PROVA SCRITTA 15 GENNAIO 2024

Esercizio 1. Scrivere una negazione della seguente formula in cui non appaia il connettivo di implicazione: $\exists y(\forall x((\varphi(x) \wedge \psi(y)) \to (\psi(y) \to \theta(x))))$

$$\neg\Big(\exists y(\forall x((\varphi(x) \wedge \psi(y)) \to (\psi(y) \to \theta(x))))\Big) = \forall y \neg \Big(\forall x((\varphi(x) \wedge \psi(y)) \to (\psi(y) \to \theta(x)))\Big) =$$
$$= \forall y(\exists x(\neg((\varphi(x) \wedge \psi(y)) \to (\psi(y) \to \theta(x))))) = \forall y(\exists x((\varphi(x) \wedge \psi(y)) \wedge \neg(\psi(y) \to \theta(x))))$$
$$= \forall y(\exists x((\varphi(x) \wedge \psi(y)) \wedge (\psi(y) \wedge \neg\theta(x))))$$

Il risultato ottenuto è $\forall y(\exists x((\varphi(x) \wedge \psi(y)) \wedge (\psi(y) \wedge \neg(\theta(x)))))$

✓ CORRETTO

Esercizio 2. Dare una definizione di partizione di un insieme ed enunciare il teorema fondamentale su partizioni e relazioni di equivalenza. Fornire una partizione di $\mathbb{Z}$ di cardinalità 2^{10}

Definizione di partizione: Sia a un insieme ed $f \subseteq \mathcal{P}(A)$, f è una partizione di A se:

1) $(\forall x \in f)(x \neq \emptyset)$
2) $(\forall x, y \in f)(x \neq y \to x \cap y = \emptyset)$
3) $\bigcup f = a$

Teorema: Sia x un insieme. Esiste una funzione
$$f : \sim \in EQ(x) \longmapsto x/\!\sim \in \mathrm{PART}(x)$$
biiettiva, secondo cui per ogni relazione è possibile ricavare una partizione e per ogni partizione si ha una relazione

Esempio

2^{100} INSIEME COMPOSTO DA 2^{100} EL. È $\mathbb{Z}_{2^{100}}$

Una partizione di $\mathbb{Z}$ con cardinalità 2^{10} è $\mathbb{Z}_{2^{10}}$

Non potevo saperlo, è una regola sull'insieme delle classi di resto
Il teorema da vedere è: Caratterizzazione di $\mathbb{Z}_m$

Esercizio 3. Determinare i numeri naturali n tali che $2^n < n!$. Per quali insiemi finiti a si ha che $|P(a)| < |Sym(a)|$?

AD INTUITO (non basta)

$2^n < n!$

$n=0$	$1 < 1$	F
$n=1$	$2 < 1$	F
$n=2$	$4 < 2$	F
$n=3$	$8 < 6$	F
$n=6$	$64 <$	✓
$n=4$	$16 < 24$	✓
$n=5$	$32 < 120$	✓

Noto che $2^n < n!$ partendo da $n=4$ compreso. Lo devo dimostrare

PRINCIPIO DI INDUZIONE

CASO BASE: $n=4$ $\qquad 2^4 < 4! = 16 < 24$ ✓

Il caso base è verificato. Assumendo che l'ipotesi valga per n, vediamo se è vera anche per $n+1$

PASSO INDUTTIVO:
Ipotesi: $2^{n+1} = (n+1)!$

$$2^{m+1} = (m+1)! \iff 2^m \cdot 2 < (m+1)\,m!$$

$\hookrightarrow m! = m(m-1)!$ x definizione

$(m+1)! = m+1\,(m+\cancel{1}-\cancel{1}) = (m+1)\,m!$

Per il caso base, noi sappiamo che $2^m < m!$ e sappiamo anche che il numero minimo per cui vale l'operazione è $m=4$. Quindi sostituiamo $m=4$ nella parte restante della formula, cioè in $2 < m+1$ Poiché $m+1$ può essere massimo 5, allora 2 è sempre minore di $m+1$. Quindi formalmente:

$$(\forall m \in \mathbb{N})(m \geq 4 \to 2 < m+1)$$

e poiché per ipotesi induttiva sappiamo anche che $2^m < m!$, allora è vero anche $2^m \cdot 2 < (m+1)\,m!$

