# ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

## ΤΜΗΜΑ **Β΄**

## ΛΥΣΕΙΣ ΑΣΚΗΣΕΩΝ ΕΠΑΝΑΛΗΨΗΣ

ΔΙΔΑΣΚΩΝ: Α. Μπεληγιάννης

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

**Πέμπτη 19 Ιανουαρίου 2017**

**Άσκηση 1.** (1) *Να λυθεί η γραμμική Διοφαντική εξίσωση:*

$$13521x + 732y = 11225 \tag{1}$$

(2) *Να βρεθούν:* $(\alpha)$ *όλες οι λύσεις, και* $(\beta)$ *όλες οι θετικές λύσεις, της γραμμικής Διοφαντικής εξίσωσης*

$$17x + 19y = 23 \tag{2}$$

*Λύση.* (1) Από την Θεωρία γνωρίζουμε ότι η διοφαντική εξίσωση $(1)$ έχει λύση αν και μόνον αν $d \mid 11225$, όπου $d = (13521, 732)$.

Με χρήση του αλγόριθμου του Ευκλείδη, υπολογίζουμε:

$$\begin{aligned} 13521 &= 18 \cdot 732 + 345 \\ 732 &= 2 \cdot 345 + 42 \\ 345 &= 8 \cdot 42 + 9 \\ 42 &= 4 \cdot 9 + 6 \\ 9 &= 1 \cdot 6 + 3 \\ 6 &= 1 \cdot 3 + 0 \end{aligned}$$

και επομένως $d = (13521, 732) = 3$.

Επειδή προφανώς $3 \nmid 11225$, έπεται ότι η Διοφαντική εξίσωση $(1)$ δεν έχει ακέραιες λύσεις.

(2) Από την Θεωρία γνωρίζουμε ότι η διοφαντική εξίσωση $(2)$ έχει λύση αν και μόνον αν $d \mid 23$, όπου $d = (19, 17)$. Επειδή προφανώς $d = (19, 17) = 1$ και $1 \mid 23$, έπεται ότι η Διοφαντική εξίσωση $(2)$ έχει ακέραιες λύσεις.

Γνωρίζουμε ότι αν $(x_0, y_0)$ είναι μια ακέραια λύση μιας Διοφαντικής εξίσωσης $ax + by = c$, όπου $d \mid (a, b)$, τότε όλες οι λύσεις της $(2)$ δίνονται από τους τύπους:

$$x = x_0 + \frac{b}{d}t \quad \& \quad y = y_0 - \frac{a}{d}t, \qquad t \in \mathbb{Z}$$

Για την εύρεση μιας λύσης $(x_0, y_0)$ της $(2)$, εργαζόμαστε ως εξής.

Με χρήση του αλγόριθμου του Ευκλείδη, υπολογίζουμε:

$$\begin{aligned} 19 &= 1 \cdot 17 + 2 \\ 17 &= 2 \cdot 8 + 1 \\ 8 &= 1 \cdot 8 + 0 \end{aligned}$$

Από τις παραπάνω σχέσεις, θα έχουμε:

$$1 = 17 - 2 \cdot 8 = 17 - 8 \cdot (19 - 17) = 17 \cdot 9 + 19 \cdot (-8)$$

και τότε

$$23 = 23 \cdot 1 = 23 \cdot (17 \cdot 9 + 19 \cdot (-8)) = 17 \cdot (23 \cdot 9) + 19 \cdot (-8 \cdot 23) = 17 \cdot 207 + 19 \cdot (-184)$$

Επομένως, θέτοντας

$$x_0 = 207 \quad \& \quad y_0 = -184$$

αποκτούμε μια λύση της $(2)$.

Από την παραπάνω ανάλυση, έπεται ότι όλες οι ακέραιες λύσεις της $(2)$ είναι οι εξής:

$$x = 207 + 19t \quad \& \quad y = -184 - 17t, \quad t \in \mathbb{Z}$$

Για την εύρεση όλων των θετικών λύσεων της $(2)$, εργαζόμαστε ως εξής. Η λύση $(x, y)$ είναι θετική αν και μόνον αν, εξ' ορισμού, ισχύει $x > 0$ και $y > 0$. Επομένως

$$207 + 19t > 0 \quad \& \quad -184 - 17t > 0 \quad \Longrightarrow \quad -\frac{207}{19} < t < -\frac{184}{17}$$

Επειδή $\frac{207}{19} = 10.82...$ και $\frac{184}{17} = 10.89...$, θα έχουμε

$$-10.82... < t < -10.89...$$

Επειδή οι θετικές ακέραιες λύσεις της $(2)$ δίνονται από το σύνολο

$$\{(207 + 19t, -184 - 17t) \mid -10.82... < t < -10.89...\} \cap \mathbb{Z}$$

το οποίο είναι προφανώς κενό, έπεται ότι η $(2)$ δεν έχει θετικές ακέραιες λύσεις (κάτι το οποίο μπορούσε να διαπιστωθεί εύκολα από την αρχή λόγω της μορφής της Διοφαντικής εξίσωσης). ■

**Άσκηση 2.** *Να βρεθούν τα υπόλοιπα των διαιρέσεων:*

$$\frac{17^{2241}}{8700} \qquad \& \qquad \frac{n^{257} - n}{255}, \quad n \in \mathbb{Z}$$

*Λύση.* (1) Εύκολα βλέπουμε ότι η πρωτογενής ανάλυση του αριθμού $8700$ είναι:

$$8700 = 2^2 \cdot 3 \cdot 5^2 \cdot 29$$

απ' όπου βλέπουμε άμεσα ότι:

(α') $(8700, 17) = 1$.

