ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

ΤΜΗΜΑ **Β′**

ΛΥΣΕΙΣ ΑΣΚΗΣΕΩΝ - 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 $2^x \equiv 1 \pmod{7}$.

Λύση. «$\Longrightarrow$» Έστω ότι ο θετικός ακέραιος x ικανοποιεί την ισοτιμία $a^x \equiv 1 \pmod{n}$. Τότε $n \mid a^x - 1$. Δείχνουμε πρώτα ότι $(n, a) = 1$. Πράγματι, αν $(n, a) = d$, τότε $d \mid a$ και άρα $d \mid a^x$. Επειδή $d \mid n$, θα έχουμε $d \mid a^x - 1$, και επομένως $d \mid a^x - (a^x - 1) = 1$. Έτσι πράγματι $d = (a, n) = 1$ και επομένως ορίζεται η τάξη $\mathsf{ord}_n(a)$ του $a \pmod{n}$. Από την Ευκλείδεια Διαίρεση του x με την τάξη $\mathsf{ord}_n(a)$, θα έχουμε:

$$x = q \cdot \mathsf{ord}_n(a) + r, \qquad 0 \leq r < \mathsf{ord}_n(a)$$

Τότε:

$$a^x \equiv 1 \pmod{n} \implies a^{q \cdot \mathsf{ord}_n(a) + r} \equiv 1 \pmod{n} \implies (a^{\mathsf{ord}_n(a)})^q \cdot a^r \equiv 1 \pmod{n} \implies a^r \equiv 1 \pmod{n}$$

Επειδή $r < \mathsf{ord}_n(a)$, έπεται ότι $r = 0$ και επομένως $x = q \cdot \mathsf{ord}_n(a)$, δηλαδή $\mathsf{ord}_n(a) \mid x$.

«$\Longleftarrow$» Έστω $\mathsf{ord}_n(a) \mid x$, και επομένως $x = q \cdot \mathsf{ord}_n(a)$, για κάποιον ακέραιο q. Τότε

$$a^x = a^{q \cdot \mathsf{ord}_n(a)} = (a^{\mathsf{ord}_n(a)})^q \equiv 1^q \equiv 1 \pmod{n}$$

Σύμφωνα με τα παραπάνω, ο ακέραιος x είναι λύση της ιοτιμίας $2^x \equiv 1 \pmod{7}$ αν και μόνον αν $\mathsf{ord}_7(2) \mid x$. Γνωρίζουμε ότι $\mathsf{ord}_7(2) \mid \phi(7) = 6$. Επομένως $\mathsf{ord}_7(2) = 1$ ή 2 ή 3 ή 6. Επειδή $2^1 = 2 \not\equiv 1 \pmod{7}$, $2^2 = 4 \not\equiv 1 \pmod{7}$, και $2^3 = 8 \equiv 1 \pmod{7}$, έπεται ότι $\mathsf{ord}_7(2) = 3$. Επομένως ο ακέραιος x είναι λύση της ισοτιμίας $2^x \equiv 1 \pmod{7}$ αν και μόνον αν $3 \mid x$, ή ισοδύναμα $x = 3 \cdot k$ για κάποιον ακέραιο k.

Έτσι για παράδειγμα, επειδή $3 \mid 15$, ο ακέραιος $x = 15$ είναι λύση της ισοτιμίας $2^x \equiv 1 \pmod{7}$, και επειδή $3 \nmid 10$, ο ακέραιος $x = 10$ δεν είναι λύση 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: $2 \mid \phi(n)$.

Λύση. Έστω $d = (n-1, n)$. Τότε

$$\begin{cases} d \mid n-1 \\ \\ d \mid n \end{cases} \implies d \mid 1 \implies d = 1$$

Άρα $(n-1, n) = 1$ και επομένως ορίζεται η τάξη του ακεραίου $n-1 \pmod n$, δηλαδή έχει νόημα ο αριθμός $\mathsf{ord}_n(n-1)$. Έχουμε

$$(n-1)^2 = n^2 - 2n + 1 \equiv 1 \pmod n$$

και

$$n - 1 \equiv -1 \pmod n$$

Επειδή $n \geq 3$ έχουμε ότι $-1 \not\equiv 1 \pmod n$. Πράγματι, αν $-1 \equiv 1 \pmod n$ τότε $n \mid 2$ και άρα $n \leq 2$, κάτι το οποίο είναι άτοπο. Επομένως θα έχουμε ότι

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

Γνωρίζουμε ότι για κάθε $a \in \mathbb{Z}$ με $(a, n) = 1$ ισχύει ότι

$$\mathsf{ord}_n(a) \mid \phi(n)$$

Συνεπώς $\mathsf{ord}_n(n-1) = 2 \mid \phi(n)$. ■

Άσκηση 3. *Έστω $n \geq 2$ ακέραιος και a, b θετικοί ακέραιοι. Δείξτε ότι:*

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

Λύση. Επειδή $ab \equiv 1 \pmod n$, θα έχουμε ότι: $n \mid ab - 1$.

Έστω $d = (a, n)$. Τότε

$$\begin{cases} d \mid n \\ \\ d \mid a \end{cases} \implies \begin{cases} d \mid n \\ \\ d \mid ab \end{cases} \implies \begin{cases} d \mid ab-1 \\ \\ d \mid ab \end{cases} \implies d \mid 1 \implies d = (a, n) = 1$$

Παρόμοια δείχνουμε ότι $(b, n) = 1$.

Έστω ότι $\mathsf{ord}_n(a) = r$ και $\mathsf{ord}_n(b) = s$. Τότε

$$a^r \equiv 1 \pmod n \quad \text{και} \quad b^s \equiv 1 \pmod n$$

Έχουμε

$$\begin{aligned} a^r \equiv 1 \pmod n \quad &\implies \quad a^r b^r \equiv b^r \pmod n \\ &\implies \quad (ab)^r \equiv b^r \pmod n \\ &\implies \quad 1^r \equiv 1 \equiv b^r \pmod n \\ &\implies \quad b^r \equiv 1 \pmod n \end{aligned}$$

και άρα

$$\mathsf{ord}_n(b) = s \mid r \tag{1}$$

Παρόμοια δείχνουμε ότι

$$\mathsf{ord}_n(a) = r \mid s \tag{2}$$

Από τις σχέσεις (1) και (2) έπεται το ζητούμενο: $\mathsf{ord}_n(a) = r = s = \mathsf{ord}_n(b)$. ■

Άσκηση 4. *Βρείτε τις τάξεις* $\bmod 16$ *των ακεραίων* $3, 5, 7$ *και* 9.