$\Rightarrow$ La formula è verificata $\{\forall m \in \mathbb{N} \mid m \geq 4\}$

Poiché $|P(a)| = 2^{|a|}$ e $|Sym(a)| = |a|!$ allora $|P(a)| < |Sym(a)|$ quando $|a| \geq 4$

Poiché $2^{|a|} < |a|!$ è in pratica lo stesso quesito di prima

Esercizio 4. Si consideri l'operazione

$*: (a,b) \in \mathbb{Z}_{10} \times \mathbb{Z}_{10} \mapsto \bar{6}a + b \in \mathbb{Z}_{10}$

i) Decidere se è associativa, commutativa, se $(\mathbb{Z}_{10}, *)$ ha elementi neutri a sx o a dx e, nel caso la domanda abbia senso, quali sono i suoi elementi simmetrizzabili. Che tipo di struttura algebrica è $(\mathbb{Z}_{10}, *)$?

ii) Siano $P: \{\bar{2}a \mid a \in \mathbb{Z}_{10}\}$ e $D: \mathbb{Z}_{10} \setminus P$. Per ciascuno di P e D decidere se è una parte chiusa rispetto a $*$ e, nel caso, rispondere, per la seguente struttura indotta, alle stesse domande del punto precedente per $(\mathbb{Z}_{10}, *)$

i) $*: (a,b) \in \mathbb{Z}_{10} \times \mathbb{Z}_{10} \mapsto \bar{6}a + b \in \mathbb{Z}_{10}$

- $*$ è commutativa?

$$(\forall a,b \in \mathbb{Z}_{10} \times \mathbb{Z}_{10})(a * b = b * a)$$

$a * b = \bar{6}a + b$

$b * a = \bar{6}b + a$

Poiché dalla definizione, l'operazione sembra non essere commutativa è meglio esplicitare un controesempio.

Prendo un qualsiasi elemento $a, b \in \mathbb{Z}_{10}$

$a = 1 \quad b = 2$

$a * b = \bar{6} \cdot \bar{1} + 2 = \bar{8} \quad \to \overline{13} \neq 8$

$b * a = \bar{6} \cdot \bar{2} + 1 = \overline{13}$

$\Rightarrow$ la struttura <u>NON</u> è commutativa

- $*$ è associativa?

$$(\forall a,b,c \in \mathbb{Z}_{10} \times \mathbb{Z}_{10})\,(a*(b*c) = (a*b)*c)$$

$$a*(b*c) = a*(\bar{6}b+c) = \bar{6}a + \bar{6}b + c$$
$$(a*b)*c) = (\bar{6}a+b)*c = \bar{6}(\bar{6}a+b)+c = \overline{36}a + 6b + c$$

($\overline{36} = \bar{6}$)

=> l'operazione è associative

- Elementi neutri

$$(\forall a \in \mathbb{Z}_{10})(a*u = a)$$
$$(\forall a \in \mathbb{Z}_{10})(u*a = a)$$

ATTENZIONE!!
Quando nelle operazioni ci sono le classi, allora per trovare i neutri si può provare a ridursi ad un equazione congruenziale

$$u*a = \bar{6}u + \cancel{a} = \cancel{a} = \bar{6}u = \bar{0}$$

-> questa può essere ridotta ad un'equazione congruenziale

Spiegazione:
$\bar{6}u = \bar{0}$ sono classi di $\mathbb{Z}_{10}$ e le possiamo scrivere così: $[6]_{10} \cdot [u]_{10} = [0]_{10}$

