Εισαγωγή στη Θεωρία Αριθμών για το Λύκειο

Σημειώσεις Προετοιμασίας για Μαθηματικούς Διαγωνισμούς

Διαιρετότητα
και
Ισοτιμίες

Αλέξανδρος Γ. Συγκελάκης
ags@math.uoc.gr

Νοέμβριος 2012

ΠΡΟΛΟΓΟΣ

Το παρόν άρθρο είναι μία συγκέντρωση κάποιων βασικών προτάσεων και παραδειγμάτων από τη θεωρία της Διαιρετότητας και των (γραμμικών κυρίως) ισοτιμιών. Σε καμία περίπτωση δεν επικαλείται ο συγγραφέας του άρθρου την πρωτοτυπία των περιεχομένων, τα οποία βρίσκονται στα βιβλία της βιβλιογραφίας που παρατίθεται στο τέλος του παρόντος, στη συλλογή μαθηματικών διαγωνισμών του γράφοντος και σε αρκετά βιβλία στοιχειώδους Θεωρίας Αριθμών. Παρά ταύτα, καταβλήθηκε ιδιαίτερη προσπάθεια ώστε η παρουσίαση της ύλης να είναι διαβαθμισμένη και όλα τα περιεχόμενα να περιέχουν ασκήσεις που ενδιαφέρουν μικρούς αλλά και μεγάλους μαθητές με ενδιαφέρον για τα μαθηματικά και συγκεκριμένα τους Μαθηματικούς Διαγωνισμούς. Με μεγάλη χαρά θα δεχτώ στο *email* μου **ags@math.uoc.gr**, τις υποδείξεις σας, καθώς επίσης και τα σχόλια - κριτικές σας. Μοναδικός υπεύθυνος για τα γραφόμενα, είναι ο συγγραφέας που έκανε την επιλογή των προτάσεων και των ασκήσεων από τα βιβλία της βιβλιογραφίας. Τελειώνοντας, θα ήθελα να ευχαριστήσω τον Καθηγητή του Πανεπιστημίου Κρήτης κο Μιχάλη Λάμπρου για την πολύτιμη συμβολή του στις διορθώσεις του παρόντος.

Αλέξανδρος Γ. Συγκελάκης
Νοέμβριος 2012

ΣΥΜΒΟΛΙΣΜΟΙ

$a|b$: «Ο a διαιρεί τον b» δηλαδή υπάρχει $k \in \mathbb{Z}$, τέτοιος ώστε $b = k \cdot a$.

$p^k \| a$: «Το p^k είναι η μεγαλύτερη δύναμη του p που διαιρεί το a.» Δηλαδή το p^k διαιρεί ακριβώς το a (αρα $p^k|a$ ενώ $p^{k+1} \nmid a$).

$a \nmid b$: «Ο a δεν διαιρεί τον b ».

$\min\{a_1, \ldots, a_n\}$: Ο μικρότερος μεταξύ των αριθμών $a_1, \ldots a_n$.

$\max\{a_1, \ldots, a_n\}$: Ο μεγαλύτερος μεταξύ των αριθμών $a_1, \ldots a_n$.

$(a_1, \ldots, a_n)$: Ο Μ.Κ.Δ. των αριθμών $a_1, \ldots a_n$.

$[a_1, \ldots, a_n]$: Το Ε.Κ.Π. των αριθμών $a_1, \ldots a_n$.

$n!$: Διαβάζεται «n παραγοντικό» και ορίζεται να είναι $n! = 1 \cdot 2 \cdot \cdots \cdot n \quad n \geq 2$ και 0!=1, 1!=1.

$a \equiv b \pmod{n}$: «Ο a είναι ισότιμος με τον b modulo n (ή κατά μέτρο n) » δηλαδή $n|(a-b)$.

$ord_n(a)$: «Τάξη του a $mod n$» με $(a, n) = 1$, ονομάζουμε τον ελάχιστο ακέραιο r για τον οποίο ισχύει $a^r \equiv 1 \pmod{n}$. Αποδεικνύεται (πολύ εύκολα) ότι $ord_n(a)|\phi(n)$.

