26/3/2018

ΠΡΟΤΑΣΗ Έστω G ομάδα $a \in G$ με $ord(a) = d < \infty$ και $s \in \mathbb{Z}$. Τότε $ord(a^s) = \frac{d}{ΜΚΔ(d,s)}$

ΑΠΟΔΕΙΞΗ

Θέτουμε $n = \frac{d}{ΜΚΔ(d,s)}$

Βήμα 1ο. ΙΣΧΥΡΙΣΜΟΣ 1 $(a^s)^n = e$

ΑΠΟΔ. Αφού $(a^s)^n = a^{s \cdot n}$ αρκεί να δείξουμε ότι $d \mid s \cdot n$. Έχουμε

$$s \cdot n = s \cdot \frac{d}{ΜΚΔ(d,s)} = d \cdot \frac{s}{ΜΚΔ(d,s)}$$

Άρα πράγματι $d \mid n \cdot s$, άρα $a^{s \cdot n} = e$.

Βήμα 2ο ΙΣΧΥΡΙΣΜΟΣ 2. Έστω $m > 0$ με $(a^s)^m = e$. Τότε $n \mid m$

ΑΠΟΔ.

$$(a^s)^m = e \Rightarrow a^{sm} = e \xrightarrow{\text{ΠΡΟΤ.}} d \mid sm.$$

$$\Rightarrow \frac{d}{ΜΚΔ(d,s)} \mid \frac{d}{ΜΚΔ(d,s)} \cdot m \quad (1)$$

Από Θεωρία αριθμών

$$\text{ΜΚΔ}\left(\frac{d}{\text{ΜΚΔ}(d,s)}, \frac{s}{\text{ΜΚΔ}(d,s)}\right) = 1$$

Άρα $(1) \Rightarrow \frac{d}{\text{ΜΚΔ}(d,s)} \mid m$, δηλ. $n \mid m$

Η πρόταση έπεται.

ΠΑΡΑΔΕΙΓΜΑ Έστω G ομάδα και $a \in G$ με

$\text{ord}(a) = 8$. Τότε $\text{ord}(a^2) = \frac{8}{\text{ΜΚΔ}(8,2)} = \frac{8}{2} = 4$

$$\text{ord}(a^3) = \frac{8}{\text{ΜΚΔ}(8,3)} = \frac{8}{1} = 8$$

$$\text{ord}(a^4) = \frac{8}{\text{ΜΚΔ}(8,4)} = \frac{8}{4} = 2$$

$$\text{ord}(a^5) = \frac{8}{\text{ΜΚΔ}(8,5)} = \frac{8}{1} = 8$$

$$\text{ord}(a^6) = \frac{8}{\text{ΜΚΔ}(8,6)} = \frac{8}{2} = 4$$

$$\text{ord}(a^7) = \frac{8}{\text{ΜΚΔ}(8,7)} = \frac{8}{1} = 8$$

$$\text{ord}(a^{-2018}) = \frac{8}{\text{ΜΚΔ}(8,-2018)} = \frac{8}{\text{ΜΚΔ}(8,2018)} = \frac{8}{2} = 4$$

$2018 = 252 \cdot 8 + 2$

$8 = 4 \cdot 2 + 0$ άρα $\text{ΜΚΔ}(8,2018) = 2$

ΕΡΩΤΗΜΑ Από πρόταση $\langle a \rangle = \{a, a^2, \dots, a^7, a^8 = e\}$

Ποιό από τα στοιχεία είναι το a^{2018};

ΛΥΣΗ $2018 = 252 \cdot 8 + 2 \Rightarrow$

$-2018 = (-252) \cdot 8 - 2 =$

$(-252) \cdot 8 - 8 + 8 - 2 = (-253) \cdot 8 + 6$

Από πρόταση αφού $-2018 \equiv 6 \bmod 8$

έχουμε $a^{-2018} = a^6$

(ΥΠΕΝΘΥΜΙΣΗ Πρόταση: Αν $ord(a) = d$ τότε

$a^{k_1} = a^{k_2} \iff k_1 \equiv k_2 \bmod d$)

