ΚΥΚΛΙΚΕΣ ΟΜΑΔΕΣ ΜΙΚΡΗΣ ΤΑΞΗΣ:

(1). $|G|=1$, τότε $G=\{e\}$ όπου $<e>=G$ $(e^2=e)$

(2). $|G|=2$, τότε $G=\{e,a\}$ και πίνακα πράξης:

$\cdot$	e	a
e	e	a
a	a	e

→ $a^2=e$ (διότι όντας G ομάδα θα πρέπει να έχει αντίστροφο στοιχείο το ίδιο το a).

άρα, $G=<a>$ αφού $o(a)=|G|$

(3) $|G|=3$, τότε $G=\{e,a,b\}$ και πίνακα πράξης:

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$a^3=a\cdot b=e \Rightarrow o(a)=3=|G|$
αλλά και
$b=a^{-1} \Rightarrow o(a)=o(a^{-1})=3=|G|$ $\}$ $G=<a>=<b>$

(4) $|G|=4$ με $G=\{e,a,b,c\}$ (Η ομάδα του Klein)

ορίζονται δύο πίνακες πράξης και θα το αποδείξουμε θέλοντας να συμπληρωθεί ο πίνακας:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	?	?	?
b	b	?	?	?
c	c	?	?	?

Λόγω άρτιου αριθμού πλήθους στοιχείων ας είναι $a\neq e$: $a\cdot a=e$ και αφού η ομάδα είναι πεπερασμένη τότε κάθε στήλη και κάθε γραμμή του πίνακα πρέπει να έχει κάθε στοιχείο της G από μία φορά.

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e ή a	a ή e
c	c	b	a ή e	e ή a

για το γινόμενο $b\cdot b=e$ ή $b\cdot b=a$

για τον 1ο πίνακα, βλέπουμε ότι:

$a\cdot a=e$, $b\cdot b=e$, $c\cdot c=e$, $e\cdot e=e$
άρα η ομάδα (του 1ου πίνακα) δεν γεννάται από κανένα στοιχείο της | όχι κυκλική

Ενώ για το 2ο πίνακα, βλέπουμε ότι:

$b^3=b\cdot a=c \Rightarrow b^4=bc=e$
$c^3=c\cdot a=b \Rightarrow c^4=cb=e$ $\}$ Άρα, $G=<b>=<c>$ διότι $o(b)=o(c)=|G|$ είναι κυκλική ομάδα

ΚΥΚΛΙΚΕΣ ΟΜΑΔΕΣ – ΤΑΞΗ ΣΤΟΙΧΕΙΟΥ

ΟΡΙΣΜΟΣ: Μια ομάδα G καλείται κυκλική, εαν:

$(\exists a \in G)(\forall b \in G): b = a^k$ ή $b = ka$, $k \in \mathbb{Z}$

Ο a καλείται γεννήτορας και γράφουμε

$G = \langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$ (ή $G = \langle a \rangle = \{ka \mid k \in \mathbb{Z}\}$)

ΟΡΙΣΜΟΣ: Τάξη ομάδας G είναι το πλήθος στοιχείων της και την συμβολίζουμε $|G|$. Επίσης, για τυχόν $a \in G$ θα έχει πεπερασμένη τάξη αν υπάρχει φυσικός k: $a^k = e$. Αλλιώς, θα έχει άπειρη τάξη

ΟΡΙΣΜΟΣ: Εάν $k \in \mathbb{N}: a^k = e$ (ή $ka = e$), με k ο ελάχιστος φυσικός ώστε να ισχύει η παραπάνω ιδιότητα καλείται τάξη του $a \in G$. Γράφουμε $o(a) = k$. Αλλιώς, γράφουμε $o(a) = \infty$.

ΑΣΚΗΣΕΙΣ – ΕΦΑΡΜΟΓΕΣ:

1) Να βρεθεί η τάξη των στοιχείων που ακολουθούν:

i). Στην ομάδα $(GL(2,\mathbb{R}), \cdot)$ τα: $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ και $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

ii). Στην ομάδα $(\mathbb{C}^*, \cdot)$ το: $a = i$

iii). Στην ομάδα $(\mathbb{Z}_3, \oplus)$ το: $a = [2]_3$

ΛΥΣΗ

i) Καταρχάς η ομάδα $(GL(2,\mathbb{R}), \cdot)$ είναι άπειρης τάξης

$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow o\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = 2$

$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \Rightarrow \ldots$

Άρα, $o\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \infty$.