$\mathbb{Z}$: Το σύνολο των ακεραιών αριθμών $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

$\mathbb{N}$: Το σύνολο των φυσικών αριθμών $\{0, 1, 2, 3 \ldots\}$.

$\exists$: Ο υπαρξιακός ποσοδείκτης. Διαβάζεται «Υπάρχει» (τουλάχιστον ένα).

$|a|$: «Απόλυτη τιμή του αριθμού a» δηλαδή $|a| = \begin{cases} a, & \text{εαν } a \geq 0 \\ a, & \text{εαν } a < 0 \end{cases}$

1 Διαιρετότητα

1.1 Ευκλείδεια Διαίρεση

Είναι γνωστό από την ευκλείδεια διαίρεση ότι εαν έχουμε δύο φυσικούς αριθμούς Δ (Διαιρετέος) και δ (διαιρέτης) με $\delta \neq 0$ τότε υπάρχουν μοναδικοί ακέραιοι π (πηλίκο) και υ (υπόλοιπο) τέτοιοι ώστε να ισχύει

$$\boxed{\Delta = \pi \cdot \delta + \upsilon, \;\; 0 \leq \upsilon < \delta}$$

Το παραπάνω Θεώρημα ισχύει και γενικότερα για οποιουσδήποτε ακέραιους α και β.

Θεώρημα 1.1 *Εαν α και β ακέραιοι με $\beta \neq 0$, τότε υπάρχουν μοναδικοί ακέραιοι κ και υ τέτοιοι, ώστε*

$$\boxed{\alpha = \kappa \cdot \beta + \upsilon, \;\; 0 \leq \upsilon < |\beta|.}$$

Παράδειγμα 1.1 *Εαν $\alpha = -231$ και $\beta = 26$ τότε από τη διαίρεση του 231 με το 26 έχουμε $231 = 8 \cdot 26 + 23$ επομένως*

$$\begin{aligned} -231 &= -8 \cdot 26 - 23 \\ &= -8 \cdot 26 - 26 + 26 - 23 \\ &= -9 \cdot 26 + 3 \end{aligned}$$

και $0 \leq 3 < 26$ δηλαδή το πηλίκο της διαίρεσης του -231 με το 26 είναι -9 και το υπόλοιπο είναι 3.

Άσκηση: *Με τον ίδιο τρόπο να εκτελέσετε τις διαιρέσεις του -231 με το -26 και του 231 με το -26.*

□

Παρατήρηση: Όπως γίνεται αντιληπτό από τα παραπάνω, όταν ο διαιρέτης της ευκλείδειας διαίρεσης είναι ο n τότε τα δυνατά υπόλοιπα της διαίρεσης οποιουδήποτε αριθμού με το n είναι $0, 1, \ldots, n-1$. Άρα κάθε αριθμός α είναι της μορφής $k \cdot n, \; k \cdot n + 1, \; \ldots, \; k \cdot n + (n-1)$. Ειδικά όταν $n = 2$ τότε τα δυνατά υπόλοιπα είναι $0, 1$. Εάν $\upsilon = 0$ τότε ο $\alpha = 2k$ λέγεται **άρτιος**, ενώ εαν $\upsilon = 1$ τότε ο $\alpha = 2k+1$ λέγεται **περιττός**.

Παράδειγμα 1.2 *Εαν ο a είναι ακέραιος τότε και ο $A = \dfrac{a(a^2+2)}{3}$ είναι ακέραιος.*

Απόδειξη:

Επειδή τα δυνατά υπόλοιπα του a με το 3 είναι 0,1,2, ο ακέραιος a έχει μία από τις μορφές $a = 3k$ ή $a = 3k+1$ ή $a = 3k+2$, $k \in \mathbb{Z}$.

