# ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

## ΤΜΗΜΑ **Β΄**

## ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΑΣΚΗΣΕΙΣ - ΦΥΛΛΑΔΙΟ **9**

ΔΙΔΑΣΚΩΝ: Α. Μπεληγιάννης

ΙΣΤΟΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ:
http://users.uoi.gr/abeligia/NumberTheory/NT2016/NT2016.html

**Πέμπτη 12 Ιανουαρίου 2017**

**Άσκηση 1.** *Να βρεθούν οι τάξεις:*

$$\mathsf{ord}_5(2), \quad \mathsf{ord}_{10}(3), \quad \mathsf{ord}_{13}(10), \quad \mathsf{ord}_{10}(7)$$

**Άσκηση 2.** *Να βρεθούν οι τάξεις:*

$$\mathsf{ord}_{11}(3), \quad \mathsf{ord}_{17}(3), \quad \mathsf{ord}_{21}(10), \quad \mathsf{ord}_{25}(2)$$

**Άσκηση 3.** *Βρείτε τις τάξεις* $\bmod 24$ *των ακεραίων* $5$*,* $7$*,* $9$*, και* $11$*.*

**Άσκηση 4.** *Έστω* $n > 1$ *ένας φυσικός, και* $a, b$ *δύο θετικοί ακέραιοι, όπου* $(a, n) = 1 = (b, n)$*. Δείξτε ότι:*

$$\frac{[\mathsf{ord}_n(a), \mathsf{ord}_n(b)]}{(\mathsf{ord}_n(a), \mathsf{ord}_n(b))} \ \leq \ \mathsf{ord}_n(ab) \ \leq \ [\mathsf{ord}_n(a), \mathsf{ord}_n(b)]$$

**Άσκηση 5.** *Έστω* $F_n = 2^{2^n} + 1$ *ο* $n$*-οστός αριθμός του Fermat. Δείξτε ότι*

$$\mathsf{ord}_{F_n}(2) \ \leq \ 2^{n+1}$$

*Επιπλέον δείξτε ότι ο αριθμός* $2$ *δεν είναι πρωταρχική ρίζα* $\bmod F_n$*.*

**Άσκηση 6.** *Βρείτε αρχικές ρίζες* $\bmod n$ *για* $n = 18$ *και* $n = 27$*.*

**Άσκηση 7.** *Βρείτε όλες τις πρωταρχικές ρίζες* $\bmod 98$*.*

**Άσκηση 8.** *Δείξτε ότι δεν υπάρχουν πρωταρχικές ρίζες* $\bmod 105$*.*

**Άσκηση 9.** *Δείξτε ότι το* $5$ *είναι αρχική ρίζα* $\bmod 23$*. Ακολούθως, λύστε την ισοτιμία*

$$x^6 \equiv 4 \bmod 23.$$

**Άσκηση 10.** *Γνωρίζοντας ότι το* $6$ *είναι μια πρωταρχική ρίζα* $\mathsf{mod}\,41$*, να βρείτε όλες τις λύσεις της ισοτιμίας:*

$$x^{21} \equiv 27\,(\mathsf{mod}\,31)$$

**Άσκηση 11.** *Έστω* $p$ *ένας περιττός πρώτος και* $r$ *μια πρωταρχική ρίζα* $\mathsf{mod}\,p$*, όπου* $(r,p)=1$*. Δείξτε ότι*

$$r^{\frac{p-1}{q}} \not\equiv 1\,(\mathsf{mod}\,p)$$

*για κάθε πρώτο διαιρέτη* $q$ *του* $p-1$*.*

**Άσκηση 12.** *Δείξτε ότι το* $3$ *είναι μια πρωταρχική ρίζα* $\mathsf{mod}\,31$*. Ακολούθως να βρείτε όλες τις λύσεις της ισοτιμίας:*

$$36^{5x} \equiv 1\,(\mathsf{mod}\,41)$$

**Άσκηση 13.** *Έστω* $n \in \mathbb{N}$ *και υποθέτουμε ότι* $n = rs$*, όπου* $(r,s)=1$ *και* $r,s>2$*. Να δειχθεί ότι για κάθε ακέραιο* $a$ *με* $(a,n)=1$*, ισχύει ότι:*

$$a^{\frac{\varphi(n)}{2}} \equiv 1\,(\mathsf{mod}\,n)$$

**Άσκηση 14.** *Έστω ότι* $g$ *μια πρωταρχική ρίζα* $\mathsf{mod}\,n$*, και επομένως*

$$\mathsf{U}(\mathbb{Z}_n) = \left\{1, g, g^2, \cdots, g^{\phi(n)-1}\right\}$$

*Αν* $a \in \mathsf{U}(\mathbb{Z}_n)$*, δηλαδή* $(a,n)=1$*, τότε* $a \equiv g^k\,(\mathsf{mod}\,n)$*, για έναν μοναδικό μη-αρνητικό ακέραιο* $k$ *έτσι ώστε:* $0 \le k \le \phi(n)-1$*, ο οποίος καλείται* **δείκτης του** $a$ **ως προς βάση** $g$*, και συμβολίζεται με* $\mathsf{ind}_g(a)$*, δηλαδή:*

$$\mathsf{ind}_g(a) = k \quad \Longleftrightarrow \quad a \equiv g^k\,(\mathsf{mod}\,n)$$

*Δείξτε ότι αν* $a,b \in \mathbb{Z}$*, είναι τέτοιοι ώστε* $(a,n)=1=(b,n)$*, τότε:*

$$a \equiv b\,(\mathsf{mod}\,n) \quad \Longleftrightarrow \quad \mathsf{ind}_g(a) = \mathsf{ind}_g(b)$$

**Άσκηση 15.** *Έστω ότι* $g$ *είναι μια πρωταρχική ρίζα* $\mathsf{mod}\,n$*. Δείξτε ότι:*

(1) $\mathsf{ind}_g(ab) = \mathsf{ind}_g(a) + \mathsf{ind}_g(b)\,(\mathsf{mod}\,\phi(n))$.
(2) $\mathsf{ind}_g(1) = 0$ *και* $\mathsf{ind}_g(g) = 1$.

**Άσκηση 16.** *Αφού δείξετε ότι το* $2$ *είναι μια πρωταρχική ρίζα* $\mathsf{mod}\,13$*, να βρεθούν οι δείκτες* $\mathsf{ind}_2(a)$ *ως προς βάση* $2$ *των στοιχείων του συνόλου* $\mathsf{U}(\mathbb{Z}_{13})$*.*

*Ποιός είναι ο δείκτης* $\mathsf{ind}_2(2013)$*;*