1. Algebra e Logica a.a. 2019-'20. Appello 3 del 02 settembre 2020.

Es. 1.1. Si consideri, al variare di $k \in \mathbb{Z}$, l'equazione

$$51x + 93y = 5k$$

(a) Determinare per quali $k \in \mathbb{Z}$ esistono soluzioni $(\overline{x}, \overline{y}) \in \mathbb{Z} \times \mathbb{Z}$ di tale equazione.
(b) Per tali $k \in \mathbb{Z}$ determinare (in funzione di k) tutte le soluzioni $(\overline{x}, \overline{y}) \in \mathbb{Z} \times \mathbb{Z}$ di tale equazione.

Soluzione. (a) Con l'algoritmo euclideo si trova che $MCD(93, 51) = 3$ Dunque l'equazione in questione ha soluzioni intere se e solo se $5k$ è un mutiplo di 3, cosa che avviene se e solo se k è un multiplo di 3. Dunque $k = 3h$, $h \in \mathbb{Z}$.

(b) Dividendo per 3, l'equazione $51x + 93y = 5 \cdot 3h$ è equivalente a $17x + 31y = 5h$. Con l'algoritmo euclideo si trova che $17 \cdot 11 + 31 \cdot (-6) = 1$. Moltiplicando per $5h$ si trova la soluzione particolare $(11 \cdot 5h, -6 \cdot 5h)$. Dunque, per un fissato $h \in \mathbb{Z}$, le soluzioni sono tutte e sole le coppie della forma $(11 \cdot 5h + 31s\,,\, -6 \cdot 5h - 17s)$, al variare di $s \in \mathbb{Z}$.

Es. 1.2. Sia X l'insieme di tutti i numeri primi ≥ 17 e < 50. Si consideri la seguente relazione d'ordine R su X:
dati $x, y \in X$, $x\,R\,y$ se ogni cifra della rappresentazione in base 4 di x è minore o uguale della corrispondente cifra della rappresentazione in base 4 di y.

Determinare tutti gli elementi massimali e tutti gli elementi minimali di X rispetto alla relazione d'ordine R.

Soluzione. L'insieme dei primi in questione è $X = \{17, 19, 23, 29, 31, 37, 41, 43, 47\}$. Usando il metodo descritto nelle lezioni, si trovano le scritture in base 4:
$17 = (101)_4$, $19 = (103)_4$, $23 = (113)_4$, $29 = (131)_4$, $31 = (133)_4$, $37 = (211)_4$, $41 = (221)_4$, $43 = (223)_4$, $47 = (233)_4$.

Usando la definizione della relazione R, da un esame diretto si vede che l'unico elemento minimale (che quindi è il minimo) è 17 e che l'unico elemento massimale è 47 (che quindi è il massimo).

Es. 1.3. Sull'insieme $\mathbb{Z}_5 \times (\mathbb{Z}_5 \setminus \{\overline{0}\})$ si consideri la relazione R così definita:
dati $(\overline{x}, \overline{y}), (\overline{z}, \overline{t}) \in \mathbb{Z}_5 \times (\mathbb{Z}_5 \setminus \{\overline{0}\})$, $(\overline{x}, \overline{y})\, R\, (\overline{z}, \overline{t})$ se $\overline{x}\overline{t} = \overline{y}\overline{z}$.

Stabilire se R è una relazione di equivalenza e, in caso affermativo, stabilire quante sono le classi di equivalenza e descriverle.

Soluzione. R è una relazione di equivalenza sull.insieme $X := \mathbb{Z}_5 \times (\mathbb{Z}_5 \setminus \{\overline{0}\})$.
Infatti è riflessiva perchè $(\overline{x}, \overline{y})\, R\, (\overline{x}, \overline{y})$ per ogni $(\overline{x}, \overline{y}) \in X$, perchè $\overline{x}\overline{y} = \overline{y}\overline{x}$ (commutatività dell'anello $\mathbb{Z}_5$).
Inoltre è simmetrica perchè se $\overline{x}\overline{t} = \overline{y}\overline{z}$ allora $\overline{z}\overline{y} = \overline{t}\overline{x}$.
Infine è transitiva. Dobbiamo dimostrare che se $(\overline{x}, \overline{y})\, R\, (\overline{z}, \overline{t})$ e $(\overline{z}, \overline{t})\, R\, (\overline{u}, \overline{v})$ allora $(\overline{x}, \overline{y})\, R\, (\overline{u}, \overline{v})$.
Infatti se

$$\overline{x}\overline{t} = \overline{y}\overline{z} \qquad \text{e} \qquad \overline{z}\overline{v} = \overline{t}\overline{u} \tag{1}$$

allora $\overline{x}\overline{t}\overline{z}\overline{v} = \overline{y}\overline{z}\overline{t}\overline{u}$. Abbiamo che $\overline{t}$, essendo diverso da $\overline{0}$ in $\mathbb{Z}_5$, è invertibile in $\mathbb{Z}_5$ (5 è un primo). Dunque possimo dividere per $\overline{t}$ e risulta che

$$\overline{x}\overline{z}\overline{v} = \overline{y}\overline{z}\overline{u}. \tag{2}$$