(β') $\phi(8700) = \phi(2^2 \cdot 3 \cdot 5^2 \cdot 29) = \phi(2^2) \cdot \phi(3) \cdot \ \phi(5^2)\phi(\cdot 29) = 2240$.

Επειδή $(8700, 17) = 1$, από το Θεώρημα του Euler, τότε θα έχουμε:

$$17^{\phi(8700)} \equiv 1 \,(\mathsf{mod}\, 8700) \quad \Longrightarrow \quad 17^{2240} \equiv 1 \,(\mathsf{mod}\, 8700)$$

Πολλαπλασιάζοντας την τελευταία ισοτιμία με 17, θα έχουμε

$$17^{2241} \equiv 17 \,(\mathsf{mod}\, 8700)$$

και επομένως το υπόλοιπο της διαίρεσης του αριθμού $17^{2241}$ με τον αριθμό $8700$ είναι $17$.

(2) Θα δείξουμε ότι το υπόλοιπο της διαίρεσης του αριθμού $n^{257} - n$ με τον αριθμό $255$ είναι $0$ ή ισοδύναμα θα δείξουμε ότι:

$$n^{257} \equiv n \,(\mathsf{mod}\, 255) \qquad (*)$$

Εύκολα υπολογίζουμε ότι η πρωτογενής ανάλυση του αριθμού $255$ είναι:

$$255 = 3 \cdot 5 \cdot 17$$

Επειδή οι αριθμοί $2, 5, 17$ είναι ανα δύο πρώτοι μεταξύ τους,για να δείξουμε την σχέση $(*)$, αρκεί να δείξουμε ότι:

$$3 \mid n^{257} - n \quad \& \quad 5 \mid n^{257} - n \quad \& \quad 17 \mid n^{257} - n \qquad (**)$$

Η απόδειξη των σχέσεων διαιρετότητας $(**)$ είναι παρόμοια:

- Διακρίνουμε περιπτώσεις:

(α΄) Αν $3 \mid n$, τότε $n \equiv 0 \pmod 3$ και άρα $n^{257} \equiv 0 \pmod 3 \equiv n \pmod 3$. Επομένως $3 \mid n^{257} - n$.

(β΄) Αν $3 \nmid n$, τότε μπορούμε να εφαρμόσουμε το μικρό Θεώρημα του Fermat και να έχουμε:

$$n^{\phi(3)} \equiv 1 \pmod 3 \quad \Longrightarrow \quad n^2 \equiv 1 \pmod 3$$

και τότε

$$(n^2)^{128} \equiv n^{256} \equiv 1 \pmod 3 \quad \Longrightarrow \quad n^{257} \equiv n \pmod 3$$

Άρα αν $3 \nmid n$, πάλι θα έχουμε ότι $3 \mid n^{257} - n$.

Συνοψίζοντας δείξαμε ότι σε κάθε περίπτωση ισχύει ότι:

$$3 \mid n^{257} - n \tag{a}$$

- Διακρίνουμε περιπτώσεις:

(α΄) Αν $5 \mid n$, τότε $n \equiv 0 \pmod 5$ και άρα $n^{257} \equiv 0 \pmod 5 \equiv n \pmod 5$. Επομένως $5 \mid n^{257} - n$.

(β΄) Αν $5 \nmid n$, τότε μπορούμε να εφαρμόσουμε το μικρό Θεώρημα του Fermat και να έχουμε:

$$n^{\phi(5)} \equiv 1 \pmod 5 \quad \Longrightarrow \quad n^4 \equiv 1 \pmod 5$$

και τότε

$$(n^4)^{64} \equiv n^{256} \equiv 1 \pmod 5 \quad \Longrightarrow \quad n^{257} \equiv n \pmod 5$$

Άρα αν $5 \nmid n$, πάλι θα έχουμε ότι $5 \mid n^{257} - n$.

Συνοψίζοντας δείξαμε ότι σε κάθε περίπτωση ισχύει ότι:

$$5 \mid n^{257} - n \tag{b}$$

- Διακρίνουμε περιπτώσεις:

(α΄) Αν $17 \mid n$, τότε $n \equiv 0 \pmod{17}$ και άρα $n^{257} \equiv 0 \pmod{17} \equiv n \pmod{17}$. Επομένως $17 \mid n^{257} - n$.

(β΄) Αν $17 \nmid n$, τότε μπορούμε να εφαρμόσουμε το μικρό Θεώρημα του Fermat και να έχουμε:

$$n^{\phi(17)} \equiv 1 \pmod{17} \quad \Longrightarrow \quad n^{16} \equiv 1 \pmod{17}$$

και τότε

$$(n^{16})^{16} \equiv n^{256} \equiv 1 \pmod{17} \quad \Longrightarrow \quad n^{257} \equiv n \pmod{17}$$

Άρα αν $17 \nmid n$, πάλι θα έχουμε ότι $17 \mid n^{257} - n$.

