# ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

## Τμημα **Β΄**

## Λυσεις Ασκησεων - Φυλλαδιο **7**

Διδασκων: Α. Μπεληγιάννης

Ιστοσελιδα Μαθηματος:
http://users.uoi.gr/abeligia/NumberTheory/NT2016/NT2016.html

**Πέμπτη 7 Δεκεμβρίου 2016**

**Άσκηση 1.** *Για κάθε $n \in \mathbb{N}$, να προσδιορισθούν τα υπόλοιπα των διαιρέσεων:*

$$\frac{251^{143}}{7} \quad \& \quad \frac{3^{2n}+3^n+1}{13} \quad \& \quad \frac{2n^3+3n^2+n}{6}$$

*Λύση.* **1.** Θα έχουμε $251 = 35 \cdot 7 + 6$. Επομένως $[251]_7 = [6]_7$. Επειδή $[6]_7 = [-1]_7$, θα έχουμε $[251]_7 = [-1]_7$ και τότε:

$$[251^{143}]_7 = [251]_7^{143} = [-1]_7^{143} = [(-1)^{143}]_7 = [-1]_7 = [6]_7$$

Επομένως το υπόλοιπο της διαίρεσης είναι 6.

**2.** Ο αριθμός $n$ θα έχει μια από τις παρακάτω μορφές: $n = 3k$, ή $n = 3k+1$, ή $n = 3k+2$.

– Υποθέτουμε πρώτα ότι $n = 3k$. Τότε:

$$3^{2n}+3^n+1 = 3^{2(3k)}+3^{3k}+1 = 3^{6k}+3^{3k}+1 = (3^3)^{2k}+(3^3)^k+1 = 27^{2k}+27^k+1$$

Επειδή $[27]_{13} = [1]_{13}$, θα έχουμε:

$$[3^{2n}+3^n+1]_{13} = [27^{2k}+27^k+1]_{13} = [27]_{13}^{2k}+[27]_{13}^k+[1]_{13} = [1]_{13}^{2k}+[1]_{13}^k+[1]_{13} = [1]_{13}+[1]_{13}+[1]_{13} = [3]_{13}$$

και επομένως, όταν $n = 3k$, το υπόλοιπο της διαίρεσης είναι 3.

– Υποθέτουμε ότι $n = 3k+1$. Τότε:

$$3^{2n}+3^n+1 = 3^{2(3k+1)}+3^{3k+1}+1 = 3^{6k}3^2+3^{3k}3+1 = 9\cdot 3^{6k}+3\cdot 3^{3k}+1 = 9\cdot 27^{2k}+3\cdot 27^k+1$$

Επειδή $[27]_{13} = [1]_{13}$, θα έχουμε:

$$[3^{2n}+3^n+1]_{13} = [9\cdot 27^{2k}+3\cdot 27^k+1]_{13} = 9\cdot [27]_{13}^{2k}+3\cdot [27]_{13}^k+[1]_{13} =$$

$$= 9\cdot [1]_{13}+3\cdot [1]_{13}+[1]_{13} = 13[1]_{13} = [13]_{13} = [0]_{13}$$

και επομένως, όταν $n = 3k+1$, το υπόλοιπο της διαίρεσης είναι 0.

– Υποθέτουμε ότι $n = 3k+2$. Τότε:

$$3^{2n}+3^n+1 = 3^{2(3k+2)}+3^{3k+2}+1 = 3^{6k}3^4+3^{3k}3^2+1 = 81\cdot 3^{6k}+9\cdot 3^{3k}+1 = 9\cdot 27^{2k}+3\cdot 27^k+1$$

Επειδή $[81]_{13} = [3]_{13}$ και $[27]_{13} = [1]_{13}$, θα έχουμε:

$$[3^{2n}+3^n+1]_{13} = [81\cdot 27^{2k}+9\cdot 27^k+1]_{13} = 3\cdot [27]_{13}^{2k}+9\cdot [27]_{13}^k+[1]_{13} =$$

$$= 3\cdot [1]_{13}+9\cdot [1]_{13}+[1]_{13} = 13[1]_{13} = [13]_{13} = [0]_{13}$$

και επομένως, όταν $n = 3k+1$, το υπόλοιπο της διαίρεσης είναι 0.

Συνοψίζουμε:

$$[3^{2n}+3^n+1]_{13} = \begin{cases} [3]_{13}, & \text{αν} \quad 3 \mid n \\ \\ [0]_{13}, & \text{αν} \quad 3 \nmid n \end{cases}$$

Επομένως το υπόλοιπο της διαίρεσης είναι 3 όταν $3 \mid n$ και 0 όταν $3 \nmid n$.

**3.** Αν $n = 1$, τότε $2n^3+3n^2+n = 6$, και αν $n = 2$, τότε $2n^3+3n^2+n = 30$. Έτσι αν $1 \leq n \leq 2$, τότε $6 \mid 2n^3+3n^2+n$. Αν $n \geq 3$, τότε θα έχουμε:

$$2n^3+3n^2+n = n\cdot(2n^2+3n+1) = n\cdot(n+1)\cdot(2n+1) =$$

$$= n\cdot(n+1)\cdot[(n+2)+(n-1)] = (n-1)\cdot n\cdot(n+1)+n\cdot(n+1)\cdot(n+2)$$

Επειδή[1] το γινόμενο τριών διαδοχικών ακεραίων διαιρείται από το 6, έπεται ότι $6 \mid (n-1)\cdot n\cdot(n+1)$ και $6 \mid n\cdot(n+1)\cdot(n+2)$. Επομένως $6 \mid 2n^3+3n^2+n$, δηλαδή

$$2n^3+3n^2+n = 0 \,(\mathsf{mod}\, 6)$$

και άρα το υπόλοιπο της διαίρεσης είναι ίσο με 0. ■

**Σχόλιο 1.** Υπενθυμίζουμε ότι το σύνολο των αντιστρεψίμων κλάσεων υπολοίπων $\mathsf{mod}\, n$ είναι:

$$\mathsf{U}(\mathbb{Z}_n) = \left\{ [a]_n \in \mathbb{Z}_n \;\mid\; \exists\, [b]_n \in \mathbb{Z}_n :\; [a]_n\cdot[b]_n = [1]_n = [b]_n\cdot[a]_n \right\}$$

και γνωρίζουμε ότι:

$$[a]_n \in \mathsf{U}(\mathbb{Z}_n) \quad \Longleftrightarrow \quad (a,n) = 1$$

Έστω $[a]_n \in \mathsf{U}(\mathbb{Z}_n)$. Για την εύρεση της (μοναδικής) κλάσης ισοτιμίας $[b]_n$ έτσι ώστε $[a]_n\cdot[b]_n = [1]_n$, δηλαδή της κλάσης $[a]_n^{-1}$, εργαζόμαστε ως εξής: Επειδή $(a,n) = 1$, έπεται ότι υπάρχουν ακέραιοι $b, k$ έτσι ώστε: $a\cdot b + n\cdot k = 1$. Τότε:

$$a\cdot b+n\cdot k = 1 \quad \Longrightarrow \quad [a\cdot b+n\cdot k]_n = 1_n \quad \Longrightarrow \quad [a]_n\cdot[b]_n+[n]_n\cdot[k]_n = 1_n \quad \Longrightarrow \quad [a]_n\cdot[b]_n = [1]_n$$

Επομένως $[a]_n^{-1} = [b]_n$, όπου $a\cdot b + k\cdot n = 1$.

Αν γνωρίζουμε το Θεώρημα του Euler, τότε μπορούμε να υπολογίσουμε την κλάση $[a]_n^{-1}$ ως εξής. Από τη σχέση $a^{\varphi(n)} \equiv 1\,(\mathsf{mod}\, n)$, θα έχουμε

$$a\cdot a^{\varphi(n)-1} \equiv 1\,(\mathsf{mod}\, n) \qquad \Longrightarrow \qquad [a]_n^{-1} = [a^{\varphi(n)-1}]_n = [a]_n^{\varphi(n)-1} \qquad \surd$$

**Άσκηση 2.** **1.** *Δείξτε ότι η κλάση υπολοίπων* $[10]_{21}$ *είναι αντιστρέψιμη ως στοιχείο του* $\mathbb{Z}_{21}$*, και βρείτε την αντίστροφη κλάση της.*

**2.** *Δείξτε ότι η κλάση* $[62]_{155}$ *δεν είναι αντιστρέψιμη ως στοιχείο του* $\mathbb{Z}_{155}$.

*Λύση.* **1.** Επειδή $(10,21) = 1$ έπεται ότι η κλάση υπολοίπων $[10]_{21}$ είναι αντιστρέψιμη ως στοιχείο του $\mathbb{Z}_{21}$. Για την εύρεση της αντίστροφης κλάσης $[10]_{21}^{-1}$, θα έχουμε:

$$\begin{aligned} 21 = 2\cdot 10+1 \quad &\Longrightarrow \quad 1 = 1\cdot 21+(-2)\cdot 10 \\ &\Longrightarrow \quad [1]_{21} = [21]_{21}+[-2]_{21}\cdot[10]_{21} \\ &\Longrightarrow \quad [1]_{21} = [-2]_{21}\cdot[10]_{21} \\ &\Longrightarrow \quad [10]_{21}^{-1} = [-2]_{21} \\ &\Longrightarrow \quad [10]_{21}^{-1} = [19]_{21} \end{aligned}$$

Επομένως η αντίστροφη κλάση της $[10]_{21}$ είναι η $[19]_{21}$.

[1] Υπενθυμίζουμε ότι αν $A$ είναι το γινόμενο τριών διαδοχικών αριθμών, τότε $2 \mid A$ διότι ένας εκ των αριθμών είναι άρτιος, και $3 \mid A$ διότι γνωρίζουμε ότι γενικά το γινόμενο $k$ το πλήθος διαδοχικών αριθμών διαιρείται από το $k$. Επομένως επειδή $(2,3) = 1$, έπεται ότι $6 \mid A$.

**2.** Έχουμε

$$(62, 155) = (2 \cdot 31, 5 \cdot 31) = 31$$

Επειδή $(62, 155) = 31 \neq 1$ έπεται ότι η κλάση $[62]_{155}$ δεν αντιστρέφεται.

■

**Άσκηση 3.** *Δείξτε ότι αν $a, n \in \mathbb{Z}$ με $n \geq 1$ τότε το σύνολο*

$$\{a, a+1, \ldots, a+n-1\}$$

*αποτελεί ένα πλήρες σύστημα υπολοίπων* $\mathsf{mod}\, n$.

*Λύση.* Αρκεί να δείξουμε ότι αν $a + i \equiv a + j (\mathsf{mod}\, n)$ τότε $i = j$, όπου $0 \leq i \leq j \leq n-1$. Έχουμε

$$a + i \equiv a + j (\mathsf{mod}\, n) \implies n \mid a + i - a - j \implies n \mid i - j \implies n \mid j - i$$

Αν $j - i \neq 0$ έχουμε $n \leq j - i$, το οποίο ειναι αντίφαση, γιατί $j < n$ και $i \geq 0$. Άρα $i = j$. Συνεπώς το σύνολο $\{a, a+1, \ldots, a+n-1\}$ αποτελεί ένα πλήρες σύστημα υπολοίπων $\mathsf{mod}\, n$. ■

**Άσκηση 4.** *Έστω $\{a_1, a_2, \cdots, a_p\}$ και $\{b_1, b_2, \cdots b_p\}$ δύο πλήρη συστήματα υπολοίπων* $\mathsf{mod}\, p$*, όπου $p$ είναι ένας πρώτος. Να δείξετε ότι αν $p > 2$, τότε το σύνολο*

$$\left\{a_1 b_1, a_2 b_2, \cdots, a_p b_p\right\}$$

*δεν είναι ποτέ πλήρες σύστημα υπολοίπων* $\mathsf{mod}\, p$.

