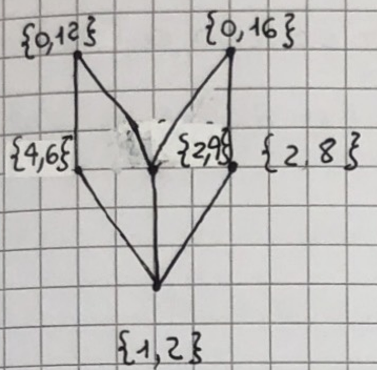
TRACCIA - 15 LUGLIO 2024

Esercizio 1

(i)



Credevo fosse sbagliato

~~Sicuramente non è un reticolo in quanto non per ogni coppia di elementi non confrontabili è possibile definire l'estremo inferiore e superiore. Ad esempio, per {4,6} e {2,8} non c'è l'estremo superiore.~~

~~(ii)~~

~~Non è possibile determinarlo.~~

(iii)

$a \in A$ è un minorante di $\{1,4\}$ $\iff$ $a \,\sigma\, \{1,4\}$ $\iff$ $\forall x \in a \,(\forall y \in \{1,4\}\,(x \text{ divide } y))$.

Non esiste tale elemento. Dunque $\{1,4\}^{\downarrow} = \emptyset$.

L'estremo inferiore è il massimo dei minoranti. Ma dato che abbiamo detto che l'insieme dei minoranti di $\{1,4\}$ è vuoto, allora non ci sarà $\inf(\{1,4\}, \{1,6\})$.

L'estremo superiore invece è il minimo dei maggioranti. Il m.c.m $(4,6) = 12$. Quindi bisogna prendere una coppia con una coordinata che sia almeno 12. L'altra coordinata la prendiamo con il minimo valore multiplo di 12. Questo valore è 0. Quindi il $\sup(\{1,4\}, \{1,6\}) = \{0,12\}$.

(iv)

Il minimo e massimo non esistono. Gli elementi minimali sono tutti gli insiemi del tipo $\{1,p\}$, con p primo. Mentre gli elementi massimali sono solo $\{1,-1\}$ perché non esiste nessun elemento in A tale che $\{1,-1\} \,\sigma\, \{x,y\}$. (Dubbio sul massimale)

(v)

Aggiungendo l'insieme $\{0,48\}$, $B \cup \{0,48\}$ diventa un reticolo.

Esercizio 2

Un'equazione congruenziale del tipo $ax \equiv_m b$ ha soluzione se e solo se il MCD(a,m) divide b.

Per questo, l'equazione congruenziale ha soluzione per $c \in \{20, 60, [illegible]\}$.

Per $c = 20$, otteniamo $470x \equiv_{350} 60 \iff 47x \equiv_{35} 6$. Usiamo l'algoritmo di Euclide:

$$
\begin{aligned}
47 &= (1)35 + 12 & \quad 12 &= (1)47 + (-1)35 \\
35 &= (2)12 + 11 & \Rightarrow \quad 11 &= (1)35 + (-2)12 \\
12 &= (1)11 + 1 & \Rightarrow \quad 1 &= (1)12 + (-1)11 \\
11 &= (11)1 + 0
\end{aligned}
$$

$$1 = (1)12 + (-1)11 =$$

$$= (1)47 + (-1)35 + (-1)35 + (2)12$$

$$= (1)47 + (-2)35 + (2)47 + (-2)35 = (3)47 + (-4)35$$

Moltiplichiamo ambo i membri dell'equazione per 3:

$x \equiv_{35} \overline{18} \Rightarrow$ L'insieme delle soluzioni è dato da $\{n \in \mathbb{Z} \,/\, n = \overline{18} + \overline{35}k, k \in \mathbb{Z}\}$

Per $c = 60$ facciamo lo stesso procedimento:

$470x \equiv_{350} 180 \Rightarrow 47x \equiv_{35} 18$.

Moltiplicando ambo i membri per 3 otteniamo:

$x \equiv_{35} 19. \Rightarrow$ Insieme soluzioni è dato da $\{n \in \mathbb{Z} \,/\, n = \overline{19} + \overline{35}k, k \in \mathbb{Z}\}$.

~~Per $c = 55$: $470x \equiv_{350} 165$ => dividendo per 5 => $94x \equiv_{70} 33$.~~

~~$94 = (1)70 + 24$~~
~~$70 = (2)24 + 22$~~
~~$24 = (1)22 + 2$~~
~~$22 = (11)2 + 0$~~

Esercizio 3

(a)

È dato dal coefficiente binomiale $\binom{13}{8} = \dfrac{13!}{8!(13-8)!}$ *

(b)

Il risultato è 0 in quanto $|S| = 13 < 18$.

(c)

$\binom{12}{6}$ perché, fissato h, restano da scegliere 6 elementi dagli altri 12.

(d)

$2^{13} \times 2^{13} = 2^{169}$. Questo perché una relazione binaria è un sottoinsieme del prodotto cartesiano $S \times S$, che ha $13 \times 13 = 169$ elementi.