Συνοψίζοντας δείξαμε ότι σε κάθε περίπτωση ισχύει ότι:

$$17 \mid n^{257} - n \tag{c}$$

Από τις σχέσεις $(a), (b)$ και $(c)$, έπεται ότι

$$3 \cdot 5 \cdot 17 = 255 \mid n^{257} - n$$

Επομένως το υπόλοιπο της διαίρεσης του αριθμού $n^{257} - n$ με τον αριθμό $255$ είναι $0$. ■

**Άσκηση 3.** *Αν $n > 1$ είναι ένας θετικός ακέραιος με πρωτογενή ανάλυση $n = p_1^{a_1} \cdots p_r^{a_r}$, δείξτε ότι:*

$$\sum_{d \mid n} \frac{\mu^2(d)}{\tau(d)} = \frac{3^r}{2^r}$$

*Λύση.* Γνωρίζουμε ότι οι αριθμητικές συναρτήσεις $\mu, \tau : \mathbb{N} \longrightarrow \mathbb{C}$ είναι πολλαπλασιαστικές. Επειδή $\tau(n) \neq 0$, $\forall n \in \mathbb{N}$, ορίζεται η αριθμητική συνάρτηση

$$f := \frac{\mu}{\tau} : \mathbb{N} \longrightarrow \mathbb{C}, \qquad f(n) = \frac{\mu}{\tau}(n) = \frac{\mu(n)}{\tau(n)}$$

η οποία εύκολα βλέπουμε ότι είναι πολλαπλασιαστική. Τότε θα έχουμε:

$$\sum_{d|n} \frac{\mu^2(d)}{\tau(d)} = \sum_{d|n} \mu(d) \frac{\mu(d)}{\tau(d)} = \sum_{d|n} \mu(d) f(d)$$

Από τη Θεωρία γνωρίζουμε ότι αν $h : \mathbb{N} \longrightarrow \mathbb{C}$ είναι μια πολλαπλασιαστική συνάρτηση και $n = p_1^{a_1} \cdots p_r^{a_r}$ είναι η πρωτογενής ανάλυση του φυσικού αριθμού $n > 1$, τότε ισχύει ότι:

$$\sum_{d|n} \mu(d) h(d) = \prod_{i=1}^{r} (1 - h(p_i)) = (1 - h(p_1)) \cdot (1 - h(p_2)) \cdot \cdots \cdot (1 - h(p_r))$$

Επομένως θα έχουμε:

$$\sum_{d|n} \mu(d) f(d) = (1 - f(p_1)) \cdot (1 - f(p_2)) \cdot \cdots \cdot (1 - f(p_r))$$

Όπως, για κάθε $i = 1, 2, \cdots, r$:

$$1 - f(p_r) = 1 - \frac{\mu(p_i)}{\tau(p_i)} = 1 - \frac{-1}{2} = 1 + \frac{1}{2} = \frac{3}{2}$$

Επομένως

$$\sum_{d|n} \frac{\mu^2(d)}{\tau(d)} = \sum_{d|n} \mu(d) f(d) = (1 - f(p_1)) \cdot (1 - f(p_2)) \cdot \cdots \cdot (1 - f(p_r)) = \overbrace{\frac{3}{2} \cdot \frac{3}{2} \cdot \cdots \cdot \frac{3}{2}}^{r \text{ φορές}} = \frac{3^r}{2^r} \qquad \blacksquare$$

**Άσκηση 4.** *Έστω $m, n$ φυσικοί αριθμοί, όπου $m > 2$. Αν*

$$(m - 1) \cdot \sigma(n) = n \cdot m$$

*να δείξετε ότι ο $n$ είναι πρώτος και $n = m - 1$.*

*Λύση.* Παρατηρούμε πρώτα ότι $n \neq 1$. Πράγματι, αν $n = 1$, τότε $\sigma(1) = 1$ και τότε η δοθείσα σχέση δίνει $(m - 1) \cdot 1 = 1 \cdot m$ και άρα $m - 1 = m$. Αυτό φυσικά είναι άτοπο. Επομένως $n > 1$.

Από την δοθείσα σχέση $(m - 1) \cdot \sigma(n) = n \cdot m$, θα έχουμε:

$$(m - 1) \cdot \sigma(n) = n \cdot m \quad \Longrightarrow \quad \sigma(n) = \frac{n \cdot m}{m - 1} = n + \frac{n}{m - 1}$$

Θέτοντας

$$k := \frac{n}{m - 1}, \qquad \text{θα έχουμε} \qquad \sigma(n) = n + k \tag{†}$$

και επομένως ο αριθμός $k$ είναι φυσικός αριθμός, διότι $k = \sigma(n) - n \in \mathbb{N}$ και $\sigma(n) > n$.

