Esercizio 1. Determinare il MCD ed un'identità di Bezout per $a = 14322$ e $b = 6153$.

$14322 = 6153 \cdot 2 + 2016 \quad 6153 = 2016 \cdot 3 + 105 \quad 2016 = 105 \cdot 19 + 21$

$105 = 21 \cdot 5 + 0 \Rightarrow MCD(14322, 6153) = 21$

IDENTITÁ:

$2016 = 14322 - 6153 \cdot 2$

$105 = 6153 - 2016 \cdot 3$

$21 = 2016 - \underline{105} \cdot 19 \Rightarrow 21 = 2016 - \underline{(6153 - 2016 \cdot 3)} \cdot 19 = 2016 - (6153 \cdot 19 - 2016 \cdot 57)$

$= 2016 - 6153 \cdot 19 + 2016 \cdot 57 = 6153 \cdot (-19) + \underline{2016} \cdot 58 = 6153 \cdot (-19) + \underline{(14322 - 6153 \cdot 2)} \cdot 58$

$= 6153 \cdot (-19) + 14322 \cdot 58 + 6153 \cdot (-116) = 6153 \cdot (-135) + 14322 \cdot (58)$

Esercizio 2. Trovare tutte le soluzioni mod 33 dell'equazione congruenziale

$$121X \equiv 22(33)\,.$$

$MCD(121, 33) = 11$ divide 22.

$121 = 33 \cdot 3 + 22, \quad 33 = 22 \cdot 1 + 11$

$121x + 33y = 22$

$22 = 11 \cdot 2 + 0 \quad 11 = 33 - 22$

$(x_0, y_0) = (-1, 4)$

$11 = 33 - (121 - 33 \cdot 3) \Rightarrow 11 = 33 - 121 + 33 \cdot 3$

CONSIDERO $\frac{c}{d} = \frac{22}{11} = 2 \Rightarrow (-1 \cdot 2, 4 \cdot 2)$

$\Rightarrow 11 = 121 \cdot (-1) + 33 \cdot 4$

$\Rightarrow (-2, 8)$ Tutte le sol. di $121x + 33y = 22$ sono $(-2 + K \cdot 3, 8 - K \cdot 11)$

TUTTE LE SOL DI $121X \equiv 22\ (33)$ SONO $-2 + K \cdot 3$ CON $K \in \mathbb{Z}$

Esercizio 3.

1. Verificare che i numeri 897 e 4403 sono coprimi.

2. Determinare una soluzione $(\tilde{x}, \tilde{y}) \in \mathbb{Z} \times \mathbb{Z}$ dell'equazione diofantea

$$897x + 4403y = 1 \tag{1}$$

3. Verificare che se $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ è una soluzione dell'equazione omogenea associata, $897x + 4403y = 0$, allora $(\tilde{x} + x_0, \tilde{y} + y_0)$ è una soluzione di (1).
Viceversa, verificare che se $(x', y') \in \mathbb{Z} \times \mathbb{Z}$ è soluzione di (1) allora esiste (x_0, y_0) tale che $(x', y') = (\tilde{x}, \tilde{y}) + (x_0, y_0)$.
Suggerimento: $(x', y') = (\tilde{x}, \tilde{y}) + ((x', y') - (\tilde{x}, \tilde{y}))$. [1].

4. Determinare tutte le soluzioni di (1).
Suggerimento: per risolvere l'equazione omogenea il Lemma di Euclide può risultare utile.

1- trovo $MCD(897, 4403)$:

$4403 = 897 \cdot 4 + 815 \Rightarrow 897 = 815 \cdot 1 + 82 \Rightarrow 815 = 82 \cdot 9 + 77 \Rightarrow 82 = 77 \cdot 1 + 5$

$\Rightarrow 77 = 5 \cdot 15 + 2 \Rightarrow 5 = 2 \cdot 2 + 1 \Rightarrow MCD(897, 4403) = 1 \Rightarrow$ sono coprimi

2- trovo l'identità di Bezout, esplicito i resti:

$815 = 4403 - 897 \cdot 4 \quad 82 = 897 - 815 \quad 77 = 815 - 82 \cdot 9 \quad 5 = 82 - 77 \cdot 1$

$2 = 77 - 5 \cdot 15$

$1 = 5 - \underline{2} \cdot 2 = 5 - \underline{(77 - 5 \cdot 15)} \cdot 2 = 5 - 77 \cdot 2 + 5 \cdot 30 = \underline{5} \cdot 31 - 77 \cdot 2 = \underline{(82 - 77)} \cdot 31 - 77 \cdot 2$

$82 \cdot 31 - 77 \cdot 31 - 77 \cdot 2 = 82 \cdot 31 - \underline{77} \cdot 33 = 82 \cdot 31 - \underline{(815 - 82 \cdot 9)} \cdot 33 =$

$82 \cdot 31 - 815 \cdot 33 + 82 \cdot 297 = \underline{82} \cdot 328 - 815 \cdot 33 = \underline{(897 - 815)} \cdot 328 - 815 \cdot 33 =$