ΠΑΡΑΤΗΡΗΣΗ Από τους υπολογισμούς προκύπτει ότι:

1) $\langle a \rangle = \langle a^1 \rangle = \langle a^3 \rangle = \langle a^5 \rangle = \langle a^7 \rangle$

2) Αν $s = 2, 4, 6, 8$ τότε $\langle a^s \rangle \neq \langle a \rangle$,

διατί $\# \langle a^s \rangle < 8$

$\| \quad$

$ord(a^s)$

ΠΟΡΙΣΜΑ Έστω G ομάδα και $a \in G$ με $ord(a) = d < \infty$

1) Αν $s \in \mathbb{Z}$ με $1 \leq s \leq d$ και $ΜΚΔ(s, d) = 1$

τότε $\langle a^s \rangle = \langle a \rangle$, δηλ. a^s γεννήτορας της $\langle a \rangle$

2) Αν $s \in \mathbb{Z}$ με $1 \leq s \leq d$ και $ΜΚΔ(s, d) \neq 1$, τότε

$\langle a^s \rangle \subsetneq \langle a \rangle$ δηλ a^s ΟΧΙ γεννήτορας της $\langle a \rangle$

ΑΠΟΔΕΙΞΗ Έχουμε $\langle a^s \rangle = \langle a \rangle \iff ord(a^s) = d$

$\iff \frac{d}{ΜΚΔ(d, s)} = d \iff ΜΚΔ(d, s) = 1$

ΠΑΡΑΤΗΡΗΣΗ Αν G ομάδα $a \in G$ με $ord(a) = d < \infty$, το πόρισμα μας υποδίγει το σύνολο $\{g \in G : \langle g \rangle = \langle a \rangle\}$

και έχουμε ότι αυτό το σώμα έχει ακριβώς $\phi(d)$ στοιχεία όπου ϕ η συνάρτηση ϕ του Euler. Στο παράδειγμα $d=8$ και $\phi(8) = \phi(2^3) = (2-1)\cdot 2^2 = 4$.

ΠΡΟΤΑΣΗ Έστω G ομάδα, $a \in G$ $ord(a) = +\infty$ και $s \in \mathbb{Z}$.

1) Αν $s=0$ τότε $a^s = e$, άρα $ord(a^s) = 1$
2) Αν $s \neq 0$ τότε $ord(a^s) = +\infty$

ΑΠΟΔΕΙΞΗ

1) Προφανές
2) Έστω από πρόταση αρκεί να δείξουμε ότι αν $m \in \mathbb{Z}$ με $m > 0$ $(a^s)^m \neq e$

Πράγμα $(a^s)^m = a^{sm} \neq e$ αφού $sm \in \mathbb{Z} \setminus \{0\}$ και $ord(a) = +\infty$

ΠΑΡΑΔΕΙΓΜΑ Αν $G = (\mathbb{Z}, +)$ και $a = 1$, τότε $G = \langle a \rangle$ και έχουμε $ord(0) = 1$ $ord(k) = +\infty$ όταν $k \in \mathbb{Z} \setminus \{0\}$

ΠΟΡΙΣΜΑ Έστω G ομάδα, $a \in G$ με $ord(a) = +\infty$ και $s \in \mathbb{Z}$. Τότε $\langle a^s \rangle = \langle a \rangle$ αν και μόνο αν $s = 1$ ή $s = -1$

ΑΠΟΔΕΙΞΗ Αν $s = 1$, $\langle a^s \rangle = \langle a^1 \rangle = \langle a \rangle$
Αν $s = -1$, $a = (a^{-1})^{-1} \in \langle a^{-1} \rangle$
άρα $\langle a \rangle \subseteq \langle a^{-1} \rangle$. Από ορισμό $\langle a \rangle$ έχουμε $\langle a \rangle = \langle a^{-1} \rangle$. Συνεπώς $\langle a^{-1} \rangle = \langle a \rangle$