Από τη άλλη πλευρά θα έχουμε $n = k \cdot (m - 1)$ και επομένως ο φυσικός αριθμός $k$ είναι διαιρέτης του $n$. Τότε στην σχέση (†) το πρώτο μέλος είναι, εξ' ορισμού, το άθροισμα των φυσικών διαιρετών του $n$ και το δεύτερο μέλος είναι το άθροισμα δύο εκ των φυσικών διαρετων του $n$. Τότε όμως από την σχέση (†) έπεται ότι οι φυσικοί διαιρέτες $k$ και $n$ είναι όλοι οι φυσικοί διαιρέτες του $n$ και κατά συνέπεια $k = 1$ (η περίπτωση $n = 1$ έχει αποκλειστεί στο πρώτο τμήμα της απόδειξης). Επομένως οι μόνοι φυσικοί διαιρέτες του $n$ είναι οι αριθμοί 1 και $n$ και επομένως ο αριθμός $n$ είναι πρώτος.

Τέλος επειδή $k = 1$, θα έχουμε: $n = m - 1$. $\blacksquare$

**Άσκηση 5.** *Αν $n > 1$ είναι ένας φυσικός αριθμός, να υπολογισθεί το άθροισμα:*

$$\sum_{1\leq k<n \ \ \& \ \ (k,n)=1} k$$

*Λύση.* Έστω

$$\mathcal{S} = \big\{k \in \mathbb{N} \mid 1 \leq k < n \quad \& \quad (k,n) = 1\big\}$$

Τότε

$$\sum_{1\leq k<n \ \ \& \ \ (k,n)=1} k = \sum_{k\in\mathcal{S}} k \tag{††}$$

Επειδή $n > 1$, προφανώς θα έχουμε

$$\mathcal{S} = \big\{k \in \mathbb{N} \mid 1 \leq k \leq n \quad \& \quad (k,n) = 1\big\}$$

και το πλήθος των στοιχείων του παραπάνω συνόλου είναι:

$$|\mathcal{S}| = \phi(n)$$

Έστω λοιπόν

$$\mathcal{S} = \big\{t_1, t_2, \cdots, t_{\phi(n)}\big\}$$

τα στοιχεία του συνόλου $\mathcal{S}$. Παρατηρούμε ότι, για κάθε $i = 1, 2, \cdots, \phi(n)$, ισχύει ότι:

$$1 \leq t_i < n \ \ \& \ \ (t_i, n) = 1 \qquad \Longleftrightarrow \qquad 1 \leq n - t_i < n \ \ \& \ \ (n - t_i, n) = 1$$

με άλλα λόγια: $t_i \in \mathcal{S} \iff n - t_i \in \mathcal{S}$. Δηλαδή οι φυσικοί αριθμοί $n - t_1, n - t_2, \cdots, n - t_{\phi(n)}$ είναι οι φυσικοί αριθμοί $t_1, t_2, \cdots, t_{\phi(n)}$, ενδεχομένως με διαφορετική σειρά.

Επομένως από τη σχέση (††), θα έχουμε:

$$\sum_{1\leq k<n \ \ \& \ \ (k,n)=1} k = \sum_{k\in\mathcal{S}} k = t_1 + t_2 + \cdots + t_{\phi(n)} = (n - t_1) + (n - t_2) + \cdots + (n - t_{\phi(n)})$$

Τότε όμως θα έχουμε:

$$t_1 + t_2 + \cdots + t_{\phi(n)} = \overbrace{n + n + \cdots + n}^{\phi(n) \text{ φορές}} - (t_1 + t_2 + \cdots + t_{\phi(n)})$$

και επομένως:

$$2 \cdot (t_1 + t_2 + \cdots + t_{\phi(n)}) = n \cdot \phi(n) \qquad \Longrightarrow \qquad t_1 + t_2 + \cdots + t_{\phi(n)} = \frac{n \cdot \phi(n)}{2}$$

Επομένως καταλήγουμε ότι:

$$\sum_{1\leq k<n \ \ \& \ \ (k,n)=1} k = \sum_{k\in\mathcal{S}} k = t_1 + t_2 + \cdots + t_{\phi(n)} = \frac{n \cdot \phi(n)}{2}$$ ■

**Άσκηση 6.** *Αν $n > 1$, να υπολογισθεί το άθροισμα*

$$\sum_{d|n} \Big(\frac{1}{d} \sum_{1\leq k\leq d \ \ \& \ \ (k,d)=1} k\Big)$$

*Λύση.* Θέτουμε

$$f(n) = \frac{1}{n} \cdot \sum_{1\leq k\leq n \ \ \& \ \ (k,n)=1} k$$

Τότε το ζητούμενο άθροισμα είναι

$$\sum_{d|n} f(d)$$

Από την Άσκηση 5 έπεται ότι

$$f(n) = \frac{1}{n} \cdot \frac{n \cdot \phi(n)}{2} = \frac{\phi(n)}{2}$$

Χρησιμοποιώντας την παραπάνω σχέση, θα έχουμε:

$$\begin{aligned}
\sum_{d|n} f(d) &= f(1) + \sum_{d|n \ \& \ d>1} f(d) \\
&= 1 + \frac{1}{2} \sum_{d|n \ \& \ d>1} \phi(d) \\
&= 1 + \frac{1}{2}(\sum_{d|n} \phi(d) - \phi(1)) \\
&= 1 + \frac{1}{2}(\sum_{d|n} \phi(d) - 1) \\
&= 1 - \frac{1}{2} + \frac{1}{2} \sum_{d|n} \phi(d) \\
&= 1 - \frac{1}{2} + \frac{1}{2} \cdot n \\
&= \frac{n+1}{2}
\end{aligned}$$

Επομένως το ζητούμενο άθροισμα είναι ίσο με:

$$\sum_{d|n} \big(\frac{1}{d} \cdot \sum_{1 \le k \le d \ \& \ (k,d)=1} k\big) = \frac{n+1}{2}$$

■

**Άσκηση 7.** (1) *Αν ο $n$ είναι περιττός και $3 \nmid n$, τότε:* $n^2 \equiv 1 \pmod{24}$.
(2) *Αν $(a, 35) = 1$, δείξτε ότι:* $35 \mid a^{12} - 1$.