*Λύση.* Αφού $\{a_1, a_2, \cdots, a_p\}$ και $\{b_1, b_2, \cdots b_p\}$ είναι δύο πλήρη συστήματα υπολοίπων $\mathsf{mod}\, p$, τότε για κάποια $i, j \in \{1, \ldots, p\}$ έχουμε ότι $a_i \equiv 0 (\mathsf{mod}\, p)$ και $b_j \equiv 0 (\mathsf{mod}\, p)$. Χωρίς βλάβη της γενικότητας υποθέτουμε ότι $i = p$, δηλαδή

$$a_p \equiv 0 (\mathsf{mod}\, p)$$

Έχουμε τότε δύο περιπτώσεις:

(1) Αν $j \neq p$, τότε $a_j b_j \equiv 0 (\mathsf{mod}\, p)$ και $a_p b_p \equiv 0 (\mathsf{mod}\, p)$. Επομένως $a_j b_j \equiv a_p b_p (\mathsf{mod}\, p)$, και άρα το σύνολο $\left\{a_1 b_1, \cdots, a_p b_p\right\}$ δεν είναι πλήρες σύστημα υπολοίπων $\mathsf{mod}\, p$.

(2) Υποθέτουμε τώρα ότι $j = p$. Επειδή $\{a_1, a_2, \cdots, a_p\}$ είναι ένα πλήρες σύστημα υπολοίπων $\mathsf{mod}\, p$, υπάρχει μια «1-1» και «επί» απεικόνιση

$$\sigma : \{1, 2, \ldots, p-1\} \longrightarrow \{a_1, a_2, \ldots, a_{p-1}\}, \quad \text{έτσι ώστε} \quad a_i \equiv \sigma(i) (\mathsf{mod}\, p)$$

Συνεπώς επειδή

$$\prod_{i=1}^{p-1} a_i = \prod_{i=1}^{p-1} \sigma(i) = \prod_{i=1}^{p-1} i = 1 \cdot 2 \cdot \cdots \cdot (p-1)$$

από το Θεώρημα Wilson έπεται ότι

$$a_1 \cdot a_2 \cdots a_{p-1} = 1 \cdot 2 \cdots p - 1 = (p-1)! \equiv (-1) (\mathsf{mod}\, p)$$

και όμοια έπεται ότι

$$b_1 \cdot b_2 \cdots b_{p-1} \equiv (-1) (\mathsf{mod}\, p)$$

Τότε όμως

$$a_1 b_1 \cdot a_2 b_2 \cdots a_{p-1} b_{p-1} \equiv (-1)^2 \equiv 1 (\mathsf{mod}\, p)$$

Επομένως το σύνολο $\left\{a_1 b_1, a_2 b_2, \cdots, a_p b_p\right\}$ δεν είναι ένα πλήρες σύστημα υπολοίπων $\mathsf{mod}\, p$, διότι αν ήταν τότε θα έπρεπε $a_1 b_1 \cdot a_2 b_2 \cdots a_{p-1} b_{p-1} \equiv -1 (\mathsf{mod}\, p)$, που είναι άτοπο (επειδή $p > 2$, έπεται ότι $1 \not\equiv -1 (\mathsf{mod}\, p)$).

Άρα σε κάθε περίπτωση το σύνολο $\left\{a_1 b_1, \cdots, a_p b_p\right\}$ δεν είναι πλήρες σύστημα υπολοίπων $\mathsf{mod}\, p$. ■

**Άσκηση 5.** (1) *Δείξτε ότι:*

$$a \equiv b \,(\mathsf{mod}\, n_1) \quad \& \quad b \equiv c \,(\mathsf{mod}\, n_2) \quad \Longrightarrow \quad a \equiv c \,(\mathsf{mod}(n_1, n_2))$$

(2) *Δείξτε ότι αν* $a, b, n_1, \ldots, n_k \in \mathbb{Z}$ *με* $n_i \geq 1$ *για κάθε* $i = 1, 2, \cdots, k$*, τότε*

$$a \equiv b \,(\mathsf{mod}\, n_i), \quad \textit{για κάθε } i = 1, 2, \cdots, k \quad \Longleftrightarrow \quad a \equiv b \,(\mathsf{mod}[n_1, \ldots, n_k])$$

*Λύση.* (1) Έχουμε

$$\begin{cases} a \equiv b \,(\mathsf{mod}\, n_1) \\ \\ b \equiv c \,(\mathsf{mod}\, n_2) \end{cases} \Longrightarrow \begin{cases} n_1 \mid a - b \\ \\ n_2 \mid b - c \end{cases}$$

Έστω $d = (n_1, n_2)$ ο μέγιστος κοινός διαιρέτης των $n_1$ και $n_2$. Τότε $d \mid n_1$ και $d \mid n_2$ και άρα έχουμε

$$\begin{cases} d \mid a - b \\ \\ d \mid b - c \end{cases} \Longrightarrow \; d \mid a - b + b - c \; \Longrightarrow \; d \mid a - c \; \Longrightarrow \; a \equiv c \,(\mathsf{mod}\, d)$$

(2) Έστω $a \equiv b \,(\mathsf{mod}\, n_i)$ για κάθε $i = 1, 2, \cdots, k$. Τότε

$$n_i \mid a - b \;\; \forall\, i = 1, \ldots, k \;\; \Longrightarrow \;\; [n_1, \ldots, n_k] \mid a - b \;\; \Longrightarrow \;\; a \equiv b \,(\mathsf{mod}[n_1, \ldots, n_k])$$

Υποθέτουμε αντίστροφα ότι $a \equiv b \,(\mathsf{mod}[n_1, \ldots, n_k])$. Τότε $[n_1, \ldots, n_k] \mid a - b$ και επειδή

$$n_1 \mid [n_1, \ldots, n_k], \cdots, n_k \mid [n_1, \ldots, n_k]$$

έπεται ότι $n_i \mid a - b$ για κάθε $i = 1, \ldots, k$. Άρα $a \equiv b \,(\mathsf{mod}\, n_i)$ για κάθε $i = 1, 2, \cdots, k$. ■

**Άσκηση 6.** *Αν* $n > 1$ *είναι ένας θετικός ακέραιος, να δειχθεί ότι:*

$$n : \;\; \textit{πρώτος} \qquad \Longleftrightarrow \qquad (n-2)! \equiv 1 \,(\mathsf{mod}\, n)$$

*Λύση.* «$\Longrightarrow$» Έστω ότι ο αριθμός $n$ είναι πρώτος. Από το Θεώρημα του Wilson έπεται ότι $(n-1)! \equiv -1 \,(\mathsf{mod}\, n)$, και άρα $n \mid (n-1)! + 1$. Επειδή $(n-1)! + 1 = (n-2)! \cdot (n-1) + 1 = n \cdot (n-2)! - (n-2)! + 1$ και $n \mid n \cdot (n-2)!$, έπεται ότι

$$n \mid -(n-2)! + 1 \quad \Longrightarrow \quad n \mid (n-2)! - 1 \quad \Longrightarrow \quad (n-2)! \equiv 1 \,(\mathsf{mod}\, n)$$

«$\Longleftarrow$» Έστω ότι $(n-2)! \equiv 1 \,(\mathsf{mod}\, n)$, δηλαδή $n \mid (n-2)! - 1$. Τότε:

$$n \mid (n-1) \cdot ((n-2)! - 1) \quad \Longrightarrow \quad n \mid (n-1)! - (n-1) \qquad (*)$$

Έστω ο $n$ δεν είναι πρώτος. Τότε $n = a \cdot b$, όπου $1 < a, b < n$. Επειδή $a \mid n$, από την $(*)$, έπεται ότι $a \mid (n-1)! - (n-1)$. Επειδή $a < n$, έπεται ότι $a \leq n - 1$ και επομένως $a \mid (n-1)!$. Τότε προφανώς θα έχουμε $a \mid n - 1$. Επειδή $a \mid n$, έπεται ότι $a \mid 1$, δηλαδή $a = 1$, το οποίο είναι άτοπο. Άρα ο αριθμός $n$ είναι πρώτος. ■

**Άσκηση 7.** *Δείξτε ότι*

(1)
$$2^{20} - 1 \equiv 0 \;\; \mathsf{mod}\, 41$$

(2)
$$2^{50} \equiv 4 \;\; \mathsf{mod}\, 7$$

(3)
$$41^{65} \equiv 6 \;\; \mathsf{mod}\, 7$$

(4)
$$1! + 2! + 3! + \cdots + 100! \equiv 9 \;\; \mathsf{mod}\, 12$$

(5)

$$1^5 + 2^5 + 3^5 + \cdots + 100^5 \equiv 0 \mod 4$$

*Λύση.* (1) Έχουμε

$$\begin{aligned} 2^5 = 32 \equiv -9 \,(\mathsf{mod}\, 41) &\implies (2^5)^4 \equiv (-9)^4 \,(\mathsf{mod}\, 41) \\ &\implies 2^{20} \equiv 81^2 \,(\mathsf{mod}\, 41) \\ &\implies 2^{20} \equiv (2 \cdot 41 - 1)^2 \,(\mathsf{mod}\, 41) \\ &\implies 2^{20} \equiv (-1)^2 \,(\mathsf{mod}\, 41) \\ &\implies 2^{20} \equiv 1 \,(\mathsf{mod}\, 41) \\ &\implies 2^{20} - 1 \equiv 1 - 1 \,(\mathsf{mod}\, 41) \\ &\implies 2^{20} - 1 \equiv 0 \,(\mathsf{mod}\, 41) \end{aligned}$$

(2) Έχουμε

$$2^5 = 32 \equiv 4 \,(\mathsf{mod}\, 7) \implies (2^5)^{10} \equiv 4^{10} \,(\mathsf{mod}\, 7) \implies 2^{50} \equiv 4^{10} \,(\mathsf{mod}\, 7)$$

Όμως

$$4^2 \equiv 2 \,(\mathsf{mod}\, 7) \implies (4^2)^5 \equiv 2^5 \,(\mathsf{mod}\, 7) \implies 4^{10} \equiv 4 \,(\mathsf{mod}\, 7)$$

Επομένως έπεται ότι $2^{50} \equiv 4^{10} \equiv 4 \,(\mathsf{mod}\, 7)$.

(3) Έχουμε

$$41 \equiv -1 \,(\mathsf{mod}\, 7) \implies 41^{65} \equiv (-1)^{65} \,(\mathsf{mod}\, 7) \equiv -1 \,(\mathsf{mod}\, 7)$$

και άρα $41^{65} \equiv 6 \mod 7$.

