

Esercitazione del 15/11/2023

1) $20x \equiv 50 \pmod{30}$, ammette soluzione dato che $\text{MCD}(20, 30) = 10$ divide 50.

$$\text{Risolvo } 20x + 30y = 50 \Rightarrow \text{MCD}(20, 30) = 10 \Rightarrow 10 = 20x_1 + 30y_1 \Rightarrow 10 = 20 \cdot (-1) + 30 \cdot (1) \Rightarrow x_0 = (-1) \Rightarrow \tilde{x} = \frac{50}{10} \cdot (-1) = -5$$

$$\Rightarrow x = -5 + t \cdot \frac{30}{10} = -5 + 3t$$

2) $\begin{cases} 4x \equiv 1 \pmod{5} \\ x \equiv 5 \pmod{6} \\ 4x \equiv 3 \pmod{7} \end{cases} \Rightarrow \begin{matrix} \text{MCD}(4, 5) = 1 \mid 1 \checkmark \\ \text{MCD}(1, 6) = 1 \mid 5 \checkmark \\ \text{MCD}(4, 7) = 1 \mid 3 \checkmark \end{matrix} \Rightarrow \text{Ammette soluzione.}$

Applico il teorema cinese del resto, considero $R = 5 \cdot 6 \cdot 7$

$$\begin{cases} R_1 = 6 \cdot 7 = 42 \text{ risolvo } 42x + 5y = 1 \Rightarrow 42 \cdot (-2) + 5 \cdot 17 = 1 \Rightarrow \tilde{x}_1 = (-2) \cdot 4 = -8 \\ R_2 = 5 \cdot 7 = 35 \text{ risolvo } 35x + 6y = 1 \Rightarrow 35 \cdot (-1) + 6 \cdot 6 = 1 \Rightarrow \tilde{x}_2 = (-1) \cdot 5 = -5 \\ R_3 = 6 \cdot 5 = 30 \text{ risolvo } 30x + 7y = 1 \Rightarrow 30 \cdot (-3) + 7 \cdot 13 = 1 \Rightarrow \tilde{x}_3 = (-3) \cdot 6 = -18 \end{cases} \Rightarrow \tilde{x} = -8 \cdot 42 - 5 \cdot 35 - 18 \cdot 30 = -336 - 175 - 540 = -1051 \pmod{210} = 209$$

3) Gli invertibili di \mathbb{Z}_{15} sono gli elementi co-primi con 15, sia φ la funzione di Eulero, ho che:

$$\varphi(15) = \varphi(5 \cdot 3) = \varphi(5) \cdot \varphi(3) = 4 \cdot 2 = 8 \text{ ho che } \mathcal{U}(\mathbb{Z}_{15}) = \{[1], [2], [4], [7], [8], [11], [13], [14]\}$$

$$\text{Sappiamo che } \forall a \in \mathbb{Z}_n, a^{\varphi(n)} \equiv 1 \pmod{n} \Rightarrow a^{\varphi(n) \cdot k} \equiv 1 \pmod{n} \forall k \in \mathbb{N}, 1347 = 1344 + 3 = (8 \cdot 168) + 3$$

$$\Rightarrow \forall a \in \mathcal{U}(\mathbb{Z}_{15}), a^{1347} = a^{(168 \cdot 8) + 3} = a^{(168 \cdot 8)} \cdot a^3 = 1 \cdot a^3 = a^3 \pmod{15}$$

$$\cdot 2^{1347} = 2^3 = 8 \pmod{15} \cdot 4^3 = 64 \equiv 4 \pmod{15} \cdot 7^3 = 343 \equiv 13 \pmod{15} \cdot 8^3 = 512 \equiv 2 \pmod{15} \cdot 11^3 \dots \text{e cos\`i } \forall a.$$

4) Ho $\varphi: G \rightarrow G$, e $H \leq G$ **PUNTO 1**: $\tilde{a} \cdot b = \tilde{a} \cdot b \cdot 1 = \tilde{a} \cdot b \cdot a \cdot \tilde{a} = \tilde{a} \cdot a \cdot b \cdot \tilde{a} = 1 \cdot b \cdot \tilde{a} = b \tilde{a}$ ■

PUNTO 2: ho $K := \{x \mid x \in G, \varphi(xh) = \varphi(hx) \forall h \in H\}$, Sia $x \in K$, e sia x' il suo inverso, ho che

$$\varphi(x'h) = \varphi(x') \cdot \varphi(h) = \varphi(x)^{-1} \cdot \varphi(h), \text{ per ipotesi, } \varphi(xh) = \varphi(x) \varphi(h) = \varphi(h) \varphi(x) = \varphi(hx), \text{ ma dal PUNTO 1}$$

ne consegue che $\varphi(x)^{-1} \varphi(h) = \varphi(h) \varphi(x)^{-1} = \varphi(h) \varphi(x') = \varphi(hx')$, quindi $x \in K \Rightarrow x' \in K$.

Per il criterio so che, K e' un sottogruppo $\Leftrightarrow a \cdot b' \in K \forall a, b \in K$, ho gi\`a dimostrato che l'inverso di $x \in K$ e' in K , dimostro che il prodotto di $a \cdot b \in K \forall a, b$:

$$\varphi(abh) = \varphi(a) \varphi(b) \varphi(h) = \varphi(a) \varphi(h) \varphi(b) = \varphi(a) \varphi(h) \varphi(b) = \varphi(h) \varphi(a) \varphi(b) = \varphi(hab) \quad \blacksquare$$

PUNTO 3: $aK = Ka \Leftrightarrow \forall k \in K, \forall a \in G, ak = ka \Rightarrow ak\tilde{a}' = k\tilde{a}' \Rightarrow K$ e' normale se $ak\tilde{a}' \in K$

$$\Leftrightarrow \varphi(ak\tilde{a}'h) = \varphi(hak\tilde{a}'). \text{ Ma } H \text{ e' normale, quindi } h \cdot \tilde{a}' = \tilde{a}' \cdot h \wedge kh = hk \wedge ah = ha$$

$$\Rightarrow \varphi(ak\tilde{a}'h) = \varphi(akh\tilde{a}') = \varphi(hak\tilde{a}') = \varphi(hak\tilde{a}'). \quad \blacksquare$$