ΑΣΚΗΣΗ: Έστω $G =< \alpha >$ κυκλική τάξεως m και $H =< \beta > \leqslant G$ τάξεως n. Τότε υπάρχει γεννήτορας α' της G τέτοιος, ώστε $\beta = {\alpha'}^{\frac{m}{n}}$.

ΑΠΟΔΕΙΞΗ 1η-Ομαδοθεωρητική: Επαγωγή στο δείκτη $|G:H| = \dfrac{m}{n}$. Για $|G:H| = 1$ προφανές. Έστω $|G:H| > 1 \Leftrightarrow n < m$.

Αν πάλι $H = 1 \Leftrightarrow n = 1$, πάλι τετριμμένο. Υποθέτουμε λοιπόν ότι $1 < |H| < |G|$.

Προφανώς η ακεικόνιση $\varphi : G \to H$ με $\varphi(x) = x^{\frac{m}{n}}$ είναι καλά ορισμένη και επί. $\Big($Η κυκλική ομάδα $G\Big/H$ έχει τάξη $\left|G\Big/H\right| = \dfrac{m}{n}$. Επομένως $x^{\frac{m}{n}}H = (xH)^{\frac{m}{n}} = 1_{G/H} = H$, για κάθε $x \in G$, δηλαδή $\varphi(x) = x^{\frac{m}{n}} \in H$, για κάθε $x \in G$. Η τάξη του $\alpha^{\frac{m}{n}} = \varphi(\alpha)$ είναι προφανώς m και κατά συνέπεια το $\varphi(\alpha) = \alpha^{\frac{m}{n}}$ είναι γεννήτορας της $H\Big)$.

1η παραλλαγή: Εφόσον η $\varphi : G \to H$ είναι είναι επί, υπάρχει $\gamma \in G$ τέτοιο, ώστε $\varphi(\gamma) = \gamma^{\frac{m}{n}} = \beta$. Διακρίνουμε δύο περιπτώσεις:

α) $\gamma \notin H$. Αν $H' :=< \gamma >= G$, δηλαδή το γ γεννήτορας της G, τελειώσαμε. Έστω ότι $H' =< \gamma >$ γνήσια υποομάδα της G. Τότε $H' =< \gamma > \supsetneq H =< \beta >$, γιατί $\beta = \gamma^{\frac{m}{n}} \in < \gamma >= H'$ και $\gamma \notin H$.

Τότε $|H' : H|, |G : H'| < |G : H|$. Με επαγωγή στο δείκτη $|G : H|$ υπάρχουν δ γεννήτορας της H' και α' γεννήτορας της G τέτοιοι, ώστε $\delta^{|H':H|} = \beta$ και ${\alpha'}^{|G:H'|} = \delta$. Επομένως ${\alpha'}^{|G:H|} = {\alpha'}^{|G:H'|\cdot|H':H|} = ({\alpha'}^{|G:H'|})^{|H':H|} = \delta^{|H':H|} = \beta$.

β) $\gamma \in H$. Η $\varphi|_H : H \to H$ είναι επί $\big(\beta = \varphi(\gamma)$ γεννήτορας της $H\big)$, άρα αυτομορφισμός της H. Κατά συνέπεια $H \cap \mathrm{Ker}\varphi = 1$. Αλλά $\mathrm{Ker}\varphi$ κυκλική υποομάδα της G τάξεως $\dfrac{m}{n} > 1$. Έστω $\mathrm{Ker}\varphi =< \varepsilon >$. Θέτουμε $\gamma' = \gamma\varepsilon \notin H$. $\big(\gamma \in H$ και $\varepsilon \notin H\big)$. Προφανώς ${\gamma'}^{\frac{m}{n}} = \gamma^{\frac{m}{n}} \cdot \varepsilon^{\frac{m}{n}} \underset{\varepsilon\in\mathrm{Ker}\varphi}{=} \gamma^{\frac{m}{n}} = \beta$. Αναγόμαστε έτσι στην προηγούμενη περίπτωση με γ' στη θέση του γ. ■

2η παραλλαγή: Όπως προηγουμένως, το $\alpha^{\frac{m}{n}}$ είναι γεννήτορας της H και άρα ο άλλος γεννήτορας αυτής β θα είναι της μορφής $\alpha^{\lambda\cdot\frac{m}{n}}$, όπου $(\lambda, n) = \big(\lambda, |H|\big) = 1$. Θεωρούμε τον ομομορφισμό $\psi : G \to G$ με $\psi(x) = x^\lambda$, για κάθε $x \in G$. Η $\psi|_H$ απεικονίζει τον γεννήτορα $\alpha^{\frac{m}{n}}$ της H στον γεννήτορα β αυτής. Άρα η $\psi|_H$ είναι ένας αυτομορφισμός της H. Επομένως $H \cap \mathrm{Ker}\psi = 1$. Θεωρούμε το στοιχείο $\gamma = \psi(\alpha) = \alpha^\lambda$. Προφανώς $\gamma^{\frac{m}{n}} = \beta$.