*Λύση.* (1) Επειδή $3 \nmid n$, από το μικρό Θεώρημα του Fermat, έπεται ότι $n^{\phi(3)} \equiv n^2 \equiv 1 \pmod{3}$. Επομένως θα έχουμε

$$3 \mid n^2 - 1 \qquad (a)$$

Από την άλλη πλευρά επειδή ο αριθμός $n$ είναι περιττός, θα έχουμε $n = 2k + 1$, για κάποιον ακέραιο $k$. Τότε

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 \quad \Longrightarrow \quad n^2 - 1 = 4k(k+1)$$

Επειδή, όπως γνωρίζουμε το γινόμενο δύο διαδοχικών ακεραίων διαιρείται από το 2, θα έχουμε $2 \mid k(k+1)$ Τότε όμως η παραπάνω σχέση δίνει ότι:

$$8 \mid n^2 - 1 \qquad (b)$$

Επειδή $(3, 8) = 1$, από τις σχέσεις $(a)$ και $(b)$ έπεται ότι

$$3 \cdot 8 = 24 \mid n^2 - 1$$

και επομένως

$$n^2 \equiv 1 \pmod{24}$$

(2) Επειδή $(a, 35) = 1$, θα έχουμε προφανώς

$$(a, 5) = 1 = (a, 7)$$

και τότε από το μικρό Θεώρημα του Fermat θα έχουμε:

$$a^{\phi(5)} \equiv a^4 \equiv 1 \pmod{5} \quad \Longrightarrow \quad (a^4)^3 \equiv a^{12} \equiv 1 \pmod{5} \qquad (a)$$

και

$$a^{\phi(7)} \equiv a^6 \equiv 1 \pmod{7} \quad \Longrightarrow \quad (a^6)^2 \equiv a^{12} \equiv 1 \pmod{7} \qquad (b)$$

Οι σχέσεις $(a)$ και $(b)$ γράφονται ισοδύναμα ως εξής:

$$5 \mid a^{12}-1 \quad \& \quad 7 \mid a^{12}-1$$

Επειδή $(5,7)=1$ οι παραπάνω σχέσεις δίνουν το ζητούμενο

$$5\cdot 7 = 35 \mid a^{12}-1$$

■

**Άσκηση 8.** *Να βρεθεί το υπόλοιπο της διαίρεσης του αριθμού*

$$A = 11^{11} + 11^{11^2} + \cdots + 11^{11^{11}}$$

*με τον αριθμό* $7$.

*Λύση.* Ζητάμε να προσδιορίσουμε έναν αριθμό $k \in \mathbb{N}$ έτσι ώστε $A \equiv k \pmod 7$ όπου $0 \le k \le 6$. Έχουμε:

$$\begin{cases} 11 \equiv 4 \pmod 7 \\ 11^{11} \equiv 4^{11} \pmod 7 \\ 11^{11^2} \equiv 4^{11^2} \pmod 7 \\ \quad \vdots \\ 11^{11^{11}} \equiv 4^{11^{11}} \pmod 7 \end{cases} \implies A \equiv 4^{11} + 4^{11^2} + \cdots + 4^{11^{11}} \pmod 7$$

Για να απλοποιήσουμε τις πράξεις, θα προσπαθήσουμε να ελλατώσουμε τις δυνάμεις του $11$ οι οποίες εμφανίζονται στην έκφραση του $A$. Παρατηρούμε ότι

$$11 \equiv 2 \pmod 3 \implies 11^{2k} \equiv 2^{2k} \equiv 4^k \equiv 1 \pmod 3 \implies \begin{cases} 11^{2k} \equiv 1 \pmod 3 \\ 11^{2k+1} \equiv 11 \equiv 2 \pmod 3 \end{cases}$$

και άρα

$$\begin{cases} 11^{2k} = 3\lambda + 1, & \lambda \in \mathbb{Z} \\ 11^{2k+1} = 3\mu + 2, & \mu \in \mathbb{Z} \end{cases}$$

Επειδή $4^2 \equiv 2 \pmod 7$ και $4^3 = 64 \equiv 1 \pmod 7$ έχουμε

$$4^{11^{2k}} = 4^{3\lambda+1} = 4^{3\lambda}\cdot 4 \equiv 1 \cdot 4 \equiv 4 \pmod 7$$

και

$$4^{11^{2k+1}} = 4^{3\mu+2} = 4^{3\mu}\cdot 4^2 \equiv 1 \cdot 2 \equiv 2 \pmod 7$$