(4) Παρατηρούμε ότι

$$\begin{cases} 1! + 2! + 3! \equiv 9 \,(\mathsf{mod}\, 12) \\ 4! = 24 \equiv 0 \,(\mathsf{mod}\, 12) \\ \forall\, k \geq 4 : \;\; k! = 4! \cdot 5 \cdot 6 \cdots k \equiv 0 \,(\mathsf{mod}\, 12) \end{cases}$$

Τότε

$$1! + 2! + 3! + \cdots + 100! \equiv 9 + 0 + 0 + \cdots + 0 \,(\mathsf{mod}\, 12) \equiv 9 \,(\mathsf{mod}\, 12)$$

(5) Έστω $n = 2k$ όπου $k = 1, \ldots, 50$. Τότε

$$n^5 = (2k)^5 = 2^5 \cdot k^5 = 2^2 \cdot (2^3 \cdot k^5) = 4 \cdot (2^3 \cdot k^5) \equiv 0 \,(\mathsf{mod}\, 4)$$

και άρα

$$2^5 + 4^5 + 6^5 + \cdots + 100^5 \equiv 0 \,(\mathsf{mod}\, 4) \qquad (*)$$

Για τους υπόλοιπους πενήντα όρους του αθροίσματος, οι οποίοι είναι της μορφής $(2k+1)^5$, $0 \leq k \leq 49$, έχουμε

$$\begin{aligned} 1 \equiv 1 \,(\mathsf{mod}\, 4) &\implies 1^5 \equiv 1 \,(\mathsf{mod}\, 4) \\ 3 \equiv -1 \,(\mathsf{mod}\, 4) &\implies 3^5 \equiv (-1)^5 \equiv -1 \,(\mathsf{mod}\, 4) \\ 5 \equiv 1 \,(\mathsf{mod}\, 4) &\implies 5^5 \equiv 1^5 \equiv 1 \,(\mathsf{mod}\, 4) \\ 7 \equiv -1 \,(\mathsf{mod}\, 4) &\implies 7^5 \equiv (-1)^5 \equiv -1 \,(\mathsf{mod}\, 4) \\ &\vdots \\ 97 \equiv 1 \,(\mathsf{mod}\, 4) &\implies 97^5 \equiv 1^5 \equiv 1 \,(\mathsf{mod}\, 4) \\ 99 \equiv -1 \,(\mathsf{mod}\, 4) &\implies 99^5 \equiv (-1)^5 \equiv -1 \,(\mathsf{mod}\, 4) \end{aligned}$$

Άρα έχουμε

$$1^5 + 3^5 + \cdots + 97^5 + 99^5 \equiv [1 + (-1)] + \cdots + [1 + (-1)] \equiv 0 + 0 + \cdots + 0 \equiv 0 \,(\mathsf{mod}\, 4) \qquad (**)$$

Από τις σχέσεις $(*)$ και $(**)$ έπεται ότι[2]:

$$1^5 + 2^5 + 3^5 + \cdots + 100^5 \equiv 0 \,(\mathsf{mod}\, 4)$$ ■

**Άσκηση 8.** *Εαν οι $a, b$ είναι ακέραιοι και $p$ είναι ένας πρώτος αριθμός δείξτε ότι*[3]

$$(a+b)^p \equiv a^p + b^p \,(\mathsf{mod}\, p)$$

*Λύση.* Από το διωνυμικό ανάπτυγμα έχουμε

$$\begin{aligned} (a+b)^p &= \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k \\ &= \binom{p}{0} \cdot a^p + \binom{p}{1} \cdot a^{p-1} \cdot b + \cdots + \binom{p}{p-1} \cdot a \cdot b^{p-1} + \binom{p}{p} \cdot b^p \\ &= a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} \cdot a^{p-k} \cdot b^k \end{aligned}$$

**1ος Τρόπος:** Γνωρίζουμε ότι $\binom{p}{k} \in \mathbb{N}$. Θέτουμε

$$A = \binom{p}{k} = \frac{p!}{k!(p-k)!} \qquad \text{και τότε:} \qquad p! = A \cdot k! \cdot (p-k)!$$

---

[2] Διαφορετική Απόδειξη: Για κάθε $n = 1, 2, \cdots, 100$:

(α΄) Όταν ο $n$ είναι άρτιος, και άρα της μορφής $n = 2k$, τότε $n^5 = (2k)^5 = 4k^2 \cdot 4k^2 \cdot 2k \equiv 0 \,(\mathsf{mod}\, 4)$.

(β΄) Όταν ο $n$ είναι περιττός, τότε προφανώς $(n, 4) = 1$. Τότε από το Θεώρημα του Euler έπεται ότι $n^{\varphi(4)} \equiv 1 \,(\mathsf{mod}\, 4)$, δηλαδή $n^2 \equiv 1 \,(\mathsf{mod}\, 4)$. Τότε θα έχουμε $n^5 \equiv n \,(\mathsf{mod}\, 4)$.

Συνδυάζοντας τα παραπάνω θα έχουμε

$$\sum_{k=1}^{100} k^5 \equiv \sum_{k=1}^{50} (2k)^5 + \sum_{k=1}^{50} (2k-1)^5 \equiv 0 + \sum_{k=1}^{50} (2k-1) \equiv 50^2 \equiv 4 \cdot 25^2 \equiv 0 \,(\mathsf{mod}\, 4)$$

όπου παραπάνω χρησιμοποιήσαμε τη σχέση

$$\sum_{k=1}^{n} (2k-1) = n^2$$

βλέπε την Άσκηση **4** του Φυλλαδίου **1.**

[3] Παρατηρείστε ότι αν ο $p$ δεν είναι πρώτος, τότε η παραπάνω σχέση δεν ισχύει, διότι για παράδειγμα

$$4 \nmid \binom{4}{2} = 6$$

Επειδή $p \mid p!$, έπεται ότι $p \mid A \cdot k! \cdot (p-k)!$. Αν $p \mid k! = 1 \cdot 2 \cdots k$, τότε επειδή ο $p$ είναι πρώτος, από το Λήμμα του Ευκλείδη έπεται ότι $p \mid j$ για κάποιο $j \leq k \leq p-1$, και άρα $p \leq j < p$ και αυτό είναι άτοπο. Αν $p \mid (p-k)! = 1 \cdot 2 \cdots (p-k)$, τότε επειδή ο $p$ είναι πρώτος, από το Λήμμα του Ευκλείδη έπεται ότι $p \mid j$ για κάποιο $j \leq p-k \leq p-1$, και άρα $p \leq j < p$ και αυτό είναι άτοπο. Επομένως επειδή ο $p$ είναι πρώτος, από το Λήμμα του Ευκλείδη έπεται ότι αναγκαστικά θα έχουμε $p \mid A = \binom{p}{k}, \forall k = 1, 2 \cdots, p-1$.

Τότε $p \mid \sum_{k=1}^{p-1} \binom{p}{k} = (a+b)^p - (a^p + b^p)$ και επομένως $(a+b)^p \equiv a^p + b^p \pmod{p}$.

**2ος Τρόπος:** Θα δείξουμε ότι

$$p \mid \binom{p}{k} = \frac{p!}{k! \cdot (p-k)!} = \frac{1 \cdot 2 \cdots p}{(1 \cdot 2 \cdots k) \cdot (1 \cdot 2 \cdots (p-k))} \in \mathbb{N}$$

για κάθε $1 \leq k \leq p-1$.

Έστω $1 \cdot 2 \cdots p = p \cdot p_1^{a_1} \cdots p_n^{a_n}$ η πρωτογενής ανάλυση του $p!$ και έστω $(1 \cdot 2 \cdots k) \cdot (1 \cdot 2 \cdots p-k) = q_1^{b_1} \cdots q_m^{b_m}$ η πρωτογενής ανάλυση του αριθμού $(1 \cdot 2 \cdots k) \cdot (1 \cdot 2 \cdots p-k)$. Όμως

$$p \neq p_1, \cdots, p_n \quad \text{και} \quad p \neq q_1, \cdots, q_m$$

διότι οι αριθμοί $1, 2, 3, \cdots, p-1 \leq p$ και $k, p-k \leq p$ επίσης. Άρα για να είναι θετικός ακέραιος ο

$$\binom{p}{k}$$

θα πρέπει στη πρωτογενή του ανάλυση να έχουμε ότι κάθε $q_i$ είναι κάποιο $p_j$ και $b_i \leq a_i$. Επειδή λοιπόν ο πρώτος αριθμός $p \notin \{q_1, \cdots, q_m\}$ έπεται ότι η πρωτογενής ανάλυση του

$$\binom{p}{k}$$

θα περιέχει τον $p$ και άρα

$$p \mid \binom{p}{k}$$

Επομένως

$$\binom{p}{k} \equiv 0 \pmod{p} \quad \Longrightarrow \quad \sum_{k=1}^{p-1} \binom{p}{k} \cdot a^{p-k} \cdot b^k \equiv 0 \pmod{p}$$

και άρα από το διωνυμικό ανάπτυγμα έχουμε το ζητούμενο: $(a+b)^p \equiv a^p + b^p \pmod{p}$. ■

**Άσκηση 9.** *Έστω $n$ ένας θετικός ακέραιος.*

**1.** *Αν $a \in \mathbb{Z}$ και $(a, n) = 1 = (a-1, n)$, να δειχθεί ότι:*

$$1 + a + a^2 + \cdots + a^{\phi(n)-1} \equiv 0 \pmod{n}$$

**2.** *Αν ο $n$ είναι σύνθετος ακέραιος και $n > 4$, να δειχθεί ότι:*

$$(n-1)! \equiv 0 \pmod{n}$$

*Λύση.* **1.** Επειδή $(a, n) = 1$, από το Θεώρημα του Euler έπεται ότι $a^{\phi(n)} \equiv 1 \pmod{n}$. Επομένως $n \mid a^{\phi(n)} - 1$. Επειδή $a^{\phi(n)} - 1 = (a-1) \cdot (a^{\phi(n)-1} + a^{\phi(n)-2} + \cdots + a + 1)$ και $(n, a-1) = 1$, από το Λήμμα του Ευκλείδη έπεται ότι $n \mid a^{\phi(n)-1} + a^{\phi(n)-2} + \cdots a + 1$, και επομένως:

$$1 + a + a^2 + \cdots + a^{\phi(n)-1} \equiv 0 \pmod{n}$$

**2.** Αρκεί να δείξουμε ότι

$$n \mid (n-1)!$$

Επειδή ο $n$ είναι σύνθετος έχουμε ότι $n = s \cdot t$, με $1 \lneqq s, t \leq n-1$. Διακρίνουμε δυο περιπτώσεις:

• Έστω $s \neq t$ και χωρίς βλάβη της γενικότητας υποθέτουμε ότι $s < t$. Τότε

$$(n-1)! = 1 \cdot 2 \cdot 3 \cdots s \cdots t \cdots n-1 \implies n = s \cdot t \mid (n-1)!$$

• Έστω $s = t$. Τότε $n = s^2$ και άρα $n - 1 = s^2 - 1 = (s-1) \cdot (s+1)$. Επειδή $n = s^2 > 4$ έχουμε ότι $s > 2$ και άρα

$$s - 1 \geq 2 \implies n - 1 \geq 2 \cdot (s+1) = 2s + 2 > 2s$$

Άρα $s, 2s < n - 1$, και συνεπώς οι αριθμοί $s$ και $2s$ είναι παράγοντες του $(n-1)!$, δηλαδή

$$(n-1)! = 1 \cdot 2 \cdots s \cdots 2s \cdots n-1 \implies n = s^2 \mid (n-1)!$$

Έτσι σε κάθε περίπτωση έχουμε ότι $n \mid (n-1)!$. ■

**Άσκηση 10.** *Έστω $X = \{x_1, x_2, \cdots, x_n\}$ ένα πλήρες σύστημα υπολοίπων* mod $n$*, όπου $n > 1$ είναι περιττός φυσικός. Δείξτε ότι:*

$$\sum_{i=1}^{n} x_i \equiv 0 \,(\mathsf{mod}\, n)$$

*Λύση.* Το σύνολο $Y = \{1, 2, \ldots, n\}$ είναι ένα πλήρες σύστημα υπολοίπων mod $n$. Τότε όπως γνωρίζουμε: $\{[1]_n, [2]_n, \cdots, [n]_n\} = \{[x_1]_n, [x_2]_n, \cdots, [x_n]_n\}$, και άρα υπάρχει μια «1-1» και «επί» απεικόνιση $\sigma \colon \{[1]_n, [2]_n, \cdots, [n]_n\} \longrightarrow \{[x_1]_n, [x_2]_n, \cdots, [x_n]_n\}$ έτσι ώστε $[x_i]_n = [\sigma(i)]_n$, $\forall i = 1, 2, \cdots, n$. Ισοδύναμα, υπάρχει μια «1-1» και «επί» απεικόνιση $\sigma \colon Y \longrightarrow X$ έτσι ώστε

$$x_i \equiv \sigma(i) \,(\mathsf{mod}\, n)$$

για κάθε $1 \leq i \leq n$.

