Dire se l'insieme $K = \{\alpha \in S_{11} | \alpha^2\sigma = \sigma\alpha^2\}$ *è un sottogruppo di* S_{11}*.*

Svolgimento.

(a) Dobbiamo trovare almeno 288 elementi che commutino con σ. In base al Lemma 18.18, sicuramente tutte le permutazioni con supporto disgiunto da quello di σ soddisfano tale proprietà. Queste sono le permutazioni di S_{11} che fissano contemporaneamente 1,2,3,4,5,6,7. L'insieme di tali elementi è un sottogruppo di S_{11} isomorfo a S_4, alla luce della Proprietà 5, ed ha quindi 24 elementi. Sia K questo sottogruppo.

Si osservi che H è un sottogruppo di S_{11}. Sicuramente $id \in H$. Inoltre, per ogni $\alpha, \beta \in H$, si ha che:

- $(\alpha\beta)\sigma = \alpha(\beta\sigma) = \alpha(\sigma\beta) = (\alpha\sigma)\beta = (\sigma\alpha)\beta = \sigma(\alpha\beta)$;
- $\alpha\sigma = \sigma\alpha \Rightarrow \sigma\alpha^{-1} = \alpha^{-1}\sigma$.

per cui $\alpha\beta, \alpha^{-1} \in H$.

Grazie a questa proprietà, possiamo dire che ogni prodotto di potenze di elementi che commutano con σ commuta ancora con σ.

Ora,

$$L =< \sigma >$$

è un sottogruppo di S_{11} di ordine $o(\sigma) = 12$ (Proposizione 18.26), ovviamente contenuto in H.

Le permutazioni di L sono tutte disgiunte dalle permutazioni di K. Ma allora, alla luce della Proprietà 2 e della Proprietà 4,

$$T = \{\tau^{h_1} s^{h_2} | \tau \in L, s \in K, h_i \in \mathbb{Z}\}$$

è un sottogruppo di S_{11} di ordine $|L||K| = 12 \cdot 24 = 288$.

Il generico elemento di T è prodotto di elementi di H, che è un sottogruppo di S_{11}. Dunque $T \subset H$, e ciò prova che $|H| \geq 288$.

Curiosità 1. Il sottogruppo H del precedente esercizio è detto *centralizzante* dell'elemento σ in S_{11}. Il Teorema Orbita-Stabilizzatore, che è un risultato molto generale riguardante le *azioni* di gruppi su insiemi,

e che verrà presentato nel corso di Algebra n.2, permetterà di stabilire che

$$|S_{11}| = |H| \cdot |C(\sigma)|,$$

essendo $C(\sigma) := \{\tau\sigma\tau^{-1} | \tau \in S_{11}\}$ (tale insieme è chiamato *orbita di σ sotto l'azione di coniugio di S_{11} su se stesso*). Verrà dimostrato che le permutazioni che appartengono a tale insieme sono tutte e sole quelle con la stessa struttura ciclica di σ. È possibile contare il numero degli elementi di struttura ciclica $(4, 3)$, grazie alla Proposizione 18.4. Infatti, esso è

$$\left(\frac{1}{4} \cdot \frac{11!}{7!}\right) \cdot \left(\frac{1}{3} \cdot \frac{7!}{4!}\right) = \frac{1}{12} \cdot \frac{11!}{4!} = 138600.$$

Per cui $|H| = \frac{11!}{138600} = 288$. Risulta, cioè, che H ha esattamente 288 elementi.

(b) Alla luce della Proprietà 2 e della Proprietà 4, se $\gamma = (8, 9, 10, 11)$, l'insieme

$$L = \{\sigma^h \gamma^k | h, k \in \mathbb{Z}\}$$

è un sottogruppo di S_{11} di ordine $12 \cdot 4 = 48$.

Inoltre, essendo i suoi elementi prodotti di potenze di elementi di H, ed essendo H un sottogruppo, si ha che $L \subset H$.

Ogni elemento di L è nella forma $\sigma^h \gamma^k$ per opportuni esponenti. Visto che $\sigma e \gamma$ sono permutazioni disgiunte e quindi commutano tra di loro, è immediato verificare che ogni elemento nella forma riportata commuta con ogni altro elemento dello stesso tipo. Dunque L è un sottogruppo commutativo di H.

(c) Proviamo a dimostrare direttamente che K è un sottogruppo, usando la definizione. Certamente $id \in K$, che è pertanto non vuoto. Siano $\alpha, \beta \in K$. Allora sicuramente $\alpha^{-1} \in K$, visto che

$$\alpha^2\sigma = \sigma\alpha^2 \Rightarrow \sigma\alpha^{-2} = \alpha^{-2}\sigma.$$

Tentiamo ora di dimostrare che $(\alpha\beta)^2\sigma = \sigma(\alpha\beta)^2$. Se si avesse $(\alpha\beta)^2 = \alpha^2\beta^2$ (che sicuramente accade se α e β commutano tra di loro, in base alla Proposizione 17.6(d)) oppure che α e β commutano con σ, sicuramente si potrebbe concludere. Tuttavia, senza queste ipotesi non c'è nessuna ragione immediata per la quale quanto scritto sopra debba accadere. Ciò suggerisce che K non sia in effetti un sottogruppo, e fornisce anche un modo per produrre un controesempio: dobbiamo sicuramente cominciare trovando due permutazioni α e β che non commutano con σ e che non commutano l'una con l'altra, ma tali che i loro quadrati commutano con σ. La scelta più facile è prendere dei 2-cicli, il cui quadrato (la permutazione identica) certamente commuta con σ. Ovviamente dovremmo prenderle non disgiunte, e non disgiunte da σ. Per esempio, consideriamo $\alpha = (1,2)$, $\beta = (2,3) \in K$. Allora

$$(1,2)(2,3) = (1,2,3) \neq (1,3,2) = (2,3)(1,2),$$

$$(1,2)\sigma = (2,3,4)(5,6,7) \neq (1,3,4)(5,6,7) = \sigma(1,2),$$
$$(2,3)\sigma = (1,3,4)(5,6,7) \neq (2,4,1)(5,6,7) = \sigma(2,3).$$

Dunque α, β sono due ottimi candidati. Resta solo da verificare che il quadrato del loro prodotto non commuta con σ.

Infatti, dato che $(\alpha\beta)^2 = (1,3,2)$, si ha

$$(\alpha\beta)^2\sigma = (3,4)(5,6,7) \neq (1,4)(5,6,7) = \sigma(\alpha\beta)^2.$$

Dunque K non è un sottogruppo di S_{11}.

□

Esercizio (Traccia N.84, 6 novembre 2017)**.**
Sia data la permutazione

$$\sigma = (1,2,3)(4,5,6,7)(8,9,10,11,12,13,14,15,16,17) \in S_{17}.$$

(a) Determinare l'insieme $H = \{\alpha \in < \sigma > | Supp(\alpha) = \{1,2,\ldots,17\}\}$.

(b) Dire se l'insieme $K = \{\alpha \in < \sigma > | \alpha(8) \in \{8, 10, 12, 14, 16\}\}$ *è un sottogruppo di* S_{17}.

Svolgimento.

(a) La struttura ciclica di σ è $(10, 4, 3)$ (in particolare, in base alla Proposizione 18.26, σ ha periodo 60).

Il nostro obiettivo è determinare tutte le potenze di σ che non lasciano fisso alcun indice $1 \leq h \leq 17$. Vogliamo quindi che nessun elevamento a potenza abbia l'effetto di "eliminare" alcuno dei cicli di σ. I cicli possono essere "eliminati" solamente elevando σ ad un esponente che sia multiplo o di 3, o di 4, o di 10.

Pertanto, gli esponenti che cerchiamo sono tutti e soli quelli che non sono divisibili per 3, per 4 e per 10.

Dunque,

$$H = \{\sigma^k | 3 \nmid k \wedge 4 \nmid k \wedge 10 \nmid k\}.$$

Possiamo facilmente determinare la cardinalità di H: è sufficiente contare tutti i numeri $k \in \{1, \ldots, 60 = o(\sigma)\}$ che soddisfano la richiesta di non essere divisibili per 3,per 4 e per 10.

Contandoli esplicitamente, essi sono:

$$1, 2, 7, 11, 13, 14, 17, 19, 22, 23, 25, 26, 29, 31, 34,$$

$$35, 37, 38, 41, 43, 46, 47, 49, 53, 55, 58, 59$$

che sono 28.

(b) Gli indici coinvolti sono solo quelli mossi dal 10-ciclo di σ, che chiamiamo τ. Possiamo pertanto concentrarci solo su questo ciclo.

Si ha che

$$\tau^k(8) = \begin{cases} 8 \iff k \equiv 0 \pmod{10} \\ 10 \iff k \equiv 2 \pmod{10} \\ 12 \iff k \equiv 4 \pmod{10} \\ 14 \iff k \equiv 6 \pmod{10} \\ 16 \iff k \equiv 8 \pmod{10} \end{cases}$$

Gli stessi risultati si ottengono ragionando direttamente su σ. Dunque, gli esponenti che cerchiamo sono tutti e soli quelli la cui cifra delle unità della rappresentazione decimale appartiene all'insieme $\{0, 2, 4, 6, 8\}$: in altri termini, sono tutti e soli i numeri pari. Per cui è chiaro che

$$K = < \sigma^2 >$$

è un sottogruppo.

□

Esercizio (Traccia N.85, 9 gennaio 2018)**.**
Siano date in S_{20} le permutazioni

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

$$\tau = (13, 17, 16, 15, 14)(18, 19, 20).$$

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

(b) Determinare in S_{20} un sottogruppo ciclico contenente $< \sigma > \cup < \tau >$.

(c) Determinare in S_{20} un sottogruppo contenente $< \sigma > \cup < \tau >$ di ordine 960.

Svolgimento.

(a) Cominciamo con il determinare i periodi di σ e τ. In base alla Proposizione 18.26, si ha $o(\sigma) = 20, o(\tau) = 15$.

Questo permette di stimare a priori l'ordine del sottogruppo

$$H := < \sigma > \cap < \tau > .$$

Infatti, in base alla Proposizione 17.35, H sarà ciclico, dunque il suo ordine coincide con il periodo di un suo generatore. Questo sarà un elemento di entrambi i gruppi ciclici che formano l'intersezione e pertanto il suo ordine deve dividere sia 20 che 15, per il Teorema di Lagrange (Teorema 17.19), e dunque deve dividere $5 = MCD(20, 15)$.

In altri termini, $|H| \in \{1, 5\}$.

Questo vuol dire che, se troviamo in $|H|$ un elemento non banale, si avrà che $|H| = 5$. In effetti, è immediato osservare che, detto α il 5-ciclo di σ, e detto β il 5-ciclo di τ, risulta che $\alpha^{-1} = \tau$.

α è dunque un ottimo candidato ad essere un elemento non banale di H: infatti può essere ottenuto sia come potenza di σ che potenza di τ.

Per esempio, vogliamo elevare a potenza σ in modo da "eliminare" i 4-cicli e lasciare inalterato α. Dunque vogliamo trovare un esponente che sia multiplo di 4 e congruo ad 1 modulo 5. Evidententemente 16 è un tale esponente. Nel caso in cui non si riesca ad identificare immediatamente un tale numero, sarà sufficiente risolvere il sistema di congruenze lineari

$$\begin{cases} x \equiv 0 \mod 4 \\ x \equiv 1 \mod 5 \end{cases}.$$

Analogamente, essendo $\beta^4 = \alpha$, per ottenere α da una potenza di τ, sarà necessario eliminare il 3-ciclo e ottenere β^4. Dobbiamo trovare, quindi, un esponente che sia multiplo di 3 e congruo a 4 modulo 5. Anche in questo caso, evidentemente 9 è un tale esponente (altrimenti si risolva un opportuno sistema di congruenze lineari).

Dunque $|H| = 5$. Essendo ciclico, avrà, per il Corollario 17.37, $\varphi(5) = 4$ generatori. Dunque ogni elemento non banale è un generatore di H

(oppure, si osservi che $\alpha \in H$ ha periodo 5 e quindi lo genera). In ogni caso,

$$H =< \alpha > .$$

(b) Dobbiamo trovare un elemento di S_{20} tale che due sue opportune potenze coincidano con σ e τ.

Abbiamo già osservato il legame tra i 5-cicli di σ e τ. Osserviamo che nella decomposizione di σ compaiono, inoltre, solo 4-cicli, e in τ solo un 3-ciclo. Essendo $3, 4, 5$ coprimi, questo suggerisce che, prendendo

$$\alpha = (1, 2, 3, 4)(5, 6, 7, 8)(9, 10, 11, 12)(13, 14, 15, 16, 17)(18, 19, 20),$$

sia possibile "eliminare", per opportune potenze, separatamente i 4-cicli o i 3-cicli.

In effetti, per ottenere σ, dobbiamo trovare un esponente che "elimini" il 3-ciclo, e che lasci invariati i 4-cicli e il 5-ciclo. Dobbiamo trovare quindi un esponente che risolva il sistema di congruenze lineari

$$\begin{cases} x \equiv 1 \mod 4 \\ x \equiv 1 \mod 5 \\ x \equiv 0 \mod 3 \end{cases},$$

una cui soluzione particolare è $x = 21$.

Invece, per ottenere τ, seguendo lo stesso ragionamento dobbiamo trovare una soluzione del sistema di congruenze lineari

$$\begin{cases} x \equiv 0 \mod 4 \\ x \equiv 4 \mod 5 \\ x \equiv 1 \mod 3 \end{cases},$$

una cui soluzione particolare è $x = 4$.

(c) Per risolvere questo esercizio, ci appoggeremo alla Proprietà 4. Prima di tutto, osserviamo che $960 = 2^6 \cdot 3 \cdot 5 = 4^3 \cdot 3 \cdot 5$. Questa decomposizione

ci ricorda le lunghezze dei cicli di σ e τ: tre 4-cicli, un 3-ciclo e un 5-ciclo. Inoltre abbiamo già osservato la relazione che sussiste tra i due 5-cicli. In base alla Proprietà 2 e alla Proprietà 4, si ha che, per

$$\gamma_1 = (1,2,3,4), \gamma_2 = (5,6,7,8), \gamma_3 = (9,10,11,12),$$

$$H = \{\gamma_1^{h_1}\gamma_2^{h_2}\gamma_3^{h_3}\tau^{h_4} | h_i \in \mathbb{Z}\},$$

è un sottogruppo di S_{20} di ordine $|H| = 4 \cdot 4 \cdot 4 \cdot 15 = 960$, visto che i suoi generatori hanno supporti a due a due disgiunti. Inoltre è evidente che contenga σ e τ: per esempio, basta prendere $(h_1, h_2, h_3, h_4) = (1,1,1,9)$ per ottenere σ e $(h_1, h_2, h_3, h_4) = (0,0,0,1)$ per ottenere τ.

□

Esercizio (Traccia N.86, 24 gennaio 2018)**.**
Siano date in S_{11} le permutazioni

$$\sigma = (1,2,3)(4,5,6,7)(8,9,10,11)$$

$$\tau = (4,8,5,9,6,10,7,11).$$

(a) Determinare l'insieme $H = \{\alpha \in < \sigma > | < \alpha > \cap < \tau > \neq \{id\}\}$.

(b) Determinare in S_{11} un sottogruppo ciclico contentente $< \sigma > \cup < \tau >$.

Svolgimento.

(a) Cominciamo con il determinare il periodo di σ, in maniera tale da avere una stima sulle potenze da esaminare. In base alla Proposizione 18.26, si ha $o(\sigma) = 12$. Inoltre, $o(\tau) = 8$.

Dobbiamo determinare tutte le potenze non banali di σ che possano coincidere con una potenza non banale di τ. Per fare ciò, conviene ragionare sulle strutture cicliche.

Osserviamo che una potenza di τ può spezzarsi non banalmente in quattro 2-cicli o in due 4-cicli. Dunque, non c'è dubbio che dobbiamo

"eliminare" il 3-ciclo di σ. In altri termini, possiamo prendere come esponenti per σ i multipli di 3 più piccoli di 12, ovvero $3, 6$ e 9.

La struttura ciclica di σ^k sarebbe, per $k = 3, 9$, $(4, 4, 1, 1, 1)$ oppure, per $k = 6$, $(2, 2, 2, 2, 1, 1, 1)$. Affinché si ottenga una struttura ciclica simile per una potenza non banale di τ, occorrerà quindi considerare esponenti pari positivi più piccoli di 8, cioè $h = 2, 4, 6$.

Avendo un numero molto basso di casi, possiamo svolgere direttamente i conti, ottenendo

$$\sigma^3 = (4, 7, 6, 5)(8, 11, 10, 9)$$

$$\sigma^6 = (4, 6)(5, 7)(8, 10)(9, 11)$$

$$\sigma^9 = (4, 5, 6, 7)(8, 9, 10, 11)$$

$$\tau^2 = (4, 5, 6, 7)(8, 9, 10, 11)$$

$$\tau^4 = (4, 6)(5, 7)(8, 10)(9, 11)$$

A questo punto possiamo fermarci. Perché? Riconosciamo immediatamente che $\sigma^9 = \tau^2$. Dunque per $< \sigma^9 > \cap < \tau > \neq \{id\}$. Ma $< \sigma^9 > = < \sigma^3 >$, per cui non occorre verificare (come sarà) che $\tau^6 = \sigma^3$.

Allo stesso modo, si vede che $\sigma^6 = \tau^4$.

Occorre dunque determinare gli elementi $\alpha \in < \sigma >$ tali che uno tra σ^3 e σ^6 appartenga a $< \alpha >$. Poiché vale l'implicazione $\sigma^3 \in < \alpha > \Rightarrow \sigma^6 \in < \alpha >$, la condizione da considerare è $\sigma^6 \in < \alpha >$. Posto $\alpha = \sigma^h$, con $1 \leq h \leq 11$, essa si verifica se e solo se la congruenza lineare $hx \equiv 6 \pmod{12}$ è risolubile, ossia se e solo se $MCD(12, h)|6$, ossia se e solo se 4 non divide h. Ciò fornisce immediatamente H, ossia

$$H = \{\sigma, \sigma^2, \sigma^3, \sigma^5, \sigma^6, \sigma^7, \sigma^9, \sigma^{10}, \sigma^{11}\}.$$

Osservazione 1. Lo svolgimento proposto fornisce una condizione per ottenere immediatamente H: il punto fondamentale è l'osservazione che l'appartenenza di σ^3 ad $< \alpha >$ implica l'appartenenza di σ^6. Qualora

non ci si renda conto che da questo è possibile dedurre subito la forma degli elementi di H, è anche possibile un'approccio diretto, ma molto più articolato e elaborato, che proponiamo di seguito.

Vogliamo determinare gli elementi $\alpha \in < \sigma >$ tali che uno tra σ^3 e σ^6 appartenga a $< \alpha >$.

- In base alla Proposizione 17.35, per ogni $k = 1, \ldots, 11$, risulta che $< \sigma^k > \cap < \sigma^3 >$ è un sottogruppo ciclico di entrambi i sottogruppi che stiamo intersecando. Il Teorema di Lagrange (Teorema 17.19) ci dice che allora il suo ordine (cioè il periodo di un suo generatore) deve essere divisore di $o(\sigma^k) = 12/MCD(12, k)$ (Lemma 17.36) e $o(\sigma^3) = 4$, e dunque del loro massimo comune divisore. D'altro canto, noi vorremmo che $\sigma^3 \in < \sigma^k >$, dunque che l'intersezione sia proprio $< \sigma^3 >$. Ma allora, affinché $4|12/MCD(12, k)$, dobbiamo prendere $k \in \{1, 3, 5, 7, 9, 11\}$. Ovviamente $\alpha = \sigma, \sigma^3, \sigma^9$ va bene. Per quanto concerne i restanti osserviamo che per $k = 5, 7, 11$ σ^k genera σ, visto che le congruenze lineari

$$5x \equiv 1 \pmod{12}$$

$$7x \equiv 1 \pmod{12}$$

$$11x \equiv 1 \pmod{12}$$

  ammettono soluzione.

- Con procedimento analogo, affinché $\sigma^6 \in < \sigma^k >$, si deve avere che $2|12/MCD(12, k)$. Dunque $k \in \{1, 2, 3, 5, 6, 7, 9, 10, 11\}$. Non siamo interessati a controllare le potenze $1, 3, 5, 7, 9, 11$, in quanto sappiamo già che $\sigma^k \in H$ per tali potenze, dal punto precedente. Ovviamente $2, 6$ vanno bene. Per quanto riguarda $k = 10$, osserviamo che la congruenza lineare $10x \equiv 6 \pmod{12}$ ammette soluzione, dato che $MCD(10, 12) = 2|6$. Dunque anche 10 va bene.

Anche in questo caso abbiamo ottenuto

$$H = \{\sigma, \sigma^2, \sigma^3, \sigma^5, \sigma^6, \sigma^7, \sigma^9, \sigma^{11}\}.$$

(b) Utilizziamo un approccio "per tentativi ragionati". Osserviamo che il prodotto dei due 4-cicli di σ è τ^2. Pertanto appare intuitivo costruire un generatore di un gruppo ciclico che contenga σ e τ a partire dall'8-ciclo τ. Aggiungiamo il 3-ciclo $(1, 2, 3)$. Proviamo dunque con

$$\alpha = (1, 2, 3)(4, 8, 5, 9, 6, 10, 7, 11).$$

Ottenere τ come potenza di α è facile: basta "eliminare" il 3-ciclo e lasciare l'8-ciclo invariato. Possiamoq quindi prendere come esponente il primo multiplo positivo di 3 che sia congruo a 1 modulo 8: infatti $\alpha^9 = \tau$.

Per quanto riguarda σ, vorremmo che l'effetto dell'elevamento a potenza fosse quello di lasciare invariato il 3-ciclo e sostituire l'8-ciclo con il suo quadrato. Gli esponenti con le proprietà richieste sono le soluzioni del sistema di congruenze lineari

$$\begin{cases} x \equiv 1 \mod 3 \\ x \equiv 2 \mod 8 \end{cases},$$

del quale si vede che $x = 10$ è una soluzione particolare.

Se, invece, non volessimo risolvere il sistema, potremmo provare a calcolare $\alpha^2 = (1, 3, 2)(4, 5, 6, 7)(8, 9, 10, 11)$. Vediamo che non è σ, ma osserviamo che se in α sostituissimo $(1, 2, 3)$ con $(1, 3, 2)$, avremmo $\alpha^2 = \sigma$ e ovviamente ancora $\alpha^9 = \tau$.

Dunque $\beta = (1, 3, 2)(4, 8, 5, 9, 6, 10, 7, 11)$ è un generatore del gruppo che cerchiamo, (e ovviamente anche α andava bene).

□

Esercizio (Traccia N.87, 8 febbraio 2018)**.**
Si considerino in S_{21} *le permutazioni*

$$\sigma, \text{ di struttura ciclica } (10, 5, 4, 1, 1)$$
$$\tau, \text{ di struttura ciclica } (15, 2, 2, 2),$$

e, in S_{12}*, le permutazioni*

$$\alpha, \text{ di struttura ciclica } (8, 4),$$
$$\beta, \text{ di struttura ciclica } (4, 4, 2, 2).$$

(a) Provare che l'ordine di $< \sigma > \cap < \tau >$ *è* 1 *oppure* 5*.*

(b) Determinare α *e* β *in modo che* $< \alpha > \cap < \beta >$ *abbia ordine* 2*.*

(c) Determinare α *e* β *in modo che* $< \alpha > \cap < \beta >$ *sia il sottogruppo banale.*

Svolgimento.

(a) Cominciamo con il determinare i periodi di σ e τ. In base alla Proposizione 18.26, si ha $o(\sigma) = 20, o(\tau) = 30$.

Questo permette di stimare a priori l'ordine del sottogruppo

$$H := < \sigma > \cap < \tau > .$$

Infatti, in base alla Proposizione 17.35, H sarà ciclico, dunque il suo ordine coincide con il periodo di un suo generatore. Questo sarà un elemento di entrambi i gruppi ciclici che formano l'intersezione e pertanto il suo ordine deve dividere sia 20 che 30, per il Teorema di Lagrange (Teorema 17.19), e dunque deve dividere $10 = MCD(20, 30)$.

Dunque l'ordine di H può essere $1, 2, 5$ oppure 10.

Ora, un elemento di H deve essere nella forma σ^h per qualche $h = 0, \ldots, 19$ e contemporaneamente nella forma τ^k per qualche $k = 0, \ldots, 29$. Selezioniamo, allora, gli esponenti "plausibili", cioè quelli che possano

determinare strutture cicliche coincidenti per le potenze di σ e le potenze di τ. Determiniamo, cioè, le coppie (h, k) per cui σ^h e τ^k abbiano la stessa struttura ciclica.

Osserviamo che σ ha due 1-cicli, che rimarranno tali per qualunque sua potenza. L'unico modo affinché τ^k abbia degli 1-cicli è che l'esponente k sia pari. Diversamente, i tre 2-cicli di τ rimarrebbero invariati, e resterebbero gli unici tre 2-cicli, visto che nessuna potenza di un 15-ciclo può spezzarsi nel prodotto di 2-cicli. Ma è facile vedere che nessuna potenza di σ può avere soli tre 2-cicli.

