1^o **ESONERO DI ALGEBRA**
(Studenti di Informatica — canale D'Andrea)
7 novembre 2018

Cognome e Nome: Matricola:

☐ L'iniziale del mio cognome è compresa tra A e L.

---

1. Dire quali dei seguenti sottoinsiemi $H \subset G$ siano sottogruppi:
- $G = (\mathbb{Z}, +)$, $H = \{0. \pm 2^n \mid n \in \mathbb{N}\} = \{0. \pm 1, \pm 2, \pm 4, \pm 8, \dots\}$;
- $G = \mathrm{S}_6$, $H = \{\mathrm{id}, (1\,4)(2\,5)(3\,6), (1\,3\,5)(2\,4\,6), (1\,5\,3)(2\,6\,4), (1\,2\,3\,4\,5\,6), (1\,6\,5\,4\,3\,2)\}$;
- $G = \mathbb{Z}_{13}^{\times}$, $H = \{[1], [5], [8], [12]\}$.

e quali di tali sottogruppi siano ciclici.

Soluzione:
- Sappiamo che i sottogruppi $\neq \{0\}$ di $(\mathbb{Z}, +)$ sono generati dal loro minimo elemento positivo. Poiché $1 \in H$, se H fosse un sottogruppo di $(\mathbb{Z}, +)$ dovrebbe coincidere con $\mathbb{Z}$, ma così non è. In conclusione, H non è un sottogruppo.
- H contiene tutte e sole le potenze di $(1\,2\,3\,4\,5\,6)$ ed è pertanto il sottogruppo (ciclico) generato da tale elemento.
- Si calcola facilmente:
  - $5^2 = 25 \equiv 12 \mod 13$;
  - $5^3 \equiv 12 \cdot 5 = 60 \equiv 8 \mod 13$;
  - $5^4 = (5^2)^2 \equiv 12^2 \equiv (-1)^2 = 1 \mod 13$.

  Pertanto H è il sottogruppo di $\mathbb{Z}_{13}^{\times}$ generato da $[5]$. In particolare è un sottogruppo, ed è ciclico.

2. Decidere se i seguenti elementi siano moltiplicativamente invertibili in $\mathbb{Z}_{105}$. In caso affermativo, calcolarne inverso e ordine; altrimenti, spiegare perché non siano invertibili.
- $[91]$;
- $[43]$;
- $[57]$.

Soluzione: I numeri coinvolti sono piccoli, ed è facile fattorizzarli nel prodotto di primi. Poiché $105 = 3 \cdot 5 \cdot 7$, $91 = 7 \cdot 13$, $57 = 3 \cdot 19$, mentre 43 è primo, vediamo che $\mathrm{MCD}(43, 105) = 1$, mentre $\mathrm{MCD}(91, 105) = 7, \mathrm{MCD}(57, 105) = 3$. Di conseguenza, $[91]$ e $[57]$ non appartengono a $\mathbb{Z}_{105}^{\times}$, mentre $[43]$ sì.

L'inverso $[x]$ di $[43]$ si trova producendone l'identità di Bézout, oppure calcolandone l'inverso modulo $3, 5, 7$. Poiché

$$43 \equiv 1 \mod 3, \qquad 43 \equiv 3 \mod 5, \qquad 43 \equiv 1 \mod 7,$$

ricordando che l'inverso di $[3]$ in $\mathbb{Z}_5$ è $[2]$, x dovrà essere soluzione del sistema di congruenze

$$\begin{cases} x \equiv 1 \mod 3 \\ x \equiv 2 \mod 5 \\ x \equiv 1 \mod 7. \end{cases}$$

La soluzione, per il teorema cinese dei resti, è unica modulo 105; si vede abbastanza facilmente che $x = 22$ soddisfa il sistema. Pertanto l'inverso di $[43]$ in $\mathbb{Z}_{105}$ è $[22]$.

3. Dire se i seguenti elementi x, y siano coniugati nel gruppo G:
- $x = (1\,2)(3\,4)$, $y = (1\,3)(2\,4)$, $G = \mathrm{A}_5$;
- $x = (1\,3\,5)(2\,4)$, $y = (1\,4)(2\,5\,3)$, $G = \mathrm{S}_5$;
- $x = s$, $y = sr$, $G = \mathrm{D}_6$ [qui s indica una simmetria e r la rotazione di 60 gradi];
- $x = [2]$, $y = [9]$, $G = \mathbb{Z}_{11}^{\times}$.