Αντίστροφα, έστω $s \in \mathbb{Z}$ $\langle a^s \rangle = \langle a \rangle$
Αφού $a \in \langle a \rangle$, έχουμε $a \in \langle a^s \rangle$. Άρα υπάρχει

$k \in \mathbb{Z}$ με $a = (a^s)^k \Rightarrow a^1 = a^{sk}$ (1)

Αφού $ord(a) = +\infty$ από πρόταση αν $k_1, k_2 \in \mathbb{Z}$ με $a^{k_1} = a^{k_2}$ τότε $k_1 = k_2$. Άρα η (1) $\Rightarrow$ $sk = 1 \Rightarrow$ s|1 στο $\mathbb{Z} \Rightarrow$

$s = 1$ ή $s = -1$

Φυλ 2, Ασκ 2 $G = (GL_2\mathbb{R}, \cdot)$ Να υπολογιστεί $\langle A \rangle$ όταν

1) $A = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$

ΛΥΣΗ $A \in G$, γιατί $\det A = 1$

$$A^2 = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

$$A^3 = A \cdot A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \quad A^4 = A \cdot A^3 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$$

$$A^5 = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \quad A^6 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Άρα $ord(A) = 6$ Από πρόταση
$\langle A \rangle = \{A, A^2, A^3, A^4, A^5, A^6\}$

2) $A = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$ Φανερά $A \in G$, γιατί $\det A = -1$

Έχουμε $A^2 = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}\cdot\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$

Άρα από πρόταση $ord(A) = 2$ και $\langle A \rangle = \{A, A^2\}$

3) $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ Τότε $A^2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$

$$A^3 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$$

ΙΣΧΥΡΙΣΜΟΣ 1 Έστω $m>0$ Τότε $A^m = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$

Απόδειξη Με επαγωγή την έχουμε κάνει

Συνεπώς $ord(A) = +\infty$ $\langle A \rangle = \{A^k : k \in \mathbb{Z}\}$ και

$k_1 \neq k_2 \Rightarrow A^{k_1} \neq A^{k_2}$

ΙΣΧΥΡΙΣΜΟΣ 2

$$A^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

Απόδειξη Άμεση

ΙΣΧΥΡΙΣΜΟΣ 3 Έστω $m>0$. Τότε $A^{-m} = \begin{pmatrix} 1 & -m \\ 0 & 1 \end{pmatrix}$

ΑΠΟΔΕΙΞΗ Επαγωγή στο m. Εύκολη άσκηση

Συμπέρασμα $\langle A \rangle = \left\{ \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} : m \in \mathbb{Z} \right\}$ χρησιμοποιούμε $A^{-m} = (A^{-1})^m$

4) $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ $A^2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$

ΙΣΧΥΡΙΣΜΟΣ Έστω $r \geq 2$. Γράφουμε $A^r = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

Τότε $a \geq 2$, $b, c, d \geq 0$

ΑΠΟΔΕΙΞΗ

Για $r=2$ ισχύει. Έστω $r \geq 2$ και ότι ισχύει για r. Τότε $A^{r+1} = A \cdot A^r = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} =$

$\begin{pmatrix} a' = a+c & b' = b+d \\ c' = a & d' = b \end{pmatrix}$ Άρα $a' = a+c \geq a \geq 2$

$b' = b+d \geq b \geq 0$, $c' = a \geq 2 \geq 0$, $d' = b \geq 0$

Επομένως ο ισχυρισμός ισχύει

Άρα για $r \geq 1$ $A^r \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, άρα για $r=1$