Inoltre, è chiaro che dobbiamo "alterare" il 15-ciclo di τ, visto che i cicli di σ hanno tutti lunghezza minore di 15. Allora dobbiamo elevare ad un multiplo di 3 o di 5 (oltre che di 2). D'altro canto, τ^{10} e τ^{20} hanno struttura ciclica

$$(3, 3, 3, 3, 3, 1, 1, 1, 1, 1, 1),$$

struttura mai raggiungibile da una potenza di σ. Tutto sommato, si deve quindi avere $k \in \{0, 6, 12, 18, 24\}$. Per tutti questi esponenti diversi da 0 (per il quale si ha la struttura ciclica banale), la struttura ciclica è sempre la stessa, cioè

$$(5, 5, 5, 1, 1, 1, 1, 1, 1).$$

Questo rende molto più semplice l'analisi dell'esponente h di σ. Per avere una struttura ciclica del tipo appena citato (o quella banale), non possiamo che elevare σ ad un multiplo di 4. Dunque $h \in \{0, 4, 8, 12, 16\}$.

Ricordiamo ora che $|H| \in \{1, 2, 5, 10\}$. Assumiamo che $H =< \sigma^h >$ (o, equivalentemente, $H =< \tau^k >$), con h uno degli esponenti selezionati. Siccome $20|5h$, si ha sempre $\sigma^{5h} = id$, per cui nessuna potenza selezionata di σ ha periodo 10.

Analogamente, $2h \in \{0, 8, 16, 24, 32\}$, pertanto σ^{2h} non è mai l'identità, cioè nessuna potenza selezionata di σ ha periodo 2.

Di conseguenza, tale potenza può avere solo periodo 1 oppure 5, e solo tale può essere l'ordine di H.

Osservazione 2. In realtà, il nostro ragionamento si sarebbe potuto fermare nel momento in cui abbiamo determinato le possibili strutture cicliche di τ^k, in quanto sono solamente due: quella banale e $(5,5,5,1,1,1,1,1,1)$. Da qui, risulta evidente che tale potenza può avere periodo esattamente 1 oppure 5.

(b) Con un ragionamento simile a quello del punto (a), risulta evidente che un elemento non banale di $K :=< \alpha > \cap < \beta >$ non può che essere del tipo $\alpha^2, \alpha^4, \alpha^6$ (mentre sono ammissibili tutte le tre potenze non banali di β).

Dunque $|K| \in \{1,2,4\}$. Si ha $|K| = 4$ se e solo $K =< \beta >$, se e solo se $\beta \in< \alpha >$, il che (compatibilmente con le strutture cicliche) avviene se e solo se $\beta = \alpha^2$ o $\beta = \alpha^6$. Poniamoci dunque nel caso contrario, in cui β non è né α^2 né α^6. Allora si ha $|K| = 2$ se e solo se $K =< \alpha^4 >=< \beta^2 >$, poiché α^4 e β^2 sono, rispettivamente, gli unici elementi di periodo 2 in $< \alpha >$ e $< \beta >$. Precisamente, in questo caso si ha $K = \{\mathrm{id}, \alpha^4\} = \{\mathrm{id}, \beta^2\}$, ove, per l'appunto, $\alpha^4 = \beta^2$.
Scegliamo $\alpha = (1,2,3,4,5,6,7,8)(9,10,11,12)$.

Osserviamo che

$$\alpha^2 = (1,3,5,7)(2,4,6,8)(9,11)(10,12)$$

$$\alpha^4 = (1,5)(2,6)(3,7)(4,8).$$

Dunque per scegliere β è sufficiente alterare uno dei 4-cicli di α^2, facendo in modo che abbia lo stesso quadrato del ciclo non alterato. Questo si può fare invertendo due elementi non successivi, per esempio scambiando 1 e 5 nel primo ciclo. Si sceglie, cioè

$$\beta = (5,3,1,7)(2,4,6,8)(9,11)(10,12).$$

Queste permutazioni soddisfano la richiesta.

(c) Procediamo in maniera simile al punto (b). Stavolta vogliamo anche evitare che α^4 e β^2 coincidano.

Per fare ciò, con le stesse notazioni del punto (b) è sufficiente alterare il primo ciclo di α^2, facendo in modo di alterare anche il suo quadrato. Stavolta possiamo pertanto invertire due elementi vicini, per esempio 3 e 5. Si sceglie, cioè,

$$\beta = (1,5,3,7)(2,4,6,8)(9,11)(10,12).$$

□

Esercizio (Traccia N.88, 20 aprile 2018)**.**
Sia $\alpha \in S_9$. Si considerino inoltre le seguenti permutazioni di S_9:

$$\sigma = (1,2,3)(4,5,6,7)(8,9),$$

$$\tau = (1,2,3)(4,5,6)(7,8,9).$$

(a) Provare che se α commuta con σ, allora α commuta anche con $(1,2,3)$.

(b) Provare o confutare la seguente affermazione: se α commuta con τ, allora α commuta anche con $(1,2,3)$.

(c) Determinare un sottogruppo di S_9 avente ordine $2^2 \cdot 3^2 \cdot 4 \cdot 5 \cdot 6$ e al quale appartengono σ e τ.

Svolgimento.

(a) Una volta osservato che $(1,2,3) = \sigma^4$ è immediato verificare che α commuta con σ^4. Infatti,

$$\alpha\sigma^4 = \alpha\sigma\sigma^3 = \sigma\alpha\sigma^3 = \cdots = \sigma^4\alpha.$$

Mostriamo, comunque, almeno altri due approcci che fanno uso di tecniche diverse, e da cui scaturiscono alcune osservazioni utili per la risoluzione del punto (b).

Per ipotesi sappiamo che

$$\alpha\sigma = \sigma\alpha \iff \alpha\sigma\alpha^{-1} = \sigma.$$

Vogliamo provare che $\alpha(1,2,3) = (1,2,3)\alpha$, o, equivalentemente, che $\alpha(1,2,3)\alpha^{-1} = (1,2,3)$.

Si osservi che $(1,2,3) = \sigma^4$. Risulta, allora:

$$\alpha\sigma\alpha^{-1} = \sigma \Rightarrow (\alpha\sigma\alpha^{-1})^4 = (\sigma)^4 \Rightarrow \alpha(1,2,3)\alpha^{-1} = (1,2,3),$$

dove, la seconda implicazione segue dal fatto che

$$(\alpha\sigma\alpha^{-1})^4 = (\alpha\sigma\alpha^{-1})(\alpha\sigma\alpha^{-1})(\alpha\sigma\alpha^{-1})(\alpha\sigma\alpha^{-1}) = \alpha\sigma^4\alpha^{-1}.$$

Un' altra possibile risoluzione è quella basata sull'osservare che l'insieme

$$C(\alpha) := \{\beta \in S_9 | \alpha\beta = \beta\alpha\}$$

è un sottogruppo di S_9, a cui σ appartiene per ipotesi e a cui, di conseguenza, appartiene anche $\sigma^4 = (1,2,3)$.

Infatti, sicuramente $id \in C(\alpha)$. Inoltre, per ogni $\beta, \gamma \in C(\alpha)$, si ha che:

- $(\beta\gamma)\alpha = \beta(\gamma\alpha) = \beta(\alpha\gamma) = (\beta\alpha)\gamma = (\alpha\beta)\gamma = \alpha(\beta\gamma)$;
- $\beta\alpha = \alpha\beta \Rightarrow \beta^{-1}\alpha = \alpha\beta^{-1}$.

per cui $\beta\gamma, \beta^{-1} \in C(\alpha)$.

(b) Supponiamo di voler provare che l'affermazione data è vera. Potremmo pensare di procedere come nel caso precedente. Il problema è che, stavolta, non è possibile esprimere il 3-ciclo $(1,2,3)$ come potenza di τ: visto che la struttura ciclica di τ è $(3,3,3)$, nessun elevamento a potenza di τ ha l'effetto di "eliminare" i 3-cicli $(4,5,6)$ e $(7,8,9)$ lasciando invariato il primo 3-ciclo.

Per le stesse ragioni, neanche il secondo approccio visto nel punto (a) ci aiuta, a meno di non avere ulteriori informazioni sugli elementi che commutano con α.

Cerchiamo dunque un controesempio all'affermazione data. Si consideri $\alpha = (1,4,2,5,3,6)$. Dato che $\alpha^2 = (1,2,3)(4,5,6)$, ossia il prodotto dei primi due 3-cicli di τ, si ha che $(1,2,3)(4,5,6) \in < \alpha >$, e quindi commuta con α. Inoltre, anche $(7,8,9)$ commuta con α, in quanto permutazione disgiunta da essa. Dunque α commuta con τ. Tuttavia, un calcolo diretto mostra che

$$\alpha(1,2,3) \neq (1,2,3)\alpha,$$

confutando l'affermazione.

(c) Si osservi, innanzitutto, che $2^2 \cdot 3^2 \cdot 4 \cdot 5 \cdot 6 = 3! \cdot 6!$.

Per la Proprietà 5, il sottoinsieme H di S_9 composto dalle permutazioni che fissano gli elementi $4,5,6,7,8,9$ è un sottogruppo di S_9 isomorfo a S_3: ha quindi cardinalità $3!$.

Analogamente, il sottoinsieme K di S_9 formato dalle permutazioni che fissano gli elementi $1,2,3$ è un sottogruppo di S_9 isomorfo a S_6, e ha quindi cardinalità $6!$.

Inoltre, ogni permutazione di H è disgiunta da ogni permutazione di K: se $\beta \in H$ e $\gamma \in K$, si ha che il supporto di β è contenuto in $\{1,2,3\}$, mentre quello di γ è contenuto in $\{4,5,6,7,8,9\}$.

Dunque, per la Proprietà 4, l'insieme

$$L = \{\beta\gamma | \beta \in H, \gamma \in K\}$$

è un sottogruppo di S_9 avente ordine $|H||K| = 3!6!$.

Inoltre, dato che $(1,2,3) \in H$ e $(4,5,6,7)(8,9), (4,5,6)(7,8,9) \in K$, i loro prodotti, ossia σ e τ, appartengono a L.

□

Esercizio (Traccia N.89, 5 giugno 2018)**.**
Sia H un sottogruppo di S_4.

(a) Provare che se $\{(1,2,3),(1,2,4)\} \subset H$, allora $A_4 \subset H$.

(b) Provare che se $\{(1,2),(1,3),(1,4)\} \subset H$, allora $H = S_4$.

Svolgimento.

(a) Iniziamo cercando di comprendere come deve essere fatta una permutazione pari di S_4: in base alla Proposizione 18.32 e ai Corollari 18.33 e 18.34, una permutazione di S_4 diversa dalla permutazione identica è pari se e solo se è un 3-ciclo o un prodotto di 2-cicli.

Grazie alla Proposizione 18.4, sappiamo che, in S_4, ci sono

$$\frac{1}{3}\frac{4!}{(4-3)!} = 8$$

3-cicli. Inoltre, ci sono

$$\frac{1}{2}\left(\frac{1}{2}\frac{4!}{(4-2)!}\right)\left(\frac{1}{2}\frac{2!}{(2-2)!}\right) = 3$$

permutazioni di struttura ciclica (2,2) (il fattore $\frac{1}{2}$ davanti è necessario perché questo calcolo combinatorio, a priori, conta, ad esempio, $(1,2)(3,4)$ come diversa da $(3,4)(1,2)$).

In effetti, considerando anche la permutazione identica, risulta

$$1 + 8 + 3 = 12 = |A_4|.$$

Dunque, dobbiamo provare che in H ci sono gli otto 3-cicli e le tre permutazioni di struttura ciclica (2,2) (è ovvio che $id \in H$, essendo H un sottogruppo).

Chiamiamo $\alpha := (1,2,3), \beta := (1,2,4)$.

Dal momento che $\alpha, \beta \in H$, anche $\alpha^{-1} = (1,3,2), \beta^{-1} = (1,4,2) \in H$. Abbiamo, pertanto, già quattro dei 3-cicli che dobbiamo trovare.

Ora, ogni possibile prodotto di queste permutazioni è in H. Si ha:

- $\alpha\beta = (1,3)(2,4) \in H$.
- $\beta\alpha = (1,4)(2,3) \in H$.

Dato che $o(\alpha\beta) = 2$, si ha $\alpha\beta = (\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}$, e analogamente $\beta\alpha = \alpha^{-1}\beta^{-1}$: dunque, non ha senso fare prodotti tra gli inversi di α e β, perché non otterremmo nulla di nuovo. Moltiplichiamo tra di loro le due permutazioni appena trovate, ottenendo

$$(1,3)(2,4)(1,4)(2,3) = (1,2)(3,4) \in H.$$

Dunque, abbiamo trovato tutte le permutazioni di struttura ciclica (2,2). Restano da trovare i restanti quattro 3-cicli.

Proviamo calcolando i prodotti tra un 3-ciclo e una delle permutazioni di struttura ciclica (2,2). Si ha:

- $(1,3)(2,4)(1,2,3) = (1,4,2)$: l'avevamo già trovata.
- $(1,4)(2,3)(1,2,3) = (1,3,4)$: è un nuovo 3-ciclo. Osserviamo che abbiamo quindi anche il suo inverso, ossia $(1,4,3)$. Usiamo questa permutazione al prossimo punto.
- Pur procedendo essenzialmente per tentativi, è possibile fare delle scelte migliori di altre per ottimizzare il numero di prove: osservando i 3-cicli che abbiamo già ottenuto, notiamo che nessuno di essi fissa 1. Quindi gli ultimi due 3-cicli devono farlo. Se, per esempio, scegliamo di partire da $(1,3,4)$, se moltiplichiamo a sinistra per una permutazione che scambia (1,3), l'indice 1 seguirà il percorso

  $$1 \mapsto 3 \mapsto 1,$$

  venendo complessivamente fissato. In effetti, si ha,

  $$(1,3)(2,4)(1,3,4) = (2,4,3)$$

  e, di conseguenza, otteniamo anche $(2,3,4)$.

Abbiamo dunque provato che $A_4 \subset H$.

(b) Osserviamo che, sicuramente,

$$(1,3)(1,2) = (1,2,3) \in H,$$

$$(1,4)(1,2) = (1,2,4) \in H.$$

Dunque, per il punto (a), $A_4 \subset H$. A questo punto, sappiamo anche in H ci sono gli elementi di A_4 dati dai prodotti di due 2-cicli, cioè

$$(1,2)(3,4), (1,3)(2,4), (1,4)(2,3) \in H.$$

Moltiplicandole, rispettivamente, per $(1,2), (1,3), (1,4)$, otteniamo che

$$(3,4), (2,4), (2,3) \in H.$$

Dunque, in H abbiamo sei trasposizioni. Ma, per la Proposizione 18.4, il numero totale dei 2-cicli in S_4 è proprio

$$\frac{1}{2}\frac{4|}{(4-2)!} = 6.$$

In H abbiamo, pertanto, tutte le trasposizioni di S_4. Ma allora, per il Corollario 18.31, $H = S_4$, visto che ogni altra permutazione può essere ottenuta come un opportuno prodotto di trasposizioni.

□

Esercizio (Traccia N.90, 20 giugno 2018)**.**
Siano date le seguenti permutazioni di S_{28}*:*
$\sigma = (1,2,3,4,5,6,7,8,9,10)$,
$\tau = (24,18,11,26,14,28,\boldsymbol{1},21,16,19,23,27,13,17,12,\boldsymbol{4},22,25,15,20)$,
$\rho = (24,18,11,26,14,28,\boldsymbol{1},21,16,19,23,27,13,17,12,22,\boldsymbol{6},25,15,20)$.
Siano inoltre,

- H *un sottogruppo di* S_{28} *tale che* $\{\sigma,\tau\} \subset H$*,*

- *K un sottogruppo di S_{28} tale che $\{\sigma, \rho\} \subset K$.*

(a) Determinare un sottogruppo ciclico di H avente ordine 9.

(b) Determinare un sottogruppo non ciclico di K avente ordine 4.

Svolgimento.

(a) Il nostro obiettivo è determinare un elemento di periodo 9 appartenente ad H. Ma cosa vuol dire per una permutazione avere periodo 9? In base alla Proposizione 18.26, il periodo di una permutazione è il minimo comune multiplo della lunghezza dei suoi cicli.

Sia $\alpha \in S_{28}$ una permutazione di periodo 9 e sia $(a_1, \dots, a_l)$ la sua struttura ciclica (dove, ricordiamo, $a_1 \geq a_2 \geq \cdots \geq a_l$). Inoltre, per ogni $i = 1, \dots, l$, $a_i | 9 = \text{mcm}(a_1, \dots, a_l)$.

Se a_1 non fosse 9, allora tutte le lunghezze sarebbero 3 o 1, e quindi anche il minimo comune multiplo (periodo di α) sarebbe 3 o 1.

Dunque, dobbiamo cercare una permutazione che abbia almeno un 9-ciclo tra i suoi cicli disgiunti.

La prima cosa che osserviamo è che σ è un 10-ciclo. Ci chiediamo se sia possibile "accorciare" la lunghezza. L'operazione che si può fare è quella di "saltare" un elemento. Supponiamo per esempio di voler "rimuovere" l'indice 2. Allora possiamo moltiplicare a destra per la trasposizione $(1, 2)$, perché, in tal caso, il 2 seguirà il percorso

$$2 \mapsto 1 \mapsto 2.$$

In effetti,

$$\sigma \cdot (1, 2) = (1, 3, 4, 5, 6, 7, 8, 9, 10).$$

Non è necessario usare una trasposizione: l'effetto voluto, in effetti, deve essere solo quello di "eliminare" il 2 (e solo il 2) dall'orbita di 1. Questo può essere fatto moltiplicando per una permutazione α tale che

$\alpha(1) = 2$ e tale che $1, 2$ siano gli unici elementi in comune tra i supporti di σ e α.

Infatti, in tal caso, α fissa qualsiasi elemento del supporto di σ diverso da 1 e 2. Dunque, l'orbita di 1 sotto l'azione di $\sigma\alpha$ sarà

$$\begin{aligned} 1 \mapsto \sigma\alpha(1) = \sigma(2) = 3 \mapsto \sigma\alpha\sigma(2) = \sigma\sigma(2) = \sigma^2(2) = 4 \mapsto \dots \\ \mapsto \sigma^8(2) = 10 \mapsto \sigma^9(2) = \sigma^{10}(1) = 1 \end{aligned}$$

ovvero, l'orbita di 1 è

$$\{1, 3, 4, 5, 6, 7, 8, 9, 10\}.$$

Cerchiamo di capire se possiamo applicare questa idea per ottenere un 9-ciclo da σ. Osserviamo che, gli unici elementi comuni nei supporti di σ e τ sono 1 e 4. Per poter applicare il ragionamento precedente, occorre dunque considerare le seguenti permutazioni di H:

$\sigma^3 = (\mathbf{1,4}, 7, 10, 3, 6, 9, 2, 5, 8)$,

$\tau^9 = (\mathbf{1,4}, 14, 17, 11, 27, 24, 19, 15, 21, 22, 28, 12, 26, 13, 18, 23, 20, 16, 25)$.

In questo modo ci siamo ricondotti ad una situazione simile a quella dell'esempio. In effetti, considerando $\sigma^3\tau^9$, l'orbita di 4 sarà

$$4 \mapsto 14 \mapsto 17 \mapsto \dots \mapsto 25 \mapsto 4,$$

mentre l'orbita di 1 sarà

$$1 \mapsto 7 \mapsto 10 \mapsto \dots \mapsto 8 \mapsto 1.$$

Dunque, questo prodotto avrà l'effetto voluto di far "saltare" il 4 nel 10-ciclo. Inoltre, "salterà" l'1 nel 20-ciclo. Dunque, la struttura ciclica di $\sigma^3\tau^9$ sarà $(19, 9)$ (lo si verifichi facendo esplicitamente il prodotto). Ma allora

$$\alpha := (\sigma^3\tau^9)^{19}$$

è un elemento di periodo 9 appartenente ad H.

(b) Ricordiamo che A_4 contiene un sottogruppo di ordine 4 non ciclico, ossia

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

Qui tutti gli elementi che non sono l'identità hanno periodo 2. Inoltre, il prodotto di due elementi di periodo 2 fornisce il terzo elemento di periodo 2.

Possiamo provare a ragionare seguendo questo esempio: troviamo due elementi di periodo 2 il cui prodotto è un elemento di periodo 2.

Sfruttiamo il fatto che, stavolta, gli unici due elementi in comune tra i supporti di σ e ρ sono 1 e 6. Si ha che σ^5 e ρ^{10} hanno periodo 2. Inoltre,

$$\sigma^5 = (1,6)(2,7)(3,8)(4,9)(5,10),$$

$$\rho^{10} = (1,6)\alpha,$$

essendo α il prodotto degli altri 2-cicli che formano ρ^{10} (visto che non muove nessun elemento mosso anche da σ^5, sappiamo che commuterà con σ^5).

Si ha che

$$\sigma^5\rho^{10} = (2,7)(3,8)(4,9)(5,10)\alpha.$$

Questo è ancora un prodotto di trasposizioni, e ha quindi periodo 2.

Si osservi ora che, in generale, se $\beta, \gamma \in S_n$ hanno periodo 2 e $\beta\gamma$ ha periodo 2, allora β e γ commutano. Infatti, dato che una permutazione di periodo 2 coincide con il suo inverso, si ha che

$$\beta\gamma = (\beta\gamma)^{-1} = \gamma^{-1}\beta^{-1} = \gamma\beta.$$

Sfruttando questa proprietà, è immediato verificare che

$$V' = \{id, \sigma^5, \rho^{10}\,\sigma^5\rho^{10}\}$$

è un sottogruppo (di ordine 4 e non ciclico).

Infatti, ogni elemento coincide con il suo inverso, che quindi appartiene a V'. Inoltre, dato che, per quanto appena provato σ^5 e ρ^{10} commutano, si prova facilmente che V' è chiuso rispetto al prodotto.

□

Esercizio (Traccia N.91, 5 luglio 2018)**.**
Siano date le seguenti permutazioni di S_{16}*:*

$$\sigma = (1,2,3,4)(5,6,7,8,9)(10,11,12,13,14,15),$$
$$\tau = (1,2,3,4,5,6,7,8,9)(10,11,12,13,14,15,16).$$

(a) Dimostrare che se un sottogruppo H *di* S_{16} *contiene* $\{\sigma,\tau\}$*, allora* H *ha un sottogruppo di ordine 27.*

(b) Dimostrare che se un sottogruppo di K *di* S_{16} *contiene* $\{\sigma,\tau\}$*, allora* K *ha almeno 3 distinti sottogruppi di ordine 9.*

Svolgimento.

(a) Dato che $27 = 3^3$, 27 non è mai ottenibile come minimo comune multiplo di numeri più piccoli di 27 stesso. Alla luce della Proposizione 18.26, una condizione necessaria affinché una permutazione abbia ordine 27 è che abbia un 27-ciclo tra i suoi cicli disgiunti. Tuttavia, essendo, in questo caso, 16 la massima lunghezza di un ciclo, non esistono elementi di ordine 27. Dunque, il sottogruppo che cerchiamo non può essere ciclico.

Possiamo sfruttare la Proprietà 3 per costruire sottogruppi di ordine opportuno. Abbiamo bisogno, in questo caso, di due o più permutazioni a due a due disgiunte tali che il prodotto dei rispettivi ordini sia 27. Visto che cerchiamo tale sottogruppo in H, che contiene σ e τ, possiamo cercare queste permutazioni come prodotti e potenze di σ e τ.

Dal momento che la struttura ciclica di τ è $(9,7)$, è possibile costruire a partire da essa un 9-ciclo. Precisamente, è possibile ottenere il ciclo

$(1,2,3,4,5,6,7,8,9)$ considerando τ^k, ove k è un opportuno intero, tale che

$$\begin{cases} k \equiv 1 \mod 9 \\ k \equiv 0 \mod 7 \end{cases}.$$

Per esempio, $k = 28$ è un siffatto intero.

Abbiamo pertanto un 9-ciclo. Cerchiamo ora una permutazione di periodo 3, disgiunta da $\alpha := \tau^{28}$.

È possibile ottenerla a partire da σ. Infatti, dato che la sua struttura ciclica è $(6,5,4)$, possiamo considerare una opportuna potenza di σ che abbia l'effetto di "eliminare" il 5-ciclo e il 4-ciclo, e di "spezzare" il 6-ciclo in due 3-cicli: in tal caso, il risultato sarà una permutazione di periodo 3, avendo come struttura ciclica $(3,3,1,\ldots,1)$. A tal fine, dobbiamo determinare un intero h tale che

$$\begin{cases} h \equiv 2 \mod 6 \\ h \equiv 0 \mod 5 \\ h \equiv 0 \mod 4 \end{cases}.$$

Per esempio, consideriamo $h = 20$. Dunque

$$\beta := \sigma^{20} = (10,12,14)(11,13,15).$$

Pertanto, per la Proprietà 3,

$$L = \{\alpha^m \beta^n | m, n \in \mathbb{Z}\} \leq H$$

è un sottogruppo di ordine $9 \cdot 3 = 27$.

(b) Analogamente a quanto già osservato nel punto (a), $\alpha = \tau^{28}$ è una permutazione di ordine 9 contenuta in K. Dunque,

$$K_1 := < \alpha >,$$

è un sottogruppo (ciclico) di K di ordine 9.

Un altro modo per ottenere un sottogruppo di ordine 9 è sfruttare ancora la Proprietà 3, cercando due permutazioni disgiunte di ordine 3.

Abbiamo già determinato nel punto (a) la permutazione $\beta = \sigma^{20}$, avente periodo 3. Inoltre, α è un 9-ciclo disgiunto da β. Allora $\gamma := \alpha^3$ è prodotto di tre 3-cicli, e ha dunque periodo 3. Pertanto,

$$K_2 := \{\beta^m \gamma^n | m, n \in \mathbb{Z}\}$$

è un sottogruppo di ordine 9 contenuto in K. Esso è distinto da K_1 perché non contiene alcun elemento di ordine 9. Infatti, i suoi elementi non banali sono prodotti di due o più 3-cicli disgiunti.