Λύση. Υπολογίζουμε:

• $\mathsf{ord}_{16}(3)$: $3^2 = 9,\ 3^3 = 27 \equiv 11 \,(\mathsf{mod}\, 16),\ 3^4 = 33 \equiv 1 \,(\mathsf{mod}\, 16)$. Άρα

$$\boxed{\mathsf{ord}_{16}(3) = 4}$$

• $\mathsf{ord}_{16}(5)$: $5^2 = 25 \equiv 9 \,(\mathsf{mod}\, 16),\ 5^3 = 45 \equiv 13 \,(\mathsf{mod}\, 16),\ 5^4 = 65 \equiv 1 \,(\mathsf{mod}\, 16)$. Συνεπώς

$$\boxed{\mathsf{ord}_{16}(5) = 4}$$

• $\mathsf{ord}_{16}(7)$: $7^2 = 49 \equiv 1 \,(\mathsf{mod}\, 16)$. Επομένως

$$\boxed{\mathsf{ord}_{16}(7) = 2}$$

• $\mathsf{ord}_{16}(9)$: $9^2 = 81 \equiv 1 \,(\mathsf{mod}\, 16)$. Άρα

$$\boxed{\mathsf{ord}_{16}(9) = 2}$$

Συνοψίζοντας, οι τάξεις $\mathsf{mod}\, 16$ των ακεραίων $3, 5, 7$ και 9 είναι $4, 4, 2$ και 2 αντίστοιχα. ■

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.*

Λύση. Επειδή $(a, m) = 1$ από το Θεώρημα του Euler, έπεται ότι $a^{\phi(m)} \equiv 1 \,(\mathsf{mod}\, m)$. Επομένως θα έχουμε $\mathsf{ord}_m(a) \mid \phi(m)$. Επειδή από την υπόθεση έχουμε $\mathsf{ord}_m(a) = m - 1$, έπεται ότι:

$$m - 1 \ \mid \ \phi(m) \quad \Longrightarrow \quad m - 1 \ \leq \ \phi(m)$$

Επειδή $\phi(m) = m$ αν και μόνον αν $m = 1$, και επειδή από την υπόθεση $m > 1$, έπεται ότι $\phi(m) \leq m - 1$, και επομένως θα έχουμε:

$$\phi(m) = m - 1$$

Αυτό σημαίνει ότι:

$$\big|\big\{k \in \mathbb{N} \mid 1 \leq k \leq m \ \ \&\ \ (k, m) = 1\big\}\big| = m - 1$$

Επομένως ιδιαίτερα θα έχουμε ότι ο m δεν έχει γνήσιους διαιρέτες και άρα ο m είναι πρώτος. ■

Σχόλιο 1. Επειδή για κάθε δύο ακέραιους a και b με την ιδιότητα $(a, n) = 1 = (b, n)$, ισχύει ότι $a \equiv b \,(\mathsf{mod}\, n) \implies \mathsf{ord}_n(a) = \mathsf{ord}_n(b)$, έπεται ότι η τάξη ενός ακεραίου a εξαρτάται μόνο από την κλάση ισοτιμίας του $(\mathsf{mod}\, n)$. Έτσι θεωρώντας το σύνολο $\mathsf{U}(\mathbb{Z}_n)$ των αντιστρεψίμων κλάσων ισοτιμίας $(\mathsf{mod}\, n)$, μπορούμε ισοδύναμα να ορίσουμε την τάξη του στοιχείου $[a]_n \in \mathsf{U}(\mathbb{Z}_n)$ ως εξής:

$$\mathsf{ord}_n([a]_n) = \mathsf{ord}_n(a) = \min\big\{k \in \mathbb{N} \mid [a]_n^k = [1]_n\big\}$$

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 $\mathbb{Z}_n$.*

Λύση. (1) Υπολογισμός τάξεων των στοιχείων του $\mathsf{U}(\mathbb{Z}_9)$.
Ο συμβολισμός $[a]$ σημαίνει εδώ $[a]_9$.
Επειδή $9 = 3^2$ έχουμε $\phi(9) = 9(1 - 1/3) = 6$ και

$$\mathsf{U}(\mathbb{Z}_9) = \big\{[1], [2], [4], [5], [7], [8]\big\}$$

Από την Θεωρία ξέρουμε ότι αν a είναι ακέραιος με $(a,9)=1$ τότε $\mathsf{ord}_9(a) \mid \phi(9)=6$, και άρα $\mathsf{ord}_9(a) \in \{1,2,3,6\}$. Φανερά $\mathsf{ord}_9(1)=1$ και αφού $[8]=[-1]$ έχουμε $\mathsf{ord}_9(8)=2$. Έχουμε $[2^2]=[4], [2^3]=[8]$ και επομένως $\mathsf{ord}_9(2)=6$. Έχουμε

$$[4^2]=[16]=[7]=[-2], \qquad [4^3]=[4][-2]=[-8]=[1]$$

και επομένως $\mathsf{ord}_9(4)=3$. Επίσης

$$[5^2]=[25]=[7]=[-2], \qquad [5^3]=[5][-2]=[-10]=[-1]$$

και επομένως $\mathsf{ord}_9(5)=6$. Τέλος

$$[7^2]=[(-2)^2]=[4], \qquad [7^3]=[7][4]=[1]$$

και άρα $\mathsf{ord}_9(7)=3$.

(2) Υπολογισμός τάξεων των στοιχείων του $\mathsf{U}(\mathbb{Z}_{10})$.
Ο συμβολισμός $[a]$ σημαίνει εδώ $[a]_{10}$.
Αφού $10=2\cdot 5$ έχουμε $\phi(10)=10(1-1/2)(1-1/5)=4$ και

$$\mathsf{U}(\mathbb{Z}_{10})=\Big\{[1],[3],[7],[9]\Big\}$$

Από την Θεωρία ξέρουμε ότι αν a είναι ακέραιος με $(a,10)=1$ τότε $\mathsf{ord}_{10}(a) \mid \phi(10)=4$, και άρα $\mathsf{ord}_{10}(a) \in \{1,2,4\}$. Φανερά έχουμε $\mathsf{ord}_{10}(1)=1$ και αφού $[9]=[-1]$ έχουμε $\mathsf{ord}_{10}(9)=2$. Επίσης $[3^2]=[9]=[-1]$ και επομένως $\mathsf{ord}_{10}(3)=4$. Τέλος έχουμε $[7^2]=[(-3)]^2=[-1]$ και επομένως $\mathsf{ord}_{10}(7)=4$. ■

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

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

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

Λύση. Έστω $1 \le t < n$. Τότε

$$a^t \not\equiv 1 \,(\mathsf{mod}\, a^n-1)$$

διότι διαφορετικά αν

$$a^t \equiv 1 \,(\mathsf{mod}\, a^n-1) \implies a^n-1 \mid a^t-1 \implies a^n-1 \le a^t-1 \implies a^n \le a^t$$

που είναι άτοπο αφού οι a,t και n είναι θετικοί ακέραιοι και $t<n$. Από την άλλη πλευρά όμως έχουμε προφανώς ότι

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

και άρα έπεται ότι

$$n=\mathsf{ord}_{a^n-1}(a)=\min\big\{k\in\mathbb{N} \mid a^k \equiv 1 \,(\mathsf{mod}\, a^n-1)\big\}$$

Τέλος από γνωστή ιδιότητα έχουμε ότι $\mathsf{ord}_{a^n-1}(a)=n \mid \phi(a^n-1)$. ■

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

Λύση. Επειδή $a^{n-1}\equiv 1\,(\mathsf{mod}\, n)$, θα έχουμε $n \mid a^{n-1}-1$ και επομένως υπάρχει $k\in\mathbb{Z}$ έτσι ώστε $a^{n-1}-1=kn$. Έτσι $a^{n-1}+(-k)n = a\cdot a^{n-1}+(-k)n=1$ και επομένως $(a,n)=(a^{n-1},n)=1$. Η τελευταία σχέση δείχνει ότι ορίζεται η τάξη $r:=\mathsf{ord}_n(a)$. Επειδή $a^{n-1}\equiv 1\,(\mathsf{mod}\, n)$, θα έχουμε $r \mid n-1$. Επειδή από την υπόθεση $a^d \not\equiv 1\,(\mathsf{mod}\, n)$ για κάθε γνήσιο θετικό διαιρέτη d του $n-1$, έπεται ότι ο $n-1$ είναι ο μικρότερος θετικός ακέραιος k έτσι ώστε $a^k\equiv 1\,(\mathsf{mod}\, n)$. Επομένως $r=n-1$.