Προφανές, ενώ για $r \geq 2$ από ισχυρισμό το $(1,1)$ στοιχείο του A είναι $\neq e$ άρα διάφορο του I. Από πρόταση $ord(A) = +\infty$

ΕΡΩΤΗΣΗ Πως υπολογίζουμε A^r για $r \in \mathbb{Z}$;

Απάντηση α' τρόπος Με χρήση ότι A διαγωνίσιμος (δες Γρ. Αλγ. II)

β' τρόπος Με χρήση επαγωγής και ακολουθία Fibonacci (δες ιστοσελίδα του κ. Μπελιγιάννη)

ΑΣΚΗ ΦΥΛ 2

1) $G = (\mathbb{Z}, +)$ $H_1 = (2\mathbb{Z}, +)$ $H_2 = (3\mathbb{Z}, +)$

2) $G = (\mathbb{Q}, +)$ $H_1 = \left\langle \frac{1}{2} \right\rangle = \left\{ \frac{k}{2}, k \in \mathbb{Z} \right\}$

$H_2 = \left\langle \frac{1}{3} \right\rangle = \left\{ \frac{k}{3} : k \in \mathbb{Z} \right\}$

3) $(S_3, \circ)$ Το έχουμε κάνει

4) $(8\mathbb{Z}, +) = \{\ldots, -16, -8, 0, 8, 16, 24, \ldots\}$

$H_1 = \langle 16 \rangle = 16\mathbb{Z}$ $H_2 = \langle 40 \rangle = 40\mathbb{Z}$

ΦΥΛ 2 ΑΣΚ 8

ΠΑΡΑΤΗΡΗΣΗ Έστω G ομάδα και $a, b \in G$. Τα ακόλουθα είναι ισοδύναμα.

1) $ord(a) = ord(b)$

2) Αν $k \in \mathbb{Z}, k \neq 0$ $a^k = e$ αν και μόνο αν $b^k = e$.

ΑΠΟΔΕΙΞΗ ΠΑΡΑΤΗΡΗΣΗΣ.

1) $\Rightarrow$ 2) Αν $ord(a) = ord(b) = +\infty$, τότε $a^k \neq e$ για κάθε $k \in \mathbb{Z}$ με $k > 0$ και $b^k \neq e$ για κάθε $k \in \mathbb{Z}$. Άρα η (2) ισχύει

Υποδείξουμε $ord(a) = ord(b) = d < \infty$

Τότε $a^k = e \overset{\text{ΠΡΟΤΑΣΗ}}{\iff} d \mid k \overset{\text{ΠΡΟΤ}}{\iff} b^k = e$. Άρα η (2) ισχύει.

2) $\Rightarrow$ 1) ΠΕΡΙΠΤΩΣΗ 1 Έστω $ord(a) = +\infty$. Τότε $a^k = e$ για κάθε $k > 0$. Άρα από 2) $b^k \neq e$ για κάθε $k > 0$. Άρα $ord(b) = +\infty$

ΠΕΡΙΠΤΩΣΗ 2 Έστω $ord(a) = d < \infty$. Τότε από 2) ο ελάχιστος θετικός ακέραιος m με $b^m = e$ είναι ο d. Άρα $ord(b) = d = ord(a)$.

ΣΥΜΠΕΡΑΣΜΑ Για να δείξουμε $ord(a') = ord(b')$ αρκεί ν.δ. για κάθε $k > 0$ ότι

$(a')^k = e \iff (b')^k = e$.

a) $ord(x^{-1} * a * x) = ord(a)$

b) $ord(a * b) = ord(b * a)$

c) $ord(a^{-1}) = ord(a)$.

ΑΠΟΔΕΙΞΗ a) $(x^{-1} * a * x)^2 = (x^{-1} * a * x) * (x^{-1} * a * x) =$

$(x^{-1} * a) * (x * x^{-1}) * (a * x) = (x^{-1} * a * e * a * x) = x^{-1} * a^2 * x$

ΙΣΧΥΡΙΣΜΟΣ 1 Έστω $k > 0$. Τότε $(x^{-1} * a * x)^k =$

$x^{-1} * a^k * x$ ΑΠΟΔΕΙΞΗ Άμεση με επαγωγή.