Τότε έπεται ότι

$$\begin{aligned} A &= 11^{11} + 11^{11^2} + \cdots + 11^{11^{11}} \\ &\equiv 4^{11} + 4^{11^2} + \cdots + 4^{11^{11}} \pmod 7 \\ &\equiv 2+4+2+4+2+4+2+4+2+4+2 \\ &\equiv 32 \pmod 7 \\ &\equiv 4 \pmod 7 \end{aligned}$$

Άρα το υπόλοιπο της διαίρεσης του αριθμού $A = 11^{11} + 11^{11^2} + \cdots + 11^{11^{11}}$ με τον αριθμό $7$ είναι $4$. ■

**Άσκηση 9.** *Να δείξετε ότι:*

$$7 \mid 2222^{5555} + 5555^{2222}$$

*Λύση.* Επειδή $2222 = 7 \cdot 317 + 3$ και $5555 = 7 \cdot 793 + 4$ έχουμε

$$2222 \equiv 3 \,(\mathsf{mod}\, 7) \quad \text{και} \quad 5555 \equiv 4 \equiv -3 \,(\mathsf{mod}\, 7)$$

Επομένως

$$2222^{5555} \equiv 3^{5555} \,(\mathsf{mod}\, 7)$$

και

$$5555^{2222} \equiv (-3)^{2222} \,(\mathsf{mod}\, 7) \equiv 3^{2222} \,(\mathsf{mod}\, 7)$$

Άρα αρκεί να δείξουμε ότι

$$2222^{5555} + 5555^{2222} \equiv 3^{5555} + 3^{2222} \equiv 3^{2222}(3^{3333} + 1) \equiv 0 \,(\mathsf{mod}\, 7)$$

Έχουμε $3^{3333} + 1 = 3^{3 \cdot 1111} + 1$ και $1111 \equiv 1 \,(\mathsf{mod}\, 6)$ διότι $1111 = 6 \cdot 185 + 1$. Ακόμα από το Θεώρημα του Fermat έχουμε ότι

$$3^6 \equiv 1 \,(\mathsf{mod}\, 7)$$

Τότε

$$3^{3333} = 3^{3 \cdot 1111} = (3^{1111})^3 = (3^{6 \cdot 185 + 1})^3 = (3^{6 \cdot 185})^3 \cdot 3^3 \equiv 1 \cdot 3^3 \equiv 27 \equiv 6 \,(\mathsf{mod}\, 7)$$

και επομένως

$$3^{3333} + 1 \equiv 6 + 1 \equiv 7 \equiv 0 \,(\mathsf{mod}\, 7)$$

Άρα

$$2222^{5555} + 5555^{2222} \equiv 3^{2222}(3^{3333} + 1) \equiv 0 \,(\mathsf{mod}\, 7)$$

δηλαδή $7 \mid 2222^{5555} + 5555^{2222}$. ■

**Άσκηση 10.** *Αν $p$ είναι ένας πρώτος με $p > 5$, δείξτε ότι ο αριθμός*

$$(p-1)! + 1$$

*έχει τουλάχιστον δύο πρώτους διαιρέτες.*

*Λύση.* Χρειάζεται να δείξουμε ότι για πρώτο $p > 5$, ο ακέραιος $(p-1)! + 1$ δεν είναι δύναμη πρώτου. Ας υποθέσουμε ότι

$$(p-1)! + 1 = q^k$$

για κάποιον πρώτο $q$ και θετικό ακέραιο $k$ και θα καταλήξουμε σε αντίφαση. Από το Θεώρημα Wilson $p \mid (p-1)! + 1 = q^k$, έτσι πρέπει να έχουμε $q = p$, δηλαδή $(p-1)! + 1 = p^k$.

Από την τελευταία σχέση έπεται ότι

$$p^k = (p-1)! + 1 < (p-1)^{p-1} < p^{p-1},$$

άρα $k < p - 1$. Αφού ο $p$ είναι πρώτος μεγαλύτερος του 5 ο $p - 1$ είναι σύνθετος αριθμός μεγαλύτερος του 4, έτσι από την Άσκηση 7 του Φυλλαδίου 6 έχουμε ότι

$$0 \equiv (p-2)! \ \mathsf{mod}(p-1).$$

Επίσης έχουμε

$$(p-1)! = p^k - 1 = (p-1)(p^{k-1} + p^{k-2} + \cdots + p + 1)$$

που, χρησιμοποιώντας ότι $p \equiv 1 \,\mathsf{mod}(p-1)$ συνεπάγεται ότι

$$0 \equiv (p-2)! = p^{k-1} + p^{k-2} + \cdots + p + 1 \equiv 1 + 1 + \cdots + 1 \equiv k \,\mathsf{mod}(p-1).$$

Έτσι έχουμε $0 < k < p - 1$ και $p - 1 \mid k$ που είναι αντίφαση. Επομένως ο αριθμός $(p-1)! + 1$ έχει τουλάχιστον δύο πρώτους διαιρέτες. ■

**Άσκηση 11.** *Να βρεθεί το υπόλοιπο της διαίρεσης του αριθμού*

$$\sum_{k=1}^{2013} 7^k$$

*με τον αριθμό* 100.