$897 \cdot 328 - \underline{815} \cdot 361 = 897 \cdot 328 - (4403 - 897 \cdot 4) \cdot 361 = 897 \cdot 1772 + 4403 \cdot (-361)$ SOL: $(-361, 1772)$

3- ho che $(\tilde{x}, \tilde{y}) = (1772, -361)$, siano (x_0, y_0) una soluzione dell'omog. associata: $897 \cdot x_0 + 4403 \cdot y_0 = 0$, considero $(1772 + x_0, -361 + y_0)$, verifico:

$$897 \cdot (1772 + x_0) + 4403 \cdot (-361 + x_0) = 1 \Rightarrow (897 \cdot 1772) + 897 \cdot x_0 - (4403 \cdot 361) + 4403 \cdot y_0 = 1$$

$$\Rightarrow \boxed{\mathbb{Z} \text{ e' COMMUTATIVO}} \Rightarrow (897 \cdot 1772) - (4403 \cdot 361) + \underbrace{\boxed{897 \cdot x_0 + 4403 \cdot y_0}}_{\text{PER IPOTESI e' 0}} = 1$$

$$\Rightarrow (897 \cdot 1772) - (4403 \cdot 361) + 0 = 1 \Rightarrow 1 = 1$$

Supponiamo che una soluzione sia (x', y'), allora: $897 \cdot x' + 4403 \cdot y' = 1$, supponiamo adesso che $(\tilde{x}, \tilde{y})$ siano soluzioni, e che

$$\underline{x' = \tilde{x} + \alpha \wedge y' = \tilde{y} + \beta} \Rightarrow 897 \cdot x' + 4403 \cdot y' = 1 \Rightarrow 897 \cdot (\tilde{x} + \alpha) + 4403 \cdot (\tilde{y} + \beta)$$

per la divisibilita' in $\mathbb{Z}$, cio' e' sempre possibile.

$$\Rightarrow 897 \cdot \tilde{x} + 897 \cdot \alpha + 4403 \cdot \tilde{y} + 4403 \cdot \beta = 1 \Rightarrow \underline{897 \cdot \tilde{x} + 4403 \cdot \tilde{y}} + 897 \cdot \alpha + 4403 \cdot \beta = 1$$

ma per ipotesi $(\tilde{x}, \tilde{y})$ siano soluzioni $\Rightarrow 1 + 897 \cdot \alpha + 4403 \cdot \beta = 1$

$\Rightarrow 897 \cdot \alpha + 4403 \cdot \beta = 1 - 1 \Rightarrow 897 \cdot \alpha + 4403 \cdot \beta = 0 \Rightarrow (\alpha, \beta)$ sono soluzioni dell'eq. omogenea associata.

4- So gia' che $(\tilde{x}, \tilde{y}) = (1772, -361)$, so che le sol sono:

$$(1772 + K \cdot 4403, -361 - K \cdot 897)$$

Esercizio 4. Verificare che $[8]$ è invertibile in $\mathbb{Z}_{385}$. Determinare tale inverso ed utilizzarlo per risolvere l'equazione congruenziale

$$8x \equiv 3 \pmod{385}.$$

a e' invertibile in $\mathbb{Z}_n \Leftrightarrow MCD(a, n) = 1$

$MCD(8, 385)$: $385 = 8 \cdot 48 + 1 \Rightarrow MCD(8, 385) = 1 \Rightarrow 8$ e' invertibile.

$8X \equiv 1 \ (385) \Rightarrow 8X + 385Y = 1 \Rightarrow [8]^{-1} = [-48] = [337]$

$8X \equiv 3 \ (385) \Rightarrow$ MOLTIPLICO I MEMBRI PER $337 \Rightarrow X \equiv 1011 \ (385)$

$\Rightarrow X \equiv 241 \ (385)$

Esercizio 5. Determinare $\mathcal{U}(\mathbb{Z}_{24})$.
Quali di questi hanno quadrato uguale all'unità ?

Gli elementi invertibili di $\mathbb{Z}_{24}$ sono gli $[a] \in \mathbb{Z}_{24} \mid MCD(a, 24) = 1$.

Fattorizzo $24 \Rightarrow 24 = 2^3 \cdot 3 \Rightarrow \varphi(24) = \varphi(2^3) \cdot \varphi(3) = (2^3 - 2^2) \cdot 2 = 8$

So che $|\mathcal{U}(\mathbb{Z}_{24})| = 8$:

$\mathcal{U}(\mathbb{Z}_{24}) = \{[1], [5], [7], [11], [13], [17], [19], [23]\}$

$X^2 \equiv 1 \ (24)$? $X = 5 \Rightarrow 5^2 \equiv 1 \ (24) \Rightarrow 25 \equiv 1 \ (24)$ ✓ $\quad 11^2 = 121 \Rightarrow 121 \equiv 1 \ (24)$ ✓

$7^2 = 49 \Rightarrow 49 \equiv 1 \ (24)$ ✓ $\quad 13^2 = 169 \Rightarrow 169 \equiv 1 \ (24)$ ✓

ed ovviamente 1.