Scriviamo esplicitamente K_2. Si ha

$$K_2 = \{id, \beta, \beta^{-1}, \gamma, \gamma^{-1}, \beta\gamma, \beta\gamma^{-1}, \beta^{-1}\gamma, \beta^{-1}\gamma^{-1}\}.$$

Resta da determinare un terzo sottogruppo.

Finora abbiamo considerato sempre separatamente σ e τ, ossia abbiamo determinato i generatori di K_1 e di K_2 come potenze si σ e τ. Dato che il problema è ambientato in K, che contiene σ e τ, possiamo anche considerare i loro prodotti e le potenze di questi prodotti.

Calcoliamo $\sigma\tau$ e $\tau\sigma$. Si ha:

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

$$\tau\sigma = (1,3,5,7,9,6,8)(2,4)(10,12,14,16)(11,13,15).$$

La struttura ciclica è, in entrambi i casi, $(7, 4, \underline{\mathbf{3}}, 2)$. Dunque, possiamo, in entrambi i casi, ottenere un 3-ciclo considerando una opportuna potenza che abbia l'effetto di "eliminare" il 7-ciclo, il 4-ciclo e il 2-ciclo, lasciando invariato il 3-ciclo. L'esponente, come al solito, si ricava

risolvendo il sistema di congruenze

$$\begin{cases} k \equiv 0 \mod 4 \\ k \equiv 1 \mod 3 \\ k \equiv 0 \mod 7 \end{cases}$$

(dove omettiamo la congruenza $k \equiv 0 \pmod 2$, poiché le sue soluzioni comprendono quelle della prima equazione del sistema). Si ha che una soluzione particolare del sistema è $k = 28$.

Pertanto, otteniamo gli elementi

$$\eta = (\sigma\tau)^{28} = (10, 12, 14),$$

$$\rho = (\tau\sigma)^{28} = (11, 13, 15).$$

Essi sono due 3-cicli disgiunti. Dunque, ancora per la Proprietà 3, si ha che

$$K_3 := \{\eta^m \rho^n | n, m \in \mathbb{Z}\}$$

è un sottogruppo di K di ordine 9.

Ovviamente, esso non è ciclico avendo solamente elementi di periodo 3 oppure 1. Pertanto $K_3 \neq K_1$.

Inoltre, ad esempio, l'elemento $\eta = (10, 12, 14)$, che appartiene a K_3, non appartiene a K_2, come si vede subito dalla descrizione esplicita di K_2 vista sopra. Segue che $K_3 \neq K_2$.

Dunque K_1, K_2, K_3 sono sottogruppi di K di ordine 9 a due a due distinti.

□

Esercizio (Traccia N.92, 10 settembre 2018)**.**
Siano date in S_{10} le permutazioni

$$\sigma = (1, 2, 3, 4, 5),$$

$$\tau = (5, 4, 7, 10, 8, 6, 9).$$

(a) Provare che ogni sottogruppo di S_{10} contenente $\{\sigma, \tau\}$ contiene due sottogruppi H_1 e H_2 di ordine 9 la cui intersezione è il sottogruppo banale.

(b) Siano $m, n \in \{0, 1, 2, 3, 4\}$ e $r, s \in \{0, 1, 2, 3, 4, 5, 6\}$ tali che $(m, r) \neq (n, s)$. Provare che allora $\sigma^m \tau^r \neq \sigma^n \tau^s$.

Svolgimento.

(a) Sia H un sottogruppo di S_{10} contenente σ e τ.

Allora H contiene ogni possibile prodotto formato da σ e da τ. In particolare, $\sigma\tau, \tau\sigma \in H$. Si ha:

$$\sigma\tau = (1, 2, 3, 4, 7, 10, 8, 6, 9),$$

$$\tau\sigma = (1, 2, 3, 7, 10, 8, 6, 9, 5).$$

Osserviamo che, posto $\alpha = \sigma\tau$ e $\beta = \tau\sigma$, sia α che β sono 9-cicli, e quindi generano due sottogruppi H_1 e H_2 contenuti in H di ordine 9.

Per verificare che l'intersezione $H_1 \cap H_2$ è banale è sufficiente osservare, per esempio, che 4 appartiene al supporto di α^k per ogni $k \in \mathbb{Z}$ non divisibile per 9, mentre 4 non appartiene al supporto di β^h per alcun $h \in \mathbb{Z}$.

Ciò implica che le potenze di α che coincidono con una potenza di β possono essere solamente quelle della forma $\alpha^{9k} = id$.

(b) Supponiamo che $\sigma^m \tau^r = \sigma^n \tau^s$ e dimostriamo che $(m, r) = (n, s)$. Infatti, moltiplicando a destra ambo i membri per τ^{-r} e a sinistra per σ^{-n}, otteniamo l'uguaglianza

$$\sigma^{m-n} = \tau^{s-r}.$$

Visto che le potenze di σ che non sono la permutazione identica sono dei 5-cicli e, similmente, le potenze di τ che non sono la permutazione identica sono dei 7-cicli (in particolare, $< \sigma > \cap < \tau >= \{id\}$),

questa uguaglianza è vera se e solo se ad ambo i membri compare la permutazione identica, ossia se e solo se, in base alla Proposizione 17.16,

$$m - n \equiv 0 \mod 5$$

e

$$s - r \equiv 0 \mod 7.$$

Ma, visto che $-4 \leq m - n \leq 4$ e $-6 \leq s - r \leq 6$, si ha che $5|m - n$ se e solo se $m = n$ e $7|s - r$ se e solo se $s = r$, da cui segue la tesi.

□

Esercizio (Traccia N.93, 25 settembre 2018)**.**
Siano date in S_{17} le permutazioni

$$\sigma = (1, 2, 3)(4, 5, 6)(7, 8, 9),$$

$$\tau = (14, 15)(16, 17).$$

(a) Provare che in S_{17} esistono almeno $33 \cdot 8!$ permutazioni che commutano con σ.

(b) Determinare un sottogruppo di S_{17} di ordine 144 a cui appartengano σ e τ.

(c) Determinare un sottogruppo di S_{17} di ordine $9 \cdot (8!)^2$ a cui appartengano σ e τ.

Svolgimento.

(a) Cominciamo con l'osservare che σ agisce solo sugli elementi $1, 2, \ldots, 9$, mentre lascia fissi gli elementi $10, 11, \ldots, 17$. Dunque tutte le permutazioni che hanno supporto contenuto in $\{10, 11, \ldots, 17\}$ sono disgiunte da σ e, pertanto, per il Lemma 18.18, commutano con essa. In base alla Proprietà 5, la totalità di siffatte permutazioni forma un sottogruppo di S_{17} isomorfo a S_8, e quindi sono in numero 8!.

A questo punto, ragioniamo sulle permutazioni con supporto contenuto in $\{1, 2, \ldots, 9\}$.

Naturalmente, ognuno dei 3-cicli di σ commuta con σ. Posto

$$\gamma_1 = (1, 2, 3), \gamma_2 = (4, 5, 6), \gamma_3 = (7, 8, 9),$$

alla luce della Proprietà 4, l'insieme

$$L = \{\gamma_1^m \gamma_2^n \gamma_3^l | m, n, l \in \mathbb{Z}\}$$

è un sottogruppo di S_{17} di ordine $3^3 = 27$.

Inoltre, altri elementi che commutano con σ sono sicuramente gli elementi del gruppo ciclico $< \sigma >$. Essi sono 9. Tuttavia, alcuni di questi sono già stati contati in L, ossia le potenze di σ che sono prodotti di 3-cicli (che sono σ^3 e σ^6) e, naturalmente, la permutazione identica. Restano, pertanto, $9 - 3 = 6$ elementi.

Dunque, tra le permutazioni con supporto contenuto in $\{1, 2, \ldots, 9\}$, ne abbiamo trovate $27 + 6 = 33$ che commutano con σ. Ovviamente, ogni permutazione di questo insieme di elementi, può essere moltiplicata con ogni permutazione del primo insieme di elementi trovati, ossia le permutazioni con supporto contenuto in $\{10, 11, \ldots, 17\}$, per ottenere una nuova permutazione che commuta con σ. Complessivamente, tutti questi prodotti sono $33 \cdot 8!$.

(b) Sfruttiamo ancora la Proprietà 4 per determinare un siffatto sottogruppo. Osserviamo che $144 = 2^4 \cdot 3^2$

Abbiamo bisogno di trovare 2 o più permutazioni a due a due disgiunte tali che il prodotto dei loro periodi sia 144.

Ora, si ha che σ e τ possono essere ottenute, rispettivamente, come il cubo di un 9-ciclo e come il quadrato di un 4-ciclo. Infatti, posto

$$\alpha = (1, 4, 7, 2, 5, 8, 3, 6, 9),$$

$$\beta = (14, 16, 15, 17),$$

risulta $\sigma = \alpha^3$ e $\tau = \beta^2$.

Abbiamo determinato, pertanto, due permutazioni disgiunte di periodo 9 e 4. Dato che $144 = 9 \cdot 4 \cdot 4$, ci serve ancora una permutazione di periodo 4 disgiunta da α e β. Una possibile scelta è, ovviamente, $\gamma = (10, 11, 12, 13)$.

A questo punto, per la Proprietà 4,

$$H = \{\alpha^m \beta^n \gamma^l | m, n, l \in \mathbb{Z}\}$$

è un sottogruppo di S_{17} di ordine 144.

Inoltre, H contiene naturalmente σ e τ, visto che

$$\sigma = \alpha^3 \beta^0 \gamma^0 = \alpha^3,$$

$$\tau = \alpha^0 \beta^2 \gamma^0 = \beta^2.$$

(c) Abbiamo già individuato, nel punto (a), un sottogruppo K_1 di S_{17} di ordine 8!, formato da tutte le permutazioni con supporto contenuto in $\{10, 11, \ldots, 17\}$. Chiaramente, $\tau \in K_1$.

Ora, in maniera simile, ma considerando la totalità delle permutazioni con supporto contenuto in $\{1, \ldots, 9\}$, possiamo determinare un sottogruppo K_2 si S_{17} isomorfo a S_9, a cui appartiene σ.

Dato che ogni permutazione di K_1 è disgiunta da ogni permutazione di K_2, ancora la Proprietà 4 ci dice che

$$K = \{\rho\theta | \rho \in K_1, \theta \in K_2\}$$

è un sottogruppo di S_{17} di ordine $|K_1| \cdot |K_2| = 8! \cdot 9! = 9 \cdot (8!)^2$.

Dato che K contiene K_1 e K_2, a K appartengono σ e τ, come volevasi.

□

Esercizi di secondo tipo

Esercizio (Traccia N.61, 19 giugno 2015)**.**
Determinare tutti gli interi n per i quali il numero

$$n^{180} - n^{20} - n^{36} + 1$$

è divisibile per 209.

Svolgimento. Si ha $209 = 11 \cdot 19$.
Si tratta di determinare tutti e soli gli interi n tali che

$$n^{180} - n^{20} - n^{36} + 1 \equiv 0 \mod 209.$$

In base all'Esercizio 7.12, questo è equivalente a chiedere che

$$\begin{cases} n^{180} - n^{20} - n^{36} + 1 \equiv 0 \mod 11 \\ n^{180} - n^{20} - n^{36} + 1 \equiv 0 \mod 19 \end{cases}$$

Cominciamo con lo studiare la prima congruenza. Non c'è dubbio che $n \equiv 0 \pmod{11}$ non soddisfa la proprietà richiesta. Possiamo dunque ridurci a considerare n non congrui a 0 modulo 11, ossia coprimi con esso. Dunque, per il Teorema di Eulero (17.22), si ha che

$$n^{10} \equiv 1 \mod 11.$$

Ma allora

$$n^{180} - n^{20} - n^{36} + 1 \equiv 1 - 1 - n^6 + 1 \equiv 1 - n^6 \mod 11.$$

Si tratta dunque di risolvere la congruenza $n^6 \equiv 1 \pmod{11}$.

Gli interi che risolvono tale congruenza, per la Proposizione 17.16, sono tutti e soli gli $n \in \mathbb{Z}$ tali che $o([n]_{11})$ nel gruppo moltiplicativo $\mathbb{Z}_{11}^*$ è divisore di 6. Dato che $|\mathbb{Z}_{11}^*| = 10$, gli unici periodi possibili (divisori di 6 e di 10) sono 1 e 2.
Per la Proprietà 6, (essendo, per la Proposizione 17.41 $\mathbb{Z}_{11}^*$ ciclico), ci sono esattamente un elemento di periodo 1 e un elemento di periodo di 2, ossia $[1]_{11}$ e $[10]_{11}$, rispettivamente.
Procedendo in maniera analoga per la seconda congruenza, si ottiene che occorre risolvere la congruenza $n^2 \equiv 1 \pmod{19}$, le cui soluzioni sono ancora $n \equiv \pm 1 \pmod{19}$.
Si ottengono dunque quattro sistemi di congruenze lineari:

$$(1)\begin{cases} n \equiv 1 \mod 11 \\ n \equiv 1 \mod 19 \end{cases}, (2)\begin{cases} n \equiv 1 \mod 11 \\ n \equiv 18 \mod 19 \end{cases},$$

$$(3)\begin{cases} n \equiv 10 \mod 11 \\ n \equiv 1 \mod 19 \end{cases}, (4)\begin{cases} n \equiv 10 \mod 11 \\ n \equiv 18 \mod 19 \end{cases},$$

le cui soluzioni, sono, rispettivamente,

$$n = 1 + 209k, n = 56 + 209k, n = 153 + 209k, n = 208 + 209k,$$

che, al variare di $k \in \mathbb{Z}$, descrivono tutti gli n che soddisfano la richiesta. □

Esercizio (Traccia N.65, 15 gennaio 2016)**.**
Si consideri la congruenza $x^7 - x^5 \equiv 0$ (mod 404).

(a) Determinare tutte le sue soluzioni pari.

(b) Un noto teorema afferma che, se n e m sono interi positivi coprimi, allora esistono infiniti interi k per i quali il numero $nk + m$ è primo. Dedurne che la congruenza ha, tra le sue soluzioni, infiniti numeri primi.

Svolgimento.

(a) Alla luce dell'Esercizio 7.12, il problema è equivalente a quello di determinare la soluzione del sistema di congruenze

$$\begin{cases} x^7 - x^5 \equiv 0 \mod 101 \\ x^7 - x^5 \equiv 0 \mod 4 \end{cases}$$

Consideriamo la prima congruenza. Si ha

$$x^5(x^2 - 1) \equiv 0 \mod 101$$

se e solo se $x \equiv 0, 1, 100 \pmod{101}$ (infatti, $\mathbb{Z}_{101}$ è un dominio di integrità).

Per quanto riguarda la seconda congruenza, come nel caso precedente si ottiene che $x \equiv 0, 1, 3 \pmod 4$ sono soluzioni. In questo caso, però, anche $x \equiv 2 \pmod 4$ è soluzione, visto che, con questo assunto, x^5 è sicuramente divisibile per 4.

Le soluzioni pari della congruenza si trovano in corrispondenza dei casi $x \equiv 0, 2 \pmod 4$. Dunque, è possibile determinarle risolvendo i seguenti sei sistemi di congruenze lineari:

$$(1) \begin{cases} x \equiv 0 \mod 101 \\ x \equiv 0 \mod 4 \end{cases}, (2) \begin{cases} x \equiv 1 \mod 101 \\ x \equiv 0 \mod 4 \end{cases}, (3) \begin{cases} x \equiv 100 \mod 101 \\ x \equiv 0 \mod 4 \end{cases},$$

$$(4) \begin{cases} x \equiv 0 \mod 101 \\ x \equiv 2 \mod 4 \end{cases}, (5) \begin{cases} x \equiv 1 \mod 101 \\ x \equiv 2 \mod 4 \end{cases}, (6) \begin{cases} x \equiv 100 \mod 101 \\ x \equiv 2 \mod 4 \end{cases}.$$

Si trova che le soluzioni sono:

(1) $404k$, al variare di $k \in \mathbb{Z}$;

(2) $304 + 404k$, al variare di $k \in \mathbb{Z}$;

(3) $100 + 404k$, al variare di $k \in \mathbb{Z}$;

(4) $202 + 404k$, al variare di $k \in \mathbb{Z}$;

(5) $102 + 404k$, al variare di $k \in \mathbb{Z}$;

(6) $302 + 404k$, al variare di $k \in \mathbb{Z}$.

(b) Le soluzioni della congruenza sono del tipo $l+404k$, al variare di $k \in \mathbb{Z}$, dove l è una soluzione particolare della congruenza. Per applicare il Teorema citato, è sufficiente trovare una soluzione particolare l coprima con 404. Naturalmente, dobbiamo cercare nelle soluzioni dispari (ossia i casi che abbiamo escluso nel punto (a)) che non siano divisibili per 101 (dobbiamo escludere il caso $x \equiv 0 \pmod{101}$). Per esempio, considerando la congruenza

$$\begin{cases} x \equiv 1 \mod 101 \\ x \equiv 1 \mod 4 \end{cases}$$

si ha evidentemente che le sue soluzioni (che sono in particolare soluzioni della congruenza data) sono tutte e sole quelle dell'insieme

$$\{1 + 404k | k \in \mathbb{Z}\}.$$

In base al Teorema citato, in tale insieme ci sono infiniti numeri primi.

□

Esercizio (Traccia N.72, 12 settembre 2016)**.**

(a) Determinare due distinti omomorfismi di gruppi non nulli $\mathbb{Z}_3 \times \mathbb{Z}_4 \to \mathbb{Z}_6 \times \mathbb{Z}_7$.

(b) Determinare un omomorfismo di anelli non nullo $\mathbb{Z}_3 \times \mathbb{Z}_4 \to \mathbb{Z}_6 \times \mathbb{Z}_7$.

(c) Provare che non esiste alcun monomorfismo di gruppi $\mathbb{Z}_3 \times \mathbb{Z}_4 \to \mathbb{Z}_{34}$.

Svolgimento. La soluzione proposta si basa fortemente sulla Proprietà 10.

(a) Per la Proprietà 10, ogni omomorfismo di gruppi

$$\mathbb{Z}_3 \times \mathbb{Z}_4 \to \mathbb{Z}_6 \times \mathbb{Z}_7$$

è univocamente determinato una volta assegnate le immagini degli elementi

$$e_1 := ([1]_3, [0]_4), e_1 := ([0]_3, [1]_4),$$

a patto che tali assegnazioni tengano conto dei periodi, ossia e_1 deve essere mandato in un elemento di $\mathbb{Z}_6 \times \mathbb{Z}_7$ con periodo divisore di 3 (ossia, 1 o 3), e e_2 in un elemento con periodo divisore di 4 (ossia, 1,2 o 4).

Osserviamo che ogni elemento di $\mathbb{Z}_6 \times \mathbb{Z}_7$ che ha seconda componente diversa da $[0]_7$ ha periodo multiplo di 7. Dunque, le assegnazioni devono coinvolgere elementi del tipo $([a]_6, [0]_7)$.

In $\mathbb{Z}_6$ ci sono due elementi di periodo 3, ossia $[2]_6$ e $[4]_6$. Dunque, le assegnazioni

$$e_1 \mapsto ([2]_6, [0]_7), e_2 \mapsto ([0]_6, [0]_7),$$

$$e_1 \mapsto ([4]_6, [0]_7), e_2 \mapsto ([0]_6, [0]_7)$$

individuano univocamente due omomorfismi di gruppi distinti e non nulli (si osservi che la seconda assegnazione è pure lecita).

(b) Ogni omomorfismo di anelli deve essere, in particolare, un omomorfismo di gruppi additivi. Valgono, pertanto, le stesse condizioni necessarie di cui al punto (a).

Prima di, eventualmente, cercarne altri, verifichiamo se almeno uno dei due omomorfismi (non nulli) trovati al punto precedente (diciamo, rispettivamente, φ_1 e φ_2) è un omomorfismo di anelli. Osserviamo che, per ogni $([a]_3, [b]_4) \in \mathbb{Z}_3 \times \mathbb{Z}_4$,

$$\varphi_1(([a]_3, [b]_4)) = ([2a]_6, [0]_7),$$

$$\varphi_2(([a]_3, [b]_4)) = ([4a]_6, [0]_7).$$

Tuttavia,

$$\varphi_1(([1]_3,[0]_4)\cdot([1]_3,[0]_4)) = \varphi_1(([1]_3,[0]_4)) = ([2]_6,[0]_7)$$

e

$$\varphi_1(([1]_3,[0]_4))\cdot\varphi_1(([1]_3,[0]_4)) = ([2]_6,[0]_7)\cdot([2]_6,[0]_7) = ([4]_6,[0]_7).$$

Dunque, φ_1 non è un omomorfismo di anelli.

Siano ora $([a]_3,[b]_4),([c]_3,[d]_4) \in \mathbb{Z}_3 \times \mathbb{Z}_4$.

Si ha,

$$\begin{aligned}\varphi_2(([ac]_3,[bd]_4)) &= ([4ac]_6,[0]_7) = ([16ac]_6,[0]_7) = ([4a]_6,[0]_7)\cdot([4c]_6,[0]_7)\\ &= \varphi_2(([a]_3,[b]_4))\cdot\varphi_2(([c]_3,[d]_4)).\end{aligned}$$

Dunque, φ_2 è un omomorfismo di anelli non nullo.

(c) In base alle solite considerazioni, e_1 deve essere mandato in un elemento di periodo 1 oppure 3. D'altro canto, in $\mathbb{Z}_{34}$ non c'è alcun elemento di periodo 3, per il Teorema di Lagrange, visto che $3 \nmid 34$. Dunque $e_1 \in Ker(\varphi)$ per ogni omomorfismo di gruppi

$$\varphi : \mathbb{Z}_3 \times \mathbb{Z}_4 \to \mathbb{Z}_{34}$$

che, pertanto, non può essere ingettivo.

□

Esercizio (Traccia N.80, 21 giugno 2017)**.**
Sia n un intero e si ponga $N = n^3 + 3n^2 - 4n$.

(a) Determinare tutti i valori di n per i quali $N \equiv 0$ (mod 150).

(b) Determinare tutti i valori di n per i quali $N \equiv 6$ (mod 150).

(c) Determinare, al variare di $n \in \mathbb{N}^*$, la cifra delle unità della rappresentazione decimale di $n^{103} - n^{86} + 4n^{18} + 798656n$.

Svolgimento.

(a) In base all' Esercizio 7.12, essendo $150 = 2 \cdot 3 \cdot 5^2$, il problema è equivalente a quello di determinare tutti gli n tali che

$$\begin{cases} N \equiv 0 \mod 2 \\ N \equiv 0 \mod 3 \\ N \equiv 0 \mod 25 \end{cases}$$

Infatti, essendo 2,3,25 a due a due coprimi, N è un multiplo di mcm(2,3,25)=150 se e solo se è un multiplo comune di 2,3,25.

Osserviamo che

$$N \equiv n^3 + n^2 \equiv n^2(n+1) \equiv 0 \mod 2$$

visto che esattamente uno tra n e $n+1$ è pari, e quindi l'intero prodotto $n^2(n+1)$ lo è.

Analogamente,

$$N \equiv n^3 - n \equiv n(n+1)(n-1) \equiv 0 \mod 3$$

visto che $n, n-1$ e $n+1$ sono tre numeri consecutivi, e quindi esattamente uno è multiplo di 3, per cui lo è l'intero prodotto.

Dunque le prime due condizioni sono ininfluenti, poiché sempre soddisfatte.

In altri termini, il problema è equivalente a quello di determinare tutti gli n tali che

$$n^3 + 3n^2 - 4n \equiv 0 \mod 25. \tag{1}$$

Si osservi che $n^3 + 3n^2 - 4n = n(n^2 + 3n - 4) = n(n-1)(n+4)$.

Vogliamo che $25|n(n-1)(n+4)$. In particolare, 5 deve dividere due volte il prodotto dato. Visto che 5 è primo, per definizione 5 deve dividere uno dei fattori. Alla luce di queste considerazioni, conduciamo un'analisi dei possibili casi.

- Se $5|n$, allora non può dividere né $n+4$ né $n-1$, visto che, in caso contrario, dividerebbe $n+4-n=4$ oppure $n-(n-1)=1$. Dunque, in tal caso, 5 deve dividere due volte n, ossia $25|n$, ossia $n \equiv 0 \pmod{25}$.
- Se $5|n-1$, come nel punto precedente, non può dividere n. Tuttavia, in questo caso, divide sicuramente anche $n-1+5=n+4$. Per questo motivo, la condizione (1) è soddisfatta non appena $n-1 \equiv 0 \pmod 5$, ossia quando $n \equiv 1 \pmod 5$.
- Il caso $5|n+4$ è equivalente al precedente, per gli stessi motivi.

In definitiva, tutti e soli gli n per cui la condizione (1) è soddisfatta sono quelli appartenenti all'insieme

$$\{n \in \mathbb{N} | n \equiv 0 \pmod{25} \text{ oppure } n \equiv 1 \pmod 5\}.$$

(b) In questo caso, come nel punto (a), (applicando l'Esercizio 7.12 a $N-6$, anziché a N), il problema è equivalente a quello di determinare tutti gli n tali che

$$\begin{cases} N \equiv 6 \equiv 0 & \mod 2 \\ N \equiv 6 \equiv 0 & \mod 3 \\ N \equiv 6 & \mod 25 \end{cases}$$

Esattamente come nel punto (a), le prime due condizioni sono sempre verificate. Dunque, anche in questo caso, si tratta di determinare tutti gli n tali che

$$n^3 + 3n^2 - 4n - 6 \equiv 0 \mod 25. \tag{2}$$

In questo caso, possiamo scrivere $n^3+3n^2-4n-6 = (n+1)(n^2+2n-6)$.