- *Εαν $a = 3k$ τότε $A = \frac{3k[(3k^2)+2]}{3} = k(9k^2+2) \in \mathbb{Z}$.*

- *Εαν* $a = 3k + 1$ *τότε* $A = \frac{(3k+1)[(3k+1)^2+2]}{3} = (3k + 1)(3k^2 + 2k + 1) \in \mathbb{Z}$.
- *Εαν* $a = 3k + 2$ *τότε* $A = \frac{(3k+2)[(3k+2)^2+2]}{3} = (3k + 2)(3k^2 + 4k + 2) \in \mathbb{Z}$.

□

1.2 Βασικές Ιδιότητες Διαιρετότητος

Ορισμός 1.1 *Λέμε ότι η διαίρεση του a με το b ($b \neq 0$) είναι **τέλεια**, όταν το υπόλοιπο της διαίρεσής τους είναι ίσο με μηδέν. Σε αυτή την περίπτωση λέμε ότι το b **διαιρεί** (ακριβώς) το a ή ότι το a **διαιρείται** (ακριβώς) από το b ή ακόμα ότι ο a είναι **πολλαπλάσιο** του b, και γράφουμε $b|a$ ή $a = \pi o \lambda \lambda . b$. Άρα*

$$\boxed{b|a \Longleftrightarrow \exists\, k \in \mathbb{Z} \;\; \textit{τέτοιο} \;\; \textit{ώστε} \;\; a = k \cdot b.}$$

Παρατήρηση: Για να δηλώσουμε ότι ο ακέραιος b **δεν διαιρεί** τον ακέραιο a, γράφουμε $b \nmid a$ ή ισοδύναμα $a \neq \pi o \lambda \lambda . b$. Επίσης εαν $b|a$ τότε ισοδύναμα $a = kb$ για κάποιο $k \in \mathbb{Z}$ ή ισοδύναμα $a = (-k)(-b)$ που σημαίνει ότι εαν ο b είναι διαιρέτης του a, τότε και ο $-b$ είναι διαιρέτης του a. Επομένως οι διαιρέτες ενός ακεραίου εμφανίζονται κατά ζεύγη αντίθετων ακεραίων.

Ως άμεσες συνέπειες του παραπάνω ορισμού έχουμε τις εξής ιδιότητες:

(i) $a|0$ για κάθε $a \in \mathbb{Z}^*$,

(ii) Αν $0|b$, τότε $b = 0$,

(iii) $a|b \Leftrightarrow -a|b \Leftrightarrow a|-b \Leftrightarrow |a| \mid |b|$

(iv) $\pm 1|a$ και $\pm a|a$ για κάθε $a \in \mathbb{Z}^*$.

(v) Αν $b|a$, τότε $kb|ka$, για κάθε $k \in \mathbb{Z}^*$.

Λόγω των παραπάνω ιδιοτήτων γίνεται φανερό ότι για τη μελέτη της διαιρετότητας στο σύνολο των ακεραίων, είναι αρκετό να περιοριστούμε στο σύνολο των θετικών ακεραίων.

Παρακάτω αναφέρουμε (χωρίς απόδειξη) τις βασικότερες ιδιότητες της διαιρετότητας.

Πρόταση 1.1 *Έστω $a, b, c, d \in \mathbb{Z}$. Τότε ισχύουν οι παρακάτω ιδιότητες:*

(i) *Εαν $a|b$ και $b|c$, τότε $a|c$.*

(ii) *Εαν $a|b$ και $c|d$, τότε $ac|bd$.*

(iii) *Εαν $a|b$ τότε $a|\lambda b$ για κάθε ακέραιο $\lambda \in \mathbb{Z}$.*

(iv) *Εαν $a|b$ και $a|c$, τότε $a|b+c$.*

(v) *Εαν $a|b$ και $b \neq 0$, τότε $|a| \leq |b|$.*

(vi) *Εαν $a|b$ και $b|a$, τότε $a = b$ ή $a = -b$ (Δηλαδή $|a| = |b|$).*

Παρατήρηση: *Από τις ιδιότητες $(iii), (iv)$ της παραπάνω Πρότασης προκύπτει ότι εαν $a|b$ και $a|c$, τότε $a|kb+mc$, για κάθε $k, m \in \mathbb{Z}$. Ο ακέραιος $kb+mc$ λέγεται* ***γραμμικός συνδυασμός*** *των b και c.*