$[6u]_{10} = [0]_{10}$

Due classi sono uguali quando i rappresentanti sono in relazione tra loro e, poiché in questo caso la relazione è $\equiv_{10}$, allora $6u \equiv_{10} 0$

questa è l'equazione da risolvere

$6u \equiv_{10} 0$ MCD$(6,10)=2$ $2|0$ ✓

⇓

L'operazione ha soluzioni

TROVO IL MCD

$10 = 6 \cdot 1 + 4$

$6 = 4 \cdot 1 + 2$ -> MCD$(6,10)$

$4 = 2 \cdot 2 + 0$

SCRIVO I RESTI COME COMB LINEARE

$0 = 4 + 2(-2)$

$2 = 6 + 4(-1)$

$4 = 10 + 6(-1)$

SOSTITUISCO NELLA PRIMA COMB. LE ALTRE

$0 = 4 + \overline{2(-2)}$ -> sostituisco

$0 = 4 + (6 + 4(-1))(-2)$

$0 = 4 + 6(-2) + 4(2)$

$0 = 6(-2) + \overline{4(3)}$ -> sostituisco

$0 = 6(-2) + (10 + 6(-1))(3)$

$0 = 6(-2) + (10(3) + 6(-3))$

$0 = 6(-5) + 10(3)$

$0 = 10(3) + 6(-5)$ -> mi serve positivo $-5 +$ modulo

$-5 + 10 = 5$

$\bar{6} \cdot \bar{5}\, x \equiv_{10} \bar{0} \cdot \bar{5}$ $\qquad 6u \equiv_{10} 0$

$\bar{1} x \equiv_{10} \bar{0} \quad \longrightarrow \quad x \equiv_{10} \bar{0}$

Proviamo:

$\bar{6} \cdot \bar{0} \equiv_{10} \bar{0}$

$\bar{0} \equiv_{10} \bar{0}$ ✓

=> L' elemento neutro a sinistra è $\bar{0}$

$a * u = \bar{6}a + u = a \;\longrightarrow\; \underline{-\bar{5}a = u}$ -> questa non si può trasformare in un'equazione congruenziale perché ha 2 incognite che sono u e a

Vediamo comunque (x intuizione) se possiamo ricavarne qualcosa

$-\bar{5}a = u \;\Leftrightarrow\; [-5]_{10} \cdot [a]_{10} = [u]_{10} \;\Leftrightarrow\; \bar{5}a = u$ $\qquad -5+10 = 5$ rappresentante

A questo punto sostituisco ad a gli elementi di $\mathbb{Z}_{10}$. Posso farlo perché è un insieme finito

$a = 0 \qquad \bar{5} \cdot \bar{0} = u \;\rightarrow\; u = \bar{0}$

$a = 1 \qquad \bar{5} \cdot \bar{1} = u \;\rightarrow\; u = \bar{5}$

$a=2$ $\quad \bar{5}\cdot\bar{2}=u \quad \to u=\overline{10} \quad$ (HA) $\overline{10}=\bar{0}$ $\to 10-10=\bar{0}$

$a=3$ $\quad \bar{5}\cdot\bar{3}=u \quad \to u=\overline{15} \quad$ (HA) $\overline{15}=\bar{5}$ $\to 15-10=5$

$a=4$ $\quad \bar{5}\cdot\bar{4}=u \quad \to u=\overline{20} \quad$ (HA) $\overline{20}=\bar{0}$ $\to 20-10=\overline{10}=\bar{0}$

Notiamo quindi che se a è pari, il neutro è $\bar{0}$
se a è dispari, il neutro è $\bar{5}$

$\Rightarrow$ NON ESISTE ELEMENTO NEUTRO POICHÉ
neutro dx non esiste

$\Rightarrow$ NON HA SENSO CHIEDERSI SE CI SONO
ELEMENTI SIMMETRIZZABILI

$\Rightarrow$ La struttura è un SEMIGRUPPO

ii) Per riconoscere se un insieme è parte chiusa di un'operazione, innanzitutto dobbiamo riconoscere gli elementi di cui è composto l'insieme

$P=\{\bar{2}a \mid a\in \mathbb{Z}_{10}\}$ $\to$ Notiamo essere l'insieme dei numeri pari in $\mathbb{Z}_{10}$, cioè $\{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8}\}$

$D=\mathbb{Z}_{10}\setminus P$ $\to$ è l'insieme dei dispari in $\mathbb{Z}_{10}$, cioè $\{\bar{1},\bar{3},\bar{5},\bar{7},\bar{9}\}$

$$(\forall (a,b)\in P\times P)(*_{|P\times P}(a,b)\in P)$$

Se prendiamo un elemento $a,b\in P$ (cioè pari), allora
$a*b=\bar{6}a+b$ $\to$ Poiché so che la moltiplicazione tra 2 pari è ancora pari $[\bar{6}\cdot a]$ e che l'addizione è pari $\Rightarrow$ P è parte chiuse