*Λύση.* Σε αυτή την άσκηση ο συμβολισμός $[a]$ σημαίνει $[a]_{100}$. Έχουμε

$$[7^2] = [49], \qquad [7^3] = [343] = [43], \qquad [7^4] = [7][43] = [301] = [1]$$

Επομένως, αφού $[7^4] = [1]$, με επαγωγή στο $k$ έχουμε

$$[7^{4k+i}] = [7^i]$$

για κάθε $k \geq 0$ και $1 \leq i \leq 4$. Παρατηρούμε ότι $2013 = 4 \cdot 503 + 1$. Σαν συνέπεια

$$\sum_{k=1}^{2013} 7^k \,(\mathsf{mod}\, 100) = \left(503(7 + 7^2 + 7^3 + 7^4) + 7\right) (\mathsf{mod}\, 100)$$

Αλλά

$$\left[7 + 7^2 + 7^3 + 7^4\right] = [7 + 49 + 43 + 1] = [100] = [0].$$

Επομένως

$$[\sum_{k=1}^{2013} 7^k] = [7]$$

και άρα το υπόλοιπο της διαίρεσης του $\sum_{k=1}^{2013} 7^k$ με τον αριθμό 100 είναι ίσο με 7. ■

**Άσκηση 12.** *Αν $n \geq 2$ είναι ένας θετικός ακέραιος, δείξτε ότι:*

$$n \nmid 2^n - 1$$

*Λύση.* Αν ο $n$ είναι άρτιος, τότε η πρόταση ισχύει γιατί το $2^n - 1$ είναι περιττός. Υποθέτουμε ότι ο $n$ είναι περιττός και $n \mid 2^n - 1$ και θα καταλήξουμε σε αντίφαση. Επειδή $n \geq 2$, ο αριθμός $n$ έχει έναν πρώτο διαιρέτη. Έστω $p$ ο μικρότερος πρώτος που διαιρεί το $n$. Ο συμβολισμός $[a]$ στα ακόλουθα σημαίνει $[a]_p$. Τότε $(n, p-1) = 1$ και άρα υπάρχουν ακέραιοι $a_1, b_1$ τέτοιοι ώστε $a_1 n + b_1(p-1) = 1$. Επομένως για κάθε ακέραιο $t$ έχουμε

$$1 = a_1 n + b_1(p-1) = na_1 - (p-1)(-b_1) = n(a_1 + (p-1)t) - (p-1)(-b_1 + nt)$$

Για κατάλληλα μεγάλο $t$ έχουμε $a_1 + (p-1)t > 0$ και $-b_1 + nt > 0$. Θέτοντας $a = a_1 + t(p-1)$ και $b = -b_1 + nt$ έχουμε ότι $a, b > 0$ και

$$1 = an - b(p-1) \tag{1}$$

Αφού $2^n \equiv 1 \bmod n$ έχουμε $n \mid 2^n - 1$, και επειδή $p \mid n$, έπεται ότι $p \mid 2^{n-1}$, δηλαδή: $2^n \equiv 1 \bmod p$. Επομένως $[2^n] = [1]$ και άρα $[2^{an}] = [2^n]^a = [1]^a = [1]$. Χρησιμοποιώντας την ισότητα (1) έχουμε ότι $[2^{(1+b(p-1))}] = [2^{an}] = [1]$, το οποίο συνεπάγεται ότι

$$[2] \cdot [2^{p-1}]^b = [1]. \tag{2}$$

Από το Θεώρημα Euler-Fermat έχουμε $[2^{p-1}] = [1]$ και άρα $[2^{p-1}]^b = [1]$, οπότε η ισότητα (2) συνεπάγεται ότι $[2] = [1]$ στο σύνολο $\mathbb{Z}_n$ που είναι αντίφαση διότι $n \geq 2$. Επομένως $n \nmid 2^n - 1$. ■

**Άσκηση 13.** *Να λυθεί το σύστημα γραμμικών ισοτιμιών*

$$(\Sigma) \qquad \begin{cases} x \equiv 3 \,(\mathsf{mod}\, 34) \\ x \equiv 5 \,(\mathsf{mod}\, 107) \\ x \equiv 3 \,(\mathsf{mod}\, 1111) \\ x \equiv 8 \,(\mathsf{mod}\, 38) \end{cases}$$

*Λύση.* Έχουμε $34 = 2 \cdot 17$ και $38 = 2 \cdot 19$. Επομένως $(34, 38) = 2$. Επειδή $2 \nmid 3 - 8 = -5$ από την Θεωρία το σύστημα δεν έχει ακέραιες λύσεις. ■

**Άσκηση 14.** *Έστω $m_1, m_2, \cdots, m_n$ θετικοί ακέραιοι οι οποίοι είναι πρώτοι μεταξύ τους ανα δύο. Να δείξετε ότι η μοναδική λύση $(\mathsf{mod}\, m_1 m_2 \cdots m_n)$ του συστήματος γραμμικών ισοτιμιών*

$$(\Sigma) \quad \begin{cases} x \equiv a_1 \,(\mathsf{mod}\, m_1) \\ x \equiv a_2 \,(\mathsf{mod}\, m_2) \\ \quad \vdots \\ x \equiv a_n \,(\mathsf{mod}\, m_n) \end{cases}$$

*είναι:*

$$x \equiv a_1 M_1^{\phi(m_1)} + a_2 M_2^{\phi(m_2)} + \cdots + a_n M_n^{\phi(m_n)} \,(\mathsf{mod}\, M)$$

*όπου*

$$M = m_1 m_2 \cdots m_n \quad \& \quad M_i = \frac{M}{m_i}, \quad 1 \le i \le n$$

*Λύση.* Επειδή $(m_i, m_j) = 1$, αν $1 \le i \ne j \le n$, έπεται άμεσα ότι θα έχουμε: $(M_i, m_i) = 1$ για κάθε $i = 1, 2, \cdots, n$, και $(M_i, m_j) = m_j$ για $1 \le i \ne j \le n$.