Παράδειγμα 1.3 ***(Βασική Εφαρμογή)*** *Να αποδείξετε ότι το γινόμενο n διαδοχικών ακεραίων διαιρείται από το n.*

Απόδειξη:

Έστω $k,\ k+1,\ \ldots,\ k+(n-1)$, n το πλήθος διαδοχικοί ακέραιοι. Θέτουμε $A = k(k+1)\cdots(k+(n-1))$. Τότε, από την ευκλείδεια διαίρεση, υπάρχουν ακέραιοι q, r τέτοιοι, ώστε

$$k = nq + r, \ \ 0 \leq r \leq n-1.$$

Αν $r = 0$, τότε $n|k$, απ' όπου $n|A$. Αν $r \neq 0$ τότε $1 \leq n-r \leq n-1$. Οπότε

$$\begin{aligned} A &= k(k+1)\cdots(k+n-r)\cdots(k+n-1) \\ &= (nq+r)\cdots(nq+r+n-r)\cdots(nq+r+n-1). \end{aligned}$$

Καθώς $nq+r+n-r = n(q+1)$, παίρνουμε $n|A$.

□

Παράδειγμα 1.4 *Να προσδιορίσετε όλους τους ακέραιους αριθμούς m που ικανοποιούν τη σχέση $m+1|m^2+1$.*

Λύση:

Επειδή $m+1|m+1$, άρα λόγω της παρατήρησης της Πρότασης 1.1 έχουμε $m+1|m^2+m+2$. Καθώς όμως $m^2+m+2 = m(m+1)+2$ και $m+1|m(m+1)$, η ίδια παρατήρηση δίνει ότι $m+1|2$ απ' όπου $m+1 = \pm 1, \pm 2$ δηλαδή $m = -3, -2, 0, 1$.

□

Παράδειγμα 1.5 *(Διαγωνισμός «Ευκλείδης» 1995) Θεωρούμε 6 διαδοχικούς φυσικούς αριθμούς. Έστω a το άθροισμα των τριών πρώτων και b το άθροισμα των τριών άλλων. Είναι δυνατόν να ισχύει $ab = 19951995$;*

Λύση:

Το άθροισμα τριών διαδοχικών αριθμών είναι πάντοτε πολλαπλάσιο του 3, διότι αν n είναι ο μεσαίος τότε οι αριθμοί είναι οι $n-1, n, n+1$ με άθροισμα $3n$. Συνεπώς οι a, b είναι πολλαπλάσια του 3 κι έτσι το ab είναι πολλαπλάσιο του 9. Όμως ο αριθμός 19951995 δεν είναι πολλαπλάσιο του 9 αφού το άθροισμα των ψηφίων του δεν διαιρείται με το 9.

□

Παράδειγμα 1.6 *(Διαγωνισμός «Ευκλείδης» 1995) Να εξετάσετε εαν υπάρχουν ακέραιοι x, y που ικανοποιούν την εξίσωση $x^2+4y = 1995$.*

Λύση :

Εαν ο x *είναι περιττός δηλαδή* $x = 2k+1,\ k \in \mathbb{Z}$ *τότε* $x^2 = 4k(k+1)+1$ *δηλαδή* $x^2 =$*πολλ.4+1. Αν ο* x *είναι άρτιος δηλαδή* $x = 2k,\ k \in \mathbb{Z}$ *τότε* $x^2 = 4k^2$ *δηλαδή* $x^2 =$*πολλ.4.*

Συνεπώς αφού το $4y$ *είναι πολλ.4, θα έχουμε* $x^2 + 4y =$ *πολλ.4 είτε* $x^2 + 4y =$ *πολλ.4+1 αλλά 1995=πολλ.4+3 άρα η εξίσωση είναι αδύνατη* [1].