ΙΣΧΥΡΙΣΜΟΣ 2 Έστω $k > 0$ Τ.Α.Ε. Ι.

1) $x^{-1} * a^k * x = e$

2) $a^k = e$

ΑΠΟΔΕΙΞΗ 1) $\Rightarrow$ 2) Έστω $x^{-1} * a^k * x = e \Rightarrow$

$x * (x^{-1} * a^k * x) = x * e = x \Rightarrow (x * x^{-1}) * a^k * x = x$

$\Rightarrow a^k * x = x \Rightarrow a^k * x * x^{-1} = x * x^{-1} \Rightarrow a^k = e$

2) ⇒ 1) Υποθέτουμε $a^k = e$. Τότε
$x^{-1} * a^k * x = x^{-1} * e * x = x^{-1} * x = e$

Από ισχυρ. 2 και Παρατήρηση
$ord(x^{-1} * a * x) = ord(a)$

b) Θέτουμε $x = b$. Τότε $x^{-1} * (b * a) * x = a * b$
Επομένως από a) $ord(b*a) = ord(b*a)$

c) Έχουμε για $k > 0$ $(a^{-1})^k = a^{-k} = (a^k)^{-1}$

ΙΣΧΥΡΙΣΜΟΣ 2. Έστω $k > 0$ Τ.Α.Ε.Ι.
1) $a^k = e$
2) $(a^{-1})^k = e$

ΑΠΟΔΕΙΞΗ

1) ⇒ 2) $a^k = e \Rightarrow (a^k)^{-1} = e^{-1} = e \Rightarrow a^{-k} = e$
2) ⇒ 1) $(a^{-1})^k = e \Rightarrow a^{-k} = e \Rightarrow a^k * a^{-k} = a^k * e$.
$\Rightarrow e = a^k$.

Από παρατήρηση και ισχυρισμούς 2 έχουμε
$ord(a^{-1}) = ord(a)$

ΘΥΜΑ ΑΣΚΗΣΗ. $G = (GL_2(\mathbb{R}), \cdot)$
ΛΥΣΗ
$H_1 = \left\langle \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle$ υποομάδα της G τάξης 6.

$H_2 = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \right\rangle$ << << << << 2

ΘΥΜΑ ΑΣΚΗΣΗ 12
1) $n = 5$ Από Θεωρία έχει $\phi(5) = (5-1) \cdot 5^0 = 4$ γεννήτορες

2) $n = 12$ έχει $\phi(12)$ γεννήτορες
$12 = 3 \cdot 4 = 2^2 \cdot 3$
$\phi(12) = (2-1) \cdot 2^1 \cdot (3-1) \cdot 3^0 = 4$

3) $n=60$ Έχει $\phi(60)$ γεννήτορες

$60 = 5\cdot 12 = 5\cdot 3\cdot 2^2$ και $\phi(60) = (2-1)2^{\circ}(5-1)5^{\circ}\cdot (3-1)3^{\circ} = 2\cdot 2\cdot 4 = 16$

ΦΥΛ 2 ΑΣΚ. 14.

