mod

Corso di Studi in Informatica
Matematica Discreta

Prova scritta 15 Giugno 2020

Esercizio 1. 1. (Punti 4) Verificare che $\mathrm{MCD}(142, 112) = 2$ e determinare la corrispondente identità di Bezout.

2. (Punti 4) Determinare l'inversa moltiplicativa di $\overline{56}$ in $\mathbb{Z}_{71}$.

3. (Punti 4) Elencare esplicitamente i generatori del gruppo additivo $(\mathbb{Z}_{18}, +)$.

Soluzione.

1. L'algoritmo di divisione euclidea fornisce

$$\begin{aligned} 142 &= 112 + 30 \\ 112 &= 3 \cdot 30 + 22 \\ 30 &= 22 + 8 \\ 22 &= 2 \cdot 8 + 6 \\ 8 &= 6 + 2 \\ 6 &= 3 \cdot 2 + 0 \end{aligned}$$

confermando che $\mathrm{MCD}(142, 112) = 2$. Invertendo la procedura si ottiene l'identità di Bezout

$$2 = 15 \cdot 142 - 19 \cdot 56.$$

2. Dividendo per 2 l'identità del punto precedente si ottiene subito

$$1 = 15 \cdot 71 - 19 \cdot 112$$

da cui $[56]_{71}^{-1} = [-19]_{71} = [52]_{71}$.

3. I generatori di $\mathbb{Z}_{18}$ sono $\{\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}\}$.

Esercizio 2. Consideriamo la permutazione $\pi = (3\ 7\ 8)(2\ 3\ 5)(1\ 4\ 5\ 6\ 9)(7\ 9) \in \mathcal{S}_9$

1. (Punti 4) Determinare tipo, periodo e parità di π.

2. (Punti 4) Qual è il più piccolo $k > 0$ tale che π^k è un ciclo?

3. (Punti 4) Dimostrare che la funzione $f : \langle \pi \rangle \to \mathbb{Z}_8$, $f(\pi^t) = \overline{2t}$ è un omomorfismo ben definito. È iniettiva? È suriettiva?

Soluzione.

1. La decomposizione in cicli disgiunti di π è

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

Dunque il tipo è $(5, 4)$, il periodo 20 e la permutazione è dispari.

2. Si ha che $\pi^k = (1\ 4\ 2\ 7)^k(3\ 5\ 6\ 9\ 8)^k$ è un ciclo quando uno dei due fattori è l'identità e l'altro è un ciclo. Il più piccolo valore per cui questo accade è $k = 4$.

3. Ricordando che il periodo di π è 20 per verificare che f è ben definita basta osservare che se 20 divide $s - t$ allora 8 divide $2s - 2t = 2(s - t)$ ed è un omomorfismo perché

$$f(\pi^s \circ \pi^t) = f(\pi^{s+t}) = \overline{2(s+t)} = \overline{2s} + \overline{2t} = f(\pi^s) + f(\pi^t).$$

Non è iniettivo perché il dominio ha più elementi del codominio e non è suriettivo perchè le classi $\overline{n}$ con n dispari non sono nell'immagine di f.