Επειδή $\mathsf{ord}_n(a) \mid \varphi(n)$, θα έχουμε $n-1 \mid \varphi(n)$. Επειδή $\varphi(n)\le n$, επειδή $\phi(n)=n$ αν και μόνον αν $n=1$, και επειδή από την υπόθεση $n\ge 2$, θα έχουμε ότι $\varphi(n)\le n-1$ και επομένως $\varphi(n)=n-1$. Αυτό

σημαίνει ότι ο μόνος θετικός διαιρέτης του n εκτός του 1 είναι ο n, δηλαδή οι μόνοι θετικοί διαιρέτες του n είναι οι 1 και n, δηλαδή 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* $(\mathsf{mod}\, 20)$.

Λύση. **1.** Θα έχουμε:

(1) Έστω $n = 4$. Αναζητούμε $1 \leq a \leq 4$, έτσι ώστε $(4, a) = 1$ και $\mathsf{ord}_4(a) = \phi(4) = 2$.
Άρα $a = 1$ ή 3. Επειδή προφανώς $a = 1$ δεν είναι πρωταρχική ρίζα $\mathsf{mod}\, 4$, και επειδή $3^1 = 3 \not\equiv 1\,(\mathsf{mod}\, 4)$, και $3^2 = 9 \equiv 1\,(\mathsf{mod}\, 4)$, έπεται ότι $\mathsf{ord}_4(a) = 2$ και άρα:

$$a = 3 \quad \text{είναι πρωταρχική ρίζα} \quad (\mathsf{mod}\, 4)$$

(2) Έστω $n = 5$. Αναζητούμε $1 \leq a \leq 5$, έτσι ώστε $(5, a) = 1$ και $\mathsf{ord}_5(a) = \phi(5) = 4$.
Άρα $a = 1$ ή 2 ή 3 ή 4. Επειδή προφανώς $a = 1$ δεν είναι πρωταρχική ρίζα $\mathsf{mod}\, 5$, και επειδή $2^1 = 2 \not\equiv 1\,(\mathsf{mod}\, 5)$, και $2^2 = 4 \not\equiv 1\,(\mathsf{mod}\, 5)$, και $2^3 = 8 \equiv 3 \not\equiv 1\,(\mathsf{mod}\, 5)$, και $2^4 = 16 \equiv 1\,(\mathsf{mod}\, 5)$, έπεται ότι $\mathsf{ord}_5(2) = 4$ και άρα:

$$a = 2 \quad \text{είναι πρωταρχική ρίζα} \quad (\mathsf{mod}\, 5)$$

(3) Έστω $n = 10$. Αναζητούμε $1 \leq a \leq 10$, έτσι ώστε $(10, a) = 1$ και $\mathsf{ord}_{10}(a) = \phi(10) = 4$.
Άρα $a = 1$ ή 3 ή 7 ή 9. Επειδή προφανώς $a = 1$ δεν είναι πρωταρχική ρίζα $\mathsf{mod}\, 10$, και επειδή $3^1 = 3 \not\equiv 1\,(\mathsf{mod}\, 10)$, και $3^2 = 9 \not\equiv 1\,(\mathsf{mod}\, 10)$, και $3^3 = 27 \equiv 7 \not\equiv 1\,(\mathsf{mod}\, 10)$, και $3^4 = 21 \equiv 1\,(\mathsf{mod}\, 10)$, έπεται ότι $\mathsf{ord}_{10}(3) = 4$ και άρα:

$$a = 3 \quad \text{είναι πρωταρχική ρίζα} \quad (\mathsf{mod}\, 10)$$

(4) Έστω $n = 13$. Αναζητούμε $1 \leq a \leq 13$, έτσι ώστε $(14, a) = 1$ και $\mathsf{ord}_{14}(a) = \phi(14) = 6$.
Άρα $a = 1$ ή 2 ή $\cdots$ ή 12. Επειδή προφανώς $a = 1$ δεν είναι πρωταρχική ρίζα $\mathsf{mod}\, 13$, και επειδή όπως μπορούμε να δούμε εύκολα $3^k \not\equiv 1\,(\mathsf{mod}\, 13)$, αν $1 \leq k \leq 11$, και $2^{12} = 2^5 \cdot 2^5 \cdot 2^2 = 32 \cdot 32 \cdot 4 \equiv 6 \cdot 6 \cdot 4 = 36 \cdot 4 \equiv 10 \cdot 4 = 40 \equiv 1\,(\mathsf{mod}\, 13)$, έπεται ότι $\mathsf{ord}_{13}(2) = 12$ και άρα:

$$a = 2 \quad \text{είναι πρωταρχική ρίζα} \quad (\mathsf{mod}\, 13)$$

(5) Έστω $n = 14$. Αναζητούμε $1 \leq a \leq 14$, έτσι ώστε $(14, a) = 1$ και $\mathsf{ord}_{14}(a) = \phi(14) = 6$.
Άρα $a = 1$ ή 3 ή 5 ή 9 ή 11 ή 13. Επειδή προφανώς $a = 1$ δεν είναι πρωταρχική ρίζα $\mathsf{mod}\, 14$, και επειδή $3^1 = 3 \not\equiv 1\,(\mathsf{mod}\, 14)$, και $3^2 = 9 \not\equiv 1\,(\mathsf{mod}\, 14)$, και $3^3 = 27 \equiv 13 \not\equiv 1\,(\mathsf{mod}\, 14)$, και $3^4 = 39 \equiv 11 \not\equiv 1\,(\mathsf{mod}\, 14)$, και $3^5 = 33 \equiv 5 \not\equiv 1\,(\mathsf{mod}\, 14)$, και $3^6 = 15 \equiv 1\,(\mathsf{mod}\, 14)$, έπεται ότι $\mathsf{ord}_{14}(3) = 6$ και άρα:

$$a = 3 \quad \text{είναι πρωταρχική ρίζα} \quad (\mathsf{mod}\, 14)$$

(6) Έστω $n = 18$. Αναζητούμε $1 \leq a \leq 18$, έτσι ώστε $(18, a) = 1$ και $\mathsf{ord}_{18}(a) = \phi(18) = 6$.
Άρα $a = 1$ ή 5 ή 7 ή 11 ή 13 ή 17. Επειδή προφανώς $a = 1$ δεν είναι πρωταρχική ρίζα $\mathsf{mod}\, 14$, και επειδή $5^1 = 5 \not\equiv 1\,(\mathsf{mod}\, 18)$, και $5^2 = 25 \equiv 7 \not\equiv\ (\mathsf{mod}\, 18)$, και $5^3 = 35 \equiv -1 \not\equiv 1\,(\mathsf{mod}\, 18)$, και $5^4 = -5 \equiv 13 \not\equiv 1\,(\mathsf{mod}\, 18)$, και $5^5 = -25 \equiv -7 \not\equiv 1\,(\mathsf{mod}\, 18)$, και $5^6 = -35 \equiv 1\,(\mathsf{mod}\, 18)$, έπεται ότι $\mathsf{ord}_{18}(5) = 6$ και άρα:

$$a = 5 \quad \text{είναι πρωταρχική ρίζα} \quad (\mathsf{mod}\, 18)$$

2. Έστω $n = 20$. Αναζητούμε $1 \leq a \leq 20$, έτσι ώστε $(20, a) = 1$ και $\mathsf{ord}_{20}(a) = \phi(20) = 8$.
Άρα $a = 1$ ή 3 ή 7 ή 9 ή 11 ή 13 ή 17 ή 19. Επειδή γενικά $\mathsf{ord}_{20}(a) \mid \phi(20) = 8$, θα έχουμε $\mathsf{ord}_{20}(a) = 1$ ή 2 ή 4 ή 8. Έτσι εξετάζουμε τις δυνάμεις a^d, όπου $d = 1$ ή 2 ή 4 ή 8, και αναζητούμε, αν υπάρχει, a έτσι ώστε ο διαιρέτης $d = 8$ να είναι η μικρότερη δύναμη του a έτσι ώστε $a^d \equiv 1\,(\mathsf{mod}\, 20)$.
Υπολογίζουμε:

$$1^4 \equiv 3^4 \equiv 7^4 \equiv 9^4 \equiv 11^4 \equiv 13^4 \equiv 17^4 \equiv 19^4 \ \equiv 1\ (\mathsf{mod}\, 20)$$

Επομένως δεν υπάρχει $1 \leq a \leq 20$, έτσι ώστε $(20, a) = 1$ και $\mathsf{ord}_{20}(a) = \phi(20) = 8$, και άρα:

$$\text{δεν υπάρχει πρωταρχική ρίζα} \pmod{20} \qquad \blacksquare$$

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

Λύση. **1**. $n = 23$: Επειδή ο αριθμός 23 είναι πρώτος έπεται ότι υπάρχουν πρωταρχικές ρίζες $(\mathsf{mod}\, 23)$. Από το Θεώρημα του Fermat έχουμε

$$\forall\, a = 1, 2, \cdots, 22: \quad a^{\phi(23)} \equiv a^{23-1} \equiv 1 \,(\mathsf{mod}\, 23) \quad \Longrightarrow \quad a^{22} \equiv 1 \,(\mathsf{mod}\, 23)$$

Παρατηρούμε ότι για $a = 2$ υπάρχει μικρότερη δύναμη k από το 22 έτσι ώστε ο αριθμός 2^k να είναι $(\mathsf{mod}\, 23)$ ίσος με 1. Πράγματι έχουμε

$$2^{11} = 2048 = 89 \cdot 23 + 1 \quad \Longrightarrow \quad 2^{11} \equiv 1 \,(\mathsf{mod}\, 23)$$

Δοκιμάζοντας όπως παραπάνω αποκλείουμε τους αριθμούς 3 και 4 αντίστοιχα, δηλαδή υπάρχουν μικρότερες από το 22 δυνάμεις k έτσι ώστε ο αριθμός a^k, όπου $a = 3, 4$, να είναι $(\mathsf{mod}\, 23)$ ίσος με 1.

Θέτουμε τώρα $a = 5$. Τότε $(a, 23) = 1$ και $5^{22} \equiv 1 \,(\mathsf{mod}\, 23)$. Αν υπάρχει ένα $k \in \mathbb{N}$ έτσι ώστε $5^k \equiv 1 \,(\mathsf{mod}\, 23)$ και k ο μικρότερος δυνατός αριθμός, δηλαδή $k = \mathsf{ord}_{23}(5)$, τότε θα πρέπει

$$k \mid 22 \quad \Longrightarrow \quad k = 1,\, 2,\, 11,\, 22$$

Προφανώς $k \neq 1$ και

$$5^2 = 25 \equiv 2 \,(\mathsf{mod}\, 23)$$

Άρα το 2 απορρίπτεται. Για το 11 έχουμε

$$5^{11} = 5^2 \cdot 5^2 \cdot 5^2 \cdot 5^2 \cdot 5^2 \cdot 5 \equiv 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 64 \equiv 18 \,(\mathsf{mod}\, 23)$$

Συνεπώς και το 11 απορρίπτεται. Τότε

$$\mathsf{ord}_{23}(5) = 22$$

και επομένως το 5 είναι μια πρωταρχική ρίζα $(\mathsf{mod}\, 23)$.

2. $n = 31$: Επειδή ο αριθμός 31 είναι πρώτος έπεται ότι υπάρχουν πρωταρχικές ρίζες $(\mathsf{mod}\, 31)$. Από το Θεώρημα του Fermat έχουμε

$$\forall\, a = 1, 2, \cdots, 30: \quad a^{\phi(31)} \equiv a^{31-1} \equiv 1 \,(\mathsf{mod}\, 31) \quad \Longrightarrow \quad a^{30} \equiv 1 \,(\mathsf{mod}\, 31)$$

Παρατηρούμε ότι για $a = 2$ υπάρχει δύναμη k μικρότερη από το 30 έτσι ώστε ο αριθμός 2^k να είναι $(\mathsf{mod}\, 31)$ ίσος με 1. Πράγματι έχουμε

$$2^5 = 32 \equiv 1 \,(\mathsf{mod}\, 31)$$

Θέτουμε τώρα $a = 3$. Τότε $(a, 31) = 1$ και $3^{30} \equiv 1 \,(\mathsf{mod}\, 31)$. Αν υπάρχει ένα $k \in \mathbb{N}$ έτσι ώστε $3^k \equiv 1 \,(\mathsf{mod}\, 31)$ και k ο μικρότερος δυνατός αριθμός, δηλαδή $k = \mathsf{ord}_{31}(3)$, τότε θα πρέπει

$$k \mid 30 \quad \Longrightarrow \quad k = 1,\, 2,\, 3,\, 5,\, 6,\, 10,\, 15,\, 30$$

Προφανώς το $k = 1$ απορρίπτεται και έχουμε:

- $k = 2$: $3^2 \equiv 9 \,(\mathsf{mod}\, 31)$.
- $k = 3$: $3^3 \equiv 27 \,(\mathsf{mod}\, 31)$.
- $k = 5$: $3^5 = 243 \equiv 26 \,(\mathsf{mod}\, 31)$.
- $k = 6$: $3^6 = 26 \cdot 3 = 78 \equiv 16 \,(\mathsf{mod}\, 31)$.
- $k = 10$: $3^{10} = 3^6 \cdot 3^3 \cdot 3 \equiv 16 \cdot 27 \cdot 3 \equiv 25 \,(\mathsf{mod}\, 31)$.
- $k = 15$: $3^{15} = 3^{10} \cdot 3^5 = 25 \cdot 26 = 650 \equiv 30 \,(\mathsf{mod}\, 31)$.