□

Παράδειγμα 1.7 *Να δείξετε ότι για κάθε φυσικό αριθμό* n *ισχύει*

$$9|10^n + 3 \cdot 4^{n+2} + 5.$$

Απόδειξη :

Θα εφαρμόσουμε τη μέθοδο της μαθηματικής επαγωγής. Θέτουμε

$$P(n) = 10^n + 3 \cdot 4^{n+2} + 5.$$

Για $n = 0$ *έχουμε* $P(0) = 54$*, που διαιρείται από το 9. Υποθέτουμε ότι* $9|P(k)$ *δηλαδή ότι* $9|10^k + 3 \cdot 4^{k+2} + 5$*. Τότε*

$$\begin{aligned} P(k+1) &= 10^{k+1} + 3 \cdot 4^{k+3} + 5 = 10 \cdot 10^k + 3 \cdot 4 \cdot 4^{k+2} + 5 \\ &= 10^k + 3 \cdot 4^{k+2} + 5 + 9 \cdot 10^k + 9 \cdot 4^{k+2} = P(k) + 9(10^k + 4^{k+2}). \end{aligned}$$

Καθώς $9|P(k)$*, η παρατήρηση της Πρότασης* 1.1 *δίνει ότι* $9|P(k+1)$*. Συνεπώς ισχύει* $9|P(n)$ *για κάθε* $n \in \mathbb{N}$*.*

□

Παράδειγμα 1.8 *Να δείξετε ότι για κάθε* $n \in \mathbb{Z}$ *ισχύει* $4 \not| n^2 + 2$*.*

Απόδειξη :

Ας υποθέσουμε, αντίθετα, ότι υπάρχει ακέραιος n *τέτοιος ώστε* $4|n^2 + 2$*. Τότε έχουμε τις εξής δύο περιπτώσεις για τον ακέραιο* n *:*

- *Εαν* $n = 2k$*, όπου* $k \in \mathbb{Z}$*, τότε* $n^2 + 2 = 4k^2 + 2$*. Καθώς* $4|n^2 + 2$*, έπεται ότι* $4|4k^2 + 2$*, δηλαδή* $4|2$*, άτοπο.*
- *Εαν* $n = 2k+1$*, όπου* $k \in \mathbb{Z}$*, τότε* $n^2 + 2 = (2k+1)^2 + 2 = 4k^2 + 4k + 3$*. Επειδή όμως* $4|4k^2 + 4k$*, έπεται ότι* $4|3$*, άτοπο.*

Άρα για κάθε $n \in \mathbb{Z}$ *ισχύει* $4 \not| n^2 + 2$*.*

□

[1] Φυσικά μπορεί να επιλυθεί άμεσα με τη χρήση ισοτιμιών (για τις οποίες θα μιλήσουμε πιο κάτω).

1.3 Μέγιστος Κοινός Διαιρέτης (Μ.Κ.Δ.)

Πρόταση 1.2 ***(Αρχή της καλής διάταξης)*** *Έστω S ένα μη κενό υποσύνολο του $\mathbb{N}$. Τότε το S έχει ένα μοναδικό ελάχιστο στοιχείο, δηλαδή, ένα στοιχείο $a \in S$ τέτοιο, ώστε $a \leq x$, για κάθε $x \in S$.*