1) $G = (\mathbb{Z}_{10}, +)$

ΛΥΣΗ Έστω $a = [1]_{10}$ = έχουμε $G = \langle a \rangle$ και $ord(a) = 10$

Από θεωρία για $1 \le s \le 10$ το $s\cdot a = \underbrace{a+\dots+a}_{s\text{-φορές}}$ είναι γεννήτορας της $G = \langle a \rangle$ αν και μόνο αν $MKD(s, \underset{\text{ord}(a)}{10}) = 1$

Άρα $s \in \{1, 3, 7, 9\}$ και άρα όλοι οι γεννήτορες της G είναι $[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}$

b) $G = (\mathbb{Z}_{12}, +)$ Παρόμοια όλοι οι γεννήτορες της G είναι $[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}$

c) $G = (\mathbb{Z}_{15}, +)$ Παρόμοια όλοι οι γεννήτορες της G είναι $[1]_{15}, [2]_{15}, [4]_{15}, [7]_{15}, [8]_{15}$

$[11]_{15}, [13]_{15}, [14]_{15}$ $\phi(15) = \phi(5)\cdot\phi(5) = 2\cdot 4 = 8$

ΦΥΛ 2 ΑΣΚ 5. ΑΠΟΔΕΙΞΗ

α) τρόπος Έστω $d = ord(a) \ge 3$ Αφού το πλήθος των γεννητόρων της G είναι ίσο με $\phi(d)$ αρκεί να δείξουμε ότι $\phi(d)$ άρτιο

ΠΕΡΙΠΤΩΣΗ 1 d δύναμη του 2 έστω $d = 2^r$. Τότε $r \ge 2$ άρα $\phi(d) = \phi(2^r) = 2^{r-1}$, άρτιο αφού $r-1 \ge 1$

ΠΕΡΙΠΤΩΣΗ 2 Υπάρχει περιττός πρώτος p με $p \mid d$ Τότε από τύπο $\phi(d)$ το $(p-1)$ που είναι άρτιος

διαιρεί το φ(d)

β' τρόπος Έστω $S=\{a_1, a_2, \dots, a_r\}$ το σύνολο γεννητόρων της G.

ΙΣΧΥΡΙΣΜΟΣ 1 Αν $a \in S$ τότε $a \neq a^{-1}$
ΑΠΟΔΕΙΞΗ $a=a^{-1} \Rightarrow a^2=e$ Αλλά

$|G| \geq 3$ ανεξάρτητο
ΙΣΧΥΡΙΣΜΟΣ 2 Αν $a \in S$ τότε $a^{-1} \in S$
Προφανώς είδαμε ότι πάντα $ord(a^{-1}) = ord(a)$ Από Ισχ. 1 και Ισχ. 2. έχουμε #S άρτιο, διότι $a \in S \Rightarrow a^{-1} \in S$ και $a^{-1} \neq a$ άρα το S είναι ξένη ένωση συνόλων με δύο στοιχεία της μορφής $\{a, a^{-1}\}$

ΦΥΛ 2 ΑΣΚ6. Έχουμε δει ότι $H_1 \cap H_2$ υποομάδα
Φανερά $H_1 \cap H_2$ περιέχει τα κοινά πολλαπλάσια των n και m. Έστω f = Ελάχιστο κοινό πολλαπλάσιο των n και m.
ΙΣΧΥΡΙΣΜΟΣ $H_1 \cap H_2 = \langle f \rangle = f\mathbb{Z}$
ΑΠΟΔΕΙΞΗ ΒΗΜΑ 1 Έχουμε f κοινό πολλαπλάσιο των n και m. Άρα $f \in H_1$ και $f \in H_2$
Άρα $f \in H_1 \cap H_2$
Συνεπώς $\langle f \rangle \subseteq H_1 \cap H_2$

ΒΗΜΑ 2 Θ.Δ.Ο. $H_1 \cap H_2 \subseteq \langle f \rangle$
Έστω $x \in H_1 \cap H_2$. Κάνουμε Ευκλείδια Διαίρεση $x = qf + r$ με $0 \leq r < f$ Άρα $r = x - qf$ (*)
$q, r \in \mathbb{Z}$
Συνεπώς x, f κοινά πολλαπλάσια των n και m από (*) το r έχει την ίδια ιδιότητα.
Άρα αν $r \neq 0$ αντίφαση στον ορισμό του f
Άρα $r=0 \Rightarrow x \in \langle f \rangle$