Τότε

$$\sum_{i=1}^{n} x_i \equiv \sum_{i=1}^{n} \sigma(i) \,(\mathsf{mod}\, n) \qquad (*)$$

Όμως

$$\sum_{i=1}^{n} \sigma(i) = \sum_{j=1}^{n} j = 1 + 2 + \cdots + n = \frac{n \cdot (n+1)}{2} \quad \overset{(*)}{\implies} \quad \sum_{i=1}^{n} x_i \equiv \frac{n \cdot (n+1)}{2} \,(\mathsf{mod}\, n) \qquad (1)$$

Επειδή ο αριθμός $n > 1$ είναι περιττός φυσικός έχουμε ότι $\frac{n+1}{2} \in \mathbb{N}$ και άρα

$$n \mid \frac{n \cdot (n+1)}{2} \qquad (2)$$

Από τις σχέσεις (1) και (2) έπεται ότι $\sum_{i=1}^{n} x_i \equiv 0 \,(\mathsf{mod}\, n)$. ■

**Άσκηση 11.** *Έστω $X = \{x_0, x_1, \cdots, x_{m-1}\}$ ένα πλήρες σύστημα υπολοίπων* mod $m$ *και έστω $Y = \{y_0, y_1, \cdots, y_{n-1}\}$ ένα πλήρες σύστημα υπολοίπων* mod $n$*. Αν $(n, m) = 1$, δείξτε ότι το σύνολο*

$$Z = \{nx_i + my_j \in \mathbb{N} \mid 0 \leq i \leq m-1 \;\; \& \;\; 0 \leq j \leq n-1\}$$

*ένα πλήρες σύστημα υπολοίπων* mod $mn$.

*Λύση.* Αρκεί να δείξουμε ότι

$$nx_i + my_j \not\equiv nx_k + my_\lambda \,(\mathsf{mod}\, mn)$$

για κάθε $0 \leq i \neq k \leq m-1$ και για κάθε $0 \leq j \neq \lambda \leq n-1$.

Έστω $nx_i + my_j \equiv nx_k + my_\lambda \,(\mathsf{mod}\, mn)$. Τότε

$$n \cdot (x_i - x_k) + m \cdot (y_j - y_\lambda) \equiv 0 (\mathsf{mod}\, mn) \implies mn \mid n \cdot (x_i - x_k) + m \cdot (y_j - y_\lambda)$$

Αφού $m \mid mn$ τότε από τη παραπάνω σχέση έχουμε

$$\begin{cases} m \mid n \cdot (x_i - x_k) + m \cdot (y_j - y_\lambda) \\ \\ m \mid m \cdot (y_j - y_\lambda) \end{cases} \implies m \mid n \cdot (x_i - x_k)$$

$$\overset{(m,n)=1}{\implies} m \mid x_i - x_k$$

$$\implies x_i \equiv x_k \,(\mathsf{mod}\, m)$$

Παρόμοια δείχνουμε ότι

$$y_j \equiv y_\lambda \,(\mathsf{mod}\, n)$$

και επειδή το σύνολο $X = \{x_0, x_1, \cdots, x_{m-1}\}$ είναι ένα πλήρες σύστημα υπολοίπων $\mathsf{mod}\, m$ και το σύνολο $Y = \{y_0, y_1, \cdots, y_{n-1}\}$ είναι ένα πλήρες σύστημα υπολοίπων $\mathsf{mod}\, n$ έπεται ότι

$$i = k \quad \text{και} \quad j = \lambda$$

Άρα το σύνολο $Z = \{nx_i + my_j \in \mathbb{N} \mid 0 \le i \le m-1 \quad \& \quad 0 \le j \le n-1\}$ είναι ένα πλήρες σύστημα υπολοίπων $\mathsf{mod}\, mn$. ■

**Άσκηση 12.** *Έστω $X = \{x_1, x_2, \cdots, x_{\phi(m)}\}$ ένα αναγμένο (περιορισμένο) σύστημα υπολοίπων $\mathsf{mod}\, m$ και έστω $Y = \{y_1, y_2, \cdots, y_{\phi(n)}\}$ ένα αναγμένο (περιορισμένο) σύστημα υπολοίπων $\mathsf{mod}\, n$. Αν $(n, m) = 1$, δείξτε ότι το σύνολο*

$$Z = \{nx_i + my_j \in \mathbb{N} \;\mid\; 1 \le i \le \phi(m) \quad \& \quad 1 \le j \le \phi(n)\}$$

*ένα αναγμένο (περιορισμένο) σύστημα υπολοίπων $\mathsf{mod}\, mn$.*

*Λύση.* Για να είναι το σύνολο $Z$ ένα αναγμένο (περιορισμένο) σύστημα υπολοίπων $\mathsf{mod}\, mn$ θα πρέπει να δείξουμε ότι

$$\begin{cases} (1): \quad nx_i + my_j \equiv nx_k + my_l \,(\mathsf{mod}\, mn) \iff (i,j) = (k,l) \\ \\ (2): \quad (nx_i + my_j, mn) = 1, \quad \forall\, 1 \le i \le \phi(m), \quad 1 \le j \le \phi(n) \end{cases}$$

$(1)$: Έστω $nx_i + my_j \equiv nx_k + my_l \,(\mathsf{mod}\, mn)$. Τότε

$$\begin{cases} mn \mid n(x_i - x_k) + m(y_j - y_l) \\ \\ m \mid mn \\ \\ n \mid mn \end{cases} \implies \begin{cases} m \mid n(x_i - x_k) + m(y_j - y_l) \\ \\ n \mid n(x_i - x_k) + m(y_j - y_l) \end{cases} \implies \begin{cases} m \mid n(x_i - x_k) \\ \\ n \mid m(y_j - y_l) \end{cases}$$

$$\overset{(m,n)=1}{\implies} \begin{cases} m \mid x_i - x_k \\ \\ n \mid y_j - y_l \end{cases} \implies \begin{cases} x_i \equiv x_k \,(\mathsf{mod}\, m) \\ \\ y_j \equiv y_l \,(\mathsf{mod}\, n) \end{cases}$$

Άρα $(i,j) = (k,l)$ διότι $X = \{x_1, x_2, \cdots, x_{\phi(m)}\}$ είναι ένα αναγμένο (περιορισμένο) σύστημα υπολοίπων $\mathsf{mod}\, m$ και $Y = \{y_1, y_2, \cdots, y_{\phi(n)}\}$ είναι ένα αναγμένο (περιορισμένο) σύστημα υπολοίπων $\mathsf{mod}\, n$.

$(2)$: Αφού $(n, m) = 1$ τότε

$$(nx_i + my_j, mn) = (nx_i + my_j, m) \cdot (nx_i + my_j, n)$$

Έστω $d = (nx_i + my_j, m)$. Τότε για κάθε $i = 1, \dots, \phi(m)$ έχουμε

$$\begin{cases} d \mid nx_i + my_j \\ \\ d \mid m \end{cases} \implies \begin{cases} d \mid nx_i \\ \\ d \mid mx_i \end{cases} \implies d \mid (nx_i, mx_i) \implies d \mid (n,m)x_i \implies d \mid x_i$$

Συνεπώς $d \mid (x_i, m) = 1$ διότι το $X$ είναι ένα παναγμένο (περιορισμένο) σύστημα υπολοίπων $\mathsf{mod}\, m$, και άρα $d = 1$. Παρόμοια δείχνουμε ότι $(nx_i + my_j, n) = 1$ και άρα το $(2)$ ισχύει. ■

**Άσκηση 13.** *Έστω $p$ ένας περιττός πρώτος αριθμός και $n$ ένας θετικός ακέραιος έτσι ώστε:*

$$2^n \not\equiv 1 \,(\mathsf{mod}\, p)$$

*Να δειχθεί ότι:*

$$1^n + 2^n + \cdots + (p-1)^n \equiv 0 \,(\mathsf{mod}\, p)$$

*Λύση.* Προφανώς το σύνολο $\{1, 2, \cdots, p-1\}$ είναι ένα αναγμένο (περιορισμένο) σύστημα υπολοίπων $\mathsf{mod}\, p$. Επειδή ο $p$ είναι περιττός πρώτος, θα έχουμε $(2, p) = 1$, και άρα[4] το σύνολο $\{2 \cdot 1, 2 \cdot 2, \cdots, 2 \cdot (p-1)\} = \{2, 4, \cdots, 2 \cdot (p-1)\}$ είναι επίσης ένα αναγμένο (περιορισμένο) σύστημα υπολοίπων $\mathsf{mod}\, p$. Αυτό σημαίνει ότι

$$\{[2]_p, [4]_p, \cdots, [2 \cdot (p-1)]_p\} = \{[1]_p, [2]_p, \cdots, [p-1]_p\}$$

και άρα υπάρχει μια μετάθεση $\sigma$ των κλάσεων ισοτιμίας $[k]_p$, $1 \le k \le p-1$ έτσι ώστε:

$$[2k]_p = [\sigma(k)]_p, \quad 1 \le k \le p-1 \quad \implies \quad 2k \equiv \sigma(k) \,(\mathsf{mod}\, p), \quad 1 \le k \le p-1$$

Τότε:

$$2k \equiv \sigma(k) \,(\mathsf{mod}\, p) \quad \implies \quad (2k)^n \equiv \sigma(k)^n \,(\mathsf{mod}\, p), \qquad 1 \le k \le p-1$$

Προσθέτοντας τις παραπάνω ισοτιμίες, θα έχουμε:

$$\sum_{k=1}^{p-1} (2k)^n \equiv \sum_{k=1}^{p-1} \sigma(k)^n \,(\mathsf{mod}\, p) \implies 2^n + 4^n + \cdots + (2(p-1))^n \equiv \sigma(1)^n + \sigma(2)^n + \cdots + \sigma(p-1)^n \,(\mathsf{mod}\, p)$$

Επειδή τα στοιχεία $\sigma(1), \sigma(2), \cdots, \sigma(p-1)$ είναι τα στοιχεία $1, 2, \cdots, p-1$, ενδεχομένως με διαφορετική σειρά, έπεται ότι:

$$\sigma(1)^n + \sigma(2)^n + \cdots + \sigma(p-1)^n = 1^n + 2^n + \cdots + (p-1)^n$$

και επομένως

$$2^n + 4^n + \cdots + (2(p-1))^n \equiv 1^n + 2^n + \cdots + (p-1)^n \,(\mathsf{mod}\, p) \implies 2^n \sum_{k=1}^{p-1} k^n \equiv \sum_{k=1}^{p-1} k^n \,(\mathsf{mod}\, p)$$

Επειδή $2^n \not\equiv 1 \,(\mathsf{mod}\, p)$, έπεται ότι $p \nmid 2^n - 1$. Τότε θα έχουμε:

$$p \mid 2^n \sum_{k=1}^{p-1} k^n - \sum_{k=1}^{p-1} k^n \implies p \mid (2^n - 1)\Big(\sum_{k=1}^{p-1} k^n\Big) \overset{(*)}{\implies} p \mid \sum_{k=1}^{p-1} k^n \implies \sum_{k=1}^{p-1} k^n \equiv 0 \,(\mathsf{mod}\, p)$$

όπου στην συνεπαγωγή $(*)$ χρησιμοποιήσαμε ότι επειδή ο $p$ είναι πρώτος και $p \nmid 2^n - 1$, αναγκαστικά θα έχουμε $p \mid \sum_{k=1}^{p-1} k^n$. Επομένως: $1^n + 2^n + \cdots + (p-1)^n \equiv 0 \,(\mathsf{mod}\, p)$. ■

**Άσκηση 14.** **1.** *Έστω $m, n$ δύο φυσικοί αριθμοί έτσι ώστε: $(m, n) = 1$. Δείξτε ότι:*

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \,(\mathsf{mod}\, mn)$$

[4] Υπενθυμίζουμε ότι αν $\{x_1, x_2, \cdots, x_{\phi(n)}\}$ είναι ένα αναγμένο (περιορισμένο) σύστημα υπολοίπων $\mathsf{mod}\, n$ και $a \in \mathbb{Z}$, όπου $(a, n) = 1$, τότε το σύνολο $\{ax_1, ax_2, \cdots, ax_{\phi(n)}\}$ είναι ένα αναγμένο (περιορισμένο) σύστημα υπολοίπων $\mathsf{mod}\, n$.