ii) Καταρχάς η ομάδα $(\mathbb{C}^*, \cdot)$ είναι άπειρης τάξης

$i \cdot i = i^2 = -1 \Rightarrow -1 \cdot i = -i \Rightarrow -i \cdot i = -i^2 = 1 \Rightarrow o(i) = 4$

iii) καταρχάς η ομάδα $(\mathbb{Z}_3, \oplus)$ είναι πεπερασμένης τάξης

$\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ και μάλιστα $|\mathbb{Z}_3| = 3$

Έστω ο πίνακας πράξης του $\mathbb{Z}_3$:

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

Παρατηρούμε:

$\bar{1} \oplus \bar{1} = \bar{2} \Rightarrow \bar{1} \oplus \bar{2} = \bar{3} \equiv \bar{0} \Rightarrow o(\bar{1}) = 3$

$\bar{2} \oplus \bar{2} \equiv \bar{1} \Rightarrow \bar{1} \oplus \bar{2} = \bar{3} \equiv \bar{0} \Rightarrow o(\bar{2}) = 3.$

Δηλαδή, το $\bar{1}$ και $\bar{2}$ παράγουν την ομάδα $(\mathbb{Z}_3, \oplus)$

Έτσι, $\mathbb{Z}_3 = <\bar{1}> = <\bar{2}>$ (κυκλική)

Μια άλλη παρατήρηση είναι ότι $(1,3) = (2,3) = 1$

Επίσης, παρατηρούμε ότι στο $(\mathbb{Z}_3, \oplus)$ $o(\bar{1}) = o(\bar{2}) = |\mathbb{Z}_3| = 3$

και τότε έπεται ότι $\bar{1}$ και $\bar{2}$ γεννήτορες του $\mathbb{Z}_3$.

2) Εαν a, b δύο μη τετριμμένα στοιχεία της ομάδας G τέτοια ώστε: $o(b) = 2$ και $bab^{-1} = a^2$, να βρεθεί η τάξη του στοιχείου a.

<u>ΛΥΣΗ</u>

$o(b) = 2 \Leftrightarrow b^2 = e \Leftrightarrow b \cdot b = e \Leftrightarrow b^{-1} = b$

Επίσης, $bab^{-1} = a^2 \Leftrightarrow (bab^{-1})^2 = (a^2)^2 \Leftrightarrow$

$\Leftrightarrow bab^{-1} \cdot bab^{-1} = a^4 \Leftrightarrow ba^2b^{-1} = a^4 \xLeftrightarrow{\text{Υποθ.}}$

$\Leftrightarrow b(bab^{-1})b^{-1} = a^4 \Leftrightarrow b^2 a (b^{-1})^2 = a^4 \Leftrightarrow$

$\Leftrightarrow e \cdot a \cdot e = a^4 \Leftrightarrow a = a^4 \Leftrightarrow a^3 = 1 \Leftrightarrow \boxed{o(a) = 3.}$

3) Να βρείτε την τάξη της ομάδας $(\mathbb{Z}_2 \times \mathbb{Z}_2, \oplus)$ και να εξετάσετε εαν είναι κυκλική.

<u>ΛΥΣΗ</u>

$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{1},\bar{0}), (\bar{1},\bar{1})\} \Rightarrow |\mathbb{Z}_2 \times \mathbb{Z}_2| = 4$

Η ομάδα $(\mathbb{Z}_2 \times \mathbb{Z}_2, \oplus)$ δεν είναι κυκλική

$(\bar{0},\bar{1}) \oplus (\bar{0},\bar{1}) = (\bar{0},\bar{0}) \Rightarrow o(\bar{0},\bar{1}) = 2$

$(\bar{1},\bar{0}) \oplus (\bar{1},\bar{0}) = (\bar{0},\bar{0}) \Rightarrow o(\bar{1},\bar{0}) = 2$

$(\bar{1},\bar{1}) \oplus (\bar{1},\bar{1}) = (\bar{0},\bar{0}) \Rightarrow o(\bar{1},\bar{1}) = 2$

Κανένα στοιχείο δεν γεννάει την ομάδα $(\mathbb{Z}_2 \times \mathbb{Z}_2, \oplus)$

(ισοδύναμη της ομάδας Klein $\{e, a, b, c\}$ για $a \cdot a = e$, $b \cdot b = e$, $c \cdot c = e$)