Έστω $a_1, \ldots, a_n$ ακέραιοι αριθμοί από τους οποίους ένας τουλάχιστον είναι $\neq 0$. Κάθε ακέραιος που διαιρεί καθένα από τους $a_1, \ldots, a_n$ λέγεται **κοινός διαιρέτης** των $a_1, \ldots, a_n$. Συμβολίζουμε με S το σύνολο των θετικών κοινών διαιρετών των $a_1, \ldots, a_n$. Το S είναι μη κενό διότι $1 \in S$. Αν $a_k \neq 0$ και $d \in S$ τότε $d|a_k$ και επομένως $d \leq |a_k|$. Άρα το σύνολο S είναι πεπερασμένο. Το μέγιστο στοιχείο του S είναι ένας θετικός ακέραιος που λέγεται **μέγιστος κοινός διαιρέτης (Μ.Κ.Δ.)** των $a_1, \ldots, a_n$ και συμβολίζεται με $(a_1, \ldots, a_n)$. Για κάθε $a \in \mathbb{Z}$, το σύνολο των θετικών διαιρετών του a συμπίπτει με αυτό του $-a$. Επομένως ισχύει $(a_1, \ldots, a_n) = (|a_1|, \ldots, |a_n|)$, δηλαδή ο Μ.Κ.Δ. είναι ανεξάρτητος προσήμων. Επίσης, καθώς κάθε ακέραιος είναι διαιρέτης του 0, έχουμε $(0, a_1, \ldots, a_n) = (a_1, \ldots, a_n)$. Συνεπώς μπορούμε να υποθέσουμε ότι κανένας εκ των ακεραίων $a_1, \ldots, a_n$ δεν είναι μηδέν.

Αν $(a_1, \ldots, a_n) = 1$, τότε οι ακέραιοι $a_1, \ldots, a_n$ καλούνται **πρώτοι μεταξύ τους**. Επίσης εαν $(a_i, a_j) = 1$ για κάθε $i, j \in \{1, \ldots, n\}$ με $i \neq j$, τότε οι ακέραιοι $a_1, \ldots, a_n$ καλούνται **πρώτοι μεταξύ τους ανά δύο**. Είναι προφανές ότι εαν οι ακέραιοι $a_1, \ldots, a_n$ είναι πρώτοι μεταξύ τους ανά δύο, τότε είναι και πρώτοι μεταξύ τους. Το αντίστροφό όμως δεν ισχύει εν γένει.

Θεώρημα 1.2 ***(Λήμμα Bezout)*** *Έστω $a_1, \ldots, a_n$ μη μηδενικοί ακέραιοι και $d = (a_1, \ldots, a_n)$. Τότε υπάρχουν ακέραιοι $k_1, \ldots, k_n$ τέτοιοι, ώστε*

$$d = k_1 a_1 + \cdots + k_n a_n.$$

Πόρισμα 1.1 *Έστω $a_1, \ldots, a_n$ μη μηδενικοί ακέραιοι. Ο θετικός ακέραιος d είναι ο Μ.Κ.Δ. των $a_1, \ldots, a_n$ αν και μόνο αν, ισχύουν τα εξής:*

(i) $d|a_1, \ldots, d|a_n$,

(ii) Αν δ είναι θετικός ακέραιος με $\delta|a_1, \ldots, \delta|a_n$, τότε $\delta|d$.

Πόρισμα 1.2 *Έστω $a_1, \ldots, a_n$ μη μηδενικοί ακέραιοι. Αν d είναι ένας θετικός κοινός διαιρέτης των $a_1, \ldots, a_n$ με $d = k_1 a_1 + \cdots + k_n a_n$, όπου $k_1, \ldots, k_n \in \mathbb{Z}$, τότε $d = (a_1, \ldots, a_n)$.*

Πόρισμα 1.3 *Έστω $a_1, \ldots, a_n$ μη μηδενικοί ακέραιοι. Οι ακέραιοι $a_1, \ldots, a_n$ είναι πρώτοι μεταξύ τους, αν και μόνο αν, υπάρχουν $k_1, \ldots, k_n \in \mathbb{Z}$ τέτοιοι ώστε $1 = k_1 a_1 + \cdots + k_n a_n$.*

Παράδειγμα 1.9 *Έστω ακέραιοι a, b πρώτοι μεταξύ τους. Να δείξετε ότι*

$$(9a + 7b, 4a + 3b) = 1.$$

Απόδειξη:

Έστω d ο Μ.Κ.Δ. των ακεραίων $9a + 7b$ και $4a + 3b$. Τότε $d|9a + 7b$ και $d|4a + 3b$. Οπότε $d|4(9a+7b)-9(4a+3b)$ και $d|3(9a+7b)-7(4a+3b)$, απ' όπου παίρνουμε $d|b$ και $d|a$ αντίστοιχα. Συνεπώς, το Πόρισμα 1.1 δίνει $d|(a, b)$ απ' όπου $d|1$. Επομένως $d = 1$.