**2.** *Έστω $p, q$ δύο πρώτοι, όπου $p \neq q$. Δείξτε ότι:*
(α΄)
$$p^{q-1} + q^{p-1} \equiv 1 \,(\mathsf{mod}\, pq)$$
(β΄)
$$p-1 \mid q-1 \quad \& \quad (a, pq) = 1 \quad \Longrightarrow \quad a^{q-1} \equiv 1 (\mathsf{mod}\, pq)$$

*Λύση.* **1.** Από το Θεώρημα του Euler έχουμε:

$$\begin{cases} m^{\phi(n)} \equiv 1 \,(\mathsf{mod}\, n) \\ \\ n^{\phi(m)} \equiv 1 \,(\mathsf{mod}\, m) \end{cases} \Longrightarrow \begin{cases} n \mid m^{\phi(n)} - 1 \\ \\ m \mid n^{\phi(m)} - 1 \end{cases}$$

$$\Longrightarrow \quad m \cdot n \mid (m^{\phi(n)} - 1) \cdot (n^{\phi(m)} - 1)$$

$$\Longrightarrow \begin{cases} m \cdot n \mid \left(m^{\phi(n)} \cdot n^{\phi(m)} - (m^{\phi(n)} + n^{\phi(m)} - 1)\right) \\ \\ m \cdot n \mid m^{\phi(n)} \cdot n^{\phi(m)} \end{cases}$$

$$\Longrightarrow \quad m \cdot n \mid m^{\phi(n)} + n^{\phi(m)} - 1$$

$$\Longrightarrow \quad m^{\phi(n)} + n^{\phi(m)} \equiv 1 \,(\mathsf{mod}\, mn)$$

**2.** (α΄) Αφού $p \neq q$ έχουμε $(p, q) = 1$ και άρα από το ερώτημα $(1)$ έπεται ότι
$$p^{\phi(q)} + q^{\phi(p)} \equiv 1 \,(\mathsf{mod}\, pq) \;\Longrightarrow\; p^{q-1} + q^{p-1} \equiv 1 \,(\mathsf{mod}\, pq)$$

(β΄) Έστω ότι $p-1 \mid q-1$ και $(a, pq) = 1$. Τότε $q-1 = (p-1) \cdot k$ για κάποιο $k \in \mathbb{N}$, και επειδή $(p, q) = 1$ έχουμε

$$(a, pq) = 1 \;\Longrightarrow\; (a, p)(a, q) = 1 \;\Longrightarrow\; (a, p) = 1 \quad \text{και} \quad (a, q) = 1$$
$$\Longrightarrow \quad p \nmid a \quad \text{και} \quad q \nmid a$$

Από το Θεώρημα του Fermat έχουμε

$$\begin{cases} a^{p-1} \equiv 1 \,(\mathsf{mod}\, p) \\ \\ a^{q-1} \equiv 1 \,(\mathsf{mod}\, q) \end{cases} \Longrightarrow \; a^{(p-1)k} \equiv 1^k \,(\mathsf{mod}\, p) \quad \Longrightarrow \quad a^{q-1} \equiv 1 \,(\mathsf{mod}\, p)$$

$$\Longrightarrow \quad \begin{cases} a^{q-1} \equiv 1 \,(\mathsf{mod}\, p) \\ \\ a^{q-1} \equiv 1 \,(\mathsf{mod}\, q) \end{cases}$$

$$\Longrightarrow \quad \begin{cases} p \mid a^{q-1} - 1 \\ \\ q \mid a^{q-1} - 1 \end{cases}$$

$$\overset{(p,q)=1}{\Longrightarrow} \quad pq \mid a^{q-1} - 1$$

Επομένως $a^{q-1} \equiv 1 (\mathsf{mod}\, pq)$. ■

**Άσκηση 15.** *Δείξτε ότι για κάθε $n \in \mathbb{N}$, ο αριθμός*
$$\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$$
*είναι ακέραιος.*

*Λύση.* Έχουμε

$$A = \frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n = \frac{3n^5 + 5n^3 + 7n}{15}$$

και άρα:

$$A \in \mathbb{Z} \iff 15 \mid 3n^5 + 5n^3 + 7n$$

- Έστω $B = 3n^5 + 5n^3 + 7n$. Τότε το $B$ γράφεται ως εξής:

$$B = 3 \cdot (n^5 + 2n^3 + 2n) - (n^3 - n) \tag{1}$$

Επειδή ο αριθμός 3 είναι πρώτος τότε για κάθε $n \in \mathbb{Z}$ έχουμε

$$n^3 \equiv n \,(\mathsf{mod}\, 3) \implies \begin{cases} 3 \mid n^3 - n \\ \\ 3 \mid 3 \cdot (n^5 + 2n^3 + 2n) \end{cases} \overset{(1)}{\implies} 3 \mid B \tag{2}$$

- Επίσης το $B$ γράφεται και ως

$$B = 5 \cdot (n^5 + n^3 + n) - 2 \cdot (n^5 - n) \tag{3}$$

Όμοια με παραπάνω, επειδή ο αριθμός 5 είναι πρώτος τότε για κάθε $n \in \mathbb{Z}$ έχουμε

$$n^5 \equiv n \,(\mathsf{mod}\, 5) \implies \begin{cases} 5 \mid n^5 - n \\ \\ 5 \mid 5 \cdot (n^5 + n^3 + n) \end{cases} \overset{(3)}{\implies} 5 \mid B \tag{4}$$

Από τις σχέσεις $(2)$ και $(4)$ και επειδή $(3, 5) = 1$ έπεται ότι

$$15 \mid B \implies 15 \mid 3n^5 + 5n^3 + 7n \implies A = \frac{3n^5 + 5n^3 + 7n}{15} \in \mathbb{N} \qquad \blacksquare$$

**Άσκηση 16.** **1.** *Δείξτε ότι:* $11 \mid 10! + 1$ *και* $13 \mid 12! + 1$

**2.** *Να βρεθούν τα υπόλοιπα των διαιρέσων:*

$$\frac{16!}{19} \quad \& \quad \frac{5!25!}{31} \quad \& \quad \frac{7 \cdot 8 \cdot 9 \cdot 15 \cdot 16 \cdot 17 \cdot 23 \cdot 24 \cdot 25 \cdot 43}{11} \quad \& \quad \frac{5^{100}}{7} \quad \& \quad \frac{6^{2000}}{11}$$

*Λύση.* **1.** Έχουμε[5]

$$\begin{aligned} 10! + 1 &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 + 1 \\ &= 1 \cdot (2 \cdot 6) \cdot (3 \cdot 4) \cdot (5 \cdot 9) \cdot (7 \cdot 8) \cdot 10 + 1 \\ &= 1 \cdot 12 \cdot 12 \cdot 45 \cdot 56 \cdot 10 + 1 \\ &\equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot (-1) + 1 \,(\mathsf{mod}\, 11) \\ &\equiv 0 \,(\mathsf{mod}\, 11) \\ &\implies 11 \mid 10! + 1 \end{aligned}$$

[5] Διαφορετικά μπορούμε να χρησιμοποιήσουμε το Θεώρημα του Wilson:

$$p: \text{ πρώτος} \qquad \implies \qquad (p-1)! \equiv -1 \,(\mathsf{mod}\, p)$$

- Επειδή ο αριθμός 11 είναι πρώτος, έπεται ότι $(11-1)! \equiv -1 \,(\mathsf{mod}\, 11)$, δηλαδή $10! + 1 \equiv 0 \,(\mathsf{mod}\, 11)$ και άρα $11 \mid 10! + 1$.
- Επειδή ο αριθμός 13 είναι πρώτος, έπεται ότι $(13-1)! \equiv -1 \,(\mathsf{mod}\, 13)$, δηλαδή $12! + 1 \equiv 0 \,(\mathsf{mod}\, 13)$ και άρα $13 \mid 12! + 1$.

Επίσης έχουμε

$$\begin{aligned} 12!+1 &= 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9\cdot 10\cdot 11\cdot 12+1 \\ &= 1\cdot (2\cdot 7)\cdot (3\cdot 9)\cdot (4\cdot 10)\cdot (5\cdot 8)\cdot (6\cdot 11)\cdot 12+1 \\ &= 1\cdot 14\cdot 27\cdot 40\cdot 40\cdot 66\cdot 12+1 \\ &\equiv 1\cdot 1\cdot 1\cdot 1\cdot 1\cdot 1\cdot (-1)+1 \pmod{13} \\ &\equiv 0 \pmod{13} \\ &\Longrightarrow 13 \mid 12!+1 \end{aligned}$$

**2.** Από το Θεώρημα του Wilson γνωρίζουμε ότι αν $p$ είναι ένας πρώτος αριθμός, τότε:

$$(p-1)!\equiv -1 \pmod{p}$$

- $\boxed{\dfrac{16!}{19}}$: Για $p=19$ έχουμε

$$\begin{aligned} 18!\equiv -1 \pmod{19} &\Longrightarrow 18!\equiv 18 \pmod{19} \\ &\Longrightarrow 18\equiv 18!\equiv 16!\cdot 17\cdot 18\equiv 16!\cdot (-2)\cdot (-1)\equiv 16!\cdot 2 \pmod{19} \\ &\Longrightarrow \begin{cases} 9\cdot 2\equiv 16!\cdot 2 \pmod{19} \\ (2,19)=1 \end{cases} \\ &\Longrightarrow 9\equiv 16! \pmod{19} \end{aligned}$$

Τότε $9-16!=19\cdot k$ και άρα $16!=(-k)\cdot 19+9$. Επομένως το υπόλοιπο της διαίρεσης $\frac{16!}{19}$ είναι 9.

- $\boxed{\dfrac{5!25!}{31}}$: Έχουμε

$$\begin{aligned} 5!\cdot 25! &= 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 25! \\ &\equiv (-30)\cdot (-29)\cdot (-28)\cdot (-27)\cdot (-26)\cdot 25! \pmod{31} \\ &\Longrightarrow 5!\cdot 25!\equiv (-1)^5\cdot 30! \pmod{31} \\ &\overset{\text{Wilson}}{\Longrightarrow} 5!\cdot 25!\equiv (-1)^5\cdot (-1) \pmod{31} \\ &\Longrightarrow 5!\cdot 25!\equiv 1 \pmod{31} \end{aligned}$$

Άρα το υπόλοιπο της διαίρεσης $\frac{5!25!}{31}$ είναι 1.