Anche in questo caso vogliamo che 5 divida due volte il prodotto dato. Procediamo ancora con un'analisi dei possibili casi.

- Se $5|n+1$, allora non può dividere anche n^2+2n-6. Infatti, in tal caso, si avrebbe $n \equiv 4 \pmod 5$, ma

$$(4)^2 + 2 \cdot 4 - 6 = 18 \not\equiv 0 \mod 5.$$

  Un'altra possibilità è osservare che, se $5|n+1$, allora $5|n(n+1) = n^2+n$. Dunque, se dividesse n^2+2n-6, allora dovrebbe dividere anche $n^2 + 2n - 6 - n^2 - n = n - 6$, e di conseguenza anche $n + 1 - (n - 6) = 7$, che è impossibile.

  In ogni caso, 5 deve dividere due volte $n + 1$, ossia $n \equiv 24 \pmod{25}$.

- Si osservi che, in realtà, 5 non può mai dividere $n^2 + 2n - 6$.Per esempio, possiamo procedere per sostituzione per i restanti quattro casi ancora non esaminati ($n \equiv 0, 1, 2, 3 \pmod 5$) e constatare che non otteniamo mai la congruenza con 0 (modulo 5).

In conclusione, tutti e soli gli n per cui la condizione (2) è soddisfatta sono quelli appartenenti all'insieme

$$\{n \in \mathbb{N} | n \equiv 24 \bmod 25\}.$$

(c) Il problema richiede di trovare $x \in \{0, \ldots, 9\}$ tale che

$$n^{103} - n^{86} + 4n^{18} + 798656n \equiv x \mod 10.$$

Come nei casi precedenti, il problema è equivalente a quello di determinare un x tale che

$$\begin{cases} x \equiv n^{103} - n^{86} + 4n^{18} + 798656n \equiv n^{103} - n^{86} & \mod 2 \\ x \equiv n^{103} - n^{86} + 4n^{18} + 798656n \equiv n^{103} - n^{86} + 4n^{18} + n & \mod 5 \end{cases}$$

con la limitazione $0 \leq x \leq 9$.

Ovviamente $n^{103} - n^{86} \equiv 0 \pmod 2$ per ogni $n \in \mathbb{N}$, come è immediato verificare (o per sostituzione, oppure osservando che potenze di numeri pari (rispettivamente, dispari) sono numeri pari (rispettivamente, dispari) e la differenza è pari). Dunque $x \equiv 0 \pmod 2$: l'ultima cifra del numero dato è pari.

Poniamo $N := n^{103} - n^{86} + 4n^{18} + n$. Esaminiamo tutti i possibili casi.

- Se $n \equiv 0 \pmod 5$, allora $N \equiv 0 \pmod 5$, e dunque $x \equiv 0 \pmod 5$. Pertanto, in base alle limitazioni che abbiamo, si ha $x = 0$.
- Se $n \not\equiv 0 \pmod 5$, allora, per il Teorema di Eulero (17.22), si ha

$$\begin{aligned} N &= (n^4)^{25}n^3 - (n^4)^{21}n^2 + 4(n^4)^4n^2 + n \equiv n^3 - n^2 + 4n^2 + n \\ &\equiv n^3 + 3n^2 + n \equiv n(n^2 + 3n - 4) = n(n-1)(n+4) \mod 5 \end{aligned}$$

  Dunque si hanno i seguenti quattro casi:

  * Se $n \equiv 1 \pmod 5$, allora

$$x \equiv 1(1-1)(1+4) \equiv 0 \mod 5$$

    e dunque $x = 0$.
  * Se $n \equiv 2 \pmod 5$, allora

$$x \equiv 2(2-1)(2+4) \equiv 2 \mod 5$$

    e dunque $x = 2$.
  * Se $n \equiv 3 \pmod 5$, allora

$$x \equiv 3(3-1)(3+4) \equiv 42 \equiv 2 \mod 5$$

    e dunque $x = 2$.
  * Se $n \equiv 4 \pmod 5$, allora

$$x \equiv 4(4-1)(4+4) \equiv 96 \equiv 1 \mod 5$$

    e dunque $x = 6$.

In conclusione, si ha che

$$x = \begin{cases} 0 & \text{se } n \equiv 0, 1 \pmod 5 \\ 2 & \text{se } n \equiv 2, 3 \pmod 5 \\ 6 & \text{se } n \equiv 4 \pmod 5 \end{cases}$$

□

Esercizio (Traccia N.81, 5 luglio 2017)**.**

(a) Determinare la cifra delle unità della rappresentazione decimale di $13^{13^{25317}}$.

(b) Determinare l'inverso di $[99]_{101}^{98}$ *nell'anello* $\mathbb{Z}_{101}$.

Svolgimento.

(a) Il problema richiede di determinare $x \in \{0, \ldots, 9\}$ tale che

$$x \equiv 13^{13^{25317}} \mod 10.$$

In base all'Esercizio 7.12, si ha che questo equivale a risolvere il sistema di congruenze lineari

$$\begin{cases} x \equiv 13^{13^{25317}} \equiv 1 & \mod 2 \\ x \equiv 13^{13^{25317}} \equiv 3^{13^{25317}} & \mod 5 \end{cases}.$$

Infatti, $10|x - 13^{13^{25317}}$ se e solo se $2|x - 13^{13^{25317}}$ e $5|x - 13^{13^{25317}}$.

Si osservi che $\bar{3}$ è un elemento di ordine 4 nel gruppo ciclico $\mathbb{Z}_5^*$ (Proposizione 17.41). Dato che $13^{25317} \equiv 1 \pmod 4$, il Corollario 17.17 garantisce che

$$3 \equiv 3^{13^{25317}} \mod 5.$$

Dunque il sistema di congruenze lineari diventa:

$$\begin{cases} x \equiv 1 & \mod 2 \\ x \equiv 3 & \mod 5 \end{cases}.$$

con la limitazione che $0 \leq x \leq 9$.

Ovviamente $x = 3$ è la soluzione cercata, ovvero l'ultima cifra del numero dato.

(b) Per il Teorema di Eulero (Teorema 17.22) si ha che

$$[1]_{101} = [99]_{101}^{100} = [99]_{101}^{98}[99]_{101}^{2}.$$

Dunque $[99]_{101}^{2}$ è l'inverso cercato. Normalizziamolo (cioè scegliamo un rappresentante canonico): possiamo scrivere

$$99^2 = (101-2)^2 \equiv (-2)^2 \equiv 4 \mod 101,$$

per cui l'inverso cercato, normalizzato, è $[4]_{101}$.

□

Esercizio (Traccia N.82, 11 settembre 2017)**.**
Siano n, m interi maggiori di 1, e sia data l'applicazione

$$\varphi : \mathbb{Z}_n \times \mathbb{Z}_m \to \mathbb{Z}_{n+m}$$

$$([a]_n, [b]_m) \mapsto [2a + 2b]_{n+m}$$

(a) Determinare tutti i valori di n, m per i quali φ è ben definita.

(b) Provare che l'unico omomorfismo di gruppi $\mathbb{Z}_4 \times \mathbb{Z}_{19} \mapsto \mathbb{Z}_{23}$ è l'omomorfismo nullo.

Svolgimento.

(a) Per risolvere questo esercizio, cominciamo con il determinare delle condizioni necessarie su n, m, controllando *a posteriori* che siano anche sufficienti.

In altri termini, assumiamo che φ sia ben definita e, usando questa ipotesi, cerchiamo di dedurre la o le relazioni che n, m devono soddisfare.

Dato che φ è ben definita, allora le immagini non devono dipendere dalla scelta dei rappresentanti. Dunque, per esempio

$$[2]_{n+m} = \varphi([1]_n, [0]_m) = \varphi([n+1]_n, [0]_m) = [2n+2]_{n+m}.$$

Ma allora, $n + m | 2n + 2 - 2 = 2n$. In particolare, dobbiamo avere $n + m \leq 2n \Rightarrow m \leq n$.

Con procedimento analogo, ma usando, in luogo di quelle precedenti, le coppie $([0]_n, [1]_m)$ e $([0]_n, [m+1]_m)$, si deduce che $n \leq m$. Dunque $n = m$, necessariamente.

Viceversa, è immediato verificare che se $n = m$ allora φ è ben definita. In conclusione, le coppie cercate sono tutte e sole quelle appartenenti all'insieme

$$\{(n, m) | n = m\}.$$

(b) Sia $\varphi : \mathbb{Z}_4 \times \mathbb{Z}_{19} \to \mathbb{Z}_{23}$ un omomorfismo di gruppi. Allora, se

$$\varphi([1]_4, [0]_{19}) = [\alpha]_{23},\ \varphi([0]_4, [1]_{19}) = [\beta]_{23},$$

si ha che, per ogni $a, b \in \mathbb{Z}$,

$$\begin{aligned} \varphi([a]_4, [b]_{19}) &= \varphi((a[1]_4, [0]_{19}) + ([0]_4, b[1]_{19})) \\ &= \varphi((a[1]_4, a[0]_{19})) + \varphi((b[0]_4, b[1]_{19})) \\ &= a\varphi(([1]_4, [0]_{19})) + b\varphi((b[0]_4, [1]_{19})) = [a\alpha + b\beta]_{23} \end{aligned} \tag{3}$$

Dunque φ è completamente determinato da α e da β. Ora, sapendo che φ è, in particolare, un'applicazione ben definita, si ha

$$[\alpha]_{23} = \varphi([1]_4, [0]_{19}) = \varphi([5]_4, [0]_{19}) = [5\alpha]_{23}$$

$$[\beta]_{23} = \varphi([0]_4, [1]_{19}) = \varphi([0]_4, [20]_{19}) = [20\beta]_{23}$$

da cui segue che $23|4\alpha$ e $23|19\beta$. Per la Proposizione 6.24, si ha allora che $23|\alpha$ e $23|\beta$. Ma allora $[\alpha]_{23} = [\beta]_{23} = [0]_{23}$. Questo implica, per quanto osservato precedentemente, che $\varphi \equiv 0$.

Curiosità 2. Un risultato che verrà presentato nel corso di Algebra n.2 che va sotto il nome di Primo Teorema di Isomorfismo, permetterà di stabilire che

$$|\mathbb{Z}_4 \times \mathbb{Z}_{19}| = |\mathrm{Ker}(\varphi)| \cdot |\mathrm{im}(\varphi)|$$

(in analogia, sostituendo le somme con i prodotti e le dimensioni con le cardinalità, al Teorema della Dimensione per una applicazione lineare visto nel corso di Geometria n.1).

Dato che $\mathrm{im}(\varphi)$ è, per la Proposizione 17.35, un sottogruppo ciclico di $\mathbb{Z}_{23}$, per il Teorema di Lagrange (17.19) il suo ordine (ovvero il periodo di un suo generatore) deve dividere 23. Dunque $|\mathrm{im}(\varphi)|$ divide 23 e $4 \cdot 19$, e dunque è 1. Pertanto si ha necessariamente che $\mathrm{im}(\varphi) = \{0\}$.

□

Esercizio (Traccia N.83, 25 settembre 2017)**.**

Dato un intero positivo n, si considerino l'insieme di matrici $A_n = \{\begin{pmatrix} a & b^n \\ b & a^n \end{pmatrix} | a, b \in \mathbb{Z}\}$ *e l'applicazione*

$$\varphi : A_n \to \mathbb{Z}_{101}$$
$$X \mapsto [\det(X)]_{101}.$$

(a) Dire se φ_{1312} *è surgettiva.*

(b) Determinare $\varphi^{-1}_{10099}(\{[0]_{101}\})$.

Svolgimento.

(a) Esplicitamente, per ogni $A = \begin{pmatrix} a & b^n \\ b & a^n \end{pmatrix} \in A_{1312}$, si ha

$$\varphi_{1312}(A) = [a^{1313}]_{101} - [b^{1313}]_{101}.$$

Allora, osservando che $1313 = 101 \cdot 13$, si ha, per il Piccolo Teorema di Fermat (17.23),

$$\varphi_{1312}(A) = [a^{13}]_{101} - [b^{13}]_{101}.$$

Per provare l'eventuale surgettività della nostra applicazione, abbiamo bisogno di trovare almeno una controimmagine per ogni elemento di $\mathbb{Z}_{101}$. Ovviamente $[0]_{101}$ ha una controimmagine (basta prendere $a = b = 1$, per esempio).

Per quanto riguarda gli elementi di $\mathbb{Z}^*_{101}$, ricordiamo che questo è un gruppo ciclico di ordine 100 (Corollario 17.42). Sia α un suo generatore. Allora α^{13} è ancora un generatore. Infatti, essendo $MCD(13, 100) = 1$, la formula del periodo (Lemma 17.36) ci dice che anche α^{13} ha periodo 100.

Sia $x \in \mathbb{Z}^*_{101}$. Allora esiste $k \in \mathbb{N}$ tale che $x = (\alpha^{13})^k = (\alpha^k)^{13}$.

Dunque, ogni elemento $x \in \mathbb{Z}^*_{101}$ è esprimibile come potenza 13-esima di un opportuno elemento di $\mathbb{Z}^*_{101}$. Sia $a \in \mathbb{Z}$ tale che $[a]^{13}_{101} = x$. Allora

$$\varphi_{1312}\left(\begin{pmatrix} a & 0 \\ 0 & a^n \end{pmatrix}\right) = [a]^{13}_{101} = x.$$

Ciò prova che φ_{1312} è surgettiva.

(b) Cominciamo con l'osservare che $10099 + 1 = 10100 = 101 \cdot 100$. Come nel punto (a), grazie al Piccolo Teorema di Fermat, si ha

$$\varphi_{10099}(A) = [a^{100}]_{101} - [b^{100}]_{101}.$$

Ora, è evidente che, se né a né b sono congrui a 0 modulo 101,

$$[a^{100}]_{101} = [b^{100}]_{101} = [1]_{101}$$

(per il Teorema di Eulero), e dunque si ha $\varphi_{10099}(A) = [0]_{101}$, così come, ovviamente, quando entrambi sono congrui a 0 modulo 101.

Se, invece, solo uno dei due è congruo a 0 modulo 101, si ha che $\varphi_{10099}(A) \in \{[1]_{101}, [-1]_{101}\}$. Dunque $\varphi^{-1}_{10099}([0]_{101})$ è l'insieme

$$\{A \in A_{10099} | (a \equiv b \equiv 0 \bmod 101) \vee (a \not\equiv 0 \bmod 101 \wedge b \not\equiv 0 \bmod 101)\}$$

□

Esercizio (Traccia N.84, 6 novembre 2017)**.**
Dati interi positivi n e m si consideri l'applicazione

$$\varphi_{n,m} : \mathbb{Z}_8 \times \mathbb{Z}_{14} \to \mathbb{Z}_8 \times \mathbb{Z}_{14}$$

$$(\alpha, \beta) \mapsto (n\alpha, n\beta).$$

(a) Determinare tutti i valori di n, m per i quali $\varphi_{n,m}$ è surgettiva.

(b) Determinare tutti i valori di n, m per i quali $\varphi_{n,m}$ è un omomorfismo di anelli.

(c) Determinare la cardinalità di $\varphi^{-1}_{10,21}(([2]_8, [7]_{14}))$.

Svolgimento.

(a) Osserviamo che la componente in $\mathbb{Z}_8$ (rispettivamente, in $\mathbb{Z}_{14}$) di $\varphi_{n,m}$ dipende solo dalla componente in $\mathbb{Z}_8$ (rispettivamente, in $\mathbb{Z}_{14}$) dell'insieme di partenza. Dunque, possiamo concentrarci singolarmente su ogni componente: determiniamo, cioè, tutti gli n per cui l'applicazione

$$\varphi_n : \alpha \in \mathbb{Z}_8 \mapsto n\alpha \in \mathbb{Z}_8$$

è surgettiva, e tutti gli m per cui

$$\varphi_m : \beta \in \mathbb{Z}_{14} \mapsto m\beta \in \mathbb{Z}_{14}$$

è surgettiva.

Supponiamo che φ_n sia surgettiva. Allora

$$\mathbb{Z}_8 = \{n\alpha | \alpha \in \mathbb{Z}_8\} = \{[n]_8\alpha | \alpha \in \mathbb{Z}_8\}.$$

Ma allora, esiste $\alpha \in \mathbb{Z}_8$ tale che $[n]_8\alpha = [1]_8$. Dunque $[n]_8$ è invertibile in $\mathbb{Z}_8$.

Viceversa, se $[n]_8$ è invertibile in $\mathbb{Z}_8$, per ogni $\beta \in \mathbb{Z}_8$ possiamo scrivere

$$\beta = [n]_8([n]_8^{-1}\beta) = n([n]_8^{-1}\beta).$$

Dunque φ_n è surgettiva.

Analogamente, si prova che φ_m è surgettiva se e solo se $[m]_{14}$ è invertibile in $\mathbb{Z}_{14}$.

Alla luce della Proposizione 8.7 questo accade se e solo se n è coprimo con 8 e m è coprimo con 14. Dunque, le coppie n, m che cerchiamo sono quelle nell'insieme

$$\{(n, m) | n, m \text{ dispari e } 7 \nmid m\}.$$

(b) Non c'è alcun dubbio che $\varphi_{n,m}$ è un omomorfismo di gruppi additivi, per ogni n, m.

Per quanto già osservato nel punto (b), possiamo ragionare singolarmente sulle applicazioni parziali φ_n e φ_m precedentemente introdotte, dal momento che nel prodotto diretto di anelli il prodotto è computato componente per componente.

La condizione che φ_n sia un omomorfismo di anelli equivale a chiedere che per ogni $\alpha, \alpha' \in \mathbb{Z}_8$ si abbia

$$n\alpha\alpha' = n^2\alpha\alpha'. \tag{4}$$

Visto che ciò deve accadere per qualunque scelta di α, α', prendiamo, in particolare, $\alpha = \alpha' = [1]_8$. Dunque si ha

$$[n^2]_8 = [n]_8.$$

Questo implica che

$$8 | n(n-1).$$

Visto che solo uno tra n e $n-1$ è pari, e $8 = 2^3$, allora $8|n$ oppure $8|n-1$. Questa è dunque una condizione necessaria che deve soddisfare n. Controlliamo che sia anche sufficiente.

Supponiamo che $8|n$ oppure $8|n-1$. Allora la condizione (1) è certamente soddisfatta, visto che $8|n^2aa' - naa' = n(n-1)aa'$ (essendo $a, a' \in \mathbb{Z}$ due rappresentanti per α, α' rispettivamente).

Analogamente, si prova che, affinché φ_m sia un omomorfismo di anelli si deve avere $14|m(m-1)$. Visto che sicuramente $2|m(m-1)$ (esattamente uno tra m e $m-1$ è pari), la condizione è equivalente a chiedere che $7|m$ o $7|m-1$.

In conclusione, gli interi che cerchiamo sono quelli dell'insieme

$$\{(n,m)|(8|n \vee 8|n-1) \wedge (7|m \vee 7|m-1)\}.$$

(c) Dobbiamo determinare tutti gli $(\alpha, \beta) \in \mathbb{Z}_8 \times \mathbb{Z}_{14}$ tali che

$$(10\alpha, 21\beta) = (([2]_8, [7]_{14})).$$

Come nei punti (a) e (b), possiamo ragionare singolarmente su ciascuna componente.

Determinare gli $\alpha \in \mathbb{Z}_8$ tali che $10\alpha = [2]_8$ equivale a determinare, se esistono, le soluzioni della congruenza lineare

$$10x \equiv 2 \mod 8.$$

Tale congruenza è sicuramente risolubile dato che $MCD(8,10) = 2|2$ (Proposizione 9.2). Alla luce dell'Osservazione 9.4, la congruenza data equivale alla congruenza

$$5x \equiv 1 \mod 4,$$

una cui soluzione particolare è $x_0 = 1$. La soluzione generale è quindi nella forma $x = 1 + 4k$, al variare di $k \in \mathbb{Z}$. Gli interi di questa forma rappresentano esattamente due classi distinte in $\mathbb{Z}_8$, ovvero $[1]_8$ e $[5]_8$.

Per quanto riguarda la seconda componente, procedendo analogamente, concludiamo che dobbiamo risolvere la congruenza lineare

$$y \equiv 1 \mod 2,$$

la cui soluzione generale è $y = 1 + 2h$, al variare di $h \in \mathbb{Z}$. Tali interi individuano esattamente sette classi distinte in $\mathbb{Z}_{14}$ (le classi dei numeri dispari), cioè $[1]_{14}, [3]_{14}, [5]_{14}, [7]_{14}, [9]_{14}, [11]_{14}$ e $[13]_{14}$.

Dunque, la cardinalità della controimmagine cercata è $2 \cdot 7 = 14$.

□

Esercizio (Traccia N.85, 9 gennaio 2018)**.**
Dati interi positivi n ed m, si consideri l'applicazione

$$\varphi_{n,m} : \mathbb{Z}_n \times \mathbb{Z}_m \to \mathbb{Z}_{n^2} \times \mathbb{Z}_{m^2}$$

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

$$\varphi_{n,m}([a]_n, [b]_m) = ([2na]_{n^2}, [3mb]_{m^2}).$$

(a) Determinare tutti i valori di n e m per i quali $\varphi_{n,m}$ è iniettiva.

(b) Determinare tutti i valori di n e m per i quali $\varphi_{n,m}$ è un omomorfismo di anelli.

Svolgimento.

(a) Cominciamo con l'osservare che $\varphi_{n,m}$ è sempre ben definita. Infatti se $a \equiv a' \pmod{n}$, si ha che $n|a - a'$ e quindi $n^2|2n(a - a') = 2na - 2na'$, cioè $2na \equiv 2na' \pmod{n^2}$. Similmente si procede se $b \equiv b' \pmod{m}$.

Visto che la componente in $\mathbb{Z}_{n^2}$ dipende solo dalla componente in $\mathbb{Z}_n$ e la componente in $\mathbb{Z}_{m^2}$ dipende solo dalla componente in $\mathbb{Z}_m$, possiamo ragionare separatamente sulle componenti (ricordando che in un prodotto diretto due elementi sono uguali se e solo se sono uguali componente per componente).

Proviamo a dimostrare direttamente l'iniettività, cercando di determinare una condizione sufficiente su n.

Vogliamo provare che se $2na \equiv 2na' \pmod{n^2}$, allora $a \equiv a' \pmod{n}$. Avendosi $n^2|2n(a - a')$, si deve avere $n|2(a - a')$.

Ora, sicuramente, se $2 \nmid n$, per la Proposizione 6.24, $n|a - a'$. Dunque, se n è dispari, abbiamo l'ingettività sulla prima componente.

Proviamo che la condizione è necessaria. Infatti, se $2|n$, allora possiamo scrivere $n = 2k$ per qualche k intero positivo. Supponiamo per assurdo l'ingettività nella prima componente.

Prendiamo $a = 1, a' = k+1$. Allora chiaramente $2na \equiv 2na' \pmod{n^2}$. Infatti,

$$n^2 = 4k^2 | 4k(a' - a) = 2n(a' - a).$$

Ma allora dovremmo avere $k + 1 \equiv 1 \pmod{n}$, ovvero $k \equiv 0 \pmod{n}$. Ma questo è impossibile visto che $0 < k < n$.

Dunque se $2|n$, la funzione non può essere ingettiva.

Similmente, sostituendo n con m e 2 con 3, si prova che l'ingettività nella seconda componente è equivalente alla condizione che $3 \nmid m$.

Dunque l'insieme delle coppie (n, m) per cui $\varphi_{n,m}$ è ingettiva si ottiene intersecando le due condizioni trovate, ovvero considerando l'insieme

$$\{(n, m) | 2 \nmid n, 3 \nmid m\}.$$

(b) Per determinare quali siano i valori di n, m cercati, proviamo a determinare una condizione necessaria su n, m, che a posteriori proveremo essere anche sufficiente.

Assumiamo quindi che $\varphi_{n,m}$ sia un omomorfismo di anelli, e cerchiamo di capire, attraverso il controllo di alcuni casi particolari, quali condizioni debba soddisfare la coppia (n, m).

Come nel punto (a), possiamo ragionare separatamente sulle componenti, visto che somma e prodotto in un prodotto diretto di anelli avvengono componente per componente.

È evidente che la funzione è sempre un omomorfismo di gruppi abeliani, dunque i problemi possono sorgere solo nella proprietà di conservazione del prodotto.

Dobbiamo avere, per ogni a, a',

$$[2naa']_{n^2} = [2na]_{n^2}[2na']_{n^2} = [4n^2aa']_{n^2} = [0]_{n^2}.$$

In particolare, se prendiamo $a = a' = 1$, si deve avere

$$[2n]_{n^2} = [2n^2]_{n^2} = [0]_{n^2},$$

ovvero $n^2|2n$, e quindi $n|2$. Dunque $n = 1$ oppure 2.

Procedendo analogamente, si prova che si deve avere $m = 1$ o $m = 3$.

Proviamo ora che la condizione è sufficiente.

Quando $n = 2$ e $m = 3$, si ha banalmente che $\varphi_{2,3} = 0$ è l'omomorfismo nullo.

Se $n = n^2 = 1$ o $m = m^2 = 1$, abbiamo un caso estremo, essendo $\mathbb{Z}_1 = \{0\}$ l'anello banale. Ovviamente l'unica applicazione

$$\psi : \{0\} \to \{0\}$$

è un omomorfismo di anelli, che è ancora una volta l'omomorfismo nullo.

In ogni caso, si ha che $\varphi_{n,m}$ è l'omomorfismo nullo, dunque in particolare un omomorfismo di anelli. Dunque si deve avere

$$(n, m) \in \{1, 2\} \times \{1, 3\}.$$

□

Esercizio (Traccia N.86, 24 gennaio 2018)**.**
Siano dati interi positivi n e m

(a) Provare che nm e $n+m$ sono coprimi se e solo se n e m sono coprimi.