Επομένως όλες οι παραπάνω δυνάμεις απορρίπτονται και άρα

$$30 = \min\left\{k \in \mathbb{N} \mid 3^k \equiv 1 \,(\mathsf{mod}\, 31)\right\} \quad \Longrightarrow \quad \mathsf{ord}_{31}(3) = 30 = \phi(31)$$

δηλαδή το 3 είναι πρωταρχική ρίζα $\pmod{31}$. ■

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 $(\mathsf{ord}_n(a), \mathsf{ord}_n(b)) \neq 1$.

Λύση. Επειδή $(a, n) = 1 = (b, n)$, έπεται ότι ορίζονται οι τάξεις $\mathsf{ord}_n(a)$ και $\mathsf{ord}_n(b)$ των a και $b \pmod n$. Έστω

$$\mathsf{ord}_n(a) = r \quad \& \quad \mathsf{ord}_n(b) = s \quad \& \quad \mathsf{ord}_n(ab) = t$$

οπότε από την υπόθεση έχουμε $(r, s) = 1$.

Θα έχουμε:

$$(ab)^{rs} = a^{rs} \cdot b^{rs} = (a^r)^s \cdot (b^s)^r \equiv 1^s \cdot 1^r \equiv 1 \pmod n \quad \Longrightarrow \quad t \mid rs \tag{$*$}$$

Επίσης θα έχουμε:

$$(ab)^t \equiv 1 \pmod n \implies (ab)^{rt} \equiv 1 \pmod n \implies a^{rt} \cdot b^{rt} \equiv 1 \pmod n \implies (a^r)^t \cdot b^{rt} \equiv 1 \pmod n \implies$$

$$\implies b^{rt} \equiv 1 \pmod n \implies s \mid rt \overset{(r,s)=1}{\implies} s \mid t \tag{$\dagger$}$$

και παρόμοια

$$(ab)^t \equiv 1 \pmod n \implies (ab)^{st} \equiv 1 \pmod n \implies a^{st} \cdot b^{st} \equiv 1 \pmod n \implies a^{st} \cdot (b^s)^t \equiv 1 \pmod n \implies$$

$$\implies a^{st} \equiv 1 \pmod n \implies r \mid st \overset{(r,s)=1}{\implies} r \mid t \tag{$\dagger\dagger$}$$

Επειδή $(s, r) = 1$, από τις σχέσεις $(\dagger)$ και $(\dagger\dagger)$ έπεται ότι:

$$rs \mid t \tag{$**$}$$

Τέλος από τις σχέσεις $(*)$ και $(**)$ έπεται το ζητούμενο $t = rs$.

– Από την Άσκηση 9, έπεται ότι $\mathsf{ord}_2(3) = 4 = \mathsf{ord}_{20}(7)$, δηλαδή $(\mathsf{ord}_2(3), \mathsf{ord}_{20}(7)) = 4$, και τότε:

$$\mathsf{ord}_{20}(3 \cdot 7) = \mathsf{ord}_{20}(21) = \mathsf{ord}_{20}(1) = 1 \neq 4 \cdot 4 = \mathsf{ord}_2(3) \cdot \mathsf{ord}_2(7)$$ ■

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

Λύση. Έστω a μια πρωταρχική ρίζα $(\bmod n)$. Τότε

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

και οι φυσικοί αριθμοί $a, a^2, \ldots, a^{\phi(n)-1}$ είναι ένα ανηγμένο (περιορισμένο) σύστημα υπολοίπων $(\bmod n)$. Επειδή

$$\mathsf{ord}_n(a) = \phi(n)$$

και επειδή γνωρίζουμε ότι

$$\mathsf{ord}_n(a^k) = \frac{\mathsf{ord}_n(a)}{(k, \mathsf{ord}_n(a))} = \frac{\phi(n)}{(k, \phi(n))}$$

έπεται ότι τα στοιχεία του συνόλου

$$S = \left\{a^k \mid 1 \leq k \leq \phi(n) \ \ \& \ \ (k, \phi(n)) = 1\right\}$$

είναι πρωταρχικές ρίζες $(\bmod n)$, διότι για κάθε k με $1 \leq k \leq \phi(n)$ και $(k, \phi(n)) = 1$ έχουμε ότι

$$\mathsf{ord}_n(a^k) = \phi(n)$$

Τα στοιχεία του S είναι ανα δυο ανισότιμα $(\bmod n)$ διότι διαφορετικά το a δεν θα ήταν πρωταρχική ρίζα.

Αντίστροφα τώρα, αν b είναι μια πρωταρχική ρίζα $(\mathsf{mod}\, n)$ θα δείξουμε ότι υπάρχει ένα k, $1 \leq k \leq \phi(n)$ και $(k, \phi(n)) = 1$, έτσι ώστε

$$b \equiv a^k \,(\mathsf{mod}\, n)$$

Πράγματι θα πρέπει $(b, n) = 1$ και $\mathsf{ord}_n(b) = \phi(n)$. Επειδή το σύνολο $\{a, a^2, \ldots, a^{\phi(n)-1}\}$ είναι ένα ανηγμένο (περιορισμένο) σύστημα υπολοίπων $(\mathsf{mod}\, n)$ έπεται ότι υπάρχει ένα $k = 1, \ldots, \phi(n)$ έτσι ώστε $b \equiv a^k \,(\mathsf{mod}\, n)$. Θα δείξουμε ότι $(k, \phi(n)) = 1$. Έχουμε

$$\phi(n) = \mathsf{ord}_n(b) = \mathsf{ord}_n(a^k) = \frac{\mathsf{ord}_n(a)}{(k, \mathsf{ord}_n(a))} = \frac{\phi(n)}{(k, \phi(n))} \implies (k, \phi(n)) = 1$$

Συνεπώς έχουμε ότι το σύνολο $\mathcal{P}_n$ των πρωταρχικών ριζών $\mathsf{mod}\, n$ είναι

$$S = \mathcal{P}_n$$

και το πλήθος τους είναι $|S| = \phi(\phi(n))$. ■

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

Λύση. Από την Άσκηση 10 έχουμε ότι το 5 είναι μια πρωταρχική ρίζα $(\mathsf{mod}\, 23)$. Από τη θεωρία γνωρίζουμε, βλέπε και την Άσκηση 12, τότε ότι όλες οι πρωταρχικές ρίζες $(\mathsf{mod}\, 23)$ είναι τα στοιχεία του συνόλου:

$$\mathcal{P}_{23} = \left\{5^k \mid 1 \leq k \leq 22 \;\text{ και }\; (k, 22) = 1\right\}$$