- $\boxed{\dfrac{7\cdot 8\cdot 9\cdot 15\cdot 16\cdot 17\cdot 23\cdot 24\cdot 25\cdot 43}{11}}$: Έχουμε

$$\begin{aligned} 7\cdot 8\cdot 9\cdot 15\cdot 16\cdot 17\cdot 23\cdot 24\cdot 25\cdot 43 &\equiv 7\cdot 8\cdot 9\cdot 4\cdot 5\cdot 6\cdot 1\cdot 2\cdot 3\cdot 10 \pmod{11} \\ &= 10! \pmod{11} \end{aligned}$$

Από το Θεώρημα Wilson έχουμε ότι $10!\equiv (-1) \pmod{11}\equiv 10 \pmod{11}$ και άρα

$$7\cdot 8\cdot 9\cdot 15\cdot 16\cdot 17\cdot 23\cdot 24\cdot 25\cdot 43\equiv 10 \pmod{11}$$

Συνεπώς το υπόλοιπο της διαίρεσης $\frac{7\cdot 8\cdot 9\cdot 15\cdot 16\cdot 17\cdot 23\cdot 24\cdot 25\cdot 43}{11}$ είναι 10.

- $\boxed{\frac{5^{100}}{7}}$: Από το Θεώρημα του Fermat έχουμε

  $$5^{100} = 5^{6\cdot 16+4} = (5^6)^{16}\cdot 5^4 \equiv 1^{16}\cdot 5^4 \equiv 5^4 \equiv 25^2 \equiv 4^2 \equiv 16 \equiv 2 \,(\mathsf{mod}\, 7)$$

  και άρα το υπόλοιπο της διαίρεσης $\frac{5^{100}}{7}$ είναι 2.

- $\boxed{\frac{6^{2000}}{11}}$: Από το Θεώρημα του Fermat έχουμε

  $$6^{10} \equiv 1(\mathsf{mod}\, 11) \implies (6^{10})^{200} \equiv 1(\mathsf{mod}\, 11) \implies 6^{2000} \equiv 1(\mathsf{mod}\, 11)$$

  Άρα το υπόλοιπο της διαίρεσης $\frac{6^{2000}}{11}$ είναι 1.

■

**Άσκηση 17.** *Δείξτε ότι:*

$$3^{999999999} \equiv -1 \,(\mathsf{mod}\, 7) \qquad \& \qquad 2^{1000000} \equiv 1 \,(\mathsf{mod}\, 17)$$

*Λύση.* Έχουμε

$$999999999 - 3 = 999999996 = 166666666 \cdot 6 \implies 999999999 \equiv 3 \,(\mathsf{mod}\, 6)$$

Άρα από το Θεώρημα του Fermat έχουμε

$$3^{999999999} = 3^{6\cdot 166666666+3} = \left(3^6\right)^{166666666}\cdot 3^3 \equiv 1^{166666666}\cdot 27 \,(\mathsf{mod}\, 7) \equiv (-1) \,(\mathsf{mod}\, 7)$$

και άρα $3^{999999999} \equiv -1 \,(\mathsf{mod}\, 7)$.

Για το δεύτερο ερώτημα παρατηρούμε ότι $1000000 = 16 \cdot 62500$. Τότε από το Θεώρημα του Fermat έχουμε

$$\begin{aligned} 2^{17-1} \equiv 1 \,(\mathsf{mod}\, 17) &\implies 2^{16} \equiv 1 \,(\mathsf{mod}\, 17) \\ &\implies \left(2^{16}\right)^{62500} \equiv 1^{62500} \,(\mathsf{mod}\, 17) \\ &\implies \left(2^{16}\right)^{62500} \equiv 1 \,(\mathsf{mod}\, 17) \\ &\implies 2^{1000000} \equiv 1 \,(\mathsf{mod}\, 17) \end{aligned}$$

και άρα έχουμε το ζητούμενο. ■

**Σχόλιο 2.** Το τελευταίο δεκαδικό ψηφίο ενός αριθμού $a > 1$ είναι προφανώς το μικρότερο δυνατό μη-αρνητικό υπόλοιπο $a_0$ της διαίρεσης του αριθμού $a$ με το 10, και τότε $[a]_{10} = [a_0]_{10}$. Πράγματι, έστω

$$a = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0, \qquad \text{όπου} \qquad a_m \neq 0 \quad \text{και} \quad 0 \leq a_i \leq 9, \;\; 0 \leq i \leq m$$

έστω η δεκαδική του παράσταση του $a$. Τότε προφανώς: $[a]_{10} = [a_0]_{10}$. Επομένως για να προσδιορίσουμε το τελευταίο δεκαδικό ψηφίο ενός αριθμού $a$ υπολογίζουμε την κλάση υπολοίπων του $a \,(\mathsf{mod}\, 10)$.

**Άσκηση 18.** *Να βρεθεί το τελευταίο δεκαδικό ψηφίο των αριθμών:*

$$3^{1000} \qquad \& \qquad 7^{999999} \qquad \& \qquad 9^{3333333}$$

*Λύση.* **1.** Επειδή $(3, 10) = 1$, από το Θεώρημα του Euler έπεται ότι: $3^{\phi(10)} \equiv 1 \,(\mathsf{mod}\, 10)$, και άρα, επειδή $\phi(10) = 4$, θα έχουμε: $3^4 \equiv 1 \,(\mathsf{mod}\, 10)$. Τότε:

$$3^{1000} = 3^{4\cdot 250} = (3^4)^{250} \equiv 1^{250} \equiv 1 \,(\mathsf{mod}\, 10) \qquad \implies \qquad [3^{1000}]_{10} = [1]_{10}$$

Άρα το τελευταίο δεκαδικό ψηφίο τιυ αριθμού $3^{1000}$ είναι 1.

**2.** Επειδή $(7,10)=1$, από το Θεώρημα του Euler έπεται ότι: $7^{\phi(10)} \equiv 1 \pmod{10}$, και άρα, επειδή $\phi(10)=4$, θα έχουμε: $7^4 \equiv 1 \pmod{10}$. Τότε, από την Ευκλείδεια Διαίρεση του $999999$ με τον αριθμό $4$ θα έχουμε $999999 = 4 \cdot 249999 + 3$, και επομένως:

$$7^{999999} = 7^{4\cdot 249999+3} = (7^4)^{249999} \cdot 7^3 \equiv 1^{249999} 49 \cdot 7 \equiv 63 \equiv 3 \pmod{10} \quad \Longrightarrow \quad [7^{999999}]_{10} = [3]_{10}$$

Άρα το τελευταίο δεκαδικό ψηφίο τιυ αριθμού $7^{999999}$ είναι $3$.

**3.** Επειδή $(9,10)=1$, από το Θεώρημα του Euler έπεται ότι: $9^{\phi(10)} \equiv 1 \pmod{10}$, και άρα, επειδή $\phi(10)=4$, θα έχουμε: $9^4 \equiv 1 \pmod{10}$. Τότε, από την Ευκλείδεια Διαίρεση του $3333333$ με τον αριθμό $4$ θα έχουμε $3333333 = 4 \cdot 833333 + 1$, και επομένως:

$$9^{3333333} = 9^{4\cdot 833333+1} = (9^4)^{833333} \cdot 9^1 \equiv 1^{833333} 9 \equiv 9 \pmod{10} \quad \Longrightarrow \quad [9^{3333333}]_{10} = [9]_{10}$$

Άρα το τελευταίο δεκαδικό ψηφίο του αριθμού $9^{3333333}$ είναι $9$. ■

**Άσκηση 19.** *Δείξτε ότι,* $\forall n \in \mathbb{N}$*:*

$$42 \mid n^7 - n \qquad \& \qquad 30 \mid n^9 - n$$

*Λύση.* **1.** Η πρωτογενής ανάλυση του $42$ είναι $42 = 2 \cdot 3 \cdot 7$. Έτσι αρκεί να δείξουμε ότι οι αριθμοί $2, 3, 7$ διαιρούν τον αριθμό $42$.

Έστω $n \in \mathbb{N}$. Αν ο $n$ είναι άρτιος τότε ο αριθμός $n^7$ είναι άρτιος και άρα ο $n^7 - n$ είναι επίσης άρτιος. Συνεπώς σε αυτή τη περίπτωση έχουμε $n^7 \equiv n \pmod{2}$. Αν τώρα ο $n$ είναι περιττός τότε ο αριθμός $n^7$ είναι περιττός και άρα ο $n^7 - n$ είναι άρτιος. Επομένως πάλι έχουμε $n^7 \equiv n \pmod{2}$. Άρα για κάθε $n \in \mathbb{N}$ ισχύει

$$n^7 \equiv n \pmod{2} \quad \Longrightarrow \quad 2 \mid n^7 - n \tag{1}$$

Επειδή ο αριθμός $3$ είναι πρώτος τότε

$$n^3 \equiv n \pmod{3}$$

και άρα

$$n^7 = (n^3)^2 \cdot n \equiv n^2 \cdot n \equiv n^3 \equiv n \pmod{3} \implies n^7 \equiv n \pmod{3} \quad \Longrightarrow \quad 3 \mid n^7 - n \tag{2}$$

Επίσης επειδή ο αριθμός $7$ είναι πρώτος τότε

$$n^7 \equiv n \pmod{7} \quad \Longrightarrow \quad 7 \mid n^7 - n \tag{3}$$

Επειδή οι αριθμοί $2, 3, 7$ είναι ανά δύο πρώτοι μεταξύ τους, από τις σχέσεις $(1)$, $(2)$ και $(3)$ έπεται ότι

$$2 \cdot 3 \cdot 7 = 42 \mid n^7 - n$$

**2.** Η πρωτογενής ανάλυση του $30$ είναι $30 = 2 \cdot 3 \cdot 5$. Έτσι αρκεί να δείξουμε ότι οι αριθμοί $2, 3, 5$ διαιρούν τον αριθμό $30$.