(b) Provare che nm divide $n^2 + m^2$ se e solo se $n = m$.

(c) Determinare tutti i valori di n e m per i quali $2^{m^n} \equiv 1$ (mod 5).

Svolgimento.

(a) Supponiamo che n, m non siano coprimi. Allora esiste un primo p che divide sia n che m, e che dunque divide $n+m$ e nm (Proposizione 6.9), che pertanto non sono coprimi. Ciò prova il "solo se".

Viceversa, supponiamo che nm e $n+m$ non siano coprimi. Allora esiste un primo p che divide sia nm sia $n+m$. Ora, visto che $p|nm$, per definizione p dovrà dividere uno dei fattori, diciamo n (senza perdita di generalità). Ma allora $p|n+m-n=m$ (Proposizione 6.9). Dunque n, m non sono coprimi.

(b) Risulta immediato verificare il "se". Proviamo che la condizione è necessaria.

Supponiamo che $nm|n^2+m^2$ e che, per assurdo, $n \neq m$. Allora esiste un primo p ed esistono numeri naturali a e b distinti tali che p compaia nella fattorizzazione di n con molteplicità a e nella fattorizzazione di m con molteplicità b. Senza ledere la generalità, possiamo supporre che sia $a < b$. Poiché p^{a+b} divide nm, per ipotesi e transitività, si deduce che p^{a+b} divide anche n^2+m^2. D'altra parte, p^{2b} divide m^2, e, pertanto, essendo $a+b<2b$, p^{a+b} divide m^2. Dunque, in base alla Proposizione 6.9, p^{a+b} dovrebbe dividere $n^2=(n^2+m^2)-m^2$. Tuttavia, ciò è impossibile, dato che la massima potenza che divide n^2 è p^{2a}, e $2a < a+b$.

Dunque $n = m$.

(c) Visto che i numeri interi assegnati sono non nulli (modulo 5), possiamo ridurci a studiare il problema nel gruppo ciclico $\mathbb{Z}_5^*$. In base alla Proposizione 17.16, $2^{m^n} \equiv 1 \pmod 5$ se e solo se $m^n \equiv 0 \pmod{o(2)=4}$.

Sicuramente m deve essere pari. Se m non è multiplo di 4, bisogna avere necessariamente $n > 1$, altrimenti n può essere arbitrario. Dunque le

coppie (m, n) sono tutte e sole quelle dell'insieme

$$\{(m,n)|m \text{ pari}, n > 1\} \cup \{(m,1)|m \text{ multiplo di } 4\}$$

□

Esercizio (Traccia N.87, 8 febbraio 2018)**.**

(a) Provare che $n = 2$ è l'unico intero maggiore di 1 per il quale $\varphi(n)$ è dispari.

(b) Determinare tutti gli interi $n > 1$ tali che $3^{\varphi(n^2-n)} \equiv 1$ (mod 5).

Svolgimento.

(a) Si ha, ovviamente, che $\varphi(2) = 1$ è dispari.

Viceversa, sia $n > 2$ e proviamo che $\varphi(n)$ è pari. Consideriamo $n = p_1^{k_1} \dots p_s^{k_s}$ la fattorizzazione unica di n (Teorema 7.6). In base alla Proprietà 7.2 si ha

$$\varphi(n) = \prod_{i=1}^{s} p_i^{k_i-1}(p_i - 1).$$

Essendo $n > 2$, se n non è una potenza di 2, almeno un primo p_i è maggiore di 2, cioè è dispari. Dunque almeno un fattore $p_i - 1$ è pari, e quindi l'intero prodotto è pari.

Se, invece, $n = 2^k$ (con $k > 1$), si avrà, sempre per la Proprietà 7.2,

$$\varphi(n) = 2^{k-1}.$$

Dunque $\varphi(n)$ è pari anche in questo caso.

(b) Si osservi che $\varphi(n^2 - n) = \varphi(n(n-1)) = \varphi(n)\varphi(n-1)$, in base alla Proprietà 7.1, visto che n e $n - 1$ sono coprimi in quanto numeri successivi.

Ora, visto che il problema riguarda solo elementi invertibili di $\mathbb{Z}_5$, possiamo ridurci a studiarlo nel suo gruppo moltiplicativo. In altri termini,

si tratta di determinare tutti gli $n > 1$ per cui $o([3]_5)|\varphi(n)\varphi(n-1)$ (grazie alla Proposizione 17.16). Si vede subito che $o([3]_5) = 4$ in $\mathbb{Z}_5^*$, per cui si deve avere che $4|\varphi(n)\varphi(n-1)$.

Ora, in base al punto (a), se $n-1 > 2$, allora $\varphi(n-1)$, così come $\varphi(n)$, sarà pari, e pertanto il prodotto sarà divisibile per 4. Se invece $n = 2$, si ha che $\varphi(2)\varphi(1) = 1$. Infine, se $n = 3$, si ha $\varphi(3)\varphi(2) = 2$. Dunque si deve avere $n > 3$.

□

Esercizio (Traccia N.88, 20 aprile 2018)**.**
Siano n e m numeri interi coprimi.

(a) Provare che se 6 divide n, allora 72 divide $n(m^2-1)$.

(b) Provare che se 72 divide nm, allora 6 divide $(n^2-1)(m^2-1)$.

Svolgimento.

(a) Per ipotesi, sappiamo che $MCD(n, m) = 1$. Dato che $6|n$, si ha che m non è né pari né divisibile per 3.

In particolare, $m \equiv 1 \pmod 3$ oppure $m \equiv 2 \pmod 3$: in ogni caso $m^2 \equiv 1 \pmod 3$.

Dunque $3|m^2 - 1$.

Inoltre, dato che $2 \nmid m$, si ha che $m \equiv 1 \pmod 4$ oppure $m \equiv 3 \pmod 4$. In ogni caso, $m^2 \equiv 1 \pmod 4$.

Pertanto $4|m^2 - 1$. Dato che 3 e 4 sono coprimi, si ha che $12|m^2 - 1$.

Ma allora $6 \cdot 12 = 72|n(m^2 - 1)$.

(b) Osserviamo che $72 = 2^3 \cdot 3^2$.

Si ha che $2|n$ o $2|m$. Senza ledere la generalità, supponiamo che $2|n$. Ma, essendo n e m coprimi, si ha che $2 \nmid m$, ossia, come nel punto (a), $m^2 \equiv 1 \pmod 2$.

Ci sono allora due casi: $3|m$ ovvero $3 \nmid m$.

Nel primo caso, $3 \nmid n$, ossia, come nel punto (a), $n^2 \equiv 1 \pmod 3$. Dunque $2|m^2-1$ e $3|n^2-1$, cioè 6 divide il prodotto.

Nel secondo caso, ancora come nel punto (a), si deve avere $m^2 \equiv 1 \pmod 3$. Dunque $6|m^2-1$, e quindi, a maggior ragione, $6|(n^2-1)(m^2-1)$.

□

Esercizio (Traccia N.89, 5 giugno 2018)**.**
Dato un intero n, sia $N = n^4 - 5n^3 - 15n^2 + 5n + 14$.

(a) Determinare tutti i valori di n per i quali 18 divide N.

(b) Al variare di $n \geq 7$, determinare la cifra delle unità della rappresentazione decimale di N.

Svolgimento.

(a) Si tratta di determinare tutti i valori di n per i quali

$$N \equiv 0 \mod 18.$$

In base all'Esercizio 7.12, questo è equivalente a determinare tutti i valori di n per i quali

$$\begin{cases} N \equiv 0 \mod 2 \\ N \equiv 0 \mod 9 \end{cases}.$$

Osserviamo che, se n è pari, lo è ogni sua potenza. Dunque N è somma di numeri pari, ed è dunque pari. Se, invece, n è dispari, lo è anche ogni sua potenza. Visto che nessuno dei coefficienti delle potenze di n che compaiono nell'espressione di N è pari, N è dato dalla somma di quattro numeri dispari (che è pari) e di un numero pari. Dunque, in ogni caso, N è pari: la prima congruenza è sempre soddisfatta.

Dunque, solo la seconda congruenza è interessante per i nostri scopi.

Condizione necessaria affinché $9|N$ è che $3|N$. Dunque, cominciamo col risolvere la congruenza

$$N \equiv n^4 + n^3 + 2n - 1 \equiv n^2 + n + 2n + 1 \equiv n^2 - 1 \mod 3$$

(abbiamo usato il Piccolo Teorema di Fermat (17.23) per $p = 3$.)

È chiaro che $n \equiv \pm 1 \pmod 3$ è la soluzione di questa congruenza. Dunque, le possibili soluzioni della congruenza modulo 9 sono

$$n \equiv 1, 2, 4, 5, 7, 8 \mod 9.$$

A questo punto, possiamo testarle tutte e stabilire quali sono effettivamente soluzioni e quali no, ottenendo

$$n \equiv 1, 4, 7, 8 \mod 9.$$

Una possibilità meno faticosa è quella di tentare di scomporre l'espressione polinomiale in n che definisce N. Si ha:

$$\begin{aligned} N &= n^4 - n^2 - 5n^3 + 5n - 14n^2 + 14 = (n^2 - 1)(n^2 - 5n - 14) \\ &= (n - 1)(n + 1)(n + 2)(n - 7) \end{aligned}$$

Dunque,

$$N \equiv (n - 1)(n - 8)(n - 7)^2 \mod 9.$$

Da questa espressione, si vede immediatamente che $n \equiv 1, 7, 8 \pmod 9$ sono soluzioni. Per quanto riguarda le altre possibilità ($n \equiv 2, 4, 5 \pmod 9$), si ha, sostituendo (la sostituzione ora è molto più facile), che solo $n \equiv 4 \pmod 9$ è soluzione.

Dunque $18|N$ se e solo se $n \equiv 1, 4, 7, 8 \pmod 9$.

Attenzione! Si potrebbe essere tentati dal fermarsi alle soluzioni che appaiono evidenti dalla scomposizione dell'espressione di N in $\mathbb{Z}_9$. Si badi bene, però, che $\mathbb{Z}_9$ non è un anello integro, e quindi non vale la

legge di annullamento del prodotto! Pertanto, sebbene altre possibili soluzioni non annullino i singoli fattori, esse potrebbero comunque dar luogo a dei divisori dello zero, come in effetti accade.

(b) Sia $n \geq 7$. Dobbiamo determinare $x \in \{0, \dots 9\}$ tale che

$$x \equiv N \mod 10.$$

Come nel punto (a), una volta osservato che N è sempre pari (ossia $x \in \{0, 2, 4, 6, 8\}$), dobbiamo studiare il problema

$$x \equiv N \mod 5.$$

Si ha,

$$N \equiv n^4 - 1 \equiv (n-1)(n-2)(n-3)(n-4) \mod 5.$$

Dunque, se $n \equiv 0 \pmod 5$, $x = 4$, altrimenti $x = 0$.

□

Esercizio (Traccia N.90, 20 giugno 2018)**.**

(a) Provare che non esiste alcun monomorfismo di gruppi $\mathbb{Z}_9 \to \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

(b) Provare che non esiste alcun epimorfismo di gruppi $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \to \mathbb{Z}_9$.

(c) Provare che l'anello $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ *non ha, tra i suoi sottoanelli unitari, alcun campo di ordine* 9.

Svolgimento.

(a) Si cominci con l'osservare che ogni elemento di $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ ha periodo 1 oppure 3. Infatti, se $([a]_3, [b]_3, [c]_3) \in \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$, allora

$$3 \cdot ([a]_3, [b]_3, [c]_3) = ([3a]_3, [3b]_3, [3c]_3) = ([0]_3, [0]_3, [0]_3).$$

Pertanto il periodo di questo elemento è, per la Proposizione 17.16, 1 oppure 3.

Ma allora, se $\varphi : \mathbb{Z}_9 \to \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ è un monomorfismo di gruppi, si deve avere

$$\varphi([3]_9) = 3 \cdot \varphi([1]_9) = ([0]_3, [0]_3, [0]_3) = \varphi([0]_9).$$

Per l'ingettività, segue che $[3]_9 = [0]_9$, che è assurdo.

(b) Supponiamo ora che esista $\varphi : \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \to \mathbb{Z}_9$ un epimorfismo di gruppi.

Ma allora, esiste $([a]_3, [b]_3, [c]_3) \in \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ tale che

$$[1]_9 = \varphi(([a]_3, [b]_3, [c]_3)).$$

Dunque,

$$\begin{aligned}[3]_9 &= 3 \cdot \varphi(([a]_3, [b]_3, [c]_3)) = \varphi(3 \cdot ([a]_3, [b]_3, [c]_3)) \\ &= \varphi(([0]_3, [0]_3, [0]_3)) = [0]_9,\end{aligned}$$

ma questo è assurdo.

(c) Supponiamo per assurdo che tale campo $\mathbb{F}$ di ordine 9 esista. Allora $\mathbb{F}^*$ ha ordine 8 ed è formato da elementi invertibili di $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$. Dunque,

$$\mathbb{F}^* \subseteq \mathcal{U}(\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3) = \mathcal{U}(\mathbb{Z}_3) \times \mathcal{U}(\mathbb{Z}_3) \times \mathcal{U}(\mathbb{Z}_3),$$

dove l'ultima uguaglianza segue dalla Proposizione 16.6, con un facile ragionamento induttivo. Dato che $\mathcal{U}(\mathbb{Z}_3)$ ha cardinalità 2, segue che anche $\mathfrak{U}(\mathbb{Z}_3) \times \mathfrak{U}(\mathbb{Z}_3) \times \mathfrak{U}(\mathbb{Z}_3)$ ha ordine 8, e quindi coincide con $\mathbb{F}^*$.

Ma allora,

$$\mathbb{F} = (\mathfrak{U}(\mathbb{Z}_3) \times \mathfrak{U}(\mathbb{Z}_3) \times \mathfrak{U}(\mathbb{Z}_3)) \cup \{([0]_3, [0]_3, [0]_3)\}.$$

Tuttavia, l'insieme a destra non è un campo, perché non è un sottoanello: infatti, non è chiuso rispetto alla somma.

Considerati, ad esempio, gli elementi $([2]_3, [1]_3, [1]_3)$ e $([1]_3, [1]_3, [1]_3)$ (che sono invertibili), si ha che

$$([2]_3, [1]_3, [1]_3) + ([1]_3, [1]_3, [1]_3) = ([0]_3, [2]_3, [2]_3).$$

Ma questo elemento non è invertibile in $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$, perché la prima componente non lo è in $\mathbb{Z}_3$.

□

Esercizio (Traccia N.91, 5 luglio 2018)**.**
Provare che l'anello prodotto diretto $\mathbb{Z}_6 \times \mathbb{Z}_9$ possiede, tra i suoi sottoinsiemi di cardinalità 3,

(a) un sottoanello che è un campo,

(b) un sottoanello che non è un campo,

(c) un sottogruppo che non è un sottoanello.

Svolgimento. Prima di mostrare un possibile svolgimento, occorrono delle importanti osservazioni e richiami preliminari.
Prima di tutto ricordiamo che un sottoanello di un anello unitario, in quanto sottogruppo del gruppo additivo dell'anello, deve obbligatoriamente contenere l'elemento zero dell'anello, ma non necessariamente l'elemento uno.
Una osservazione ancora più importante è che un sottoanello può essere dotato di elemento uno, ma non necessariamente esso deve coincidere con l'elemento uno dell'anello totale. Un esempio è il sottoinsieme $\{[0]_6, [3]_6\}$ di $\mathbb{Z}_6$: è immediato verificare che è un sottoanello (non unitario, in quanto non contiene $[1]_6$, unità dell'anello totale), e che l'elemento $[3]_6$ svolge il compito di elemento uno per tale sottoanello. Infatti,

$$[3]_6 \cdot [a]_6 = [a]_6 = [a]_6 \cdot [3]_6$$

per $a = 0, 3$.

Chiedere che un sottoanello sia unitario è molto più forte: significa chiedere che sia unitario come anello, e che la sua unità sia "ereditata" dall'anello ambiente.

Ovviamente, cambiando l'elemento uno, cambiano anche gli elemenenti invertibili: può accadere che elementi che non erano invertibili nell'anello totale lo siano nel sottoanello, rispetto alla sua unità: è il caso, appunto, dell'elemento $[3]_6$ nell'esempio sopra citato.

In generale, infine, per cercare i sottoanelli di $\mathbb{Z}_n$, dove n è un intero positivo, non dobbiamo fare altro che controllare, tra i suoi sottogruppi additivi, quali sono sottoanelli. In realtà, data la particolare struttura di questi anelli, si può vedere facilmente che un sottoinsieme di $\mathbb{Z}_n$ è un sottoanello se e solo se è un sottogruppo additivo. Questo è dovuto al fatto che moltiplicare in $\mathbb{Z}_n$ corrisponde a considerare un multiplo additivo, ossia, per ogni $a, b \in \mathbb{Z}$, risulta

$$a \cdot [b]_n = [a]_n \cdot [b]_n,$$

dove, si badi bene, le operazioni hanno significato differente (la prima è una moltiplicazione "esterna", che ricorda quella di uno scalare per un vettore, in uno spazio vettoriale, e la seconda è la moltiplicazione interna dell'anello), pur essendo uguale il risultato finale.

Tuttavia, i sottogruppi additivi di $\mathbb{Z}_n$ sono ben noti e facili da trovare: dato che $(\mathbb{Z}_n, +)$ è un gruppo ciclico, tali sono tutti i suoi sottogruppi (Proposizione 17.35). Inoltre, essi hanno tutti ordine divisore di n. Più in particolare, per ogni divisore di n esiste uno ed un solo sottogruppo ciclico avente ordine tale divisore (Proposizione 17.39).

Alla luce di quanto detto, i sottogruppi additivi (ossia i sottoanelli) di $\mathbb{Z}_6$ sono esattamente

$$\begin{aligned}
&< [0]_6 > = \{[0]_6\} && \text{(ordine 1)},\\
&< [3]_6 > = \{[0]_6, [3]_6\} && \text{(ordine 2)},\\
&< [2]_6 > = \{[0]_6, [2]_6, [4]_6\} && \text{(ordine 3)},\\
&< [1]_6 > = \mathbb{Z}_6 && \text{(ordine 6)}.
\end{aligned}$$

Invece, quelli di $\mathbb{Z}_9$ sono

$$\begin{aligned} &< [0]_9 > = \{[0]_9\} && \text{(ordine 1)},\\ &< [3]_9 > = \{[0]_9, [3]_9, [6]_9\} && \text{(ordine 3)},\\ &< [1]_9 > = \mathbb{Z}_9 && \text{(ordine 9)}. \end{aligned}$$

(a) Alla luce delle osservazioni fatte, per cercare un sottoanello di cardinalità 3 di $\mathbb{Z}_6 \times \mathbb{Z}_9$ che è un campo, dobbiamo trovare un sottoanello che è unitario come anello a sé stante, e, sempre in questa veste, è un campo. Infatti, se lo cercassimo tra i sottoanelli unitari, due elementi sarebbero necessariamente già "bloccati", ossia $([0]_6, [0]_9)$ e $([1]_6, [1]_9)$. Un terzo elemento, dal momento che l'unità è la stessa dell'anello totale, deve essere un elemento invertibile nell'anello dato. Tuttavia, con nessuno di essi otterremo un sottoanello, poiché nessuno verificherà la proprietà di essere un sottogruppo additivo.

Un altro esempio simile a quello citato precedentemente di sottoanello di $\mathbb{Z}_6$ non unitario, ma che è un anello unitario in senso assoluto, è il sottoanello

$$A =< [2]_6 >= \{[0]_6, [2]_6, [4]_6\}.$$

Esso è un anello unitario: $[4]_6$ è il suo elemento uno. Infatti,

$$[4]_6 \cdot [2]_6 = [8]_6 = [2]_6,$$

$$[4]_6 \cdot [4]_6 = [16]_6 = [4]_6.$$

Citando l'Osservazione 5.29, anche $\{[0]_9\}$ è un sottoanello di $\mathbb{Z}_9$ non unitario, ma unitario come anello a sé stante.

Dunque, $A \times \{[0]_9\} \subset \mathbb{Z}_6 \times \mathbb{Z}_9$ è un sottoanello in quanto prodotto di sottoanelli dei fattori diretti. Esso ha cardinalità 3. Infine, essendo prodotto di anelli unitari, esso è, per la Proposizione 16.6, un anello unitario, la cui unità è $([4]_6, [0]_9)$.

Esso è un campo, in quanto ogni elemento non nullo è invertibile. Ovviamente, l'unico elemento di cui dobbiamo verificare l'invertibilità è $([2]_6, [0]_9)$ (in quanto l'unico altro elemento non nullo è l'unità, certamente invertibile, con inverso se stesso). Se esso è invertibile, per l'unicità dell'inverso, questo deve coincidere con l'elemento stesso. Infatti,

$$([2]_6, [0]_9) \cdot ([2]_6, [0]_9) = ([4]_6, [0]_9).$$

(b) Proviamo, anche in questo caso, a costruire un sottoanello di $\mathbb{Z}_6 \times \mathbb{Z}_9$ prodotto diretto di due sottoanelli dei fattori. Guardando i sottoanelli che abbiamo precedentemente elencato, l'unico modo per ottenere un prodotto diretto di cardinalità 3 è prendere gli addendi diretti di cardinalità 3 e 1. Nel primo caso abbiamo considerato il prodotto di A (sottoanello di cardinalità 3 di $\mathbb{Z}_6$) e del sottogruppo banale di $\mathbb{Z}_9$. Stavolta consideriamo invece il prodotto diretto di $\{[0]_6\}$ e di $B =< [3]_9 >= \{[0]_9, [3]_9, [6]_9\}$.

Come prima, questo è un sottoanello di $\mathbb{Z}_6 \times \mathbb{Z}_9$. Inoltre, si osservi, per esempio, che

$$([0]_6, [3]_9) \cdot ([0]_6, [3]_9) = ([0]_6, [9]_9) = ([0]_6, [0]_9).$$

Dunque $\{[0]_9\} \times B$ è un sottoanello ma non è un campo, perché non è un dominio di integrità.

(c) Ovviamente in questo caso non possiamo andare a considerare un sottogruppo che è un prodotto diretto di due sottogruppi, sia perché, per quanto già osservato, esso sarebbe anche un sottoanello, sia perché abbiamo già considerato tutti i possibili prodotti diretti di cardinalità 3.

Possiamo partire considerando il sottoanello $A \times B$ (che ha ordine 9) e provare a estrarre da esso un sottogruppo di ordine 3. Basta trovare un elemento di ordine 3 (abbiamo speranza di trovarlo visto che $3|9$).

Per esempio, consideriamo l'elemento $([2]_6, [3]_9)$. Esso ha periodo 3, dunque genera un sottogruppo di ordine 3, precisamente

$$G = \{([0]_6, [0]_9), ([2]_6, [3]_9), ([4]_6, [6]_9)\}.$$

Esso, tuttavia, non è un sottoanello: infatti, non è chiuso rispetto al prodotto, visto che, per esempio,

$$([2]_6, [3]_9) \cdot ([2]_6, [3]_9) = ([4]_6, [0]_9) \notin G.$$

□

Esercizio (Traccia N.92, 10 settembre 2018)**.**
Siano n, m due interi positivi e sia data l'applicazione

$$\varphi : \mathbb{Z}_5 \times \mathbb{Z}_7 \to \mathbb{Z}_5 \times \mathbb{Z}_7$$

$$([a]_5, [b]_7) \mapsto (n[a]_5, m[b]_7).$$

(a) Determinare, al variare di m e n, la cardinalità dell'immagine di φ.

(b) Determinare tutti i valori m e n per i quali φ è un omomorfismo di anelli.

(c) Determinare tutti i valori m e n per i quali φ è un isomorfismo di anelli.

Svolgimento.

(a) Risulta immediato verificare che φ è sempre ben definita ed è un omomorfismo di gruppi additivi. Ora, osserviamo che φ è di fatto il "prodotto diretto" di due omomorfismi di gruppi indipendenti, ossia

$$\varphi_5 : [a]_5 \in \mathbb{Z}_5 \mapsto n[a]_5 \in \mathbb{Z}_5$$

e

$$\varphi_7 : [b]_7 \in \mathbb{Z}_7 \mapsto m[b]_7 \in \mathbb{Z}_7.$$

Infatti, la componente in $\mathbb{Z}_5$ degli elementi dell'immagine di φ è completamente determinata da n e dalla componente in $\mathbb{Z}_5$ dell'elemento di partenza. Analogamente, la componente in $\mathbb{Z}_7$ degli elementi dell'immagine di φ è completamente determinata da m e dalla componente in $\mathbb{Z}_7$ dell'elemento di partenza.

Per queste ragioni, si ha che $\mathrm{Im}(\varphi) = \mathrm{Im}(\varphi_5) \times \mathrm{Im}(\varphi_7)$. Pertanto, possiamo ragionare separatamente sulle due componenti.

Osserviamo che, se $[n]_5 \in \mathcal{U}(\mathbb{Z}_5)$, allora φ_5 è surgettiva. Infatti, se $[x]_5 \in \mathbb{Z}_5$, allora

$$\varphi_5([n]_5^{-1}[x]) = n[n]_5^{-1}[x]_5 = [n]_5[n]_5^{-1}[x]_5 = [x]_5.$$

Ciò accade, in base alla Proposizione 8.7, se e solo se 5 non divide n. In tal caso, $\mathrm{Im}(\varphi_5) = \mathbb{Z}_5$.

Invece, nel caso in cui 5 divida n, per ogni $a \in \mathbb{Z}$,

$$n[a]_5 = [na]_5 = [0]_5,$$

ossia $\mathrm{Im}(\varphi_5) = \{[0]_5\}$.