Lo stesso ragionamento vale anche per D, cioè

$(\forall (a,b) \in D \times D)(*_{|D \times D}(a,b) \in D)$

Se prendo $a, b \in D$ (cioè dispari), allora
$a * b = \bar{6}a + b$ dispari · pari = pari pari + dispari = dispari
$\Rightarrow$ D è parte chiusa

Poiché P e D sono parti chiuse di $*$, allora la traccia ci chiede di porci le stesse domande poste ci in precedenza, cioè:
associatività, commutatività, neutri, simmetrizzabili.

$\Rightarrow$ Ci chiediamo se per $(P, *_{|P \times P})$ e $(D, *_{|D \times D})$ valgono queste cose.

Le parti stabili conservano associatività e commutatività, ma non neutri e simmetrizzabili

$\Rightarrow$ L'associatività non è necessario riprovarla perché è conservata.
$\Rightarrow$ Cambia, però, la commutatività: Vediamo

$(\forall (a,b) \in P)(a * b = b * a)$

$\left.\begin{array}{l} a * b = \bar{6}a + b \\ b * a = \bar{6}b + a \end{array}\right\}$ se sostituisco es. $a = 0$ $b = 2$ $\left\{\begin{array}{l} \bar{2} \\ \bar{12} \end{array}\right.$ ma $\bar{12} = \bar{2}$ $\Rightarrow$ Diventa commutativa

Vale anche per D, infatti:

$(\forall (a,b) \in D)(a * b = b * a)$

$\left.\begin{array}{l} a * b = \bar{6}a + b \\ b * a = \bar{6}b + a \end{array}\right\}$ Sostituisco $a = \bar{1}$ $b = \bar{3}$ $\left\{\begin{array}{l} \bar{6} + \bar{3} = \bar{9} \\ \overline{18} + 1 = \overline{19} \end{array}\right.$ ma $\overline{19} = \bar{9} \Rightarrow$ D diventa commutativa

Questi risultati ci aiutano nella ricerca degli elementi neutri
Infatti, nello studio fatto in precedenza sui neutri, abbiamo ottenuto che

se a è pari, il neutro è $\bar{0}$
se a è dispari, il neutro è $\bar{5}$

$\Rightarrow$ In $(P, *_{|P \times P})$ l'elemento neutro sarà 0 $\Rightarrow u = 0 \rightarrow$ e poiché l'operazione è commutativa, $u = 0$ è l'elemento neutro generico in P

$\Rightarrow$ In $(D, *_{|D \times D})$ il neutro è $\bar{5}$ (?)

Quindi, in questo caso possiamo cercare i simmetrizzabili
- CASO P

$(\forall (a,b) \in P)(a * b = u = b * a)$

$a * b = u \leftrightarrow \bar{6}a + b = \bar{0}$ Poiché P è piccolo sostituisco tutti i suoi elementi $\{0, 2, 4, 6, 8\}$

$a = 0 \rightarrow \bar{6} \cdot 0 + b = 0 \rightarrow b = \bar{0} \in P$

$a = 2 \rightarrow 6 \cdot 2 + b = 0 \rightarrow b = 0 - 12 = -\overline{12} \rightarrow -12 + 10 = -\bar{2} + \overline{10} = \bar{8} \in P$

$a = 4 \rightarrow 6 \cdot 4 + b = 0 \rightarrow b = -\overline{24} \rightarrow -24 + 10 =$

$a = 6 \rightarrow 6 \cdot 6 + b = 0 \rightarrow b = -\overline{36}$

$a = 8 \rightarrow 6 \cdot 8 + b = 0 \rightarrow b = -48$

TUTTI GLI ELEMENTI IN P SONO SIMMETRIZZABILI

• CASO D

$(\forall (a,b) \in D)(a * b = u = b * a)$

$a * b = u \Leftrightarrow \overline{6a} + b = \overline{5}$ Proviamo tutti gli elementi