Επειδή $n^3 \equiv n \pmod{3}$ και $n^5 \equiv n \pmod{5}$ τότε έχουμε

$$n^9 - n \equiv (n^3)^3 - n \equiv n^3 - n \equiv 0 \pmod{3} \quad \Longrightarrow \quad 3 \mid n^9 - n \tag{1'}$$

και

$$n^9 - n \equiv n^5 \cdot n^4 - n \equiv n^5 - n \equiv 0 \pmod{5} \quad \Longrightarrow \quad 5 \mid n^9 - n \tag{2'}$$

Όπως παραπάνω έχουμε ότι ο αριθμός $n^9 - n$ είναι άρτιος για κάθε $n \in \mathbb{N}$. Άρα

$$n^9 - n \equiv 0 \pmod{2} \quad \Longrightarrow \quad 2 \mid n^9 - n \tag{3'}$$

Επειδή οι αριθμοί $2, 3, 5$ είναι ανά δύο πρώτοι μεταξύ τους, από τις σχέσεις $(1')$, $(2')$ και $(3')$ έπεται ότι

$$2 \cdot 3 \cdot 5 = 30 \mid n^9 - n$$

■

**Άσκηση 20.** **1.** *Να βρεθεί το υπόλοιπο της διαίρεσης*

$$\frac{987654321^{123456789}}{19}$$

**2.** *Να βρεθεί το τελευταίο ψηφίο του αριθμού*

$$2013^{2014^{2015}}$$

**3.** *Να βρεθεί το τελευταίο ψηφίο του αριθμού*

$$3^{1000} + 2 \cdot 7^{999999}$$

*Λύση.* **1.** Εκτελώντας την Ευκλείδεια Διαίρεση του $987654321$ με το $19$, θα έχουμε:

$$987654321 = 19 \cdot 51981806 + 7$$

Επομένως θα έχουμε:

$$987654321 \equiv 7 \pmod{19} \quad \Longrightarrow \quad 987654321^{123456789} \equiv 7^{123456789} \pmod{19}$$

Επειδή $(7, 19) = 1$, από το Θεώρημα του Euler, έπεται ότι $7^{\varphi(19)} \equiv 1 \pmod{19}$. Επειδή ο αριθμός $19$ είναι πρώτος, έπεται ότι $\varphi(19) = 18$, θα έχουμε:

$$7^{18} \equiv 1 \pmod{19}$$

Εκτελώντας την Ευκλείδεια Διαίρεση του $123456789$ με το $18$, θα έχουμε:

$$123456789 = 18 \cdot 6858710 + 9$$

Επομένως θα έχουμε

$$7^{123456789} = 7^{18 \cdot 6858710 + 9} = (7^{18})^{6858710} \cdot 7^9 \pmod{19} \equiv 1^{6858710} \cdot 7^9 \pmod{19} \equiv 7^9 \pmod{19} \equiv$$
$$\equiv (7 \cdot 7) \cdot (7 \cdot 7) \cdot (7 \cdot 7) \cdot (7 \cdot 7) \cdot 7 \equiv 49 \cdot 49 \cdot 49 \cdot 49 \cdot 7 \equiv 11 \cdot 11 \cdot 11 \cdot 11 \cdot 7 \equiv 121 \cdot 121 \cdot 7 \equiv$$
$$\equiv 7 \cdot 7 \cdot 7 \equiv 49 \cdot 7 \equiv 11 \cdot 7 \equiv 77 \equiv 1 \pmod{19}$$

Άρα:

$$987654321^{123456789} \equiv 1 \pmod{19}$$

και επομένως:

$$\textit{Το Υπόλοιπο της Διαίρεσης} \quad \frac{987654321^{123456789}}{19} \quad \textit{είναι ίσο με } 1$$

**2.** Το τελευταίο ψηφίο του αριθμού $2013^{2014^{2015}}$ είναι το υπόλοιπο της διαίρεσης του αριθμού αυτού με το $10$.

Προφανώς $2013 \equiv 3 \pmod{10}$, και τότε $2013^{2014^{2015}} \equiv 3^{2014^{2015}} \pmod{10}$. Άρα, ισοδύναμα, ζητάμε το υπόλοιπο της διαίρεσης

$$\frac{3^{2014^{2015}}}{10}$$

Επειδή $(3, 10) = 1$, από το Θεώρημα του Euler, έπεται ότι $3^{\varphi(10)} \equiv 1 \pmod{10}$. Επειδή $\varphi(10) = 4$, θα έχουμε:

$$3^4 \equiv 1 \pmod{10}$$

Έτσι για τις δυνάμεις του $3$, θα έχουμε:

$$3^1 \equiv 3 \pmod{10}, \quad 3^2 \equiv 9 \pmod{10}, \quad 3^3 \equiv 27 \equiv 7 \pmod{10}, \quad 3^4 \equiv 1 \pmod{10}$$

Με τι είναι ίση η $n$-οστή δύναμη του $3 \pmod{10}$ $(\forall n \geq 1)$ ;

Για να απαντήσουμε σ' αυτό το ερώτημα (και μετά να θέσουμε $n = 2014^{2015}$), εξετάζουμε τα πιθανά υπόλοιπα της διαίρεσης του θετικού ακέραιου $n$ με το $4$, τα οποία γνωρίζουμε ότι είναι $0, 1, 2, 3$. Έτσι θα έχουμε:

(α') Αν $n = 4k$, τότε:

$$3^n = 3^{4k} = (3^4)^k \equiv 1^k \equiv 1 \pmod{10}$$

(β') Αν $n = 4k+1$, τότε:

$$3^n = 3^{4k+1} = (3^4)^k \cdot 3^1 \equiv 1^k \cdot 3 \equiv 3 \pmod{10}$$

(γ') Αν $n = 4k+2$, τότε:

$$3^n = 3^{4k+2} = (3^4)^k \cdot 3^2 \equiv 1^k \cdot 9 \equiv 9 \pmod{10}$$

(δ') Αν $n = 4k+3$, τότε:

$$3^n = 3^{4k+3} = (3^4)^k \cdot 3^3 \equiv 1^k \cdot 27 \equiv 7 \pmod{10}$$

Επειδή προφανώς $2014 = 4 \cdot 503 + 2$, έπεται ότι ο αριθμός και $2014$ είναι της μορφής $4k+2$. Επειδή τότε προφανώς ο αριθμός $2014^2$ θα είναι της μορφής $4k$, έπεται ότι και ο αριθμός $2014^r$, $\forall r \geq 2$, άρα και ιδιαίτερα ο αριθμός $2014^{2015}$, θα είναι της μορφής $4k$. Σύμφωνα με τα παραπάνω, έπεται ότι

$$3^{2014^{2015}} \equiv 1 \pmod{10} \quad \Longrightarrow \quad 2013^{2014^{2015}} \equiv 1 \pmod{10}$$

Άρα

*Το τελευταίο ψηφίο του αριθμού* $2013^{2014^{2015}}$ *είναι* $1$

**3.** (*Βλέπε και την Άσκηση* 18) Το τελευταίο ψηφίο του αριθμού $3^{1000} + 2 \cdot 7^{999999}$ είναι το υπόλοιπο της διαίρεσης του αριθμού αυτού με το 10.

(α') Υπολογίζουμε τον αριθμό $3^{1000} \pmod{10}$. Επειδή $(3, 10) = 1$, από το Θεώρημα του Euler, έπεται ότι $3^{\varphi(10)} \equiv 1 \pmod{10}$. Επειδή $\varphi(10) = 4$, θα έχουμε:

$$3^4 \equiv 1 \pmod{10}$$

Επομένως:

$$3^{1000} = 3^{4 \cdot 250} = (3^4)^{250} \equiv 1^{250} \equiv 1 \pmod{10}$$

(β') Υπολογίζουμε τον αριθμό $2 \cdot 7^{999999} \pmod{10}$. Επειδή $(7, 10) = 1$, από το Θεώρημα του Euler, έπεται ότι $7^{\varphi(10)} \equiv 1 \pmod{10}$. Επειδή $\varphi(10) = 4$, θα έχουμε:

$$7^4 \equiv 1 \pmod{10}$$

Εκτελώντας την Ευκλείδεια Διαίρεση $\frac{999999}{4}$ θα έχουμε: $999999 = 4 \cdot 249999 + 3$, και τότε:

$$7^{999999} = 7^{4 \cdot 249999 + 3} = (7^4)^{249999} \cdot 7^3 \equiv 1^{249999} \cdot 7^2 \cdot 7 \equiv 49 \cdot 7 \equiv 9 \cdot 7 \equiv 63 \equiv 3 \pmod{10}$$

Επομένως:

$$2 \cdot 7^{999999} \equiv 2 \cdot 3 \equiv 6 \pmod{10}$$

Συνδυάζοντας τα παραπάνω μέρη (α') και (β'), θα έχουμε τελικά:

$$3^{1000} + 2 \cdot 7^{999999} \equiv 1 + 6 \equiv 7 \pmod{10}$$

Άρα

*Το τελευταίο ψηφίο του αριθμού* $3^{1000} + 2 \cdot 7^{999999}$ *είναι* $7$ ■

**Άσκηση 21.** *Έστω $p$ ένας πρώτος αριθμός.*

**1.** *Για κάθε ακέραιο $a$ να δειχθεί ότι*

$$p \mid a^p + a(p-1)!$$

**2.** *Αν ο $p$ είναι περιττός, για κάθε $k$, όπου $0 < k < p$, να δειχθεί ότι:*

$$(p-k)!(k-1)! \equiv (-1)^k \bmod p$$

*Λύση.* **1.** Από το μικρό Θεώρημα του Fermat έπεται ότι

$$a^p \equiv a \,(\mathsf{mod}\, p)$$

Από το Θεώρημα του Wilson έπεται ότι:

$$(p-1)! \equiv -1 \,(\mathsf{mod}\, p) \quad \Longrightarrow \quad a(p-1)! \equiv -a \,(\mathsf{mod}\, p)$$

Προσθέτοντας τις παραπάνω ισοτιμίες, έχουμε:

$$a^p + a(p-1)! = 0 \,(\mathsf{mod}\, p)$$

και επομένως $p \mid a^p + a(p-1)!$.

**2.** Επειδή

$$p-k \equiv -k \,(\mathsf{mod}\, p), \quad p-k+1 \equiv k-1 \,(\mathsf{mod}\, p), \quad \cdots, \quad 1 \equiv -(p-1) \,(\mathsf{mod}\, p)$$

θα έχουμε:

$$(p-k)!(k-1)! \equiv 1 \cdot 2 \cdots (p-k) \cdot (k-1)! \equiv (-k) \cdot (-(k+1)) \cdots (-(p-1)) \cdot (k-1)! \equiv$$

$$\equiv (-1)^{p-k} \cdot k \cdot (k+1) \cdots (p-1)(k-1)! \equiv (-1)^{p-k}(p-1)! \overset{(*)}{\equiv} (-1)^{p-k} \cdot (-1) \equiv (-1)^{p-k+1} =$$

$$= (-1)^{p-1} \cdot (-1)^k \overset{(\dagger)}{\equiv} (-1)^k \,(\mathsf{mod}\, p)$$

όπου στην ισοτιμία $(*)$ χρησιμοποιήσαμε το Θεώρημα του Wilson: $(p-1)! \equiv -1 \,(\mathsf{mod}\, p)$, και στην ισοτιμία $(\dagger)$ χρησιμοποιήσαμε ότι ο αριθμός $p-1$ είναι άρτιος διότι ο πρώτος $p$ είναι περιττός. ■

**Άσκηση 22.** *Να δειχθεί ότι,* $\forall n \geq 2$*:*

$$2^n \not\equiv 1 \,\mathsf{mod}\, n$$

*Λύση.* Θα δείξουμε ισοδύναμα ότι: $n \nmid 2^n - 1$.

– Έστω ότι ο $n$ είναι άρτιος: $2 \mid n$. Τότε ο αριθμός $2^n - 1$ είναι περιττός και επομένως δεν μπορεί αν διαιρείται από τον $n$ (αν $n \mid 2^n - 1$, τότε επειδή $2 \mid n$, καταλήγουμε στο άτοπο $2 \mid 2^n - 1$).