Ragionando analogamente per φ_7, si ottiene che $\mathrm{Im}(\varphi_7) = \mathbb{Z}_7$ se 7 non divide m e $\mathrm{Im}(\varphi_7) = \{[0]_7\}$ altrimenti.

Dunque, per $\mathrm{Im}(\varphi)$ abbiamo esattamente quattro casi:

- $\mathrm{Im}(\varphi) = \mathbb{Z}_5 \times \mathbb{Z}_7$ se 5 non divide n e 7 non divide m (cardinalità 35).
- $\mathrm{Im}(\varphi) = \{[0]_5\} \times \mathbb{Z}_7$ se 5 divide n e 7 non divide m (cardinalità 7).
- $\mathrm{Im}(\varphi) = \mathbb{Z}_5 \times \{[0]_7\}$ se 5 non divide n e 7 divide m (cardinalità 5).
- $\mathrm{Im}(\varphi) = \{[0]_5\} \times \{[0]_7\}$ se 5 divide n e 7 divide m (cardinalità 1).

(b) È stato già osservato che φ è sempre un omomorfismo di gruppi additivi. Al fine di determinare tutti e soli gli m, n per cui φ è un omomorfismo di anelli, supponiamo che questa condizione sia verificata, e cerchiamo di dedurre condizioni necessarie su m e n.

Come prima, è sufficiente ragionare ancora separatamente su φ_5 e φ_7 (si badi che questa "separazione" non è necessaria, come non lo era nel punto precedente, se non per una semplificazione notazionale).

Se φ_5 è un omomorfismo di anelli, allora, per ogni $a, b \in \mathbb{Z}$, risulta

$$[nab]_5 = [n^2ab]_5.$$

In particolare, ciò è vero per $a = b = 1$, ossia $[n]_5 = [n^2]_5$, ossia $5|n^2 - n = n(n-1)$. Dato che 5 è un numero primo, si ha che $5|n$ oppure $5|n-1$.

Viceversa, è immediato verificare che se $5|n$ oppure $5|n-1$ allora φ_5 è un omomorfismo di anelli.

Analogamente, φ_7 è un omomorfismo di anelli se e solo se $7|m$ oppure $7|m-1$.

Segue che φ è un omomorfismo di anelli se e solo se

$$(5|n \vee 5|n-1) \wedge (7|m \vee 7|m-1.)$$

(c) La condizione determinata al punto (b) deve essere necessariamente verificata affinché si abbia che φ sia un omomorfismo di anelli.

Inoltre, affinché sia un isomorfismo, φ deve essere un'applicazione bigettiva.

Dal momento che φ è un'applicazione tra due insiemi finiti aventi la stessa cardinalità, affinché essa sia bigettiva è sufficiente che sia ingettiva oppure surgettiva (stabilita una delle due, l'altra è automaticamente verificata).

Ma, nel punto (a), abbiamo stabilito che φ è surgettiva se e solo se 5 non divide n e 7 non divide m.

Alla luce di quanto detto, dobbiamo solo intersecare quest'ultima condizione con quella determinata al punto (b). Segue che φ è un isomorfismo di anelli se e solo se $5|n-1$ e $7|m-1$.

□

Esercizio (Traccia N.93, 25 settembre 2018)**.**
Siano n un intero positivo e sia data l'applicazione

$$\varphi : \mathbb{Z}_{20} \times \mathbb{Z}_{15} \to \mathbb{Z}_{20} \times \mathbb{Z}_{15}$$

$$([a]_5, [b]_7) \mapsto (n^2[a]_{20}, n[b]_{15}).$$

(a) Determinare tutti i valori di n per i quali φ è un omomorfismo di anelli.

(b) Determinare tutti i valori di n per i quali φ è un isomorfismo di anelli.

Svolgimento.

(a) È immediato verificare che φ è sempre ben definita ed è sempre un omomorfismo di gruppi additivi.

Pertanto è sufficiente controllare per quali valori di n φ conservi il prodotto di due elementi, o, equivalentemente, tali che, per ogni $a, b, c, d \in \mathbb{Z}$, valga la condizione

$$(n^2[ac]_{20}, n[bd]_{15}) = (n^4[ac]_{20}, n^2[bd]_{15}),$$

ossia

$$\begin{cases} 20|(n^4 - n^2)ac \\ 15|(n^2 - n)bd \end{cases}.$$

Dal momento che la condizione deve essere verificata per ogni scelta dei quattro interi a, b, c, d, lo deve essere, in particolare, per la scelta $a = b = c = d = 1$.

Dunque, si deve avere, in primo luogo, $20|n^4 - n^2 = n^2(n-1)(n+1)$, che è equivalente a chiedere che $4|n^2(n-1)(n+1)$ e $5|n^2(n-1)(n+1)$.

La prima condizione è verificata per ogni scelta di n. Infatti, se n è pari, allora $4|n^2$. Se, invece, n è dispari, $2|n-1$ e $2|n+1$, ossia $4|(n-1)(n+1)$.

Per quanto riguarda la seconda condizione, si deve avere

$$5|n-1 \vee 5|n \vee 5|n+1.$$

In secondo luogo, è necessario che $15|n^2-n = n(n-1)$, che è equivalente a chiedere che 3 e 5 dividano $n(n-1)$, che si traduce nella condizione

$$(3|n \vee 3|n-1) \wedge (5|n \vee 5|n-1).$$

Dunque, affinché la prima e la seconda condizione siano verificate contemporaneamente, si deve avere necessariamente

$$(3|n \vee 3|n-1) \wedge (5|n \vee 5|n-1).$$

Viceversa, assumendo questa condizione, si vede immediatamente che φ è un omomorfismo di anelli.

(b) Dobbiamo innanzitutto richiedere che φ sia un omomorfismo di anelli, ossia assumere la condizione trovata al punto precedente.

Ora, dobbiamo determinare tutti e soli gli n per cui φ risulti una funzione bigettiva. Essendo una funzione tra due insiemi finiti della stessa cardinalità, è sufficiente verificare solamente una tra l'ingettività e la surgettività, e l'altra condizione sarà automaticamente verificata.

Mostriamo una possibile strada da seguire qualora si decidesse di ragionare sull'ingettività o meno di φ.

Sapendo che φ è un omomorfismo di anelli, φ è ingettivo se e solo se ha nucleo banale, ossia se e solo se, dati due interi $a, b \in \mathbb{Z}$,

$$\varphi([a]_{20}, [b]_{15}) = ([0]_{20}, [0]_{15}) \iff ([a]_{20}, [b]_{15}) = ([0]_{20}, [0]_{15}).$$

La condizione sopra si esprime, equivalentemente, nella forma seguente:

$$20|n^2a \wedge 15|nb \iff 20|a \wedge 15|b.$$

Chiaramente, l'implicazione da destra verso sinistra è sempre verificata, quindi si tratta di determinare una condizione necessaria e sufficiente su n affinché valga l'implicazione da sinistra verso destra.

Osserviamo che, in base alla Proposizione 6.24, una condizione sicuramente sufficiente è che $\mathrm{MCD}(20, n^2) = 1$ e $\mathrm{MCD}(15, n) = 1$. Proviamo che tale condizione è anche necessaria. Supponiamo che essa non sia vera e osserviamo che l'implicazione da sinistra verso destra non vale.

Assumiamo che $\mathrm{MCD}(20, n^2) = d_1 > 1$ oppure $\mathrm{MCD}(15, n) = d_2 > 1$.

Nel primo caso, posto $a = \frac{20}{d_1}$, si avrebbe che $20|n^2a$, essendo $n^2a = n^2\frac{20}{d_1} = \frac{n^2}{d_1}20$, ma $20 \nmid a$, visto che $1 \leq a \leq 10$ (infatti, d_1 è almeno 2).

Nel secondo caso, invece, si procede in maniera analoga ponendo $b = \frac{15}{d_2}$ e mostrando che, anche in questo frangente, non vale l'implicazione da sinistra verso destra.

Segue che 20 e n^2 devono essere coprimi e 15 ed n devono essere coprimi. Dalla seconda condizione si ha che $3 \nmid n$ e $5 \nmid n$. Dalla prima, invece, si deduce anche che $4 \nmid n^2$, ossia n è dispari.

In definitiva, intersecando questa condizione con quella del punto precedente, si ottiene che φ è ingettiva (quindi bigettiva) se e solo se

$$2 \nmid n \wedge 3|n-1 \wedge 5|n-1.$$

Mostriamo ora una strada percorribile se decidessimo di ragionare sulla surgettività o meno di φ.

Assumiamo innanzitutto che φ sia un epimorfismo: allora esistono $a, b \in \mathbb{Z}$ tali che

$$(n^2[a]_{20}, n[b]_{15}) = ([1]_{20}, [1]_{15}).$$

Dall'uguaglianza tra le prime componenti segue che

$$n^2 a \equiv 1 \mod 20,$$

mentre, dall'uguaglianza tra le seconde componenti, segue che

$$nb \equiv 1 \mod 15.$$

La prima condizione ci dice che $[n^2]_{20}$ è invertibile, mentre la seconda ci dice che $[n]_{15}$ è invertibile. Ciò avviene, in base alla Proposizione 8.7, se e solo se $\text{MCD}(20, n^2) = 1$ e $\text{MCD}(15, n) = 1$.

Viceversa, assumendo che $\text{MCD}(20, n^2) = 1$ e $\text{MCD}(15, n) = 1$, si ha che $[n^2]_{20}$ e $[n]_{15}$ sono invertibili nei rispettivi anelli.

Sia ora $([x]_{20}, [y]_{15}) \in \mathbb{Z}_{20} \times \mathbb{Z}_{15}$. Allora

$$\begin{aligned}\varphi(([n^2]_{20}^{-1}[x]_{20}, [n]_{15}^{-1}[y]_{15})) &= (n^2[n^2]_{20}^{-1}[x]_{20}, n[n]_{15}^{-1}[y]_{15}) \\ &= ([n^2]_{20}[n^2]_{20}^{-1}[x]_{20}, [n]_{15}[n]_{15}^{-1}[y]_{15}) = ([x]_{20}, [y]_{15}).\end{aligned}$$

Dunque φ è un epimorfismo.

Segue che φ è surgettiva (e quindi bigettiva) se e solo se $\text{MCD}(20, n^2) = 1$ e $\text{MCD}(15, n) = 1$, condizione che, come prima, porta a

$$2 \nmid n \wedge 3 | n - 1 \wedge 5 | n - 1.$$

Possiamo concludere che la strada della surgettività era sicuramente più facilmente percorribile.

□

Esercizi di terzo tipo

Esercizio (Traccia N.61, 19 giugno 2015)**.**
Dato un numero primo $p > 2$, sia $f(x) = x^{p-2} + x + 2 \in \mathbb{Z}[x]$.

(a) Provare che la riduzione di $f(x)$ modulo p ha in $\mathbb{Z}_p$ una sola radice.

(b) Per $p = 5$, determinare la riduzione di $f(x)$ modulo 5.

(c) Provare che, per ogni p, la radice del punto (a) è semplice. (Suggerimento: procedere per assurdo, dimostrando che se la radice è multipla per la riduzione di $f(x)$ modulo p, allora la stessa radice è multipla per la riduzione modulo p del polinomio $x^3 + 2x^2 - 1$)

Svolgimento.

(a) Sia $\alpha \in \mathbb{Z}_p$ una radice di $\bar{f}(x)$. Osservando che, sicuramente, $\alpha \neq \bar{0}$, possiamo dire che $\bar{f}(\alpha) = \bar{0}$ se e solo se $\alpha\bar{f}(\alpha) = \bar{0}$. Dunque, per il Teorema di Eulero (17.22),

$$\alpha\bar{f}(\alpha) = \bar{0} \iff \alpha^{p-1} + \alpha^2 + \bar{2}\alpha = \alpha^2 + \bar{2}\alpha + \bar{1} = (\alpha + \bar{1})^2 = \bar{0}.$$

Ma allora, $\alpha = -\bar{1}$ è l'unica radice di $\bar{f}(x)$ in $\mathbb{Z}_p$.

(b) Dal punto (a), sappiamo che $\alpha = \bar{4}$ è l'unica radice di $\bar{f}(x)$ in $\mathbb{Z}_5$. Per il Teorema di Ruffini (12.5), si ha che $\bar{f}(x)$ è divisibile per $(x - \bar{4})$ in $\mathbb{Z}_5[x]$. Svolgendo la divisione, si ottiene che

$$\bar{f}(x) = (x - \bar{4})(x^2 - x + \bar{2}).$$

Il quoziente della divisione di $\bar{f}$ per $(x - \bar{4})$ è di grado 2 e $\alpha = \bar{4}$ non è sua radice (è l'unica radice possibile, dovendo essere anche una radice di $\bar{f}$).

Dunque tale polinomio è irriducibile in $\mathbb{Z}_5[x]$, essendo di grado 2 e privo di radici in $\mathbb{Z}_5$, per il Corollario 12.9.

Dunque

$$\bar{f}(x) = (x - \bar{4})(x^2 - x + \bar{2})$$

è la fattorizzazione richiesta.

(c) Mostriamo come giungere alla soluzione seguendo il suggerimento.

Supponiamo per assurdo che $-\bar{1}$ sia radice multipla di $\bar{f}(x)$. Allora, sicuramente $(x + \bar{1})^2 | \bar{f}(x)$ in $\mathbb{Z}_p[x]$. Ma allora, $(x + \bar{1})^2$ divide anche

$$x^2 \bar{f}(x) = x^p + x^3 + 2x,$$

e, essendo $p > 2$, anche $(x + \bar{1})^p = x^p + \bar{1}$ (usando la Proprietà 8). Ma, allora

$$(x + \bar{1})^2 | x^2 \bar{f}(x) - (x^p + \bar{1}) = x^3 + \bar{2}x^2 - \bar{1}.$$

Tuttavia, questa è una contraddizione, come è immediato verificare effettuando la divisione euclidea di $x^3 + \bar{2}x^2 - \bar{1}$ per $(x + \bar{1})^2$.

Una possibile soluzione alternativa, qualora non si riesca a giungere alla conclusione suggerita, è la seguente.

Sappiamo che, per il Teorema di Ruffini, $\bar{f}(x)$ si può scrivere come

$$\bar{f}(x) = (x + \bar{1})\bar{g}(x),$$

per un opportuno $\bar{g}(x) \in \mathbb{Z}_p[x]$.

Vogliamo mostrare che $\bar{g}(-\bar{1}) \neq \bar{0}$. Infatti, in tal caso, per il Teorema di Ruffini (12.5), $x + \bar{1}$ non divide $\bar{g}(x)$, e, dunque, non divide $\bar{f}(x)$ con molteplicità maggiore di 1.

Ma chi è $\bar{g}(x)$? Essendo p indeterminato, non possiamo certamente svolgere la divisione. D'altro canto, avendo provato al punto (a) che ognuna delle riduzioni modulo p ha un'unica radice, (anzi, la "stessa" radice) è lecito pensare che le loro strutture non debbano discostarsi troppo l'una dall'altra. Provando a fare la divisione per $p = 3, 5, 7$ si ottengono, rispettivamente,

$$\bar{g}(x) = \bar{2} \in \mathbb{Z}_3[x],$$

$$\bar{g}(x) = x^2 - x + \bar{2} \in \mathbb{Z}_5[x],$$

$$\bar{g}(x) = x^4 - x^3 + x^2 - x + \bar{2} \in \mathbb{Z}_7[x].$$

Osserviamo una certa regolarità (alternanza di segno e termine noto "costante"). Affermiamo, allora che, per ogni p,

$$\bar{g}(x) = x^{p-3} - x^{p-4} + \cdots - x + \bar{2} \in \mathbb{Z}_p[x].$$

In effetti, risulta

$$\begin{aligned}(x + \bar{1})&(x^{p-3} - x^{p-4} + \cdots - x + \bar{2}) \\ &= (x^{p-2} - x^{p-3} + \cdots - x^2 + \bar{2}x) + (x^{p-3} - x^{p-2} + \cdots + x^2 - x + \bar{2}) \\ &= x^{p-2} + x + \bar{2}.\end{aligned}$$

Dunque $\bar{g}(x)$ è effettivamente il quoziente cercato. In particolare, essendo $p - 3$ pari,

$$\bar{g}(-1) = \underbrace{\bar{1} + \bar{1} + \cdots + \bar{1}}_{p-3 \text{ volte}} + \bar{2} = \bar{p} - \bar{1} \neq \bar{0},$$

come volevasi.

□

Esercizio (Traccia N. 65, 15 gennaio 2016)**.**
Sia $f(x) = x^6 + 2x^5 + 5x^4 - 8x^3 - 9x^2 + 6x + 3 \in \mathbb{Z}[x]$.

(a) Scrivere una fattorizzazione di $f(x)$ in $\mathbb{Q}[x]$.

(b) Determinare due diversi numeri primi positivi p tali che la riduzione di $f(x)$ modulo p si decomponga in $\mathbb{Z}_p[x]$ nel prodotto di fattori lineari.

Svolgimento.

(a) Cominciamo col cercare eventuali radici razionali. In base alla Proposizione 14.4, esse vanno cercate nell'insieme $\{1, -1, 3, -3\}$.

Si vede subito che $1, -1$ sono radici del polinomio. Dunque, per il Teorema di Ruffini (12.5) $f(x)$ è divisibile per $x^2 - 1$. Effettuando la divisione, si ottiene

$$f(x) = (x^2 - 1)(x^4 + 2x^3 + 6x^2 - 6x - 3).$$

Ragioniamo allo stesso modo sul polinomio $x^4 + 2x^3 + 6x^2 - 6x - 3$. Si ha che 1 è ancora radice, mentre -1 no. Effettuando la divisione per $x - 1$ si ha

$$f(x) = (x - 1)^2(x + 1)(x^3 + 3x^2 + 9x + 3).$$

A questo punto è facile calcolare che, tra le quattro possibili, nessuna è radice del polinomio $x^3 + 3x^2 + 9x + 3$. Ma allora tale polinomio è irriducibile in $\mathbb{Q}[x]$ per il Secondo Corollario al Teorema di Ruffini (12.9), perché di grado 3 e privo di radici in $\mathbb{Q}$. Dunque una fattorizzazione di $f(x)$ in $\mathbb{Q}[x]$ è

$$f(x) = (x - 1)^2(x + 1)(x^3 + 3x^2 + 9x + 3).$$

(b) Sfruttando la fattorizzazione trovata al punto precedente (che è, *de facto*, in $\mathbb{Z}[x]$, e quindi possiamo ridurre fattore per fattore), il problema si riconduce a quello di determinare due primi p distinti tali che la riduzione modulo p del polinomio

$$g(x) = x^3 + 3x^2 + 9x + 3$$

si spezzi in $\mathbb{Z}_p[x]$ nel prodotto di fattori lineari.

$p = 3$ è un primo che ovviamente va bene, in quanto $g_3(x) = x^3$. Per trovarne un altro, si può osservare che la struttura del polinomio ricorda, in qualche modo, quella dello sviluppo notevole di un cubo di un binomio (pur essendo ben lontando dall'esserlo, in $\mathbb{Q}[x]$). Si potrebbe tentare di cercare il primo p in maniera tale che, a patto di scegliere rappresentanti diversi, i coefficienti del polinomio diventino quelli di un opportuno cubo di un binomio. Per esempio, se $p = 2$, il polinomio si può scrivere come

$$g_2(x) = x^3 + \bar{3}x^2 + \bar{3}x + \bar{1} = (x + \bar{1})^3.$$

Dunque $p = 2$ è un altro primo che soddisfa la richiesta.

□

Esercizio (Traccia N.72, 12 settembre 2016)**.**
Sia p un numero primo positivo, e sia $f(x) = x^{p^2} - x^p - 1 \in \mathbb{Z}[x]$.

(a) Provare che $f(x)$ non ha radici razionali.

(b) Per $p = 3$, determinare una fattorizzazione della riduzione di $f(x)$ modulo 3 in $\mathbb{Z}_3[x]$.

Svolgimento.

(a) Per la Proposizione 14.4, le eventuali radici razionali di $f(x)$ possono essere solamente ± 1, ma nessuna delle due lo è.

(b) Sfruttando la Proprietà 8 otteniamo

$$\bar{f}(x) = x^9 - x^3 - \bar{1} = (x^3 - x - \bar{1})^3.$$

Ora, il polinomio $\bar{g}(x) = x^3 - x - \bar{1} \in \mathbb{Z}_3[x]$ è irriducibile in $\mathbb{Z}_3[x]$ perché di grado 3 e privo di radici in $\mathbb{Z}_3$ (Corollario 12.9).

Dunque

$$\bar{f}(x) = (x^3 - x - \bar{1})^3$$

è la fattorizzazione cercata.

□

Esercizio (Traccia N.80, 21 giugno 2017)**.**
Sia p un numero primo maggiore di 2. Provare che il polinomio $f(x) = x^{p^2} - x^p + x^2 - \bar{1} \in \mathbb{Z}_p[x]$ non ha radici multiple in $\mathbb{Z}_p$.

Svolgimento. Sia $\alpha \in \mathbb{Z}_p$. Allora, in base al Piccolo Teorema di Fermat (17.23), si ha che $\alpha^{p^2} = \alpha^p = \alpha$. Si ha, pertanto,

$$\bar{f}(\alpha) = \alpha^2 - \bar{1} = \bar{0} \iff \alpha = \pm\bar{1}.$$

Dunque, $f(x)$ ha solamente due radici (distinte, essendo $p > 2$) in $\mathbb{Z}_p$, cioè $\pm\bar{1}$. Cerchiamo ora di determinarne la molteplicità.
Si ha, in base alla Proprietà 8,

$$\begin{aligned} f(x) &= x^{p^2} - x^p + x^2 - \bar{1} = (x^p - x)^p + x^2 - \bar{1} \\ &= x^p(x^{p-1} - \bar{1})^p + (x - \bar{1})(x + \bar{1}) \end{aligned}$$

Abbiamo già osservato che ogni elemento di $\mathbb{Z}_p$ è radice del polinomio

$$x^{p^2} - x^p = x^p(x^{p-1} - \bar{1})^p.$$

Per il Teorema di Eulero (17.22), ogni elemento non nullo (ce ne sono in tutto $p - 1$) è radice dell'addendo $x^p(x^{p-1} - \bar{1})^p$. Per ragioni di grado, ciascuno dei $p - 1$ elementi non nulli di $\mathbb{Z}_p$ è radice di molteplicità 1 del polinomio $x^{p-1} - \bar{1}$, e dunque di molteplicità p del polinomio $(x^{p-1} - \bar{1})^p$.
Essendo $p > 2$, in base a quanto appena osservato, $(x-\bar{1})^2$ e $(x+\bar{1})^2$ dividono $x^p(x^{p-1} - \bar{1})^p$.
Ora, se $(x - \bar{1})^2 | f(x)$ (ossia $\bar{1}$ ha molteplicità almeno 2), allora, in base alla Proposizione 6.9,

$$(x - \bar{1})^2 | f(x) - x^p(x^{p-1} - \bar{1})^p = (x - \bar{1})(x + \bar{1})$$

che è assurdo. Dunque $\bar{1}$ ha molteplicità esattamente 1. In maniera analoga, anche $-\bar{1}$ ha molteplicità esattamente 1.

□

Esercizio (Traccia N.81, 5 luglio 2017)**.**
Dato un primo positivo p, sia $f(x) = x^8 + x^4 - \bar{2} \in \mathbb{Z}_p[x]$.

(a) Provare che esiste un primo $p > 50$ per il quale $f(x)$ ha più di due radici (distinte) in $\mathbb{Z}_p$.

(b) Provare che, per tale valore di p, $f(x)$ ha solo radici semplici.

Svolgimento.

(a) Dal momento che siamo interessati a $p > 50$, quindi certamente $p \neq 2$, $\bar{0}$ non è mai radice di $f(x)$. Dunque possiamo ridurci a studiare il problema in $\mathbb{Z}_p^*$, che è un gruppo ciclico di ordine $p - 1$(Corollario 17.42).

Osserviamo che se $\alpha^4 = \alpha^8 = 1$, allora sicuramente α è radice di $f(x)$.

In base alla Proprietà 6, se $4|p-1$, possiamo trovare esattamente

- $\varphi(1) = 1$ elemento di periodo 1, cioè $\bar{1}$;
- $\varphi(2) = 1$ elemento di periodo 2, cioè $-\bar{1}$;
- $\varphi(4) = 2$ elementi di periodo 4.

Ognuno di questi quattro elementi (distinti) è radice di $f(x)$ in base alla Proposizione 17.16, visto che elevati alla quarta e all'ottava valgono $\bar{1}$.

Dunque, si tratta solamente di scegliere un primo $p > 50$ congruo a 1 modulo 4. Per esempio $p = 53$ va bene.

(b) Possiamo scomporre facilmente

$$f(x) = (x^4 - \bar{1})(x^4 + \bar{2}).$$

Ognuna delle 4 radici trovate al punto precedente è radice del fattore $x^4 - \bar{1}$, e non lo è dell'altro fattore. Dunque, per ragioni di grado queste sono tutte semplici.

Dobbiamo ora determinare eventuali radici di $g(x) = x^4 + \bar{2}$ in $\mathbb{Z}_{53}$ e, qualora esistano, dimostrare che sono semplici.

Ora, supponiamo che esista $\alpha \in \mathbb{Z}_{53}^*$ tale che $\alpha^4 = -\bar{2}$.

