Esercitazione del 15/11/2023

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

Risolvo $20x+30y=50 \Rightarrow MCD(20,30)=10 \Rightarrow 10=20x_0+30y_0 \Rightarrow 10=20\cdot(-1)+30\cdot(1) \Rightarrow x_0=(-1) \Rightarrow \tilde{x}=\frac{50}{10}\cdot(-1)=-5$

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

2) $\begin{cases} 4x\equiv 1 \ (5) \\ x\equiv 5 \ (6) \\ 4x\equiv 3 \ (7) \end{cases} \Rightarrow \begin{matrix} MCD(4,5)=1 \mid 1 \checkmark \\ MCD(1,6)=1 \mid 5 \checkmark \\ MCD(4,7)=1 \mid 3 \checkmark \end{matrix} \Rightarrow$ Ammette soluzione. Riduco a cinese $\Rightarrow \begin{cases} 4x\cdot\bar{4}^1\equiv\bar{4}^1 \ (5) \\ x\equiv 5 \ (6) \\ 4x\cdot\bar{4}^1\equiv 3\cdot\bar{4}^1 \ (7) \end{cases} \Rightarrow \begin{cases} 4x\cdot 4\equiv 4 \ (5) \\ x\equiv 5 \ (6) \\ 4x\cdot 2\equiv 3\cdot 2 \ (7) \end{cases} \Rightarrow \begin{cases} x\equiv 4 \ (5) \\ x\equiv 5 \ (6) \\ x\equiv 6 \ (7) \end{cases}$

Applico il teorema cinese del resto, considero $R=5\cdot6\cdot7$

$R_1=6\cdot7=42$ risolvo $42x+5y=1 \Rightarrow 42\cdot(-2)+5\cdot17=1 \Rightarrow \tilde{x}_1=(-2)\cdot 4=-8$
$R_2=5\cdot7=35$ risolvo $35x+6y=1 \Rightarrow 35\cdot(-1)+6\cdot6=1 \Rightarrow \tilde{x}_2=(-1)\cdot 5=-5$
$R_3=6\cdot5=30$ risolvo $30x+7y=1 \Rightarrow 30\cdot(-3)+7\cdot13=1 \Rightarrow \tilde{x}_3=(-3)\cdot 6=-18$

$\tilde{x}=-8\cdot42-5\cdot35-18\cdot30=-336-175-540=-1051 \ (5\cdot6\cdot7) \equiv 209$

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

$\varphi(15)=\varphi(5\cdot3)=\varphi(5)\cdot\varphi(3)=4\cdot2=8$ ho che $\mathcal{U}(\mathbb{Z}_{15})=\{[1],[2],[4],[7],[8],[11],[13],[14]\}$.

Sappiamo che $\forall a\in\mathbb{Z}_n,\ a^{\varphi(n)}=1 \pmod n \Rightarrow a^{\varphi(n)\cdot k}=1 \pmod n \ \forall k\in\mathbb{N}$, $1347=1344+3=(8\cdot168)+3$

$\Rightarrow \forall a\in\mathcal{U}(\mathbb{Z}_{15}),\ a^{1347}=a^{(168\cdot8)+3}=a^{(168\cdot8)}\cdot a^3=1\cdot a^3=a^3 \pmod{15}$.

- $2^{1347}=2^3=8 \pmod{15}$
- $4^3=64\equiv4 \ (15)$
- $7^3=343\equiv13 \ (15)$
- $8^3\equiv2 \ (15)$
- $11^3\cdots$ e così via.

4) Ho $f: G\to G$, e $H\leq G$ **PUNTO 1**: $\bar{a}^1\cdot b=\bar{a}^1\cdot b\cdot 1=\bar{a}^1\cdot b\cdot a\cdot\bar{a}^1=\bar{a}^1\cdot a\cdot b\cdot\bar{a}^1=1\cdot b\cdot\bar{a}^1=b\bar{a}^1$ ■ (IPOTESI)

PUNTO 2: ho $K:=\{x \mid x\in G,\ f(xh)=f(hx)\ \forall h\in H\}$, Sia $x\in K$, e sia $\bar{x}^1$ il suo inverso, ho che

$f(\bar{x}^1h)=f(\bar{x}^1)\cdot f(h)=f(x)^{-1}\cdot f(h)$, per ipotesi, $f(xh)=f(x)f(h)=f(h)f(x)=f(hx)$, ma dal PUNTO 1 ne consegue che $f(x)^{-1}f(h)=f(h)f(x)^{-1}=f(h)f(\bar{x}^1)=f(h\bar{x}^1)$, quindi: $x\in K\Rightarrow\bar{x}^1\in K$.

Per il criterio so che, K è un sottogruppo $\Leftrightarrow a\cdot b^{-1}\in K\ \forall a,b\in K$, ho già dimostrato che l'inverso di $x\in K$ è in K, dimostro che il prodotto di $a\cdot b\in K\ \forall a,b$:

$f(abh)=f(a)f(b)f(h)=f(a)f(h)f(b)=f(a)f(h)f(b)=f(h)f(a)f(b)=f(hab)$ ■ (IPOTESI, IPOTESI)

PUNTO 3: $aK=Ka \Leftrightarrow \forall k\in K, \forall a\in G,\ aK=Ka \Rightarrow aK\bar{a}^1=K\in K\Rightarrow K$ è normale se $aK\bar{a}^1\in K$

$\Leftrightarrow f(aK\bar{a}^1h)=f(haK\bar{a}^1)$. Mostro che:

$f(aK\bar{a}^{-1}h)=f(aK\bar{a}^1h\cdot1)=f(aK\bar{a}^1ha\cdot\bar{a}^1)=f(a)\cdot f(K)\cdot f(\bar{a}^1ha)f(\bar{a}^1)$ → MA QUESTO TERMINE, ESSENDO H normale, APPARTIENE AD H, E SE APPARTIENE AD H, POSSO SCAMBIARLO DI POSTO:

$f(a)\cdot f(K)\cdot f(\bar{a}^1ha)f(\bar{a}^1)=f(a)\cdot f(\bar{a}^1ha)\cdot f(K)\cdot f(\bar{a}^1)=f(a\bar{a}^1haK\bar{a}^1)=f(haK\bar{a}^1)\Rightarrow K$ è normale.