ESERCIZIO 1)

1.0.) $\mathrm{Im}\,\phi \leq G'$

$$\mathrm{Im}\,\phi \leq G' \iff \begin{cases} a)\ 1_{G'} \in \mathrm{Im}\,\phi \\ b)\ \forall g, h \in \mathrm{Im}\,\phi,\ gh \in \mathrm{Im}\,\phi \\ c)\ \forall g \in \mathrm{Im}\,\phi,\ g^{-1} \in \mathrm{Im}\,\phi \end{cases}$$

VERIFICO:

a) $\phi(1_G) = 1_{G'} \Rightarrow 1_{G'} \in \mathrm{Im}\,\phi$

b) $g, h \in \mathrm{Im}\,\phi$, $g = \phi(x)$, $h = \phi(y)$ CON $x, y \in G$.
$g \cdot_{G'} h = \phi(x) \cdot_{G'} \phi(y) = \phi(xy)$ CHE È UN ELEMENTO DI $\mathrm{Im}\,\phi$ $(xy \in G)$

c) $g \in \mathrm{Im}\,\phi$, $g = \phi(x)$ CON $x \in G$.
$g^{-1} = \phi(x)^{-1} = \phi(x^{-1})$

PERCHÉ: $1_G = a \cdot a^{-1}$
$1_{G'} = \phi(a \cdot a^{-1})$
$1_{G'} = \phi(a) \cdot \phi(a^{-1})$
SO CHE: $1_{G'} = \phi(a) \cdot (\phi(a))^{-1}$
PER UNICITÀ INVERSO $\phi(a^{-1}) = (\phi(a))^{-1}$

1.1.)

SE G È COMMUTATIVO $\Rightarrow \forall g, h \in G,\ g \cdot_G h = h \cdot_G g$.
$x, y \in \mathrm{Im}\,\phi$, $x = \phi(g)$, $y = \phi(h)$ CON $g, h \in G$

$$x \cdot_{G'} y = \phi(g) \cdot_{G'} \phi(h) = \phi(g \cdot_G h) \overset{G \text{ COMMUTATIVO}}{=} \phi(h \cdot_G g)$$
$$y \cdot_{G'} x = \phi(h) \cdot_{G'} \phi(g) = \phi(h \cdot_G g) = \phi(g \cdot_G h)$$

$\Rightarrow (x \cdot_{G'} y) = (y \cdot_{G'} x)$

1.2) $H \leq G \Rightarrow H \subseteq G \Rightarrow \forall h \in H, h \in G.$

$\phi H \subseteq G'$ DATO CHE TUTTI GLI ELEMENTI DI H SONO ELEMENTI DI G E CHE ϕ MAPPA QUESTI ELEMENTI IN G'.

a) $H \leq G \Rightarrow 1_G \in G \wedge 1_G \in H$, $\phi(1_G) = 1_{G'}$ $\quad 1_G \in \phi H$

b) $h, k \in \phi H$, $h = \phi(x)$, $k = \phi(y)$ CON $x, y \in H$

$h \cdot_{G'} k = \phi(x) \cdot_{G'} \phi(y) = \phi(x \cdot_G y)$ DOVE $(x \cdot_G y)$ E' UN ELEMENTO DI H

$\Rightarrow \phi(x \cdot_G y) \in \phi H \Rightarrow h \cdot_{G'} k \in \phi H.$

c) $h \in \phi H$, $h = \phi(y)$ CON $y \in H \Rightarrow h = \phi(y) \Rightarrow$

$\Rightarrow h^{-1} = \phi(y)^{-1} = \phi(y^{-1})$ DOVE $y^{-1} \in H \Rightarrow \phi(y^{-1}) \in \phi H \Rightarrow$

$\Rightarrow h^{-1} \in \phi H.$

1.3) $\ker \phi = \{ g \mid \phi g = 1_{G'} \}$

$\ker \phi \subseteq G$

a) $1_{G'} = \phi(1_G) \Rightarrow 1_G \in \ker \phi$

b) $x, y \in \ker \phi.$

DIMOSTRO CHE : $\phi(x \cdot_G y) = 1_{G'}$

$\phi(x \cdot_G y) = \phi(x) \cdot_{G'} \phi(y) = 1_{G'} \cdot_{G'} 1_{G'} = 1_{G'}.$

c) $x \in \ker \phi$

DIMOSTRO CHE : $\phi(x^{-1}) = 1_{G'}$

$1_{G'} = \phi(x) \Rightarrow (1_{G'})^{-1} = \phi(x)^{-1} \Rightarrow 1_{G'} = \phi(x^{-1})$

DOVE $1_{G'} = (1_{G'})^{-1}$ PER UNICITA' INVERSO.