Dal momento che $p - 1 = 53 - 1 = 52 = 4 \cdot 13$, per il Teorema di Eulero

$$(-\bar{2})^{13} = (\alpha^4)^{13} = \bar{1}.$$

Tuttavia, operando un calcolo esplicito, abbiamo che

$$(-\bar{2})^{13} = (-\bar{2})^6(-\bar{2})^6(-\bar{2}) = \overline{64}^2(-\bar{2}) = \overline{11}^2(-\bar{2}) =$$
$$= \overline{121}(-\bar{2}) = \overline{15}(-\bar{2}) = -\overline{30} = \overline{23}$$

il che conduce ad una contraddizione. Dunque $g(x)$ non ha radici in $\mathbb{Z}_{53}$. In conclusione, $f(x)$ ha solo radici semplici in $\mathbb{Z}_{53}$.

□

Esercizio (Traccia N.82, 11 settembre 2017)**.**
Sia $f(x) = x^4 + 1 \in \mathbb{Z}[x]$.

(a) Trovare un numero primo $p > 100$ *tale che la riduzione modulo* p *di* $f(x)$ *non abbia radici in* $\mathbb{Z}_p$.

(b) Trovare un numero primo $p > 100$ *tale che la riduzione modulo* p *di* $f(x)$ *abbia almeno una radice in* $\mathbb{Z}_p$.

Svolgimento.

(a) Cominciamo con l'osservare che, se $\alpha \in \mathbb{Z}_p$ è una radice di $\bar{f}(x)$, allora sicuramente $\alpha \neq \bar{0}$ e

$$\alpha^4 = -\bar{1} \Rightarrow \alpha^8 = \bar{1}$$

Dunque, se $o(\alpha)$ è il periodo di α nel gruppo $\mathbb{Z}_p^*$, si ha che $o(\alpha)|8$ (Proposizione 17.16). D'altro canto, $\alpha^4 \neq \bar{1}$ (infatti, visto che cerchiamo un primo $p > 100$, possiamo assumere che $p > 2$), per cui $o(\alpha) = 8$. In base alla Proprietà 6, se $8 \nmid |\mathbb{Z}_p^*| = p - 1$, allora certamente in $\mathbb{Z}_p^*$ non ci sono elementi di periodo 8 e quindi in $\mathbb{Z}_p$ non ci sono radici di $\bar{f}(x)$.

Pertanto, è sufficiente trovare un primo $p > 100$ tale che $p - 1$ non sia divisibile per 8. Per esempio, $p = 101$ va bene, visto che $100 = 2^2 \cdot 5^2$.

(b) Alla luce di quanto osservato nel punto (a), è sufficiente trovare un primo $p > 100$ tale che $8|p - 1$. Infatti, in tal caso, la Proprietà 6 garantisce che in $\mathbb{Z}_p^*$ ci saranno esattamente $\varphi(8) = 4$ elementi di periodo 8.

Sia α uno di questi elementi. Dato che 8 è proprio il periodo di α, per definizione si ha che $\alpha^4 \neq \bar{1}$. D'altro canto, α^4 ha periodo 2, e in $\mathbb{Z}_p^*$ c'è esattamente $\varphi(2) = 1$ elemento di periodo 2, cioè $-\bar{1}$. Questo implica che $\alpha^4 = -\bar{1}$, ovvero $\bar{f}(\alpha) = \bar{0}$ (cioè, α è radice di $\bar{f}(x)$).

Resta solo da trovare un primo $p > 100$ che soddisfa la proprietà richiesta. Esaminiamo i primi successivi a 101.

- $p = 103 \Rightarrow p - 1 = 102 = 2 \cdot 3 \cdot 17$, non va bene;
- $p = 107 \Rightarrow p - 1 = 106 = 2 \cdot 53$, non va bene;
- $p = 109 \Rightarrow p - 1 = 108 = 2^2 \cdot 3^3$, non va bene;
- $p = 113 \Rightarrow p - 1 = 112 = 2^4 \cdot 7$, va bene.

Dunque $p = 113$ è un primo che soddisfa la richiesta.

□

Esercizio (Traccia N.83, 25 settembre 2017)**.**
Siano p, q primi positivi distinti.

(a) Dire per quali p il polinomio $x^2 - x - p$ è irriducibile in $\mathbb{Q}[x]$.

(b) Provare che il polinomio $x^3 + 8x^2 - pq$ è irriducibile in $\mathbb{Q}[x]$.

Svolgimento.

(a) Per il Secondo Corollario al Teorema di Ruffini (Corollario 12.9), essendo $f(x) = x^2 - x - p$ di grado 2, dobbiamo determinare i primi p per i quali $f(x)$ non ha radici razionali. Per la Proposizione 14.4 queste, se esistono, possono essere cercate solo tra $p, -p, 1, -1$. Tuttavia, un rapido calcolo mostra che, se $p > 2$, nessuno di questi 4 interi è radice di $f(x)$. Invece,

$$x^2 - x - 2 = (x - 2)(x + 1).$$

Dunque $f(x)$ è irriducibile in $\mathbb{Q}[x]$ se e solo se $p > 2$.

(b) Si può procedere in maniera analoga al caso (a), visto che $g(x) = x^3 + 8x^2 - pq$ ha grado 3, e quindi il Secondo Corollario al Teorema di Ruffini è ancora applicabile. Tuttavia, testando tutte le possibili radici dovremmo, in questo caso, fare molti più controlli rispetto al primo caso. Cerchiamo una via alternativa.

Supponiamo per assurdo che $g(x)$ abbia una radice razionale. In base alla Proposizione 14.4 questa deve essere un numero intero m.

Allora, da $g(m) = 0$ segue che

$$m^2(m + 8) = pq.$$

Ora, si ha che $m^2 | pq$. Ma p e q sono due primi distinti. Se $|m| > 1$ esiste un primo il cui quadrato divide m^2 e quindi pq. Dunque $m = \pm 1$. Tuttavia, in questi due casi si avrebbe $7 = pq$ oppure $9 = pq$. Entrambi questi casi non possono verificarsi perchè 7 è primo (primo caso) e $p \neq q$ (secondo caso).

Dunque $g(x)$ non può avere radici in $\mathbb{Q}$, e quindi è irriducibile in $\mathbb{Q}[x]$.

□

Esercizio (Traccia N.84, 6 novembre 2017)**.**
Sia p un numero primo positivo, e si consideri il polinomio

$$f(x) = x^{p-1} - [2^{3700}]_p \in \mathbb{Z}_p.$$

(a) Determinare quattro valori di p per i quali $f(x)$ ha radici in $\mathbb{Z}_p$ e queste sono tutte semplici.

(b) Determinare una fattorizzazione di $f(x)$ per $p = 7$.

Svolgimento.

(a) Potremmo approcciare il problema iniziando da un procedimento per tentativi. Si ha, utilizzando il Piccolo Teorema di Fermat (17.23) per determinare un rappresentante canonico di $[2^{3700}]_p$:

- per $p = 2$,
$$f(x) = x;$$
- per $p = 3$,
$$f(x) = x^2 - [2^{3700}]_3 = x^2 - [1]_3 = (x - [1]_3)(x - [2]_3);$$
- per $p = 5$,
$$\begin{aligned} f(x) &= x^4 - [2^{3700}]_5 = x^4 - [1]_5 = (x^2 - [1]_5)(x^2 - [4]_5) \\ &= (x - [1]_5)(x - [2]_5)(x - [3]_5)(x - [4]_5); \end{aligned}$$
- per $p = 7$, visto che $3700 \equiv 1 \bmod 3 = o([2]_7)$ (dove il periodo di $[2]_7$ è considerato rispetto all'operazione moltiplicativa del gruppo delle unità $\mathbb{Z}_7^*$), per il Corollario 17.18
$$f(x) = x^6 - [2]_7.$$

Ci rendiamo conto che i primi $p = 2, 3, 5$ soddisfano la richiesta, ed è stato possibile verificarlo con poca fatica. Per $p = 7$, non è più immediato ottenere una fattorizzazione di $f(x)$, da cui è possibile dedurre le molteplicità delle radici. Potremmo procedere per tentativi con primi più grandi, ma dobbiamo tenere conto che anche il grado del polinomio tenderà ad aumentare, rendendo sempre più difficile trovare a mano una fattorizzazione. Inoltre, non abbiamo una stima dall'alto sui primi da testare: di conseguenza, potrebbero volerci moltissimi tentativi.

Occorre dunque trovare un approccio differente. Osserviamo che, nel caso $p = 3, 5$, il polinomio assumeva la forma

$$f(x) = x^{p-1} - [1]_p.$$

Questo polinomio, per qualsiasi primo p, è annullato da ogni classe non nulla in $\mathbb{Z}_p$, grazie al Teorema di Eulero (17.22). Questi elementi sono $p-1$, e quindi, per ragioni di grado, devono essere tutte e sole le radici di $f(x)$ in $\mathbb{Z}_p$. Inoltre, per gli stessi motivi, sono tutte semplici.

Abbiamo pertanto determinato una condizione sufficiente affinché p soddisfi la richiesta: si deve avere $[2^{3700}]_p = [1]_p$. Questo, alla luce della Proposizione 17.16, accade se e solo se $o([2]_p)|3700$, essendo $o([2]_p)$ il periodo di $[2]_p$ in $\mathbb{Z}_p^*$.

Si ha $3700 = 2^2 \cdot 5^2 \cdot 37$. Dunque dobbiamo cercare i primi p in maniera tale che $o([2]_p)$ sia uno dei divisori di 3700 (cioè 2,4,5,10,ecc.). Abbiamo già osservato che $p = 3, 5$ soddisfa la richiesta. In effetti, $o([2]_3) = 2|3700$ e $o([2]_5) = 4|3700$.

Osserviamo che $2^5 = 32 \equiv 1 \pmod{31}$. Inoltre, $o([2]_{31})$ è proprio 5, come è immediato verificare (infatti, $2^k < 31$ per $k = 1, 2, 3, 4$, e quindi non può essere congruo a 1 modulo 31).

Ma allora $o([2]_{31}) = 5|3700$ e pertanto $p = 31$ soddisfa la richiesta.

Avevamo già osservato che banalmente anche $p = 2$ soddisfaceva la richiesta.

Dunque quattro primi che soddisfano la richiesta sono $2, 3, 5, 31$.

Osservazione 3. Una soluzione più elegante è basata sull'osservazione che la condizione $o([2]_p)|3700 = 2^2 \cdot 5^2 \cdot 37$ è certamente soddisfatta se $p - 1|3700$, grazie al Teorema di Lagrange (17.19). Dunque possiamo scegliere anche $p = 11$ e $p = 101$ senza calcolare esplicitamente il periodo di $[2]_p$ in $\mathbb{Z}_p^*$.

(b) Nel punto (a) abbiamo già trovato che $f(x) = x^6 - [2]_7$.

Osserviamo che $3^2 = 9 \equiv 2 \bmod 7$. Dunque, si ha

$$f(x) = x^6 - [2]_7 = x^6 - [3]_7^2 = (x^3 - [3]_7)(x^3 - [4]_7).$$

Il Secondo Corollario al Teorema di Ruffini (12.9) stabilisce che provare che i due fattori di grado 3 sono riducibili equivale a provare che posseggono almeno una radice in $\mathbb{Z}_7$. In tal caso $f(x)$ ha almeno una radice in $\mathbb{Z}_7$. Supponiamo per assurdo che $\alpha \in \mathbb{Z}_p$ sia una radice di $f(x)$. Allora, sicuramente, $\alpha \neq [0]_7$ e

$$\alpha^6 = [2]_7 \Rightarrow [1]_7 = [2]_7,$$

per il Teorema di Eulero (17.22), e ciò è impossibile.

Dunque $f(x)$ non ha radici in $\mathbb{Z}_7$, e quindi nessuno dei due fattori di grado 3 trovati ha radici in $\mathbb{Z}_7$. Essi sono dunque irriducibili. Pertanto

$$f(x) = (x^3 - [3]_7)(x^3 - [4]_7)$$

è la fattorizzazione cercata.

□

Esercizio (Traccia N.85, 9 gennaio 2018)**.**
Sia p un numero primo positivo, e sia $f(x) = x^{p^4-p^3} - \bar{1} \in \mathbb{Z}_p[x]$.

(a) Determinare tutte le radici di $f(x)$ in $\mathbb{Z}_p$, con le rispettive molteplicità.

(b) Dato il polinomio $g(x) = x^{p+1} + \bar{2}x \in \mathbb{Z}_p[x]$, si determini, al variare di p, MCD$(f(x), g(x))$.

Svolgimento.

(a) Si osservi che $p^4 - p^3 = p^3(p-1)$. Per la Proprietà 8, si ha che

$$f(x) = x^{p^4-p^3} - \bar{1} = (x^{p-1})^{p^3} - \bar{1}^{p^3} = (x^{p-1} - \bar{1})^{p^3}.$$

Ora, $\bar{0}$ non è radice di $f(x)$. Dunque dobbiamo cercare eventuali radici in $\mathbb{Z}_p^*$. Sia $\alpha \in \mathbb{Z}_p$ non nullo. Allora per il Piccolo Teorema di Fermat

(Teorema 17.23), si ha che $\alpha^{p-1} = \bar{1}$. Dunque ogni elemento non nullo di $\mathbb{Z}_p$ è radice del polinomio $g(x) = x^{p-1} - \bar{1}$. Inoltre, poiché vi sono $p-1$ radici distinte, per ragioni di grado queste hanno tutte moltiplicità 1.

Ma allora essendo $f(x) = g(x)^{p^3}$, è immediato osservare che ogni $\alpha \in \mathbb{Z}_p^*$ è radice di $f(x)$ di molteplicità p^3.

(b) Osserviamo che, per la Proprietà 7, $g(x) = x(x + \bar{2})^p$. Infatti, $\bar{2}^p = \bar{2}$ per il Piccolo Teorema di Fermat (Teorema 17.23). Avendo provato che $f(x)$ si spezza nel prodotto di fattori lineari, $\mathrm{MCD}(f(x), g(x)) \neq 1$ se e solo se $f(x), g(x)$ hanno una radice in comune (per il Teorema di Ruffini, 12.5 e il suo Primo Corollario, 12.7).

Se $p = 2$, allora $g(x) = x^{p+1}$. La sua unica radice è $\bar{0}$ con molteplicità $p+1$. Ma $\bar{0}$ non è radice di $f(x)$, per cui i due polinomi saranno coprimi.

Se $p \neq 2$, allora è chiaro che il fattore $h(x) = x$ non è comune, mentre certamente $(x + \bar{2})^p | f(x)$, visto che nel punto (a) abbiamo provato che addirittura $(x + \bar{2})^{p^3} | f(x)$.

Ricapitolando:

$$\mathrm{MCD}(f(x), g(x)) = \begin{cases} (x + \bar{2})^p & p \neq 2 \\ \bar{1} & p = 2 \end{cases}$$

□

Esercizio (Traccia N.86, 24 gennaio 2018)**.**
Si consideri il polinomio $f(x) = x^6 - 1 \in \mathbb{Z}[x]$. Dato un primo positivo p, sia $\overline{f(x)}$ la sua riduzione modulo p.

(a) Provare che se $p \equiv 2$ (mod 3), $\overline{f(x)}$ non si decompone in $\mathbb{Z}_p[x]$ nel prodotto di fattori lineari.

(b) Provare che se $p \equiv 1$ (mod 3), $\overline{f(x)}$ ha in $\mathbb{Z}_p$ almeno 4 radici distinte.

Svolgimento.

(a) Osservando che $\bar{0}$ non è radice del polinomio, il problema può essere studiato in $\mathbb{Z}_p^*$, che è un gruppo finito e ciclico (Corollario 17.42). Nello specifico, il problema di studiare le radici di $\overline{f(x)}$ si riconduce a quello di trovare elementi $\alpha \in \mathbb{Z}_p^*$ tali che $\alpha^6 = 1$, ovvero elementi il cui periodo è un divisore di 6.

Supponiamo dapprima $p \neq 2$. In base alla Proprietà 6, c'è esattamente $\varphi(2) = 1$ elemento di periodo 2, ovvero $-\bar{1}$, e ovviamente l'unico elemento di periodo 1 è $\bar{1}$. Per quanto riguarda i periodi 3 e 6, osserviamo che essendo $p-1 \equiv 1 \pmod 3$, si ha che 3 (e quindi 6) non divide $p-1$, per cui non ci sono elementi di periodo 3 o 6.

Osserviamo che

$$\overline{f(x)} = (x^6-\bar{1}) = (x^3-\bar{1})(x^3+\bar{1}) = (x-\bar{1})(x^2+x+\bar{1})(x+\bar{1})(x^2-x+\bar{1}).$$

Risulta evidente che $\pm\bar{1}$ non è radice dei due fattori non lineari (dal momento che sicuramente $p \neq 3$). Dunque i due fattori non lineari sono irriducibili essendo di grado 2 e privi di radici in $\mathbb{Z}_p$ (Corollario 12.9).

Se, invece, $p = 2$, la scomposizione precedente diventa

$$\overline{f(x)} = (x^6 - \bar{1}) = (x + \bar{1})^2(x^2 + x + \bar{1})^2.$$

È evidente che il polinomio $x^2 + x + \bar{1}$ non ha radici in $\mathbb{Z}_2$, ed è quindi irriducibile. Dunque, anche in questo caso $f(x)$ non si spezza nel prodotto di fattori lineari.

Dunque $\overline{f(x)}$ non si spezza nel prodotto di fattori lineari in $\mathbb{Z}_p[x]$.

(b) Come nel punto (a), ragioniamo nel gruppo ciclico $\mathbb{Z}_p^*$. La condizione su p mostra che stavolta $3|p-1$, dunque, per la Proprietà 6 esistono esattamente due elementi distinti $\alpha_1, \alpha_2 \in \mathbb{Z}_p^*$ di periodo 3 che, in base alle nostre osservazioni precedenti sono, insieme a $\bar{1}, -\bar{1}$ radici di $\overline{f(x)}$ (inoltre, $\bar{1} \neq -\bar{1}$ visto che sicuramente $p \neq 2$).

□

Esercizio (Traccia N.87, 8 febbraio 2018)**.**
Si consideri il polinomio $f(x) = x^6 - 5x^3 + 6 \in \mathbb{Z}[x]$. *Dato un primo positivo* p, *sia* $\overline{f(x)}$ *la sua riduzione modulo* p.

(a) Provare che $\overline{f(x)}$ *non ha in* $\mathbb{Z}_p$ *radici di molteplicità maggiore di* 3.

(b) Sapendo che per $p = 643$ *il polinomio* $\overline{f(x)}$ *si decompone in* $\mathbb{Z}_{643}$ *nel prodotto di fattori lineari, provare che* $2^{214} \equiv 1$ *(mod* 643*).*

Svolgimento.

(a) Prima di tutto, osserviamo che $f(x) = (x^3 - 2)(x^3 - 3)$.

Dunque si avrà $\overline{f(x)} = (x^3 - \bar{2})(x^3 - \bar{3})$.

Visto che per qualunque primo p si ha che $\bar{2} \neq \bar{3}$ in $\mathbb{Z}_p$, $\overline{f(x)}$ non può avere radici di molteplicità maggiore di 3. Infatti, se ci fosse una radice $\alpha \in \mathbb{Z}_p$ di molteplicità almeno 4, si avrebbe che $(x-\alpha)^4 | f(x)$. Tuttavia, alla luce del Teorema di Ruffini (12.5) e del suo Primo Corollario (12.7), si avrebbe che, per ragioni di grado, α sarebbe una radice del fattore $x^3 - \bar{2}$ e anche del fattore $x^3 - \bar{3}$. Ma, allora, si avrebbe $\bar{2} = \alpha^3 = \bar{3}$.

(b) In base alla decomposizione di $\overline{f(x)}$ del punto (a), l'ipotesi che esso si spezzi nel prodotto di fattori lineari implica l'esistenza in $\mathbb{Z}_{643}$ di una radice cubica di $\bar{2}$, ovvero di un numero intero α tale che $\alpha^3 \equiv 2 \pmod{643}$.

Osserviamo che $214 \cdot 3 = 643 - 1$. Questo ci fa venire in mente il Teorema di Eulero (Teorema 17.22) (o il Piccolo Teorema di Fermat, 17.23, applicato ad elementi non nulli). Si ha, cioè, per ogni a non congruo a 0 modulo 643, $(a^3)^{214} \equiv a^{642} \equiv 1 \pmod{643}$.

Dunque elevando alla 214 ambo i membri di $\alpha^3 \equiv 2 \pmod{643}$ si ottiene la tesi.

□

Esercizio (Traccia N.88, 20 aprile 2018)**.**
Sia p un primo di Mersenne, ossia un numero primo avente la forma $2^N - 1$, ove N è un primo positivo.
Si consideri il polinomio $f(x) = x^{p^2+1} + x^{p+1} - \bar{1} \in \mathbb{Z}_p[x]$.

(a) Determinare, al variare di p, il numero delle radici di $f(x)$ in $\mathbb{Z}_p$.

(b) Per $p = 3$, posto $g(x) = x^6 + x^3 + \bar{1} \in \mathbb{Z}_3[x]$, determinare $MCD(f(x), g(x))$.

Svolgimento.

(a) Al fine di determinare le (eventuali) radici di $f(x)$ in $\mathbb{Z}_p[x]$, cerchiamo di trovare una condizione necessaria soddisfatta da una (eventuale) radice di $f(x)$ in $\mathbb{Z}_p[x]$.

Supponiamo che esista $\alpha \in \mathbb{Z}_p$ una radice di $f(x)$. Allora, sfruttando il Teorema di Eulero (17.22) e la Proprietà 8, si ha

$$\begin{aligned} f(\alpha) = \bar{0} \Rightarrow \alpha^{p^2+1} + \alpha^{p+1} - \bar{1} = \bar{0} \Rightarrow \alpha(\alpha^{p^2} + \alpha^p) = \bar{1} \\ \Rightarrow \alpha(\alpha^p + \alpha)^p = \bar{1} \Rightarrow \alpha(\bar{2}\alpha) = \bar{1} \Rightarrow \bar{2}\alpha^2 = \bar{1}. \end{aligned}$$

Visto che $p \neq 2$ (infatti, 2 non è un primo di Mersenne), sicuramente $\bar{2}$ è invertibile in $\mathbb{Z}_p$, dunque α soddisfa necessariamente l'equazione

$$\alpha^2 = \bar{2}^{-1}.$$

Dobbiamo ora sfruttare la forma particolare del primo dato. Dato che $p = 2^N - 1$ e $\bar{p} = \bar{0}$, si ha che

$$\bar{2}^N = \bar{1} \iff \bar{2}^{N-1} = \bar{2}^{-1}.$$

Segue che α deve soddisfare l'equazione

$$\alpha^2 = \bar{2}^{N-1}.$$

La domanda che dobbiamo porci è, allora, quando $\bar{2}^{N-1}$ è un quadrato in $\mathbb{Z}_p$.

Se N è un primo dispari, è chiaro che $\pm\bar{2}^{(N-1)/2}$ sono radici quadrate di $\bar{2}^{N-1}$ in $\mathbb{Z}_p$. Inoltre, esse sono distinte, perché $p \neq 2$. Infatti, se fossero uguali, si avrebbe

$$\begin{aligned} 2^{(N-1)/2} \equiv -2^{(N-1)/2} \bmod p &\iff 2 \cdot 2^{(N-1)/2} \equiv 0 \bmod p \\ &\iff 2^{(N+1)/2} \equiv 0 \bmod p. \end{aligned}$$

Ma, essendo $p > 2$, sicuramente $2^{(N+1)/2}$ non è congruo a 0 modulo p, perché 2 è l'unico fattore primo di tale numero.

Dunque, $\pm\bar{2}^{(N-1)/2}$ sono due radici quadrate distinte di 2^{N-1} in $\mathbb{Z}_p[x]$. Dato che ogni siffatta radice quadrata è radice del polinomio $x^2 - \bar{2}^{N-1} \in \mathbb{Z}_p[x]$, esse possono essere al massimo due. Segue che $\alpha_1 = \bar{2}^{(N-1)/2}$ e $\alpha_1 = -\bar{2}^{(N-1)/2}$ sono le uniche due possibili scelte per le radici di $f(x)$ in $\mathbb{Z}_p$.

Un calcolo esplicito mostra ora che esse sono effettivamente radici di $f(x)$.

Se $N = 2$, ossia $p = 3$, è chiaro che $\bar{2}$ non è un quadrato in $\mathbb{Z}_3$, per cui non ci possono essere radici del polinomio in $\mathbb{Z}_3$.

Segue che il numero di radici è due se $N > 2$, e zero se $N = 2$.

Curiosità 3 (sui primi di Mersenne). La condizione che l'esponente N sia primo non è, in realtà, riduttiva. Ci si potrebbe, infatti, chiedere se, per qualche esponente N non primo, risulta che $2^N - 1$ è primo. La risposta è no. Infatti, se N è composto, allora $2^N - 1$ è sicuramente composto.

Supponiamo, infatti, che $N = nm$, per opportuni n, m interi positivi maggiori di 1. Allora

$$2^N - 1 = 2^{nm} - 1 = (2^n - 1)(2^{n(m-1)} + 2^{n(m-2)} + \ldots 2^{2n} + 2^n + 1).$$

La domanda se esistano o meno infiniti primi di Mersenne è tuttora irrisolta.

Un'altra domanda che ci si può porre è: qual è la differenza tra i numeri nella forma $2^N - 1$ e numeri nella forma $2^N + 1$? Si potrebbe pensare che valgano proprietà simili per numeri che, in fondo, sono "vicini" ai numeri di Mersenne.

In realtà, in questo caso, la situazione cambia radicalmente: prima di tutto, si può dimostrare facilmente che se un numero nella forma $2^N + 1$ è primo, allora N è necessariamente una potenza di 2. Inoltre, conosciamo moltissimi primi di Mersenne, ma solo cinque primi della forma $2^{2^n} + 1$ (detti *primi di Fermat*): 3,5,17,257 e 65537. In effetti, è stato congetturato che esistano solo un numero finito di primi di Fermat.