α) $\gamma \notin H$. Όπως προηγουμένως, η υποομάδα $H' =< \gamma >$ περιέχει γνήσια την H. Ακολουθούμε την ίδια επιχειρηματολογία $\big($επαγωγή στο δείκτη$\big)$, όπως στο **α)** στην προηγούμενη απόδειξη.

β) $\gamma = \psi(\alpha) \in H$. Επειδή το α είναι γεννήτορας της G, $\mathrm{Im}\psi \leqslant H$. Ακριβέστερα $\mathrm{Im}\psi = H$, γιατί $\gamma^{\frac{m}{n}} \in H$ και $\gamma^{\frac{m}{n}} = \psi(\alpha^{\frac{m}{n}}) = \alpha^{\lambda\cdot\frac{m}{n}} = \beta$ που είναι γεννήτορας της H. Επομένως $\dfrac{|G|}{|\mathrm{Ker}\psi|} = \left|G\Big/\mathrm{Ker}\psi\right| = |H| < |G|$. Επομένως $1 < |\mathrm{Ker}\psi|$. Έστω ε γεννήτορας της $\mathrm{Ker}\psi$. Τότε επειδή $H \cap \mathrm{Ker}\psi = 1$ έχουμε $\gamma\varepsilon \notin H$. Αναγόμαστε στην προηγούμενη περίπτωση με $\gamma' = \gamma\varepsilon$ στη θέση του γ. ■

ΑΠΟΔΕΙΞΗ 2η-Αριθμοθεωρητική: Κατ' αρχάς η περίπτωση $n = 1$ είναι τετριμμένη. Υποθέτουμε λοιπόν ότι $n > 1$. Το πρόβλημα ανάγεται στο εξής:

Έστω $n \mid m$ και $(\lambda, n) = 1$. Υπάρχει λ' τέτοιο, ώστε $(\lambda', m) = 1$ και

$$\lambda' \cdot \frac{m}{n} \equiv \lambda \cdot \frac{m}{n} \mod m; \qquad \textbf{(1)}$$

Πράγματι, το $\alpha^{\frac{m}{n}}$ είναι γεννήτορας της H. Κάθε άλλος γεννήτορας της H είναι της μορφής $\alpha^{\lambda\cdot\frac{m}{n}}$, όπου $(\lambda, n) = 1$. Αν το $\alpha^{\lambda\cdot\frac{m}{n}}$ προέρχεται από έναν άλλο γεννήτορα β της G με ύψωση στην $\dfrac{m}{n}$, τότε το β θα είναι της μορφής $\beta = \alpha^{\lambda'}$, όπου $(\lambda', m) = 1$. Επομένως $\alpha^{\lambda\cdot\frac{m}{n}} = \beta^{\frac{m}{n}} = \alpha^{\lambda'\cdot\frac{m}{n}} \Leftrightarrow \alpha^{\lambda\cdot\frac{m}{n} - \lambda'\cdot\frac{m}{n}} = = 1 \Leftrightarrow m \mid \lambda\cdot\dfrac{m}{n} - \lambda'\cdot\dfrac{m}{n}$, γιατί m είναι η τάξη του α.

Η σχέση (1) είναι ισοδύναμη με τη σχέση $\lambda' \equiv \lambda \mod n$. **(2)**

Θεωρούμε το σύνολο A όλων των διακεκριμένων πρώτων παραγόντων του m, οι οποίοι **δεν διαιρούν ούτε τον λ και ούτε τον n**. $\big($Δηλαδή δεν διαιρούν το $[\lambda, n] \underset{(\lambda,n)=1}{=} \lambda n\big)$.

Έστω ρ το γινόμενο αυτό των πρώτων παραγόντων που ανήκουν στο A. Αν $A = \varnothing$, θέτουμε $\rho = 1$. Επίσης θέτουμε

$$\lambda' = \lambda + \rho n.$$

Προφανώς $\lambda' \equiv \lambda \mod n$. Απομένει να δείξουμε ότι $(\lambda', m) = 1$.

Έστω p ένας πρώτος παράγοντας του m.

α) Αν $p \mid \lambda$, τότε $p \notin A \Leftrightarrow p \nmid \rho$ και επίσης $p \nmid n$, γιατί $(\lambda, n) = 1$. Άρα $p \nmid \rho n$ και συνεπώς $p \nmid \lambda'$.

β) Έστω ότι $p \nmid \lambda$. Αν $p \mid n$, τότε $p \mid \rho n$. Επομένως πάλι $p \nmid \lambda'$. Αν $p \nmid n$, τότε $p \in A$, οπότε $p \mid \rho \Rightarrow p \mid \rho n$. Και πάλι $p \nmid \lambda'$.

Συμπέρασμα: $(\lambda', m) = 1$. Τέλος. ■