– Έστω ότι ο $n$ είναι περιττός και έστω $n \mid 2^n - 1$. Έστω $p$ ο μικρότερος πρώτος ο οποίος διαιρεί τον $n$. Τότε $p \mid 2^n - 1$ και προφανώς ο $p$ είναι περιττός $\geq 3$ διότι ο $n$ είναι περιττός. Τότε ο $p-1$ είναι άρτιος και άρα $(n, p-1) = 1$. Επομένως υπάρχουν ακέραιοι $a, b$ έτσι ώστε $an + b(p-1) = 1$. Τότε

$$2^{an} - 1 = (2^n)^a - 1 = (2^n - 1) \cdot (2^{n(a-1)} + 2^{n(a-2)} + \cdots + 2^n + 1) \quad \Longrightarrow \quad 2^n - 1 \mid 2^{an} - 1$$

Επειδή $p \mid 2^n - 1$ και $2^n - 1 \mid 2^{an} - 1$, έπεται ότι $p \mid 2^{an} - 1$, δηλαδή:

$$2^{an} \equiv 1 \,(\mathsf{mod}\, p) \tag{$*$}$$

Από το μικρό Θεώρημα του Fermat, επειδή $(2, p) = 1$, έπεται ότι

$$2^{p-1} \equiv 1 \,(\mathsf{mod}\, p) \quad \Longrightarrow \quad (2^{p-1})^b \equiv 1^b \equiv 1 \,(\mathsf{mod}\, p) \quad \Longrightarrow \quad 2^{b(p-1)} \equiv 1 \,(\mathsf{mod}\, p) \tag{$**$}$$

Πολλαπλασιάζοντας τις ισοτιμίες $(*)$ και $(**)$ και χρησιμοποιώντας ότι $an + b(p-1) = 1$, θα έχουμε:

$$2 = 2^1 = 2^{an + b(p-1)} = 2^{an} \cdot 2^{b(p-1)} \equiv 1 \cdot 1 = 1 \,(\mathsf{mod}\, p)$$

δηλαδή $p \mid 2 - 1 = 1$ το οποίο είναι άτοπο. Άρα $n \nmid 2^n - 1$, δηλαδή ισοδύναμα: $n \nmid 2^n - 1$. ■

**Άσκηση 23.** *Να δειχθεί για κάθε θετικό ακέραιο* $n > 2$ *και για κάθε ακέραιο* $x$*, ισχύει ότι:*

$$x^n \equiv x^{n - \phi(n)} \,(\mathsf{mod}\, n)$$

*Λύση.* Έστω $n = p^{a_1}p_2^{a_2}\cdots p_r^{a_r}$ η πρωτογενής ανάλυση του αριθμού $n$. Θα δείξουμε ότι

$$\forall i = 1, 2, \cdots, r: \qquad p_i^{a_i} \mid x^{n-\phi(n)}(x^{\phi(n)} - 1)$$

– Αν για κάποιο $i = 1, 2, \cdots, r$, έχουμε $(p_i, x) = 1$, τότε $(x, p_i^{a_i}) = 1$, και από το Θεώρημα του Euler θα έχουμε $x^{\phi(p_i^{a_i})} \equiv 1 \,(\mathsf{mod}\, p_i^{a_i})$, δηλαδή

$$p_i^{a_i} \mid x^{\phi(p_i^{a_i})} - 1 \qquad (*)$$

Επειδή $\phi(n) = \phi(p_i^{a_i}) \cdot k$, όπου $k = \phi(p_1^{a_1}) \cdots \phi(p_{i-1}^{a_{i-1}}) \cdot \phi(p_{i+1}^{a_{i+1}}) \cdots \phi(p_r^{a_r})$, θα έχουμε:

$$x^{\phi(n)} - 1 = x^{\phi(p_i^{a_i})\cdot k} - 1 = (x^{\phi(p_i^{a_i})})^k - 1 = (x^{\phi(p_i^{a_i})} - 1) \cdot \big((x^{\phi(p_i^{a_i})})^{k-1} + (x^{\phi(p_i^{a_i})})^{k-2} + \cdots + x^{\phi(p_i^{a_i})} + 1\big)$$

Επομένως

$$x^{\phi(p_i^{a_i})} - 1 \mid x^{\phi(n)} - 1 \qquad (**)$$

Από τις $(*)$ και $(**)$ έπεται ότι:

$$(p_i, x) = 1 \quad \Longrightarrow \quad p_i^{a_i} \mid x^{\phi(n)} - 1 \quad \Longrightarrow \quad p_i^{a_i} \mid x^{n-\phi(n)} \cdot (x^{\phi(n)} - 1) \qquad (\dagger)$$

– Επειδή, $\forall i = 1, 2, \cdots, r$: $p_i^{a_i - 1} \mid n$, και επειδή

$$\phi(n) = p_1^{a_1-1}p_2^{a_2-1}\cdots p_r^{a_r-1}(p_1 - 1)(p_2 - 1)\cdots(p_r - 1) \quad \Longrightarrow \quad p_i^{a_i-1} \mid \phi(n), \quad 1 \le i \le r$$

έπεται ότι:

$$\forall i = 1, 2, \cdots, r: \qquad p_i^{a_i - 1} \le n - \phi(n)$$

Επειδή $p_i \ge 2$, έπεται ότι[6]: $p_i^{a_i-1} \ge a_i$. Επομένως

$$a_i \;\le\; p_i^{a_i-1} \;\le\; n - \phi(n) \qquad (***)$$

Επομένως αν $(x, p_i) > 1$, τότε $p_i \mid x$ και άρα χρησιμοποιώντας την $(***)$, θα έχουμε

$$p_i^{a_i} \mid p_i^{n-\phi(n)} \quad \Longrightarrow \quad p_i^{a_i} \mid x^{n-\phi(n)} \quad \Longrightarrow \quad p_i^{a_i} \mid x^{n-\phi(n)} \cdot (x^{\phi(n)} - 1) \qquad (\dagger\dagger)$$

Από τις σχέσεις $(\dagger)$ και $(\dagger)$, έπεται ότι

$$\forall i = 1, 2, \cdots, r: \quad p_i^{a_i} \mid x^{n-\phi(n)} \cdot (x^{\phi(n)} - 1) \quad \Longrightarrow \quad n = p^{a_1}p_2^{a_2}\cdots p_r^{a_r} \mid x^{n-\phi(n)} \cdot (x^{\phi(n)} - 1)$$

Επομένως

$$x^{n-\phi(n)} \cdot (x^{\phi(n)} - 1) \equiv 0 \,(\mathsf{mod}\, n) \quad \Longrightarrow \quad x^n = x^{n-\phi(n)} \,(\mathsf{mod}\, n) \qquad \blacksquare$$

**Σχόλιο 3.** Η ισοτιμία $x^n \equiv x^{n-\phi(n)} \,(\mathsf{mod}\, n)$ της Άσκησης 23 είναι αληθής και στην περίπτωση $n = 1$ ή 2.

Πράγματι, για $n = 1$, θα έχουμε $x^n = x$ και $x^{n-\phi(n)} = x^{1-1} = x^0 = 1$. Επειδή $1 \mid x - 1$, έπεται ότι η ισοτιμία $x^n \equiv x^{n-\phi(n)} \,(\mathsf{mod}\, n)$ είναι αληθής, όταν $n = 1$.

Αν $n = 2$, θα έχουμε $x^n = x^2$ και $x^{n-\phi(n)} = x^{2-\phi(2)} = x^{2-1} = x^1 = x$, και $x^2 \equiv x \,(\mathsf{mod}\, 2)$ διότι $2 \mid x^2 - x$, $\forall x \in \mathbb{Z}$. Πράγματι αν ο αριθμός $x$ είναι άρτιος, τότε και ο αριθμός $x^2$ είναι άρτιος και τότε και η διαφορά $x^2 - x$ είναι άρτιος αριθμός, δηλαδή $2 \mid x^2 - x$. Αν ο αριθμός $x$ είναι περιττός, τότε και ο αριθμός $x^2$ είναι περιττός και τότε η διαφορά $x^2 - x$ είναι άρτιος αριθμός, δηλαδή $2 \mid x^2 - x$. Έτσι σε κάθε περίπτωση $2 \mid x^2 - x$ και επομένως $x^2 \equiv x \,(\mathsf{mod}\, 2)$, δηλαδή η ισοτιμία $x^n \equiv x^{n-\phi(n)} \,(\mathsf{mod}\, n)$ είναι αληθής, όταν $n = 2$. $\quad \surd$

[6] Δείχνουμε με επαγωγή ότι για κάθε $m \ge 2$ και για κάθε $k \ge 1$, ισχύει ότι: $m^{k-1} \ge k$.
– Αν $k = 1$, τότε $m^{k-1} = m^{1-1} = m^0 = 1$ και ο ισχυρισμός είναι αληθής.
– Υποθέτουμε ότι $m^{k-1} \ge k$.
– θα έχουμε: $m^{k-1} \ge k \implies m^k \ge m \cdot k \ge k + 1$, και η τελευταία ανισότητα ισχύει διότι αν $m \cdot k < k + 1$, τότε θα είχαμε $k(m - 1) < 1$ το οποίο είναι άτοπο διότι $m \ge 2$ και $m, k \in \mathbb{N}$. Άρα $m^k \ge k + 1$, και επομένως $m^{k-1} \ge k$, $\forall m \ge 2$, $\forall k \ge 1$.

**Άσκηση 24.** *Έστω $p$ και $q$ δύο περιττοί πρώτοι, όπου $p \neq q$. Αν $a$ είναι ένας θετικός ακέραιος έτσι ώστε $(a, pq) = 1$, τότε να δειχθεί ότι:*

$$a^{\frac{\phi(pq)}{2}} \equiv 1 \,(\mathsf{mod}\, pq)$$

*Λύση.* Επειδή $p \neq q$, έπεται ότι $(p, q) = 1$, και επομένως: $\phi(pq) = \phi(p)\phi(q) = (p-1) \cdot (q-1)$.

Επειδή οι πρώτοι $p$ και $q$ είναι περιττοί, θα έχουμε ότι οι αριθμοί $p-1$ και $q-1$ είναι άρτιοι και επομένως μπορούμε να γράψουμε: $p-1 = 2n$ και $q-1 = 2m$, για κάποιους θετικούς ακεραίους $n$ και $m$. Τότε:

$$m = \frac{q-1}{2} \qquad \& \qquad n = \frac{p-1}{2} \tag{$*$}$$

Επειδή $(a, pq) = 1$, και $(p, q) = 1$, θα έχουμε:

$$1 = (a, pq) = (a, p)(a, q) \quad \Longrightarrow \quad (a, p) = 1 = (a, q)$$

Από το μικρό Θεώρημα του Fermat, τότε θα έχουμε:

$$a^{\phi(p)} \equiv 1 \,(\mathsf{mod}\, p) \quad \Longrightarrow \quad a^{p-1} \equiv 1 \,(\mathsf{mod}\, p) \quad \Longrightarrow \quad a^{(p-1)m} \equiv 1^m \,(\mathsf{mod}\, p) \quad \overset{(*)}{\Longrightarrow} \quad a^{\frac{(p-1)(q-1)}{2}} \equiv 1 \,(\mathsf{mod}\, p)$$

Παρόμοια

$$a^{\phi(q)} \equiv 1 \,(\mathsf{mod}\, q) \quad \Longrightarrow \quad a^{q-1} \equiv 1 \,(\mathsf{mod}\, q) \quad \Longrightarrow \quad a^{(q-1)n} \equiv 1^n \,(\mathsf{mod}\, q) \quad \overset{(*)}{\Longrightarrow} \quad a^{\frac{(p-1)(q-1)}{2}} \equiv 1 \,(\mathsf{mod}\, q)$$

Οι δύο τελευταίες σχέσεις δίνουν:

$$p \mid a^{\frac{(p-1)(q-1)}{2}} - 1 \qquad \& \qquad q \mid a^{\frac{(p-1)(q-1)}{2}} - 1$$

Επειδή $(p, q) = 1$, έπεται ότι θα έχουμε:

$$pq \mid a^{\frac{(p-1)(q-1)}{2}} - 1 \qquad \Longrightarrow \qquad a^{\frac{\phi(pq)}{2}} = a^{\frac{(p-1)(q-1)}{2}} \equiv 1 \,(\mathsf{mod}\, pq)$$

■