και το πλήθος τους είναι

$$\phi(\phi(23)) = \phi(22) = 10$$

Τότε

$$\left\{5^k \mid 1 \leq k \leq 22 \;\;\&\;\; (k, 22) = 1\right\} = \left\{5^1, 5^3, 5^5, 5^7, 5^9, 5^{13}, 5^{15}, 5^{17}, 5^{19}, 5^{21}\right\}$$

και υπολογίζουμε:

$$\begin{aligned}
5 &\equiv 5 \,(\mathsf{mod}\, 23)\\
5^3 &\equiv 10 \,(\mathsf{mod}\, 23)\\
5^5 &\equiv 20 \,(\mathsf{mod}\, 23)\\
5^9 &\equiv 11 \,(\mathsf{mod}\, 23)\\
5^{13} &\equiv 21 \,(\mathsf{mod}\, 23)\\
5^{15} &\equiv 19 \,(\mathsf{mod}\, 23)\\
5^{17} &\equiv 15 \,(\mathsf{mod}\, 23)\\
5^{19} &\equiv 7 \,(\mathsf{mod}\, 23)\\
5^{21} &\equiv 14 \,(\mathsf{mod}\, 23)
\end{aligned}$$

Άρα οι, ανισότιμες ανά δύο, πρωταρχικές ρίζες $(\mathsf{mod}\, 23)$ είναι: 5, 7, 10, 11, 14, 15, 17, 19, 20, 21. ■

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* $\mathsf{mod}\, 9$.

Λύση. **1.** $\implies$ **2.**: Έστω ότι ο αριθμός a είναι μια πρωταρχική ρίζα $\mod n$. Τότε

$$\mathsf{ord}_n(a) = \phi(n)$$

και άρα

$$a^k \not\equiv 1 \,(\mathsf{mod}\, n)$$

για κάθε $1 \leq k < \phi(n)$. Ιδιαίτερα, αν p είναι ένας τυχαίος πρώτος διαιρέτης του $\phi(n)$, τότε διαλέγοντας $k = \frac{\phi(n)}{p}$ έπεται ότι

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

διότι $p < \phi(n)$.

2. $\implies$ **1.**: Έστω ότι $a^{\frac{\phi(n)}{p}} \not\equiv 1 \,(\mathsf{mod}\, n)$ για κάθε πρώτο διαιρέτη p του $\phi(n)$ και υποθέτουμε αντίθετα ότι το a δεν είναι πρωταρχική ρίζα $(\mathsf{mod}\, n)$. Τότε $\mathsf{ord}_n(a) \mid \phi(n)$ και $\mathsf{ord}_n(a) < \phi(n)$. Θέτοντας $\mathsf{ord}_n(a) = r$ θα έχουμε ότι $\frac{\phi(n)}{r} > 1$. Έστω p πρώτος διαιρέτης του $\frac{\phi(n)}{r}$, ο οποίος υπάρχει διότι $\frac{\phi(n)}{r} > 1$. Τότε

$$\frac{\phi(n)}{r} = p \cdot m \quad \implies \quad \frac{\phi(n)}{p} = m \cdot r \quad \implies \quad a^{\frac{\phi(n)}{p}} = a^{m \cdot r} = (a^r)^m = 1^m = 1 \equiv 1 \,(\mathsf{mod}\, n)$$

που είναι φυσικά άτοπο. Συνεπώς ο αριθμός a είναι μια πρωταρχική ρίζα $\mod n$.

Εφαρμογή:

(α) Έστω $n = 11$ και $a = 2$. Τότε $\phi(11) = 10$ και οι πρώτοι διαιρέτες του 10 είναι οι αριθμοί $2, 5$. Όμως

$$2^{\frac{10}{2}} = 2^5 = 32 \not\equiv 1 \,(\mathsf{mod}\, 11)$$

και

$$2^{\frac{10}{5}} = 2^2 = 4 \not\equiv 1 \,(\mathsf{mod}\, 11)$$

Άρα

$$\mathsf{ord}_{11}(2) = 10 = \phi(11)$$

δηλαδή το 2 είναι πρωταρχική ρίζα $(\mathsf{mod}\, 11)$. Για $a = 3$ έχουμε

$$3^{\frac{10}{2}} = 3^5 = 243 \equiv 1 \,(\mathsf{mod}\, 11)$$

και άρα το 3 δεν είναι πρωταρχική ρίζα $(\mathsf{mod}\, 11)$.

(β) Έστω $n = 9$ και $a = 2$. Τότε $\phi(9) = 6$ και οι πρώτοι διαιρέτες του 6 είναι οι αριθμοί $2, 3$. Υπολογίζουμε:

$$2^{\frac{6}{2}} = 2^3 = 8 \not\equiv 1 \,(\mathsf{mod}\, 9)$$

και

$$2^{\frac{6}{3}} = 2^2 = 4 \not\equiv 1 \,(\mathsf{mod}\, 9)$$

Άρα

$$\mathsf{ord}_9(2) = 6 = \phi(9)$$

δηλαδή το 2 είναι πρωταρχική ρίζα $(\mathsf{mod}\, 9)$. Για $a = 3$ έχουμε

$$3^{\frac{6}{2}} = 3^3 \equiv 0 \,(\mathsf{mod}\, 9) \not\equiv 1 \,(\mathsf{mod}\, 9)$$

και

$$3^{\frac{6}{3}} = 3^2 = 0 \not\equiv 1 \,(\mathsf{mod}\, 9)$$

Συνεπώς το 3 είναι πρωταρχική ρίζα $(\mathsf{mod}\, 9)$. ■

Άσκηση 15. **1.** *Δείξτε ότι το* 3 *είναι αρχική ρίζα* $\mod 17$.

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*

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

Λύση. Σε αυτή την άσκηση ο συμβολισμός $[a]$ σημαίνει $[a]_{17}$.

1. Το 17 είναι πρώτος, άρα $\phi(17) = 16$. Από την θεωρία $\mathsf{ord}_{17}(3) \mid 16$. Οι διαιρέτες του 16 είναι το σύνολο $\{1, 2, 4, 8, 16\}$. Έχουμε

$$[3]^2 = [9], \qquad [3]^3 = [9][3] = [27] = [10] = [-7],$$
$$[3^4] = [3][10] = [30] = [13] = [-4], \qquad [3]^8 = [(-4)^2] = [16] = [-1].$$

Επομένως $\mathsf{ord}_{17}\, 3 = 16$, άρα το 3 είναι αρχική ρίζα $\mathsf{mod}\, 17$.

2. Έστω a ακέραιος με $(a, 17) = 1$ και b ο μοναδικός ακέραιος με $1 \leq b \leq 16$ και $a \equiv b \,(\mathsf{mod}\, 17)$. Φανερά ο ελάχιστος θετικός ακέραιος k ώστε $a \equiv 3^k \,(\mathsf{mod}\, 17)$ είναι ίσος με τον ελάχιστο θετικό ακέραιο k_1 ώστε $b \equiv 3^{k_1} \,(\mathsf{mod}\, 17)$. Χρησιμοποιώντας τα αποτέλεσματα του (1) έχουμε μετά απο λίγες πράξεις

$$[3]^1 = [3], \quad [3]^2 = [9], \quad [3]^3 = [10], \quad [3]^4 = [13], \quad [3]^5 = [5], \quad [3]^6 = [15],$$
$$[3]^7 = [11], \quad [3]^8 = [16], \quad [3]^9 = [14], \quad [3]^{10} = [8], \quad [3]^{11} = [7], \quad [3]^{12} = [4],$$
$$[3]^{13} = 12, \quad [3]^{14} = [2], \quad [3]^{15} = [6], \quad [3]^{16} = [1]$$

Επομένως για παράδειγμα, για $b = 1$ έχουμε $k_1 = 16$, για $b = 2$ έχουμε $k_1 = 14$, για $b = 3$ έχουμε $k_1 = 1$, για $b = 4$ έχουμε $k_1 = 12$, για $b = 5$ έχουμε $k_1 = 5$ και για $b = 6$ έχουμε $k_1 = 15$.