$a = 1 \to 6 \cdot 1 + b = 5 \to b = 5 - 6 = -\overline{1} + 10 = \overline{9}$

$a = 3 \to 6 \cdot 3 + b = 5 \to b = 5 - 18 = -\overline{13} + 10 = -\overline{3} + 10 = \overline{7}$

$a = 5 \to 6 \cdot 5 + b = 5 \to b = 5 - 30 = -\overline{25} + 10 = -\overline{15} + 10 = -5 + 10 = \overline{5}$

$a = 7 \to 6 \cdot 7 + b = 5 \to b = 5 - 42$

TUTTI GLI ELEMENTI SONO SIMMETRIZZABILI

Esercizio 5.

Calcolare, utilizzando l'algoritmo euclideo, il MCD positivo tra 209 e 165 e trovare quindi tutte le soluzioni dell'equazione $209 \equiv_{165} 14$ e $165x \equiv_{209} 44$

Eseguo l'algoritmo delle divisioni successive (o euclideo) per trovare il MCD tra 209 e 165

$209 = 165 \cdot 1 + 44$

$165 = 44 \cdot 3 + 33$

$44 = 33 \cdot 1 + 11 \rightarrow MCD(209, 165)$

$33 = 11 \cdot 3 + 0$

Vedo se la 1ª equazione ha soluzioni

ma $MCD(209, 165) = 11 \wedge 11 \nmid 14 \Rightarrow$ NON CI SONO SOLUZIONI

Vedo se la 2ª equazione ha soluzioni

$MCD(209, 165) = 11 \quad 11 \mid 44 \Rightarrow$ L'EQUAZIONE HA SOLUZIONI

Risolvo la seconda equazione

1) Innanzitutto, se possibile, semplifico l'equazione

$165x \equiv_{209} 44 \quad = \quad \underline{15x \equiv_{19} 4}$ → risolvo questa equazione semplificata

2) Applico l'algoritmo delle divisioni successive sull'equazione semplificata per trovare il $MCD(15, 19)$

$19 = 15 \cdot 1 + 4$

$15 = 4 \cdot 3 + 3$

$4 = 3 \cdot 1 + 1 \to MCD(15, 19) = 1$

3) Scrivo i resti delle divisioni come combinazione lineare

$1 = 4 + 3(-1)$

$3 = 15 + 4(-3)$

$4 = 19 + 15(-1)$

4) A questo punto lo scopo è scrivere il MCD, cioè 1, come equazione lineare dei 2 termini, cioè $\overline{15}$ e $\overline{19}$. In quanto a me serve il coefficiente da porre vicino a $\overline{15}$, poiché il mio scopo è trovare l'INVERSO di 15 cosicché a sx mi resta solo la x. Quindi sostituisco nell'equazione del MCD

$1 = 4 + 3(-1)$ → sostituisco 3

$1 = 4 + (15 + 4(-3))(-1)$ → svolgo la moltiplicazione

$1 = 4 + 15(-1) + 4(3)$ → $4(1) + 4(3) = 4(3+1) = 4(4)$

$1 = 15(-1) + 4(4)$ → sostituisco 4

$1 = 15(-1) + (19 + 15(-1))(4)$ → svolgo il prodotto

$1 = 15(-1) + (19(4) + 15(-4))$ → $15(-1) + 15(-4) = 15(-5)$

$1 = 15(-5) + 19(4)$

5) Ho ottenuto i coefficienti di 15 e 19. ESSI DEVONO essere positivi => devo trovare il rappresentante positivo della classe -5. Esso è dato da $-\overline{5} + \overline{19} = \overline{14}$