4) Ποιο το πλήθος γεννητόρων μίας κυκλικής ομάδας τάξης

α. 5 και β. 12

ΛΥΣΗ

Εστω G κυκλική τάξης n

Το πλήθος γεννητόρων της G είναι ίσο με $\varphi(n)$

οπου $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ η συνάρτηση Euler

Γραφοντας το $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$ (πρωτογενής αναλυση)

Παίρνουμε οτι

α. $\varphi(5) = 5 - 1 = 4$

β. $\varphi(12) = \varphi(3 \cdot 2^2) = \varphi(3)\varphi(2^2) = 2 \cdot 2(2-1) = 4.$

Πρόταση: Έστω $(G,*)$ μια ομάδα και τυχόν $a\in G$ τέτοιο ώστε $o(a)=n$. Τότε, $(\forall k\geq 1)$: $a^k=e_G \Leftrightarrow o(a)|k$

ΑΠΟΔΕΙΞΗ:

$(\Leftarrow)$: Έστω ότι $o(a)=n|k \Rightarrow k=\lambda n$, $\lambda\in\mathbb{Z}$ και $o(a)=n \Leftrightarrow a^n=e_G$.
Τότε $a^k=a^{\lambda n}=(a^n)^\lambda=e_G$.

$(\Rightarrow)$: Έστω ότι για τυχόν $k\geq 1$ $a^k=e_G$
Εφαρμόζοντας την Ευκλείδεια Διαίρεση $k=\lambda n+v$, $1\leq v<n$
Έτσι, $a^k=a^{\lambda n+v}=(a^n)^\lambda\cdot a^v=e_G^\lambda\cdot a^v=a^v=e_G$
Αναγκαστικά $v=0$ (διότι εάν $v\neq 0$ άτοπο αφού $v<n$ και ταυτόχρονα $o(a)=n\Leftrightarrow a^n=e_G$)

ΘΕΩΡΗΜΑ: Έστω $(G,*)$ μια ομάδα και τυχόν $g\in G$ πεπερασμένης τάξης τέτοια ώστε $o(g)=n$. Τότε για κάθε $k\in\mathbb{Z}$

$$\underbrace{o(g^k)=\frac{o(g)}{(o(g),k)}=\frac{n}{(n,k)}}_{①},\quad \underbrace{k|n\Leftrightarrow o(g^k)=\frac{n}{|k|}}_{②},\quad \underbrace{(k,n)=1\Leftrightarrow o(g^k)=n}_{③}$$

ΑΠΟΔΕΙΞΗ

Ας είναι $o(g^k)=r$ και ΘΔΟ $r=\dfrac{n}{(n,k)}$

Έχουμε, $o(g^k)=r\Rightarrow g^{kr}=e_G \overset{\text{Πρόσ}}{\Leftrightarrow} n|kr$
Άρα, $kr=\mu\cdot n$, $\mu\in\mathbb{Z}$
Επειδή, τώρα $(n,k)|n$ και $(n,k)|k \Leftrightarrow n=n'\cdot(n,k)$ & $k=k'(n,k)$ ώστε $(n',k')=1$. Τότε, $n'=\dfrac{n}{(n,k)}$.
Αρκεί, νδο $r=n'$

$kr=\mu n\Rightarrow k'(n,k)=\mu\cdot n'(n,k)\Rightarrow k'r=m\cdot n'\Rightarrow n'|k'r \overset{(n',k')=1}{\Longrightarrow}$
$\Rightarrow n'|r\Rightarrow n'\leq r$ ①'

Από την άλλη, $kn'=k'(n,k)\cdot n'=k'\cdot n$
Άρα,
$$(g^k)^{n'}=g^{kn'}=g^{k'n}=(g^n)^{k'}=e_G^{k'}=e_G\Rightarrow r\leq n' \quad ②'$$
Συνεπώς, Από ①'+②' $\Longrightarrow n'=r$
Οι άλλες δύο προκύπτουν από την 1η

Πόρισμα: Εαν $(G,*)$ μια κυκλική ομάδα τάξης n, με γεννήτορα το στοιχείο a $(G=\langle a\rangle)$, τότε ένα στοιχείο a^k της G είναι γεννήτορας της G αν.ν $(k,n)=1$

ΑΠΟΔΕΙΞΗ

a^k γεννήτορας της $G \Leftrightarrow o(a^k)=o(a)$

Πράγματι, εαν a^k γεννήτορας της $G \Leftrightarrow \langle a^k\rangle = G$ και άρα $o(a^k)=o(G)=o(a)$.