ESERCIZIO 3.

$$\sigma(g) = \sigma(\phi(g)) \quad \forall g \in G$$

$$\phi(1_G) = 1_{G'}$$

$$g^t = \underbrace{g \cdot_G g \cdot_G (\dots) \cdot_G g}_{t \text{ volte.}} = 1_G$$

$$\phi(g^t) = \phi(\underbrace{g \cdot_G g \cdot_G (\dots) \cdot_G g}_{T \text{ volte}}) = \phi(1_G) = 1_{G'}$$

$$\phi(\underbrace{g \cdot_G g \cdot_G (\dots) \cdot_G g}_{t \text{ volte.}}) = \underbrace{\phi(g) \cdot_{G'} (\dots) \cdot_{G'} \phi(g)}_{t \text{ volte.}} = 1_{G'}$$

VERIFICO ORA CHE t È IL MINIMO NUMERO $\mid (\phi(g))^t = 1_{G'}$

SUPPONIAMO ESISTA $s < t \mid (\phi(g))^s = 1_{G'} \Rightarrow$

$\Rightarrow \phi(\underbrace{g \cdot_G g \cdot_G (\dots) \cdot_G g}_{s \text{ volte}}) = 1_{G'}$ MA, SAPPIAMO CHE: $\phi(\underbrace{g \cdot_G g \cdot_G g \cdot_G (\dots) \cdot_G g}_{t \text{ volte}}) = 1_{G'}$

DATO CHE ϕ È UN ISOMORFISMO OGNI ELEMENTO $g \in G$ È MAPPATO BIUNIVOCAMENTE $\Rightarrow s = t$

$\Rightarrow \sigma(g) = t \quad \sigma(\phi(g)) = t.$

QUESTO NON VALE PER GLI OMOMORFISMI IN GENERALE

AD ESEMPIO POTREMMO AVERE UN OMOMORFISMO

$$f : G \to G' \mid \forall g \in G, \ \phi g = 1_{G'}.$$

$$\sigma(g) = t \quad \sigma(\phi(g)) = 1.$$

Esercizio 5)

Esercizio 5. Verificare che l'intersezione di 2 sottogruppi di un gruppo G è un sottogruppo. Estendere il risultato a l'intersezione di una famiglia arbitraria di sottogruppi in G.

CASO CON 2 SOTTOGRUPPI.

IP:

$U \leq G$, $W \leq G$

$(U \wedge W) \leq G \Leftrightarrow$ a) $1_G \in (U \wedge W)$

b) $\forall a, b \in (U \wedge W)$, $ab \in (U \wedge W)$

c) $\forall e \in (U \wedge W)$, $e^{-1} \in (U \wedge W)$

a) $\begin{cases} U \leq G \Rightarrow 1_G \in U \\ W \leq G \Rightarrow 1_G \in W \end{cases} \Rightarrow 1_G \in (U \wedge W)$

b) $(a, b) \in (U \wedge W) \Rightarrow (a, b) \in U \wedge (a, b) \in W \Rightarrow ab \in U \wedge ab \in W$ PERCHÉ SOTTOGRUPPI $\Rightarrow ab \in (U \wedge W)$.

c) $e \in (U \wedge W) \Rightarrow e \in U \wedge e \in W \Rightarrow e^{-1} \in U \wedge e^{-1} \in W$ PERCHÉ SOTTOGRUPPI $\Rightarrow e^{-1} \in U \wedge W$.

CASO CON n SOTTOGRUPPI

INDICO GLI n SOTTOGRUPPI CON S_i, $1 \leq i \leq n$

a) $1_G \in S_i \ \forall 1 \leq i \leq n$. PERCHÉ SE $S_i \leq G \Rightarrow 1_G \in S_i$.

b) $a, b \in (S_1 \wedge S_2 \wedge \ldots \wedge S_n) \Rightarrow a \in S_i \ \forall 1 \leq i \leq n$, $b \in S_i \ \forall 1 \leq i \leq n$

$ab \in S_i \ \forall 1 \leq i \leq n$ PERCHÉ S_i SOTTOGRUPPO DI $G \Rightarrow ab \in \bigcap_{i=1}^{n} (S_i)$

c) $e \in \bigcap_{i=1}^{n} (S_i) \Rightarrow e \in S_i \ \forall 1 \leq i \leq n \Rightarrow e^{-1} \in S_i \ \forall 1 \leq i \leq n$

PERCHÉ SOTTOGRUPPO DI $G \Rightarrow e^{-1} \in \bigcap_{i=1}^{n} (S_i)$.