Moltiplico 14 a dx e sx

$$\overline{15}\cdot\overline{14}\,x \equiv_{19} \overline{4}\cdot\overline{14}$$

$$\overline{1}\,x \equiv_{19} \overline{56}$$

rappresentante di 56 $\to$ $56 \mid 19$, $18 \mid 2$

$\overline{56} = 18$

$$\boxed{x \equiv_{19} \overline{18}}$$

6) Quindi se sostituisco $\overline{18}$ alla x mi trovo

$$\overline{15}\cdot\overline{18} \equiv_{19} \overline{4}$$

$$\overline{270} \equiv_{19} \overline{4}$$

rappresentante di 270 $\to$ $270 \mid 19$, 80, $4 \mid 14$

$\overline{270} = \overline{4}$

$$\overline{4} \equiv_{19} \overline{4} \checkmark$$

Esercizio 6. Siano F l'insieme delle parti finite non vuote di $\mathbb{N}$ e $f : x \in F \to \min x + \max x \in \mathbb{N}$

i) Spiegare perché f è ben posta

ii) Determinare $\overleftarrow{f}(\{2\})$ e $|\overleftarrow{f}(\{2\})|$

iii) Iniettiva, suriettiva, biettiva?

iv) Detto δ il nucleo di equivalenza di f. Determinare $[\{2\}]_\delta$

...

i) La funzione è ben posta, cioè $(\forall x \in F)(\exists! y \in \mathbb{N} \mid x f y)$

Ciò perché nel momento in cui abbiamo $x \in F$, $f(x)$ è un numero
$\Rightarrow$ è unico poiché naturale

$\forall x \in F$ esistono sia minimo che massimo, in quanto ogni elemento del dominio è una parte finita di $\mathbb{N}$ e, in quanto finita è superiormente limitata e poiché è superiormente limitata, ammette massimo. Inoltre l'insieme $\mathbb{N}$ è ben ordinato $\Rightarrow$ ogni sua parte non vuota ammette minimo

ii) $\overleftarrow{f}(\{2\}) = \{x \in F \mid f(x) = 2\} = \{x \in F \mid \underset{\substack{1\\2\\0}}{\min x} + \underset{\substack{1\\0\\2}}{\max x} = 2\} = \{\{0,2\}, \{0,1,2\}, \{1\}\}$

$|\overleftarrow{f}(\{2\})| = 3$

$\mathcal{P}(\mathcal{P}(\mathbb{N})) \supseteq \{\{1\} \{1,2\}\} \notin F$

iii) INIETTIVA

Ci dice che non è iniettiva il punto precedente, in quanto abbiamo preso tutti gli elementi di f (3) con stessa immagine

$\{\{1\}, \{2\}, \{3\}, \{4\}\} = 1 + 4 = 5$

$\{\{1,2\}, \{2\}\} = 2 + \{1,2\} = 5$

NO INIETTIVA $f(\{0,2\}) = f(\{0,1,2\}) = f(\{1\}) = 2$ ma $\{0,2\} \neq \{0,1,2\} \neq \{1\}$

SURRIETTIVA ✓

$m \in \mathbb{N}$ $\{0, m\} \to f(\{0,m\}) = \max\{0,m\} + \min\{0,m\} = m + 0 = m$

$\Rightarrow$ riesco a trovare sempre un valore per ogni elemento del codominio

iv) $[\{2\}]_{\delta} = \{x \in F \mid f(x) = f(\{2\})\} = \max\{2\} + \min\{2\}\} = \{x \in F \mid f(x) = 4\} =$
$\{\{0,4\}, \{0,1,4\}, \{0,1,2,4\}, \{0,1,2,3,4\}, \{1,3\}, \{1,2,3\}, \{2\}\}$

Relazione di divisibilità.

Se un numero | un altro numero es $1|2$
1 è il minimo

$$33^{3333} = 33 \cdot 33 \cdot \ldots \cdot 33$$

$3|33 \wedge 11/33$

$-3 \quad -11$

Sia ora τ la relazione d'ordine in F definita da:

$(\forall x, y \in F)(x \tau y \leftrightarrow (x = y) \vee f(x)$ è divisore proprio di $f(y))$

'positivo e diverso da se stesso cioè x

v) Determinare minimali, massimali, massimo e minimo. (F, τ) è un reticolo?

