ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

ΤΜΗΜΑ **Β΄**

ΑΣΚΗΣΕΙΣ - ΦΥΛΛΑΔΙΟ **9**

ΔΙΔΑΣΚΩΝ: Α. Μπεληγιάννης

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

Πέμπτη 12 Ιανουαρίου 2017

Άσκηση 1. *Έστω a και n δύο ακέραιοι, όπου $n \geq 1$. Να δειχθεί ότι ο θετικός ακέραιος x είναι λύση της ισοτιμίας*

$$a^x \equiv 1 \pmod{n}$$

αν και μόνον αν: $\mathsf{ord}_n(a) \mid x$.

Ως εφαρμογή να βρεθούν όλες οι θετικές ακέραιες λύσεις της ισοτιμίας $2^x \equiv 1 \pmod{7}$.

Άσκηση 2. *Έστω $n \geq 3$ ακέραιος. Δείξτε ότι*

$$(n-1, n) = 1 \quad \& \quad \mathsf{ord}_n(n-1) = 2$$

Σαν συνέπεια να συμπεράνετε ότι: $2 \mid \phi(n)$.

Άσκηση 3. *Έστω $n \geq 2$ ακέραιος και a, b ακέραιοι με $ab \equiv 1 \pmod{n}$. Δείξτε ότι:*

$$(a, n) = (b, n) = 1 \quad \& \quad \mathsf{ord}_n(a) = \mathsf{ord}_n(b)$$

Άσκηση 4. *Βρείτε τις τάξεις* $\mathsf{mod}\, 16$ *των ακεραίων* $3, 5, 7$ *και* 9.

Άσκηση 5. *Έστω $n > 1$ ένας θετικός ακέραιος, και $a \in \mathbb{Z}$ ένας ακέραιος ο οποίος είναι πρώτος προς τον m, έτσι ώστε* $\mathsf{ord}_m(a) = m - 1$. *Δείξτε ότι ο m είναι πρώτος.*

Άσκηση 6. *Βρείτε τις τάξεις των στοιχείων του* $\mathsf{U}(\mathbb{Z}_9)$ *και* $\mathsf{U}(\mathbb{Z}_{10})$, *όπου* $\mathsf{U}(\mathbb{Z}_n) = \mathsf{U}_n$ *είναι το σύνολο των αντιστρεψίμων στοιχείων του $\mathbb{Z}_n$.*

Άσκηση 7. *Δείξτε ότι αν a, n είναι θετικοί ακέραιοι, τότε:*

$$\mathsf{ord}_{a^n-1}(a) = n$$

και ακολούθως να συμπεράνετε ότι: $n \mid \phi(a^n - 1)$.

Άσκηση 8. *Έστω $n \geq 2$ και $a \in \mathbb{Z}$. Υποθέτουμε ότι* $a^{n-1} \equiv 1 \pmod{n}$, *και* $a^d \not\equiv 1 \pmod{n}$ *για κάθε γνήσιο θετικό διαιρέτη d του $n - 1$. Να δειχθεί ότι ο n είναι πρώτος.*

Άσκηση 9. **1.** *Βρείτε, αν υπάρχουν, πρωταρχικές ρίζες* $(\mathsf{mod}\, n)$*, όπου* $n = 4, 5, 10, 13, 14, 18$.
2. *Βρείτε, αν υπάρχουν, πρωταρχικές ρίζες* $(\mathsf{mod}\, 20)$.

Άσκηση 10. *Βρείτε αρχικές ρίζες* $\mathsf{mod}\, n$ *για* $n = 23$ *και* $n = 31$.

Άσκηση 11. *Έστω* $n > 1$ *ένας θετικός ακέραιος, και* a, b *δύο θετικοί ακέραιοι έτσι ώστε:*

$$(a, n) = 1 = (b, n) \quad \& \quad (\mathsf{ord}_n(a), \mathsf{ord}_n(b)) = 1$$

Δείξτε ότι:

$$\mathsf{ord}_n(a \cdot b) = \mathsf{ord}_n(a) \cdot \mathsf{ord}_n(b)$$

Να δειχθεί με ένα αντιπαράδειγμα ότι η παραπάνω ισότητα δεν ισχύει αν $(\mathsf{ord}_n(a), \mathsf{ord}_n(b)) \neq 1$.

Άσκηση 12. *Δείξτε ότι αν υπάρχει μια πρωταρχική ρίζα* $\mathsf{mod}\, n$ *τότε υπάρχουν ακριβώς* $\phi(\phi(n))$ *(ανισότιμες) πρωταρχικές ρίζες* $\mathsf{mod}\, n$*. Μπορείτε να περιγράψετε το σύνολο* $\mathcal{P}_n$ *των πρωταρχικών ριζών* $\mathsf{mod}\, n$*;*

Άσκηση 13. *Βρείτε όλες τις πρωταρχικές ρίζες* $\mathsf{mod}\, 23$.

Άσκηση 14. *Έστω* n *ένας φυσικός ακέραιος και* a *ένας θετικός ακέραιος έτσι ώστε:* $(a, n) = 1$*. Να δείξετε ότι τα ακόλουθα είναι ισοδύναμα:*

1. *Ο αριθμός* a *είναι μια πρωταρχική ρίζα* $\mathsf{mod}\, n$.
2. *Για κάθε πρώτο διαιρέτη* p *του* $\phi(n)$*, ισχύει ότι:*

$$a^{\frac{\phi(n)}{p}} \not\equiv 1 \,(\mathsf{mod}\, n)$$

Ως εφαρμογή, να εξετάσετε αν οι αριθμοί $2, 3$ *είναι:*

(α) *πρωταρχικές ρίζες* $\mathsf{mod}\, 11$*, και*
(β) *πρωταρχικές ρίζες* $\mathsf{mod}\, 9$.

Άσκηση 15. **1.** *Δείξτε ότι το* 3 *είναι αρχική ρίζα* $\mathsf{mod}\, 17$.
2. *Για δοθέντα ακέραιο* a *με* $(a, 17) = 1$ *υπολογίστε του ελάχιστο θετικό ακέραιο* k *ώστε* $a \equiv 3^k \,(\mathsf{mod}\, 17)$.
3. *Λύστε την ισοτιμία*

$$x^4 \equiv 13 \,(\mathsf{mod}\, 17) \tag{1}$$

Άσκηση 16. *Έστω* $n = 4, p^m$ *ή* $2p^m$*, όπου* p *περιττός πρώτος και* $m \geq 1$ *ακέραιος. Αν* a *είναι μια αρχική ρίζα* $\mathsf{mod}\, n$*, δείξτε ότι*

$$a^{\phi(n)/2} \equiv -1 \,(\mathsf{mod}\, n)$$

Άσκηση 17. *Έστω* p *περιττός πρώτος και* a *ένας ακέραιος με* $(a, p) = 1$*. Δείξτε ότι:*

1. *Αν* $p \equiv 1 \,\mathsf{mod}\, 4$*, τότε ο* a *είναι πρωταρχική ρίζα* $\mathsf{mod}\, p$ *αν και μόνο αν ο ακέραιος* $-a$ *είναι επίσης πρωταρχική ρίζα* $\mathsf{mod}\, p$.
2. *Αν* $p \equiv 3 \,\mathsf{mod}\, 4$*, τότε ο* a *είναι πρωταρχική ρίζα* $\mathsf{mod}\, p$ *αν και μόνο αν* $\mathsf{ord}_p(-a) = \frac{p-1}{2}$.

Άσκηση 18. *Έστω a ένας περιττός θετικός ακέραιος. Να δειχθεί ότι,* $\forall m \geq 3$*:*

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