Se $\overline{z} \neq \overline{0}$ allora, per lo stesso motivo, $\overline{xv} = \overline{yu}$. Invece, se $\overline{z} = \overline{0}$, dalla prima delle (1) risulta che $\overline{x}\overline{t} = \overline{0}$. Poichè $\overline{t} \neq 0$, è invertibile, dunque, come prima, possimao divider per $\overline{t}$ e risulta $\overline{x} = 0$. Allo stesso modo, dalla seconda delle (1), si trova che $\overline{u} = \overline{0}$. Dunque anche in questo caso $\overline{xv} = \overline{yu}$. Quindi la relazione è transitiva. *(Notate che, a parte alcune precisazioni, è la stessa dimostrazione che si usa nella costruzione dei razionali a partire dagli interi.)*

Classi di equivalenza. Come nella costruzione dei razionali a partire dagli interi, è utile osservare che se $\overline{a} \neq \overline{0}$, allora le coppie $(\overline{x}, \overline{y})$ e $(\overline{x}, \overline{ya})$ sono equivalenti. Infatti $\overline{xya} = \overline{yxa}$). Dunque se moltiplichiamo le due coordinate per uno stesso elemento diverso da zero, otteniamo una coppia equivalente. In questo modo è facile trovare le classi. Partiamo da $(\overline{,}0, \overline{1})]$ e otteniamo:
$\{(\overline{0}, \overline{1}), (\overline{0}, \overline{2}), (\overline{0}, \overline{3}), (\overline{0}, \overline{4})\}$.
Partiamo ora da $(\overline{1}, \overline{1})$. Si verifica subito che non è equivalente a $(\overline{0}, \overline{1})$. Dunque sta in una classe diversa. procedendo come prima otteniamo
$\{(\overline{1}, \overline{1}), (\overline{2}, \overline{2}), (\overline{3}, \overline{3}), (\overline{3}, \overline{4})\}$.
Consideriamo ora $(\overline{2}, \overline{1})$. Si vede che non sta nelle due classi precedenti. procedendo nello stesso modo otteniamo
$\{(\overline{2}, \overline{1}), (\overline{4}, \overline{2}), (\overline{1}, \overline{3}), (\overline{3}, \overline{4})\}$.
Consideriamo ora $(\overline{3}, \overline{1})$. Si vede che non sta nelle classi precedenti. procedendo nello stesso modo otteniamo
$\{(\overline{3}, \overline{1}), (\overline{3}, \overline{2}), (\overline{4}, \overline{3}), (\overline{2}, \overline{4})\}$.
Infine troviamo l'ultima classe
$\{(\overline{4}, \overline{1}), (\overline{3}, \overline{2}), (\overline{2}, \overline{3}), (\overline{1}, \overline{4})\}$.

Dunque abbiamo 5 classi, ciascuna con 4 elementi.

Es. 1.4. (a) Sia p un numero primo > 2. Determinare quanti sono gli $\overline{x} \in \mathbb{Z}_{8p}$ tali che $\overline{x}^2 = \overline{1}$
(b) Esemplificare il ragionamento utilizzato per rispondere alla domanda (a) calcolando tutti gli $\overline{x} \in \mathbb{Z}_{40}$ tali che $\overline{x}^2 = \overline{1}$

Soluzione. (a) Per il teorema cinese dei resti l'equazione $x^2 \equiv 1 \pmod{8p}$ è equivalente al sistema $\begin{cases} x^2 \equiv 1 \pmod 8 \\ x^2 \equiv 1 \pmod p \end{cases}$. Si vede facilmente che la prima equazione è soddisfatta da tutti e quattro gli elementi di $\mathbb{Z}_8^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$. Invece sappiamo che la seconda equazione è soddisfatta solo da 1 e $p-1 \pmod p$. Dunque il sistema $\begin{cases} x^2 \equiv 1 \pmod 8 \\ x^1 \equiv 1 \pmod p \end{cases}$ si spezza in otto sistemi: $\begin{cases} x \equiv c_i \pmod 8 \\ x \equiv d_j \pmod p \end{cases}$, $c_i = 1, 3, 5, 7$, $d_j = 1, p-1$. Sempre per il Teorema dei resti questi otto sistemi hanno soluzioni distinte modulo $8p$. Dunque la risposta finale è: 8.

(b) Risolvendo gli 8 sistemi della risposta precedente per $p = 5$ risultano le soluzioni:
$\overline{1}$, $\overline{9}$, $\overline{11}$, $\overline{19}$, $\overline{21}$, $\overline{29}$, $\overline{31}$, $\overline{39}$.

Es. 1.5. Si considerino i seguenti insiemi, tutti ordinati tramite la divisibiiltà:
$X = \{1, 2, 3, 6, 9, 27, 54\}$; $Y = \{1, 2, 3, 6, 9, 18, 54\}$; $Z = \{1, 2, 3, 12, 18, 24, 36, 72\}$.

Per ciascuno di essi:
(a) stabilire se è un reticolo;
(b) se è un reticolo stabilire se è complementato;
(c) se è un reticolo stabilire se vale la seguente proprietà: se un elemento ha complemento, esso è unico.

X: è un reticolo, non è complementato (ad esempio: l'elemento 3 non ha complemento), non per tutti gli elementi che hanno complemento esso è unico. Ad esempio l'elemento 2 ha due complementi: 9 e 27.

Y: è un reticolo, non è complementato e anzi nessun elemento diverso dal massimo e dal minimo ha complemento.

Z: non è un reticolo. Ad esempio non esiste il $sup(2, 3)$.