I primi di Fermat compaiono inaspettatamente in un risultato che apparentemente sembra non avere nulla a che vedere con essi. Si può provare, infatti il seguente enunciato:

Sia $n \geq 3$. Allora il poligono regolare con n lati è costruibile con riga e compasso se e solo se

$$n = 2^m p_1 \cdots p_k,$$

ove m è un intero non negativo, e $p_1, \ldots, p_k$ sono primi di Fermat a due a due distinti.

Sul sito http://primes.utm.edu è possibile trovare maggiori informazioni, problemi aperti, proprietà note e curiosità sui numeri primi, nonché aggiornamenti sullo stato attuale della ricerca.

(b) Per $p = 3$, il polinomio $f(x)$ assume la forma

$$f(x) = x^{10} + x^4 + \bar{1}.$$

Usando la Proprietà 8, si ha che

$$g(x) = (x^2 + x + \bar{1})^3 = (x - \bar{1})^6.$$

Ma allora $g(x)$ si decompone in $\mathbb{Z}_3[x]$ nel prodotto di fattori lineari. Se $MCD(f(x), g(x)) \neq \bar{1}$, allora $f(x)$ deve essere divisibile per $x - \bar{1}$: alla luce Teorema di Ruffini (12.5) e del suo Primo Corollario (12.7), il polinomio $f(x)$ avrebbe una radice in $\mathbb{Z}_3$. Ma abbiamo già osservato nel punto (a) che questo non è vero. Dunque $f(x)$ e $g(x)$ sono coprimi in $\mathbb{Z}_3[x]$.

□

Esercizio (Traccia N.89, 5 giugno 2018)**.**

(a) Sia $f_1(x) = x^{15} + x^3 + \bar{2} \in \mathbb{Z}_7[x]$. Provare che non esiste alcun $g(x) \in \mathbb{Z}_7[x]$ tale che $f_1(x) = g(x)^3$.

(b) Sia $f_2(x) = x^{15} + x^{10} - x^4 - x^3 \in \mathbb{Z}_7[x]$. Provare che non esiste alcun $h(x) \in \mathbb{Z}_7[x]$ tale che $f_2(x) = g(x)^3$.

(c) Determinare una fattorizzazione di $f_3(x) = x^{15} + x^9 - x^3 \in \mathbb{Z}_3[x]$.

Svolgimento.

(a) Supponiamo che un siffatto polinomio $g(x) \in \mathbb{Z}_7[x]$ esista.

La strada più immediata è osservare che, se il termine noto di $g(x)$ è $\alpha \in \mathbb{Z}_7$, allora $\alpha^3 = \bar{2}$. In particolare, $\alpha \neq \bar{0}$. Dunque, per il Teorema di Eulero (17.22), si avrebbe

$$\alpha^3 = \bar{2} \Rightarrow \bar{1} = \alpha^6 = \bar{4},$$

che è assurdo.

Mostriamo ora un'altra possibile strada, percorribile nel caso in cui non ci si accorga di quanto riportato sopra, o in altri esercizi simili in cui quanto sopra non è applicabile.

Si ha che ogni (eventuale) radice di $f_1(x)$ in $\mathbb{Z}_7$ lo è anche di $g(x)$, e viceversa: infatti, per il Teorema di Ruffini (12.5), se $\alpha \in \mathbb{Z}_7$ è una radice di $f_1(x)$, allora

$$x - \alpha | f_1(x) = g(x)^3.$$

Essendo il polinomio $x-\alpha \in \mathbb{Z}_7[x]$ irriducibile, e quindi primo (Lemma 11.10), esso deve dividere $g(x)$. Il viceversa è ovvio.

Possiamo anche dire che, se k è la molteplicità di α come radice di $g(x)$, la molteplicità di α come radice di $f_1(x)$ è $3k$.

Dunque, ogni (eventuale) radice di $f_1(x)$ ha molteplicità multipla di 3. Cerchiamo di vedere se $f_1(x)$ ammette effettivamente radici in $\mathbb{Z}_7$. Una volta osservato che $\bar{0}$ non è radice, possiamo considerare $\alpha \in \mathbb{Z}_7^*$. Allora, usando il Teorema di Eulero (17.22), risulta

$$\bar{0} = f_1(\alpha) = \alpha^3 + \alpha^3 + \bar{2} = \bar{2}(\alpha^3 + \bar{1}).$$

Dunque, si deve avere $\alpha^3 = -\bar{1}$. Ma allora, il periodo di α in $\mathbb{Z}_7^*$ deve essere 2 oppure 6: infatti, per il Teorema di Lagrange (17.19), esso può essere solo 1,2,3 o 6. Ma ovviamente non è né 1 né 3. Ci sono, per la Proprietà 6, $\varphi(2) = 1$ elementi di periodo 2 e $\varphi(6) = 2$ elementi di periodo 6. Essi sono, rispettivamente,

$$-\bar{1}, \bar{3}, \bar{5}.$$

Come è immediato verificare, queste sono effettivamente radici di $f_1(x)$ e quindi di $g(x)$.

Dunque, per il Teorema di Ruffini,

$$h(x) = (x + \bar{1})(x - \bar{3})(x - \bar{5}) = x^3 + \bar{1} | g(x),$$

e quindi $(x^3 + \bar{1})^3 | f_1(x)$.

A questo punto si può effettuare la divisione di $f_1(x)$ per questo polinomio di grado 9, giungendo ad un assurdo (otterremo un resto non nullo). Se, invece, si vogliono evitare conti lunghi e complessi, cominciamo con l'osservare che

$$\begin{aligned} f_1(x) &= x^{15} + x^3 + \bar{2} = x^{15} - x^3 + \bar{2}x^3 + \bar{2} = x^3(x^{12} - \bar{1}) + \bar{2}(x^3 + \bar{1}) \\ &= x^3(x^3 - \bar{1})(x^3 + \bar{1})(x^6 + \bar{1}) + \bar{2}(x^3 + \bar{1}) \\ &= (x^3 + \bar{1})(x^3(x^3 - \bar{1})(x^6 + \bar{1}) + \bar{2}). \end{aligned}$$

Tuttavia, come è immediato verificare, nessuna delle tre radici di $f_1(x)$ è radice del polinomio

$$x^3(x^3 - \bar{1})(x^6 + \bar{1}) + \bar{2}.$$

Segue che la molteplicità di ogni radice di $f_1(x)$ è 1, che contraddice il fatto che debbano avere molteplicità almeno 3.

(b) Supponiamo per assurdo che un tale $h(x) \in \mathbb{Z}_7[x]$ esista. Come prima, si deduce che $f_1(x)$ ha le stesse radici di $h(x)$ con molteplicità triplicata.

Cerchiamo le radici di $f_2(x)$. Sia $\alpha \in \mathbb{Z}_7$ arbitrario. Allora, per il Piccolo Teorema di Fermat (17.23), risulta

$$f(\alpha) = \alpha^3 + \alpha^4 - \alpha^4 - \alpha^3 = \bar{0}.$$

Dunque, ogni elemento di $\mathbb{Z}_7[x]$ è radice del polinomio $f_2(x)$. Ma ogni radice ha molteplicità almeno 3, dunque $f_2(x)$ dovrebbe avere grado almeno 21, che è un assurdo.

(c) Sfruttando la Proprietà 8, si ha

$$f_3(x) = x^3(x^{12} + x^6 - \bar{1}) = x^3(x^4 + x^2 - \bar{1})^3.$$

Ora, il polinomio $p(x) = x^4 + x^2 - \bar{1}$ non ha radici in $\mathbb{Z}_3$. Dunque ci sono le seguenti due possibilità: $p(x)$ è irriducibile ovvero si fattorizza nel prodotto di due polinomi irriducibili di grado 2. Supponiamo che si verifichi la seconda.

Dovendo essere il termine noto $-\bar{1}$, l'unica possibilità è che uno di questi due polinomi quadratici abbia termine noto $\bar{1}$ e l'altro $-\bar{1}$. Dunque, si deve avere

$$p(x) = (x^2 + ax + \bar{1})(x^2 + bx - \bar{1}) = x^4 + (a+b)x^3 + abx^2 + (b-a)x - \bar{1},$$

per opportuni $a, b \in \mathbb{Z}_3$.

Ricordiamo che un polinomio a coefficienti in un qualsiasi anello A è, per definizione, una successione definitivamente nulla $f : \mathbb{N} \to A$. Dato che due successioni $(a_n)_{n\in\mathbb{N}}$ e $(b_n)_{n\in\mathbb{N}}$ sono uguali se e solo se $a_n = b_n$ per ogni $n \in \mathbb{N}$, affinché il prodotto ottenuto sia uguale a $p(x)$, i coefficienti di pari grado devono coincidere (si noti che abbiamo semplicemente dato una motivazione formale del famoso "Principio di Identità dei polinomi").

Dal fatto che $ab = \bar{1}$, segue facilmente che a e b sono entrambi non nulli e che $a = b$ (ogni elemento non nullo in $\mathbb{Z}_3$ coincide con il suo inverso moltiplicativo).

Ma allora $a + b = \bar{2}a \neq \bar{0}$ (coefficiente di grado 3). Dunque, due tali polinomi non possono esistere. Di conseguenza $p(x)$ è irriducibile e la fattorizzazione richiesta è

$$f_3(x) = x^3(x^4 + x^2 - \bar{1})^3.$$

□

Esercizio (Traccia N.90, 20 giugno 2018)**.**
Sia $p > 2$ un numero primo. Si consideri il polinomio $f(x) = \sum_{i=0}^{p-1} x^i \in \mathbb{Z}_p[x]$.

(a) Provare che, se α genera il gruppo $\mathbb{Z}_p^*$, allora $f(\alpha) = [1]_p$.

(b) Per $p = 7$, determinare una fattorizzazione di $f(x)$ in $\mathbb{Z}_7[x]$.

Svolgimento.

(a) Si ha

$$\{[1]_p, [2]_p, \ldots, [p-1]_p\} = \mathbb{Z}_p^* =< \alpha >= \{\alpha, \alpha^2, \ldots, \alpha^{p-1}\}.$$

Ma allora,

$$f(\alpha) = \sum_{i=0}^{p-1} \alpha^i = [1]_p + [\alpha]_p + \cdots + [\alpha^{p-1}]_p = [1]_p + [1]_p + [2]_p + \cdots + [p-1]_p$$
$$= [1]_p + \left[\frac{p(p-1)}{2}\right]_p = [1]_p.$$

Nell'ultimo passaggio abbiamo sfruttato il fatto che, essendo $p > 2$, $p-1$ è pari, e quindi $\frac{p-1}{2} \in \mathbb{Z}$, per cui

$$p\frac{p-1}{2} \equiv 0 \mod p.$$

(b) Sia $p = 7$. Si osservi che

$$(x - [1]_p)f(x) = x^7 - [1]_p.$$

Ma allora, sfruttando la Proprietà 8, si ha che

$$(x - [1]_p)f(x) = (x - [1]_p)^7.$$

Sfruttando la cancellabilità di $x - [1]_p$ in $\mathbb{Z}_7[x]$, segue che

$$f(x) = (x - [1]_p)^6.$$

Si osservi che non è mai stato sfruttato direttamente il fatto che il primo p fosse esattamente 7. Dunque

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

quale che sia $p > 2$ (in realtà, la formula vale anche banalmente per $p = 2$).

□

Esercizio (Traccia N.91, 5 luglio 2018)**.**
Si consideri il polinomio $f(x) = x^8 - 1 \in \mathbb{Z}[x]$.

(a) Provare che la riduzione di $f(x)$ *modulo* 4481 *si decompone in* $\mathbb{Z}_{4481}$ *nel prodotto di fattori lineari.*

(b) Determinare una fattorizzazione in $\mathbb{Z}_{101}[x]$ *della riduzione di* $f(x)$ *modulo* 101*.*

Svolgimento.

(a) Cominciamo con l'osservare che 4481 è un numero primo (per provarlo, per esempio, è sufficiente osservare che non è divisibile per nessun numero primo minore o uguale di $\sqrt{4481} \simeq 67$): dunque sappiamo che $\mathbb{Z}_{4481}$ è un campo.

Dobbiamo mostrare che la riduzione di $f(x)$ modulo 4481 ha 8 radici (contate con le rispettive molteplicità).

Una volta osservato che la classe nulla non è radice di $\overline{f}(x)$, possiamo cercare tali radici nel gruppo moltiplicativo $\mathbb{Z}^*_{4481}$, il quale, per la Proposizione 17.41, è ciclico, e ha ordine $4480 = 2^7 \cdot 5 \cdot 7$.

Si ha che $\alpha \in \mathbb{Z}^*_{4481}$ è radice del polinomio se e solo se $\alpha^8 = 1$, ossia, per la Proposizione 17.16, se e solo $o(\alpha) \in \{1, 2, 4, 8\}$.

Ora, visto che $8|4480$, in virtù della Proprietà 6, in $\mathbb{Z}^*_{4481}$ vi sono esattamente

- $\varphi(1) = 1$ elemento di periodo 1,
- $\varphi(2) = 1$ elemento di periodo 2,
- $\varphi(4) = 2$ elementi di periodo 4,
- $\varphi(8) = 4$ elementi di periodi 8,

che sono tutte radici del polinomio dato: esse sono esattamente 8 distinte, e quindi, in particolare, il polinomio si decompone in $\mathbb{Z}_{4481}$ nel prodotto di fattori lineari.

(b) Un primo immediato calcolo fornisce, dato che $\overline{1} = -\overline{100} = -\overline{10}^2$,

$$\begin{aligned}\overline{f}(x) &= (x^4 - \overline{1})(x^4 + \overline{1}) = (x - \overline{1})(x + \overline{1})(x^2 + \overline{1})(x^4 + \overline{1}) \\ &= (x - \overline{1})(x + \overline{1})(x - \overline{10})(x + \overline{10})(x^2 - \overline{10})(x^2 + \overline{10}).\end{aligned}$$

Dobbiamo solo capire se i polinomi di grado due comparsi in questa decomposizione sono irriducibili oppure no.

Essendo di secondo grado, per il Secondo Corollario al Teorema di Ruffini (12.9) è sufficiente controllare se i polinomi

$$g(x) = x^2 - \overline{10}, \quad h(x) = x^2 + \overline{10} \in \mathbb{Z}_{101}[x]$$

hanno oppure non hanno una radice in $\mathbb{Z}_{101}$. Una radice di $h(x)$ ovvero di $g(x)$, se esiste, va cercata tra le radici di $\overline{f}(x)$.

Dato che $101 - 1 = 100 = 2^2 \cdot 5^2$, esattamente come nel punto (a) si vede che le radici di $\overline{f}(x)$ sono tutti e soli gli elementi di $\mathbb{Z}_{101}^*$ che hanno periodo 1,2 oppure 4.

Se $\alpha \in \mathbb{Z}_{101}^*$ fosse una radice di $g(x)$, allora si avrebbe

$$\alpha^2 = \overline{10} \Rightarrow \alpha^4 = \overline{100} = -\overline{1}.$$

Tuttavia, questo implica che $o(\alpha) > 4$. Dunque una tale radice non può esistere. Analogamente si prova che $h(x)$ non ha radici in $\mathbb{Z}_{101}$.

Allora entrambi i polinomi sono irriducibili, e segue che quella precedentemente trovata è una fattorizzazione di $\overline{f}(x)$ in $\mathbb{Z}_{101}[x]$.

□

Esercizio (Traccia N.92, 10 settembre 2018)**.**
Sia p un numero primo positivo.

(a) Dire per quali p il polinomio $f(x) = x^{p^3} + x^{p^2} + x^p + \overline{1} \in \mathbb{Z}_p[x]$ si spezza in $\mathbb{Z}_p[x]$ nel prodotto di fattori lineari.

(b) Dire per quali p il polinomio $g(x) = x^{p^3} + x^{p^2} + x^p \in \mathbb{Z}_p[x]$ si spezza in $\mathbb{Z}_p[x]$ nel prodotto di fattori lineari.

Svolgimento.

(a) Affinché $f(x)$ si spezzi nel prodotto di fattori lineari, esso deve avere almeno una radice in $\mathbb{Z}_p$. Sia α una siffatta radice. Allora, per il Piccolo Teorema di Fermat (17.23)

$$\overline{0} = f(\alpha) = \alpha^{p^3} + \alpha^{p^2} + \alpha^p + \overline{1} \iff \overline{3}\alpha = -\overline{1}.$$

Ciò è chiaramente un assurdo nel caso $p = 3$, in cui risulterebbe $\overline{0} = -\overline{1}$. Dunque, in questo caso, $f(x)$ non si spezza sicuramente nel prodotto di fattori lineari, perché non ha radici in $\mathbb{Z}_3$.

Se, invece $p \neq 3$, $f(x)$ ha esattamente una radice in $\mathbb{Z}_p$, ossia $\alpha = -\overline{3}^{-1}$.

Tuttavia, se $f(x)$ si spezzasse nel prodotto di fattori lineari, si dovrebbe avere necessariamente

$$f(x) = (x - \alpha)^{p^3}.$$

Ma, alla luce della Proprietà 8, $(x-\alpha)^{p^3} = x^{p^3} - \alpha^{p^3} = x^{p^3} - \alpha \neq f(x)$.

Dunque $f(x)$ non si spezza nel prodotto di fattori lineari in $\mathbb{Z}_p$ per alcun primo p.

(b) Ragioniamo come nel caso precedente. Se $\alpha \in \mathbb{Z}_p$ è una radice di $g(x)$ in $\mathbb{Z}_p$, allora

$$\overline{0} = g(\alpha) = \alpha^{p^3} + \alpha^{p^2} + \alpha^p \iff \overline{3}\alpha = \overline{0}.$$

Se $p \neq 3$, ciò implica che l'unica radice di $g(x)$ in $\mathbb{Z}_p$ è la classe nulla.

In tal caso, se $g(x)$ si spezzasse nel prodotto di fattori lineari, si avrebbe $g(x) = x^{p^3}$, che è chiaramente un assurdo.

Se $p = 3$, allora ogni elemento di $\mathbb{Z}_3$ è radice di $g(x)$. Dobbiamo pertanto ragionare sul caso particolare.

Osserviamo che, in base alla Proprietà 8, possiamo scrivere

$$g(x) = (x^9 + x^3 + x)^3 = x^3(x^8 + x^2 + \overline{1})^3.$$

Dunque, $g(x)$ si spezza in $\mathbb{Z}_3[x]$ nel prodotto di fattori lineari se e solo se lo stesso vale per $h(x) = x^8 + x^2 + \overline{1} \in \mathbb{Z}_3[x]$.

Come abbiamo già visto, sia $\overline{1}$ sia $-\overline{1}$ sono radici di $h(x)$.

Dunque, per il Teorema di Ruffini (12.5), $(x - \overline{1})(x + \overline{1}) = x^2 - \overline{1} | h(x)$ in $\mathbb{Z}_p[x]$.

Svolgendo la divisione, risulta

$$h(x) = (x^2 - \overline{1})(x^6 + x^4 + x^2 - \overline{1}).$$

Come è immediato verficare, né $\overline{1}$ né $-\overline{1}$ sono radici di $x^6 + x^4 + x^2 - \overline{1}$.

Ciò prova che il polinomio $x^6 + x^4 + x^2 - \overline{1}$, essendo privo di radici in $\mathbb{Z}_3$, non può spezzarsi in $\mathbb{Z}_3[x]$ nel prodotto di fattori lineari. Conseguentemente, non può spezzarsi $h(x)$ e quindi $g(x)$.

Segue che, anche in questo caso, $g(x)$ non si spezza nel prodotto di fattori lineari in $\mathbb{Z}[x]$ per alcun p.

□

Esercizio (Traccia N.93, 25 settembre 2018)**.**
Sia p un numero primo positivo.

(a) Determinare, al variare di p, il numero delle radici (distinte) in $\mathbb{Z}_p$ del polinomio $f(x) = x^{(p+1)^2} - \overline{1} \in \mathbb{Z}_p[x]$.

(b) Determinare un massimo comune divisore dei polinomi $g(x) = x^{7056} - \overline{1}$, $h(x) = x^3 - \overline{2}x^2 - x + \overline{2} \in \mathbb{Z}_{83}[x]$.

Svolgimento.

(a) Osserviamo che la classe nulla non è certamente radice di $f(x)$. Supponiamo che $\alpha \in \mathbb{Z}_p^*$ sia una radice di $f(x)$. Allora, utilizzando il Piccolo Teorema di Fermat (17.23), si ha

$$\begin{aligned} f(\alpha) = \overline{0} &\iff \alpha^{(p+1)^2} = \overline{1} \iff \alpha^{p^2}\alpha^{2p}\alpha = \overline{1} \\ &\iff \alpha\alpha^2\alpha = \overline{1} \iff \alpha^4 = \overline{1}. \end{aligned}$$

Dunque, in virtù della Proposizione 17.16, $\alpha \in \mathbb{Z}_p^*$ è radice di $f(x)$ se e solo se $o(\alpha)|4$, cioè se e solo se $o(\alpha) \in \{1, 2, 4\}$.

Ora, la Proprietà 6 stabilisce che, se $2 \nmid p - 1$, non c'è, in $\mathbb{Z}_p^*$, alcun elemento di periodo 2, né tantomeno di periodo 4 (visto che, se $2 \nmid p-1$,

lo stesso vale a maggior ragione per 4). Questa eventualità si presenta solo quando $p = 2$. In tal caso, l'unico periodo ammissibile per una radice di $f(x)$ è 1, e vi è un solo elemento di periodo 1, ossia $\overline{1}$, che è, quindi, l'unica radice di $f(x)$ in $\mathbb{Z}_2$.

Ora, se $p > 2$, sicuramente $2|p-1$. Dunque vi è, sempre per la Proprietà 6, $\varphi(2) = 1$ elemento di periodo 2 (cioè $-\overline{1}$), che è quindi un'ulteriore radice di $f(x)$. Se $4 \nmid p - 1$, non ci sono elementi di periodo 4, e, pertanto ci sono esattamente due radici distinte di $f(x)$ in $\mathbb{Z}_p$.

Infine, se $4|p - 1$, possiamo trovare, oltre alle radici $\overline{1}$ (periodo 1) e $-\overline{1}$ (periodo 2), altri $\varphi(4) = 2$ elementi di periodo 4, portando a 4 il numero delle radici distinte di $f(x)$ in $\mathbb{Z}_p$.

Riassumendo, il numero di radici distinte di $f(x)$ in $\mathbb{Z}_p$ è

- 1 se $p = 2$;
- 2 se $p > 2$ e $4 \nmid p - 1$ (ossia, se $p \equiv 3 \bmod 4$);
- 4 se $4|p - 1$ (ossia, se $p \equiv 1 \bmod 4$).

(b) Osserviamo che $(83+1)^2 = 7056$. Dunque, $g(x)$ è il polinomio $f(x)$ del punto precedente nel caso $p = 83$. Visto che $4 \nmid 83 - 1 = 82$, $g(x)$ ha esattamente due radici distinte, ossia $\pm\overline{1}$.

Ora,

$$\begin{aligned} h(x) &= x^3 - \overline{2}x^2 - x + \overline{2} = x(x^2 - \overline{1}) - \overline{2}(x^2 - \overline{1}) \\ &= (x - \overline{2})(x^2 - \overline{1}) = (x - \overline{2})(x - \overline{1})(x + \overline{1}) \end{aligned}$$

è una fattorizzazione di $h(x)$ in $\mathbb{Z}_{83}[x]$, da cui leggiamo che anche $h(x)$ ha come radici $\pm\overline{1}$.

Per il Teorema di Ruffini (12.5), $(x-\overline{1})(x+\overline{1})$ divide sia $g(x)$ sia $h(x)$, e quindi divide anche il loro massimo comune divisore.

Pertanto, $\mathrm{MCD}(g(x), h(x)) = (x - \overline{1})(x + \overline{1})$.

Infatti, se così non fosse, l'unica ulteriore possibilità è che $\mathrm{MCD}(g(x), h(x)) = h(x)$, ma in tal caso il fattore $x - \overline{2}$ dovrebbe dividere $g(x)$, il che è

escluso per il Teorema di Ruffini (12.5), visto che $\overline{2}$ non è una radice di $g(x)$.

□

Lista delle tracce svolte

Sono presenti, all'interno del lavoro, gli svolgimenti di 17 tracce (per un totale di 51 esercizi).

- Traccia N.61, proposta in data 19 luglio 2015;
- Traccia N.65, proposta in data 15 gennaio 2016;
- Traccia N.72, proposta in data 12 settembre 2016;
- Traccia N.80, proposta in data 21 giugno 2017;
- Traccia N.81, proposta in data 5 luglio 2017;
- Traccia N.82, proposta in data 11 settembre 2017;
- Traccia N.83, proposta in data 25 settembre 2017;
- Traccia N.84, proposta in data 6 novembre 2017;
- Traccia N.85, proposta in data 9 gennaio 2018;
- Traccia N.86, proposta in data 24 gennaio 2018
- Traccia N.87, proposta in data 8 febbraio 2018;
- Traccia N.88, proposta in data 20 aprile 2018;
- Traccia N.89, proposta in data 5 giugno 2018;
- Traccia N.90, proposta in data 20 giugno 2018;

- Traccia N.91, proposta in data 5 luglio 2018;
- Traccia N.92, proposta in data 10 settembre 2018;
- Traccia N.93, proposta in data 25 settebre 2018.

Bibliografia

[1] M.Barile, Dispense di Algebra, Versione 2017/2018.