Foglio 3

ESERCIZIO 1)

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

$a = 14322$

$b = 6153$

1) $M.C.D(a, b)$

1) $a = 2b + 2016$

2) $b = 2016 \cdot 3 + 105$

3) $2016 = 105 \cdot 19 + 21$

4) $105 = 21 \cdot 5$

$M.C.D = 21$

2) ID. BEZ.

$ax + by = 21$

$21 = 2016 - 105 \cdot 19 =$

$21 = 2016 - (b - 2016 \cdot 3) \cdot 19 =$

$21 = 2016 - (b - (a - 2b) \cdot 3) \cdot 19 =$

$21 = a - 2b - (b - 3a + 6b) \cdot 19 =$

$21 = a - 2b + (-b + 3a - 6b) \cdot 19$

$21 = a - 2b - 19b + 57a - 114b$

$21 = 58a - 77b.$

$\Rightarrow x = 58, \; y = -135$

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

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

$121X \equiv_3 22 =$

$= 11X \equiv_3 2 =$

TROVIAMO UN NUMERO Y CHE MOLTIPLICATO PER 11 DIA 1 mod 3 PER ELIMINARE IL COEFICENTE DELLA X.

$11y \equiv_3 1$

$11y - 3X = 1$

$\boxed{y = 2}$ $X = 7$

$22 - 21 = 1$

$= [11]X \cdot [2] \equiv_3 [2] \cdot [2] =$

$[22]X \equiv_3 [4]$

$X \equiv_3 [4].$

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 omogonea 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.) $a = 897$ $\quad b = 4403$

SE SONO COPRIMI $\quad M.C.D(897, 4403) = 1$

VERIFICO.

$b = 4 \cdot a + 815$

$a = 815 + 82$

$815 = 82 \cdot 9 + 77$

$82 = 77 + 5$

$77 = 5 \cdot 15 + 2$

$5 = 2 \cdot 2 + 1$

$2 = 1 \cdot 2$

$M.C.D(a, b) = 1 \implies$ I NUMERI SONO COPRIMI.

ESERCIZIO 4)

[8] INVERTIBILE IN $\mathbb{Z}_{385}$

[8] È INVERTIBILE SOLO SE COPRIMO CON $n = 385$

PERCHÉ SE $8x + (385)y = 1$ SIGNIFICA CHE UN MULTIPLO DI 8 + UN MULTIPLO (NEGATIVO SICURAMENTE) DI 385 È UGUALE A 1 mod(385)

VERIFICHIAMO:

$a = 385 \quad b = 8$

$a = 48b + 1$

$b = 8 \cdot 1$

$MCD(a, b) = 1$

[8] è INVERTIBILE IN $\mathbb{Z}_{385}$

$[8]^{-1} = [-48]$

2) $8x \equiv 3 \pmod{385}$

$[8] \cdot [-48] x \equiv_{385} [3][-48]$

$x \equiv_{385} [-144]$

$x \equiv_{385} [241]$

Determinare $\mathcal{U}(\mathbb{Z}_{24})$

TROVO TUTTE LE X COPRIME CON 24 | X < 24

$|\mathcal{U}(\mathbb{Z}_{24})| = \varphi(24)$; $24 = 2^3 \cdot 3 \Rightarrow \varphi(24) = (2^3 - 2^2) \cdot (3-1) = 8$

CON LA FUNZIONE $\varphi(24)$ MI SONO ASSICURATO CHE $\mathcal{U}(\mathbb{Z}_{24})$ CONTIENE 8 VALORI

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

$X = \{ x \in \mathcal{U}\mathbb{Z}_{24} \mid x \cdot x = 1 \pmod{24} \}$

$X = \{[1],[5],[7],[11],[13],[17],[19],[23]\}$

$[49] \equiv_{24} [1]$ $[121] \equiv_{24} [1]$ $[169] \equiv_{24} [1]$

$[289] \equiv_{24} [1]$

$[361] \equiv_{24} [1]$

$[529] \equiv_{24} [1]$

Foglio 4

Esercizio 1)

$$\begin{cases} x \equiv_5 3 \\ x \equiv_7 4 \\ x \equiv_{11} 4 \end{cases}$$

$$R = 5 \cdot 7 \cdot 11 = 385$$

$$R_1 = \frac{385}{5} = 77$$

$$R_2 = \frac{385}{7} = 55$$

$$R_3 = \frac{385}{11} = 35$$

$77\tilde{x}_1 \equiv_5 3 \quad = 2\tilde{x}_1 \equiv_5 3 \Rightarrow \tilde{x}_1 \equiv_5 3 \cdot 3 \Rightarrow \tilde{x}_1 \equiv_5 9 \Rightarrow \tilde{x}_1 \equiv_5 4$