Soluzione:
- I due elementi sono sicuramente coniugati in S_5 poiché hanno la stessa struttura ciclica; sono coniugati anche in A_5 poiché commutano con permutazioni dispari di S_5. Ad esempio, x commuta con $(1\,2)$.
  Volendo essere più espliciti, $(1\,2)(3\,4) = (1\,2\,4)^{-1} \circ (1\,3)(2\,4) \circ (1\,2\,4)$.
- Le due permutazioni hanno la stessa struttura ciclica, e sono quindi coniugate in S_5.
- L'elemento s commuta con $\{1, s, r^3, sr^3\}$ e ha quindi al più $|\,\mathrm{D}_6\,|/4 = 12/4 = 3$ coniugati. Si vede subito che $r^{-1}sr = sr^2$, mentre $r^{-2}sr^2 = sr^4$. Ma allora gli unici coniugati di s sono i tre elementi s, sr^2, sr^4, e sr non è coniugato a s.
- Il gruppo $\mathbb{Z}_{11}^{\times}$ è abeliano, e quindi ogni elemento ha se stesso come unico coniugato. Due elementi diversi non sono quindi coniugati.

4. Date le permutazioni $\sigma = (1\,5\,3)(2\,4\,7\,6), \tau = (3\,4\,8\,5) \in \mathrm{S}_8$, calcolare $(\sigma\tau)^{20}$. Qual è l'ordine di $\sigma, \tau, \sigma\tau$? Sono permutazioni pari o dispari?

Soluzione:

Intanto, sia σ che τ sono permutazioni dispari. In effetti, un n-ciclo è pari se n è dispari ed è dispari se n è pari; pertanto un 3-ciclo è pari, mentre un 4-ciclo è dispari. Ma allora τ è dispari, mentre σ è prodotto di una permutazione pari e di una dispari ed è quindi dispari (le parità si sommano!). Di conseguenza $\sigma\tau$ sarà pari, in quanto prodotto di permutazioni dispari.

L'ordine di una permutazione è il minimo comune multiplo delle lunghezze dei suoi cicli disgiunti. Di conseguenza σ ha ordine 12 e τ ha ordine 4. Si calcola facilmente che $\sigma\tau = (1\,5)(2\,4\,8\,3\,7\,6)$ e quindi $\sigma\tau$ ha ordine 6. Calcolare $(\sigma\tau)^{20}$ è allora semplice:

$$(\sigma\tau)^{20} = ((\sigma\tau)^6)^3(\sigma\tau)^2 = (1\,5)^2(2\,4\,8\,3\,7\,6)^2 = (2\,8\,7)(3\,6\,4).$$

5. Risolvere il sistema di congruenze

$$\begin{cases} 4x \equiv 6 \mod 14 \\ 15x \equiv 10 \mod 25 \end{cases}$$

Soluzione:

Riduciamo il sistema a forma normale. La congruenza $4x \equiv 6 \mod 14$ è compatibile, poiché $\mathrm{MCD}(4, 14) = 2$ divide 6. E' allora equivalente alla congruenza $2x \equiv 3 \mod 7$, e ricordando che l'inverso di 2 modulo 7 è 4, tale congruenza è equivalente a $x \equiv 12 \equiv 5 \mod 7$.

Anche la seconda congruenza è compatibile, in quanto $\mathrm{MCD}(15, 25) = 5$ divide 10, ed è equivalente alla congruenza $3x \equiv 2 \mod 5$. Qui l'inverso di 3 modulo 5 è 2, e moltiplicando entrambi i membri per 2 si ottiene $x \equiv 4 \mod 5$. Il sistema originario è quindi equivalente a:

$$\begin{cases} x \equiv 5 \mod 7 \\ x \equiv 4 \mod 5. \end{cases}$$

A questo punto, voi calcolate la soluzione in uno dei tanti modi visti a lezione; io invece mi accorgo che 19 soddisfa entrambe le congruenze del sistema, e posso utilizzare il teorema cinese dei resti per affermare che la soluzione è $x \equiv 19 \mod 35$.

Tutte le risposte vanno giustificate. Risposte prive di giustificazione non verranno valutate.