Αντίστροφα,

εαν $o(a^k)=o(a)$, τότε η υποομάδα $\langle a^k\rangle$ της G που παράγεται απο το a^k θα έχει $o(G)=o(a)$ και άρα $\langle a^k\rangle=G$ δηλαδη a^k γεννήτορας της G

Αλλά, από το θεώρημα

$$o(a^k)=o(a) \Leftrightarrow \frac{n}{(k,n)}=n \Leftrightarrow (k,n)=1$$

ΠΡΟΤΑΣΗ 1: Έστω $(G,\cdot)$ ομάδα

1) Για κάθε $x,a\in G$: $o(x^{-1}ax)=o(a)$
2) Για κάθε $a,b\in G$: $o(ab)=o(ba)$

ΑΠΟΔΕΙΞΗ

1) Εστω τυχαία x,a στοιχεία του G και έστω $o(x^{-1}ax)=n$

$$\Leftrightarrow (x^{-1}ax)^n=e \Leftrightarrow (x^{-1}ax)(x^{-1}ax)\ldots(x^{-1}ax)=e \Leftrightarrow$$

$$\Leftrightarrow x^{-1}a^n x = e \overset{\text{ομάδα}}{\Leftrightarrow} a^n = xex^{-1} \Leftrightarrow a^n=e$$

Συνεπώς, $\{n\in\mathbb{N} \mid a^n=e\}=\{n\in\mathbb{N} \mid (x^{-1}ax)^n=e\} \Leftrightarrow$

$$\Leftrightarrow \min\{n\in\mathbb{N} \mid a^n=e\}=\min\{n\in\mathbb{N} \mid (x^{-1}ax)^n=e\} \Leftrightarrow$$

$$\Leftrightarrow o(a)=o(x^{-1}ax)=n$$

2) Εστω τυχαία $a,b\in G$. Τοτε ισχυει απο Ερωτ.(i)

$$o(ab)=o(a^{-1}\underbrace{ab}a)=o(ba)$$

ΠΡΟΤΑΣΗ 2: Έστω $(G,\cdot)$ αβελιανή ομάδα και $o(a)=n$, $o(b)=m$ όπου $(o(a),o(b))=(n,m)=1$. Τότε, $o(ab)=o(a)\cdot o(b)$.

ΑΠΟΔΕΙΞΗ

Έστω $o(ab)=r$, και θδο $r=n\cdot m$.

Δίνονται: $o(a)=n \Leftrightarrow a^n=e$, $n=\min\{n'\in\mathbb{N} \mid a^{n'}=e\}$

και $o(b)=m \Leftrightarrow b^m=e$, $m=\min\{m'\in\mathbb{N} \mid b^{m'}=e\}$

$$(a\cdot b)^{mn}=\underbrace{(a\cdot b)\cdots(a\cdot b)}_{m\cdot n \text{ φορές}}=a^{nm}\cdot b^{nm}=e^m\cdot e^n=e \Rightarrow o(ab)=r \mid nm=o(a)\cdot o(b)$$

Μένει νδο $n\cdot m \mid r$.

$o(ab)=r \Leftrightarrow (ab)^r=e$, $r=\min\{r'\in\mathbb{N} \mid (ab)^{r'}=e\}$

Έτσι, λόγω ότι G αβελιανή: $(ab)^r=a^r\cdot b^r=e \xLeftrightarrow{G \text{ ομάδα}} a^r=b^{-r} \Rightarrow$

$\Rightarrow o(a^r)=o(b^{-r})\overset{\text{ίδιος}}{=}o(b^r)$ ①. Τότε, από προαναφερόμενο θεώρημα:

$$\begin{cases} o(a^r)=\dfrac{o(a)}{(o(a),r)}=\dfrac{n}{(n,r)} \\ o(b^r)=\dfrac{o(b)}{(o(b),r)}=\dfrac{m}{(m,r)} \end{cases} \xRightarrow{①} \frac{n}{(n,r)}=\frac{m}{(m,r)} \Rightarrow n(m,r)=m(n,r) \xRightarrow{(n,m)=1}$$

$$\Rightarrow \begin{cases} n \mid (n,r) \\ m \mid (m,r) \end{cases} \xRightarrow[\text{διαιρετών}]{\text{ΜΚΔ}=\max} \begin{cases} n=(n,r) \\ m=(m,r) \end{cases} \Longrightarrow \begin{cases} n \mid r \\ m \mid r \end{cases}$$

$$\xRightarrow{(m,n)=1} m\cdot n \mid r \Rightarrow o(ab) \mid o(a)o(b)$$

Συνεπώς, $o(ab)=o(a)\cdot o(b)$