$X \subseteq F$ tale che $f(X) = 1$

$x \tau y$ se $f(y) \neq 1$

$x \in F$ e $f(x) = 1 \leftrightarrow \underbrace{\min x}_{0} + \underbrace{\max x}_{1} = 1 \leftrightarrow X = \{0, 1\}$

se $y \neq x \rightarrow f(y) \neq 1$ e $f(x) = 1 \mid f(y)$ propriamente

$\Rightarrow \{0,1\} \tau y \quad \forall y \in F \quad \rightarrow \{0,1\} = \min\{F, \tau\} \Rightarrow$ è l'unico minimale

Noi sappiamo anche che ogni intero diverso da 0 divide 0

$\Rightarrow$ se $b \neq 0$ e $b \in \mathbb{N} \Rightarrow b \mid 0$

Se consideriamo $f(\{0\}) = \min x + \max x = 0$ ed è l'unico ad avere 0 come immagine

$\Rightarrow \forall x \in F \quad x \tau \{0\}$ (se $f(x) = 0 \Rightarrow X = \{0\} \wedge x \tau \{0\}$
se $f(x) \neq 0 \Rightarrow f(x) \in \mathbb{N}^* = \mathbb{N} \setminus \{0\}$ e $f(x)$ divide propriamente 0)

$\Rightarrow \{0\} = \max(F, \tau) \Rightarrow$ è l'unico massimale

(F, τ) è un reticolo?

Se consideriam $x, y \in F$ tali che $x \neq y \wedge f(x) = f(y) \Rightarrow$ x e y non sono confrontabili

$\{x, y\}$ ammette sup e inf?

Sup.

Se $x = \{1\}$ $\quad y = \{0, 2\}$ $\quad \Rightarrow f(x) = f(y) = 2$ e $x \neq y$

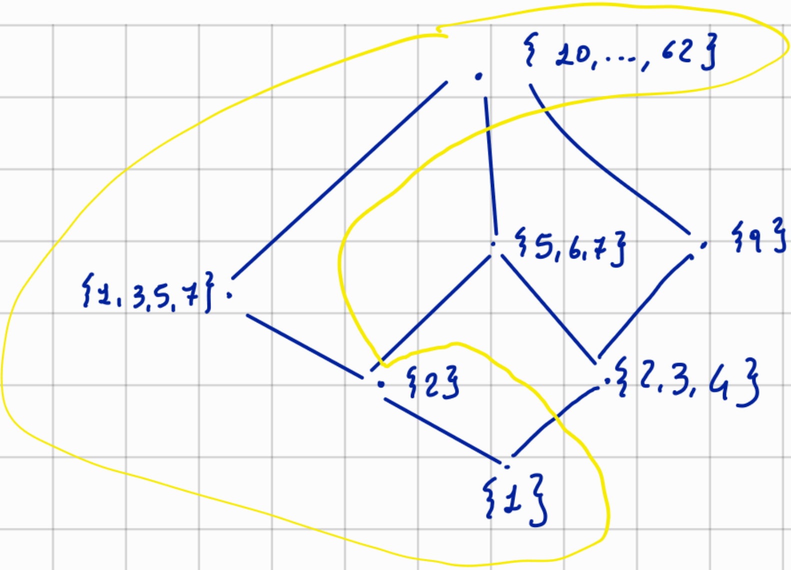
L'insieme dei maggioranti di $\{x, y\}$ è $\underbrace{\{z \in F \mid 2 \mid f(z) \text{ e } f(z) \neq 2\}}_{M}$
$= \{z \in F \mid f(z) \in$ pari e maggiore o uguale a $4\}$

Per ammettere sup ci serve il minimo dei maggioranti
$T \in F$ è il minimo $\Leftrightarrow T \tau z \quad \forall z \in M$ cioè $f(T) \mid f(z) \ \forall z \in M$

ma questo può essere solo 2 che è escluso $\Rightarrow$ non hanno sup
$\Rightarrow$ non è un reticolo perché M non ha minimo $\Rightarrow \{x, y\}$ non ha sup.

vi) Posto $M = \{\{1\}, \{2\}, \{2,3,4\}, \{1,3,5,7\}, \{5,6,7\}, \{9\}, \{10,11,15,60,62\}\}$
disegnare il diagramma di Hasse di (M, τ).
Verificare se è un reticolo. Nel caso se è distributivo, complementato, booleano

$f\{1\} = 2$
$f\{2\} = 4$
$f\{2,3,4\} = 6$
$f\{1,3,5,7\} = 8$
$f\{5,6,7\} = 12$
$f\{9\} = 18$
$f\{10,11,15,6,62\} = 72$