Επομένως, από το Θεώρημα Euler-Fermat έχουμε:

$$M_j^{\phi(m_j)} \equiv 1 \,\mathsf{mod}\, m_j, \qquad 1 \le j \le n$$

Σαν συνέπεια, θεωρώντας κλάσεις ισοτιμίας $(\mathsf{mod}\, m_j)$, όπου $1 \le j \le n$, θα έχουμε:

$$[x] = [a_1 M_1^{\phi(m_1)} + \cdots + a_j M_j^{\phi(m_j)} + \cdots + M_n^{\phi(m_n)}] = [0] + [0] + \cdots + [a_j \cdot 1] + [0] + \cdots + [0] = [a_j]$$

όπου για ακέραιο $a$ ο συμβολισμός $[a]$ σημαίνει $[a]_{m_j}$. Οι παραπάνω σχέσεις γράφονται ισοδύναμα

$$x \equiv a_j \,(\mathsf{mod}\, m_j), \qquad 1 \le j \le n$$

δηλαδή το $x$ ικανοποιεί το σύστημα $(\Sigma)$. Τότε από το Κινέζικο Θεώρημα Υπολοίπων, έπεται ότι η μοναδική λύση $\mathsf{mod}\, M$, του $(\Sigma)$ είναι η

$$x \equiv a_1 M_1^{\phi(m_1)} + a_2 M_2^{\phi(m_2)} + \cdots + a_n M_n^{\phi(m_n)} \,(\mathsf{mod}\, M)$$ ■

**Άσκηση 15.** *Να λυθεί το σύστημα γραμμικών ισοτιμιών*

$$(\Sigma) \quad \begin{cases} 2x \equiv 4 \,(\mathsf{mod}\, 8) \\ 3x \equiv 12 \,(\mathsf{mod}\, 9) \\ x \equiv 34 \,(\mathsf{mod}\, 12) \end{cases}$$

*Λύση.* Θα έχουμε:

$$d_1 = (2, 8) = 2 \mid 4 \quad \& \quad d_2 = (3, 9) = 3 \mid 9 \quad \& \quad d_3 = (1, 34) = 1 \mid 12$$

Επομένως κάθε μια εκ των ισοτιμιών του $(\Sigma)$ έχει λύση, και άρα το $(\Sigma)$ πιθανόν να έχει λύση.

Προφανώς το $(\Sigma)$ είναι ισοδύναμο με το σύστημα

$$(\Sigma') \quad \begin{cases} x \equiv 2 \,(\mathsf{mod}\, 4) \\ x \equiv 4 \,(\mathsf{mod}\, 3) \\ x \equiv 34 \,(\mathsf{mod}\, 12) \end{cases} \qquad \text{ή ισοδύναμα} \qquad (\Sigma') \quad \begin{cases} x \equiv 2 \,(\mathsf{mod}\, 4) \\ x \equiv 4 \,(\mathsf{mod}\, 3) \\ x \equiv 10 \,(\mathsf{mod}\, 12) \end{cases}$$

Θα έχουμε:

$$d_{12} = (4, 3) = 1 \mid -2 = 2 - 4 \quad \& \quad d_{13} = (4, 12) = 4 \mid -8 = 2 - 10 \quad \& \quad d_{23} = (3, 12) = 3 \mid -6 = 4 - 10$$

Επομένως το $(\Sigma')$ έχει μοναδική λύση $(\mathsf{mod}[4, 3, 12]) = (\mathsf{mod}\, 12)$.

Από την πρώτη ισοτιμία, θα έχουμε:

$$x \equiv 2 \pmod 4 \implies 4 \mid x-2 \implies x = 4t+2 \qquad (*)$$

Αντικαθιστώντας την τιμή $x = 4t+2$ στην δεύτερη ισοτιμία, θα έχουμε:

$$x \equiv 4 \pmod 3 \implies 4t+2 \equiv 4 \pmod 3 \implies 4t \equiv 2 \pmod 3$$

Η τελευταία ισοτιμία έχει μοναδική λύση $x \equiv 2 \pmod 3$. Τότε $x = 4 \cdot 2 + 2 = 10$ και άρα $x \equiv 10 \pmod{12}$ είναι η μοναδική λύση των δύο πρώτων ισοτιμιών $(\mathsf{mod}[3,4]) = (\mathsf{mod}\, 12)$. Η τελευταία ισοτιμία συμπίπτει με την τελευταία ισοτιμία του $\Sigma'$) και επ[ομένως καταλήγουμε ότι η μοναδική λύση του $(\Sigma')$, άρα και του αρχικού συστήματος, είναι η

$$x \equiv 10 \pmod{12}$$

■