Hw 4

1. $M = 17\times 19\times 23\times 29 = 223483$

$M_1 = 13147 \quad M_2 = 11764 \quad M_3 = 9712 \quad M_4 = 7709$

$y_1 = 3 \quad y_2 = 13 \quad y_3 = 4 \quad y_4 = 23$

$x = (b_1\times 13147\times 3 + b_2\times 11764\times 13 + b_3\times 9712\times 4 + b_4\times 7709\times 23) \bmod 223483$

2. $x = 15t_1 + b_1 = 21t_2 + b_2$

t_1, t_2 have solutions $\Leftrightarrow \gcd(15,21) \mid b_2 - b_1$

$\gcd(15,21) = 3$ i.d. $3 \mid b_2 - b_1$

3. $\forall X, Y, Z \in M_2(\mathbb{R})$

$\det XY = \det X \cdot \det Y \neq 0 \Rightarrow XY \in M_2(\mathbb{R})$

$XYZ = X(YZ)$

$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad EX = XE = X$

$\forall X,\ \det X \neq 0 \Rightarrow \exists X^{-1},\ XX^{-1} = X^{-1}X = E$

so. it is a group.

but $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$

so. not Abelian.

4. let $k = m \cdot o(a) + t \quad 0 \le t < o(a)$

if $a^k = 1 \Rightarrow a^{m \cdot o(a) + t} = a^t = 1$

but $o(a)$ is the smallest one.

$\Rightarrow t = 0$.

so $o(a) \mid k$

5. if $(i, m) = 1 \quad g^i = g^{i \% m}$ so, we only need consider $0 < i < m$

$e \; g \; g^2 \cdots g^{m-1} \Rightarrow g^m = e$, i,d $o(g) = m$

consider $e^i \; g^i \; (g^2)^i \cdots (g^{m-1})^i$

if $(g^{k_1})^i = (g^{k_2})^i \quad g^{(k_2 - k_1) i} = e$.

but we have proved that in question 4

that $\forall t$, $g^t = e \Rightarrow o(g) \mid t$

so $m \mid (k_2 - k_1) i \quad$ but $(m, i) = 1 \Rightarrow m \mid k_2 - k_1$

$-m < k_2 - k_1 < m \quad$ so $k_2 - k_1 = 0 \quad k_1 = k_2$

so. if $(m, i) = 1$

g^i can be a generator of G

the number of i is $\phi(m)$

so we only need to prove that

if $(m, i) \ne 1$, g^i cannot be a generator

if $\gcd(m, i) = k$

consider $(g^i)^1 \; (g^i)^2 \cdots (g^i)^{\frac{m}{k}}$

so $(g^i)^{\frac{m}{k}} = g^{\frac{mi}{k}} = (g^m)^{\frac{i}{k}} = e \quad$ so $o(g^i) \le \frac{m}{k} < m \quad$ contradiction!

In conlusion. the number of i is $\phi(m)$