$55\tilde{x}_2 \equiv_7 4 \quad = 6\tilde{x}_2 \equiv_7 4 \Rightarrow 6\tilde{x}_2 \equiv_7 4 \cdot 6 \Rightarrow \tilde{x}_2 \equiv_7 24 = 3$

$35\tilde{x}_3 \equiv_{11} 4 \quad = 2\tilde{x}_3 \equiv_{11} 4 \Rightarrow \tilde{x}_3 \equiv_1 24 = 13 = 2.$

$$\tilde{x} = (77 \cdot 4) + (55 \cdot 3) + (35 \cdot 2).$$

AMMETTE SOLUZIONI INFATTI $\forall n_i, a_i, \text{MCD}(n_i, a_i) \mid b_i$

$\wedge$ M.C.D $(n1, n2, n3) = 1$.

Esercizio 7)

$1 \leq a < p^2$

PER IL TEOREMA DI EULERO:

$$x^{\varphi(p^2)} = 1 \bmod (p^2)$$

$$x^{(p^2 - p)} = 1 \bmod (p^2)$$

ES 7

$Y = \{$ VALORI PRIVI DI INVERSO ARITMETICO MOD$(p^2)\}$

$Y = \{a \mid 1 \leq a < p^2 - \{a \mid MCD(a, n^2) = 1\}\}$

Esercizio 8)

$p > 2$ primo

Determina $\{x \in \mathbb{Z}_p : x^2 \equiv_p [1]\}$

Se p è primo tutti gli elementi $x \in \mathbb{Z}_p$ sono invertibili (esluso $[0]$)

perché $MCD(x, p) = 1 \quad \forall x \in \mathbb{Z}_p - \{[0]\}$

$MCD(x^2, p) = 1 \quad \forall x \in \mathbb{Z}_p - \{[0]\}$ perché p è divisibile per 1 e per p quindi sarà coprimo

NO

Esercizio 10

Per il teorema di Eulero $19^{\varphi(7)} \equiv_7 1$

possibile perché $M.C.D(19, 7) = 1$

$\Rightarrow 19^6 \equiv_7 1$

$$[19^{19^{19}}]_7 = [(19^6)^{19} \cdot (19^6)^{19} \cdot (19^6)^{19} \cdot (19)^{19}]_7 =$$

$$= [1 \cdot 1 \cdot 1 \cdot (19^6)^{19} \cdot (19^6)^{19} \cdot (19^6)^{19} \cdot 19]_7 =$$

$$[19]_7$$

ESERCIZIO 11

1) $a \in A \mid a^n = 0$, $b \in A \mid b^m = 0$

$(b+a)^r = 0$

? ? ?

Foglio 5) ESERCIZIO 6.)

Esercizio 6. Consideriamo il gruppo commutativo $(\mathbb{Z}, +)$ e siano H e K due suoi sottogruppi.
Sappiamo che $H = a\mathbb{Z}$ e $K = b\mathbb{Z}$ per opportuni $a, b \in \mathbb{N}$. Caratterizzare $H \cap K$ in termini del $\mathrm{mcm}(a, b)$.

ESERCIZIO 6

$$H \cap K = \{x \mid x = ak \text{ PER QUALCHE } k \in \mathbb{Z} \ \wedge \ x = bh \text{ PER QUALCHE } h \in \mathbb{Z}.\}$$

QUINDI:

$m.c.m(a,b) \in H \cap K$ PERCHÉ È IL PIÙ PICCOLO MULTIPLO DI a E b.
QUESTO SARÀ IL PIÙ PICCOLO ELEMENTO POSITIVO IN $H \cap K$.

QUESTO INSIEME SARÀ TIPO:

$$H \cap K = \{\dots, \overbrace{h_1, h_2, h_3, \dots,}^{\text{NEGATIVI.}} \overbrace{m.c.m.(a,b), \dots}^{\text{POSITIVI.}}\}$$

$H \cap K$ È SOTTOGRUPPO DI $\mathbb{Z} \Rightarrow H \cap K = m\mathbb{Z}$ PER QUALCHE $m \in \mathbb{Z}$
CIOÈ $H \cap K$ È UN INSIEME CHE CONTIENE TUTTI I MULTIPLI DI UN CERTO $m \in \mathbb{Z}$, DATO CHE $m.c.m(a,b)$ È IL PIÙ PICCOLO VALORE POSITIVO IN $H \cap K$, NON HA SOTTOMULTIPLI, MA HA SOLO

MULTIPLI (NEGATIVI E POSITIVI)

QUINDI: $n = m.c.m(a,b)$

QUINDI: $H \cap K = m.c.m(a,b)\mathbb{Z}$