3. Παρατηρούμε ότι αν a, b είναι ακέραιοι με $[a] = [b]$ και το a είναι λύση της ισοτιμίας (1), τότε και το b είναι επίσης λύση της ίδιας ισοτιμίας. Έτσι μπορούμε να μιλάμε για λύσεις της ισοτιμίας στο $\mathbb{Z}_{17}$. Έστω a μια λύση. Τότε υπάρχει ακέραιος t με

$$a^4 - 13 = 17 \cdot t$$

και άρα $a^4 = 13 + 17t$ το οποίο συνεπάγεται ότι

$$(a^4, 17) = (13 + 17t, 17) = (13, 17) = 1.$$

Σαν συνέπεια $(a, 17) = 1$ και άρα το a είναι αντιστρέψιμο στοιχείο του $\mathbb{Z}_{17}$. Από το μέρος (1) της άσκησης το 3 είναι αρχική ρίζα $\mathsf{mod}\, 17$. Άρα υπάρχει ακέραιος k με $[3^k] = [a]$. Επίσης από το μέρος (1) της άσκησης έχουμε $[13] = [3^4]$. Επομένως αναζητούμε ακέραιους k με $1 \leq k \leq 16$ ώστε

$$(3^k)^4 \equiv 3^4 \,(\mathsf{mod}\, 17) \tag{2}$$

Το 3 σαν αρχική ρίζα $(\mathsf{mod}\, 17)$ έχει τάξη $\phi(17) = 16$. Επομένως από την Θεωρία η εξίσωση (2) είναι ισοδύναμη με την γραμμική ισοτιμία $4k \equiv 4 \,(\mathsf{mod}\, 16)$ η οποία είναι ισοδύναμη με την γραμμική ισοτιμία

$$k \equiv 1 \,(\mathsf{mod}\, 4).$$

Οι λύσεις, ως προς k αυτής που είναι μεταξύ 1 και 16 είναι οι ακόλουθες: $k = 1, 5, 9, 13$. Χρησιμοποιώντας τους υπολογισμούς στο μέρος (2) της άσκησης οι λύσεις της ισοτιμίας (1) στο $\mathbb{Z}_{17}$ είναι οι ακόλουθες:

$$[3^1] = [3], \ [3^5] = [5], \ [3^9] = [14], \ [3^{13}] = [12].$$

Σαν συνέπεια οι λύσεις της ισοτιμίας (1) στο $\mathbb{Z}$ είναι το σύνολο

$$[3] \cup [5] \cup [12] \cup [14].$$

Δηλαδή, ένας ακέραιος a είναι λύση της ισοτιμίας (1) αν και μόνο αν υπάρχουν ακέραιοι q, r ώστε $a = 17q + r$ και $r \in \{3, 5, 12, 14\}$. ■

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*

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

Λύση. Σε αυτή την άσκηση ο συμβολισμός $[a]$ σημαίνει $[a]_n$.

Αφού για $n \geq 3$ ο αριθμός $\phi(n)$ είναι άρτιος, έχουμε ότι ο αριθμός $\phi(n)/2$ είναι ακέραιος. Θέτουμε $b = a^{\phi(n)/2}$. Αφού $\mathsf{ord}_n(a) = \phi(n)$, έχουμε

$$\mathsf{ord}_n(b) = \mathsf{ord}_n(a^{\phi(n)/2}) = \frac{\phi(n)}{(\phi(n)/2, \phi(n))} = \frac{\phi(n)}{\phi(n)/2} = 2.$$

Φανερά $\mathsf{ord}_n(-1) = 2$, γιατί $[-1]^2 = [1]$. Για να δείξουμε ότι $b \equiv -1 \,(\mathsf{mod}\, n)$ αρκεί να δείξουμε ότι το $[-1]$ είναι το μοναδικό αντιστρέψιμο στοιχείο του $\mathbb{Z}_n$ που έχει τάξη 2. Αφού a είναι αρχική ρίζα $(\mathsf{mod}\, n)$, τα αντιστρέψιμα στοιχεία του $\mathbb{Z}_n$ είναι το σύνολο

$$\{[a]^k \mid 1 \leq k \leq \phi(n)\} \quad = \quad \{[a],\, [a^2],\, [a^3], \ldots, [a^{\phi(n)-1}],\, [a^{\phi(n)}] = [1]\}$$

Επομένως αρκεί να δείξουμε ότι αν k ακέραιος με $1 \leq k \leq \phi(n) - 1$ και $\mathsf{ord}_n(a^k) = 2$ τότε $k = \phi(n)/2$. Αφού

$$\mathsf{ord}_n(a^k) = \frac{\phi(n)}{(k, \phi(n))}$$

η υπόθεση $\mathsf{ord}_n(a^k) = 2$ συνεπάγεται ότι

$$\frac{\phi(n)}{2} = (k, \phi(n)).$$

Άρα $\frac{\phi(n)}{2} \mid k$. Αφού $1 \leq k \leq \phi(n) - 1$, έπεται ότι

$$\frac{\phi(n)}{2} = k$$

■

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 $\mathsf{ord}_p(-a) = \frac{p-1}{2}$.*

Λύση. Σε αυτή την άσκηση ο συμβολισμός $[a]$ σημαίνει $[a]_p$.

1. Υποθέτουμε ότι $p \equiv 1 \,\mathsf{mod}\, 4$, και έστω q ακέραιος με $p - 1 = 4q$. Αφού p πρώτος έχουμε $\phi(p) = p - 1 = 4q$. Αφού $-(-a) = a$, αρκεί να υποθέσουμε ότι ο ακέραιος a με $(a, p) = 1$ είναι αρχική ρίζα $\mathsf{mod}\, p$ και να δείξουμε ότι και το $-a$ είναι αρχική ρίζα $\mathsf{mod}\, p$. Υποθέτουμε ότι το $-a$ δεν είναι αρχική ρίζα $\mathsf{mod}\, p$ και θα καταλήξουμε σε αντίφαση. Αφού το $-a$ δεν είναι αρχική ρίζα $\mathsf{mod}\, p$ έχουμε ότι $\mathsf{ord}_p(-a) < \phi(p) = 4q$, άρα υπάρχει ακέραιος διαιρέτης d του $4q$ με $1 \leq d < 4q$ ώστε $(-a)^d \equiv 1 \,\mathsf{mod}\, p$. Αν ο d είναι άρτιος, αφού $a^d = (-a)^d$ έπεται ότι και $a^d \equiv 1 \,\mathsf{mod}\, p$, αντίφαση αφού $\mathsf{ord}_p(a) = 4q$. Υποθέτουμε d περιττός. Αφού $d \mid 4q$ έχουμε ότι $d \mid q$. Άρα $(-a)^q \equiv 1 \,\mathsf{mod}\, p$ που συνεπάγεται ότι $a^q \equiv -1 \,\mathsf{mod}\, p$ και άρα ότι $a^{2q} \equiv 1 \,\mathsf{mod}\, p$, το οποίο είναι αντίφαση αφού $\mathsf{ord}_p(a) = 4q$.
2. Υποθέτουμε ότι $p \equiv 3 \,\mathsf{mod}\, 4$, και έστω q ακέραιος με $p - 3 = 4q$. Αφού p πρώτος έχουμε $\phi(p) = p - 1 = 4q + 2$.

