Foglio 3 21/10/2023

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

1.1.)

$a = 14322$	$b = 6153$	$r = 2016$
$b = 6153$	$r = 2016$	$r_2 = 105$
$r = 2016$	$r_2 = 105$	$r_3 = 21$
$r_2 = 105$	$r_3 = 21$	$r_4 = 0$

MCD = 21

1.2.)

$$2016 = x - 2y$$

$$105 = y - 3(x - 2y)$$

$$21 = (x-2y) - 19\big(\overbrace{y - 3(x-2y)}^{-3x+6y}\big)$$

$$21 = x - 2y - 19y + 57x - 114y$$

$$21 = x \cdot (58) + y \cdot (-135)$$

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

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

$\cancel{121}X \equiv_{\cancel{33}} \cancel{22}$ $/11$

$11X \equiv_3 2$

$11x + 3y = 2$

$a = 11 \quad b = 3 \quad R = 2$

$11 = 3 \cdot 3 + 2$

quindi: $11 \cdot 1 + 3(-3) = 2$

INSIEME DELLE SOLUZIONI:

$[1]$

ALTRO METODO

$11X = 2(3)$

$MCD(11x, 3) = 1$

cerco un inverso di 11 cioè (11^{-1})

$11^{-1} = x$

$(11 \cdot 11^{-1}) \equiv 1 \bmod_3 \iff 11x - 1 = 3y$ per definizione

$11x - 3y = 1$

$a = 11 \quad b = 3 \quad R = 2$

$b = 3 \quad R = 2 \quad R_1 = 1$

$(x = -1,\ y = 4)$

$2 = a - b \cdot 3$

$1 = b - (a - b \cdot 3)$

$1 = b - a + b \cdot 3$

$1 = 4b - a$

$[-1] =$ inverso di $[11]$

$[-1]_3 = [2]_3$

$[11][-1][X] = [2][2] \bmod (3)$

$[X] = [4]$ in $\mathbb{Z}_3$

$[X] = [1]$ in $\mathbb{Z}_3$

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.

3.1 DETERMINA CHE 897 E 4403 SONO COPRIMI.

questi due numeri sono coprimi se MCD (897, 4403) = 1

X EUCLIDE:

$a = 4403$	$b = 897$	$R = 815$
$b = 897$	$R = 815$	$R_1 = 82$
$R = 815$	$R_1 = 82$	$R_2 = 9$
$R_1 = 82$	$R_2 = 9$	$R_3 = 1$
$R_2 = 81$	$R_3 = 1$	[...]

MCD (897, 4403) = 1 i due valori sono coprimi.

2.2) $897x + 4403y = 1$

TROVO $\tilde{x}$ e $\tilde{y}$ tramite identità di Bezout.

$815 = a - (b \cdot 4)$

$82 = b - (a - 4b)$

$9 = a - 4b - 9(b - (a - 4b))$

$1 = b - (a - 4b) - 9(a - 4b - 9(b - (a - 4b)))$

$1 = b - a + 4b - 9(a - 4b - 9(b - a + 4b))$

$1 = b - a + 4b - 9(a - 4b - 9b + 9a - 36b)$

$1 = b - a + 4b - 9a + 36b + 81b - 81a + 324b$ NO

[...]

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

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

8 e' invertibile in $\mathbb{Z}_{385}$ se e' coprimo con 385

cioe' se $MCD(8, 385) = 1$

x EUCLIDE

$a = 385 \quad b = 8 \quad R = 1$

[...]

VERO, 8 e' coprimo con $n = 385$ quindi e' invertibile. ✓

[8] e' invertibile.

$x = 8^{-1}$

$(8 \cdot 8^{-1}) \equiv 1 \pmod{385} \Longleftrightarrow (8 \cdot 8^{-1}) - 1 = 385y$ (DIVISIBILE PER n)

$8x - 385y = 1$

$8(-48) - 385(-1) = 1$

$x = -48$
$y = -1$

Quindi $[-48]$ e' l'inverso di $[8]$

$\rightarrow \quad [8][x] \equiv [3] \bmod 385$

$[-48][8][x] \equiv [3][-48] \bmod 385$

$[x] = [-144]_{385} = [241]_{385}$.