Esercizio 4

$(\mathbb{Z}, *)$ è un semigruppo se $*$ è associativa. Ovvero se $\forall a, b, c \in \mathbb{Z}$ vale $(a * (b * c)) = ((a * b) * c)$.

$a * (b * c) = a * (3b + c) = 3a + 3b + c$

$(a * b) * c = (3a + b) * c = 9a + 3b + c$

Non è un semigruppo, quindi non sarà neanche un gruppo e un monoide.
Facendo la stessa verifica per $(\mathbb{Z}_3, *)$ e $(\mathbb{Z}_6, *)$ vediamo che entrambi sono semigruppi.

Per verificare che sono monoidi, dobbiamo verificare che esista l'elemento neutro a sinistra e a destra. Per $(\mathbb{Z}_3, *)$ dobbiamo trovare $x \in \mathbb{Z}_3$ tale che $\forall a \in \mathbb{Z}_3 \; (x * a = a * x = a)$

$x * a = 3x + a = a \iff \overline{3}x + a \equiv_3 a \iff \overline{3}x \equiv_3 0 \iff x \equiv_3 0$.

Vediamo se 0 è neutro anche a destra:

$a * x = 3a + 0 = 3a \neq a$.

Quindi $(\mathbb{Z}_3, *)$ è un semigruppo che ha elemento neutro solo a sinistra, ma non è un monoide e di conseguenza neanche un gruppo.

Per $(\mathbb{Z}_6, *)$ invece

$x * a = 3x + a = a \iff 3x + a \equiv_6 a \iff 3x \equiv_6 0 \iff x \equiv_3 0$.

0 non è neutro a destra, quindi $(\mathbb{Z}_6, *)$ è un semigruppo con elemento neutro a sinistra ma non a destra, quindi non è un monoide e di conseguenza neanche un gruppo.

Esercizio 5

(i)

$\overleftarrow{f}(\{10\}) = 6$ perché $f(6) = 2 + 3 + 5$.

$\overleftarrow{f}(\{11\}) = \emptyset$

(ii)

Non è suriettiva in quanto abbiamo visto che $\overleftarrow{f}(\{11\}) = \emptyset$.

Non è neanche suriettiva in quanto esistono elementi del dominio che hanno la stessa immagine. Ad esempio: $f(4) = 2 + 3 = 5$ e $f(3) = 2 + 3 = 5$.

Di conseguenza non è neanche biettiva.

(iii)

$[8]_R = \{x \in S / \ x \, R \, 8 \iff f(x) = f(8)\}$

$f(8) = 2 + 3 + 5 + 7 = 17.$

Se bisogna essere più specifici $[8]_R = \{7\}$.

(iv)

Poichè è sempre possibile prendere numeri primi man mano sempre maggiori (in quanto $\mathbb{N}$ è infinito), allora $|S/R|$ è infinito.

(v)

$a \in [a]_R \iff a = f(a)$

Questo capita solo per 2. Infatti $f(2) = 2$. Per valori x maggiori di 2, $f(x)$ è strettamente maggiore di x. Quindi sì, esistono tali elementi.

(vi)

$f(10) = 17$, $f(11) = 28$ $\quad f(12) = 28$ $\quad f(13) = 41$ $\quad f(14) = 41$

$f(15) = 41$ $\quad f(16) = 41$ $\quad f(17) = 58$ $\quad f(18) = 58$ $\quad f(19) = 77$

$f(20) = 77.$

$[10]_{R_T} = \{10\}$

$[11]_{R_T} = [12]_{R_T} = \{11, 12\}$

$[13]_{R_T} = [14]_{R_T} = [15]_{R_T} = [16]_{R_T} = \{13, 14, 15, 16\}$

$[17]_{R_T} = [18]_{R_T} = \{17, 18\}$

$[19]_{R_T} = [20]_{R_T} = \{19, 20\}.$

$T/R_T = \{[10]_{R_T}, [11]_{R_T}, [13]_{R_T}, [17]_{R_T}, [19]_{R_T}\} \Rightarrow |T/R_T| = 5$

Esercizio 6

(i)

(a) Vero per il teorema del resto.

(b) Falso perchè non vale per tutti gli anelli commutativi unitari.

(c) Vero per il teorema di Ruffini generalizzato, in cui A è un dominio di integrità.

(ii)

Non ne ho idea.

(iii)

(a) Nessuno. ($p^0 q^1 r^0 \Rightarrow$ grado 1 $\times$; $p^1 q^1 r^0 \Rightarrow$ grado 2 $\times$; via via così)

(b) Solo pq.

(c) pqr danno grado 6, quindi non vanno bene.
pr e qr danno grado 5.

Ogni divisore è nella forma λpr o λqr, con $\lambda \in \mathbb{Z}_{13}$.

Ci sono 12 scelte di λ in λpr e 12 in λqr. Quindi ci sono 24 divisori di grado 5.

↳ Non ne sono per niente sicura.