   Πρώτα θα υποθέσουμε ότι ο a είναι αρχική ρίζα $\mathsf{mod}\, p$ και θα δείξουμε ότι $\mathsf{ord}_p(-a) = \frac{p-1}{2}$. Από την Άσκηση 8 του παρόντος φυλλαδίου $a^{\frac{p-1}{2}} \equiv -1 \,\mathsf{mod}\, p$. Επομένως

   $$[-a] = [-1][a] = [a]^{\frac{p-1}{2}}[a] = [a]^{\frac{p-1}{2}+1} = [a]^{\frac{p+1}{2}}$$

   Επομένως από την Θεωρία έχουμε οτι

   $$\mathsf{ord}_p(-a) = \frac{p-1}{(p-1, \frac{p+1}{2})} = \frac{4q+2}{(4q+2, 2q+2)}$$

   Έχουμε

   $$(4q+2, 2q+2) = (4q+2-2(2q+2), 2q+2) = (-2, 2q+2) = 2$$

Συνεπώς $\mathsf{ord}_p(-a) = (4q+2)/2 = 2q+1 = (p-1)/2$.

Αντίστροφα, υποθέτουμε ότι $\mathsf{ord}_p(-a) = \frac{p-1}{2}$ και θα δείξουμε ότι το a είναι πρωταρχική ρίζα $\mathsf{mod}\, p$ δηλαδή ότι $\mathsf{ord}_p(a) = p-1$. Από την Θεωρία $\mathsf{ord}_p(a) \mid \phi(p) = p-1 = 4q+2$. Αρκεί να υποθέσουμε ότι για κάποιον ακέραιο k με $1 \leq k < p-1$ έχουμε $a^k \equiv 1 \,\mathsf{mod}\, p$ και να καταλήξουμε σε αντίφαση. Αν ο k είναι άρτιος, τότε $a^k = (-a)^k$ και άρα $(-a)^k \equiv 1 \,\mathsf{mod}\, p$, το οποίο συνεπάγεται ότι $2q+1 \mid k$. Αφού k άρτιος και $2q+1$ περιττός έπεται ότι $2(2q+1) = p-1 \mid k$ και άρα $k \geq p-1$, αντίφαση. Υποθέτουμε τώρα ότι ο k είναι περιττός. Τότε ο $2k$ είναι άρτιος και

$$[(-a)^{2k}] = [(-1)^{2k}][a^{2k}] = [-1^2]^k[a^k]^2 = [1][1] = [1]$$

Άρα $2q+1 \mid 2k$ το οποίο συνεπάγεται ότι $2q+1 \mid k$. Αφού $k < p-1 = 2(2q+1)$ έχουμε $k = 2q+1$. Έτσι $a^{2q+1} \equiv 1 \,\mathsf{mod}\, p$ το οποίο συνεπάγεται ότι $(-a)^{2q+1} = -a^{2q+1} \equiv -1 \,\mathsf{mod}\, p$, αντίφαση αφού υποθέσαμε ότι $\mathsf{ord}_p(-a) = 2q+1$. ■

Προφανώς το 1 είναι πρώταρχική ρίζα $\mathsf{mod}\, 2^1$ και το 3 είναι πρωταρχική ρίζα $\mathsf{mod}\, 2^2$. Η επόμενη Άσκηση δείχνει ιδιαίτερα ότι δεν υπάρχουν πρωταρχικές ρίζες $\mathsf{mod}\, 2^m$, $\forall m \geq 3$.

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

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

Λύση. Θέτουμε $n = 2^m$. Θα αποδείξουμε τον ισχυρισμό με χρήση της Αρχής Μαθηματικής Επαγωγής επί του m ξεκινώντας από το $m = 3$.

– Αν $m = 3$, τότε $a^{\frac{\varphi(2^m)}{2}} = a^{\frac{\varphi(2^3)}{2}} = a^{\frac{\varphi(8)}{2}} = a^{\frac{4}{2}} = a^2$. Επειδή ο a είναι περιττός, θα είναι της μορφής $a = 2k+1$ για κάποιον ακέραιο $k \geq 0$. Τότε $a^2 = (2k+1)^2 = 4k^2+4k+1 = 4k(k+1)+1$, δηλαδή $a^2-1 = 4k(k+1)$. Επειδή το γινόμενο δύο διαδοχικών ακέραιων είναι πάντα άρτιος αριθμός, θα έχουμε $2 \mid k(k+1)$ και επομένως $8 \mid 4k(k+1)$, δηλαδή $8 \mid a^2-1$ και επομένως Συνοψίζοντας θα έχουμε ότι $a^{\frac{\varphi(2^3)}{2}} \equiv 1 \,(\mathsf{mod}\, 2^3)$.

– Επαγωγικη Υποθεση: Υποθέτουμε ότι $m > 3$ και: $a^{\frac{\varphi(2^m)}{2}} \equiv 1 \,(\mathsf{mod}\, 2^m)$.

Τότε $2^m \mid a^{\frac{\varphi(2^m)}{2}} - 1$, και επομένως υπάρχει $s \in \mathbb{Z}$ έτσι ώστε

$$a^{\frac{\varphi(2^m)}{2}} - 1 = s2^m \implies a^{\frac{\varphi(2^m)}{2}} = s2^m + 1 \implies a^{\varphi(2^m)} = (s2^m+1)^2 = 1 + 2^{m+1}s + 2^{2m}s^2$$

Επειδή $m+1 < 2m$ (αν $m+1 \geq 2m$,τότε $1 \geq m$ το οποίο είναι άτοπο), θα έχουμε οτι $2^{m+1} \mid 2^{2m}$ δηλαδή $2^{2m} \equiv 0 \,(\mathsf{mod}\, 2^{m+1})$. Τότε η παραπάνω σχέση δίνει:

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

Τέλος επειδή

$$\frac{\varphi(2^{m+1})}{2} = \frac{2^{m+1}-2^m}{2} = \frac{2^m}{2} = 2^{m-1} = \varphi(2^m)$$

Οι τελευταίες δύο σχέσεις δείχνουν το ζητούμενο

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

Από την Αρχή Μαθηματικής Επαγωγής έπεται ότι ισχύει η ζητούμενη σχέση για κάθε $m \geq 3$. ■