È un reticolo e una sua catena massimale è ad esempio quella cerchiata, ed è massimale, in quanto se aggiungiamo anche un solo elemento non va più bene

COMPLEMENTATO

$\{5,6,7\}$ non ha complemento perché $\inf\{\{5,6,7\},\{9\}\} = \{2,3,4\} \neq \min$

$\Rightarrow$ il reticolo non è complementato

$\Rightarrow$ non è booleano

DISTRIBUTIVO

Per vederlo ci sono 2 modi

1. se non è isomorfo a ◇ e ⬠
2. se ogni elemento ha al più un complemento

$\{9\}$ ha come complementi sia $\{1,3,5,7\}$ che $\{2\}$ $\Rightarrow$ non è distributivo

Esercizio 7. Prendiamo $p>0$ primo e
$$f_p = (\bar{4}x^3 + x^2 - \bar{2}x - \bar{4})(x+\bar{1}) \in \mathbb{Z}_p[x]$$

i) Determinare l'insieme X dei primi positivi tali che il resto della divisione euclidea fra f_p e $x-\bar{2}$ sia $\bar{0}$

Ciò significa che $x-\bar{2} \mid f_p \iff 2$ è radice di f_p
Come facciamo a calcolare i primi p per cui questo accade?
Calcoliamo $f_p(\bar{2})$

$$f_p(\bar{2}) = (\overline{32} \cancel{+4} \cancel{-4} - \bar{4})(3) = \overline{28} \cdot \bar{3} = \overline{84}$$ e voglio sapere quando

$84 \equiv_p 0$ cioè quando $p \mid 84$. Mi basta determinare i divisori primi di 84. $84 = 2^2 \cdot 7 \cdot 3 \Rightarrow$ se $p = 2, 7, 3$ allora $f_p(\bar{2}) = \bar{0}$

$\Rightarrow X = \{2, 7, 3\}$

ii) Fissare $p = \max X = 7$ e decomporre f_p nel prodotto di irriducibili in $\mathbb{Z}_p[x]$

Poiché $\mathbb{Z}_7[x]$ è un campo sappiamo che f_p si può scrivere solo come un invertibile per il prodotto di fattori monici irriducibili.

$$f_7 = (x-\bar{1})(x-\bar{2})g \qquad g \in \mathbb{Z}_7[x]$$

Determiniamo g.
Sappiamo che $x-\bar{2} \mid f_7 \ \wedge\ x-2 \nmid x+\bar{1} \Rightarrow x-2 \mid 4x^3 + x^2 - 2x - 4$

$$
\begin{array}{l|l}
4x^3 + x^2 - 2x - 4 & x - 2 \\
\hline
-4x^3 + 8x^2 & 4x^2 + 9x + 2 \\
\hline
\quad 9x^2 - 2x - 4 & \\
\quad -9x^2 + 18x & \\
\hline
\qquad -16x - 4 & \\
\qquad \;\; = & \\
\qquad 2x - 4 & \\
\qquad -2 + 4 & \\
\hline
\qquad\quad = &
\end{array}
$$

$$\Rightarrow f_7 = (x+\bar{1})(x-\bar{2})(\bar{4}x^2 + \bar{2}x + \bar{2}) =$$
$$2(x+\bar{1})(x-\bar{2})\underline{(\bar{2}x^2 + x + \bar{1})}$$

non sappiamo ancora se è irriducibile

Scomponiamo ancora $\bar{2}x^2 + x + \bar{1}$. Se sostituiamo $-\bar{2}$ vediamo che $x - \bar{2} \mid 2x^2 + x + 1$,

$$
\begin{array}{l|l}
2x^2 + x + 1 & x + 2 \\
\hline
-2x^2 - 4x & 2x + 3 \\
\hline
\quad -3x + 1 & \\
\quad 3x + 6 & \\
\hline
\qquad \bar{0} &
\end{array}
$$

$$2(x+\bar{1})(x-\bar{2})(x+\bar{2})(2x+3)$$
$$(2x+2)(x-2)(x+2)(2x+3) \quad \checkmark$$

iii) f_p ha fattori irriducibili monici NO!