□

Πρόταση 1.3 *Έστω $\lambda, a_1, \ldots, a_n$ μη μηδενικοί ακέραιοι. Ισχύουν τα εξής:*

(i) $(\lambda a_1, \ldots, \lambda a_n) = |\lambda|(a_1, \ldots, a_n)$,

(ii) *αν* $(a_1, \ldots, a_n) = d$, *τότε* $\left(\frac{a_1}{d}, \ldots, \frac{a_n}{d}\right) = 1$,

(iii) $(a_1, \ldots, a_n) = (a_1 + k_2a_2 + \cdots + k_na_n, a_2, \ldots, a_n)$, *όπου* $k_2, \ldots, k_n \in \mathbb{Z}$.

Παράδειγμα 1.10 *Εαν a, b είναι δύο ακέραιοι πρώτοι μεταξύ τους, τότε να δείξετε ότι $(a + b, a - b) = 1$ ή 2.*

Απόδειξη:

Πράγματι έστω $d = (a + b, a - b)$. Τότε $d|a + b$ και $d|a - b$. Επομένως έχουμε $d|(a + b) + (a - b)$ και $d|(a + b) - (a - b)$, δηλαδή $d|2a$ και $d|2b$ οπότε $d|(2a, 2b)$ και λόγω της Πρότασης 1.3(i) παίρνουμε $(2a, 2b) = 2(a, b) = 2$ άρα $d|2$ οπότε $d = 1$ ή 2.

□

Πρόταση 1.4 *Έστω $a_1, \ldots, a_n$ μη μηδενικοί ακέραιοι με $n > 2$. Για κάθε k, $1 \leq k \leq n - 2$ ισχύει*

$$(a_1, \ldots, a_n) = (a_1, \ldots, a_k, (a_{k+1}, \ldots, a_n)).$$

Παρατήρηση: *Η παραπάνω Πρόταση ανάγει τον υπολογισμό του Μ.Κ.Δ. πεπερασμένου πλήθους ακεραίων στον υπολογισμό του Μ.Κ.Δ. δύο ακεραίων.*

Πρόταση 1.5 ***(Βασική Πρόταση)*** *Έστω a, b, c τρεις μη μηδενικοί ακέραιοι. Εαν $a|bc$ και $(a, b) = 1$ τότε $a|c$.*

Παράδειγμα 1.11 *(Ρουμανία 2000) Να αποδειχθεί ότι δεν υπάρχουν φυσικοί αριθμοί x, y και z για τους οποίους να ισχύουν ταυτόχρονα οι σχέσεις*

$$5x - 3y + 10z = 0 \quad \text{και} \quad y(x + 2z) = 2004.$$

Απόδειξη:

Έστω ότι υπάρχουν τέτοιοι φυσικοί με τις ιδιότητες

$$5x - 3y + 10z = 0 \ (1) \ \textit{και} \ y(x + 2z) = 2004.$$

Τότε η (1) *γράφεται:* $5x + 10z = 3y \Leftrightarrow 5(x + 2z) = 3y$. *Επομένως* $5|3y$ *και επειδή* $(5, 3) = 1$ *άρα* $5|y$. *Αλλά τότε* $5|y(x + 2z)$ *δηλαδή* $5|2004$ *(αφού* $y(x + 2z) = 2004$*). Αυτό όμως είναι αδύνατο, συνεπώς δεν υπάρχουν φυσικοί αριθμοί με τις ιδιότητες της εκφωνήσεως.*

□

1.4 Ευκλείδειος Αλγόριθμος

Ο Ευκλείδειος αλγόριθμος περιγράφει μία διαδικασία για την εύρεση του Μ.Κ.Δ. δύο ακεραίων.

Ας υποθέσουμε ότι $a, b \in \mathbb{Z}$, και χωρίς βλάβη της γενικότητος, $b > 0$, διότι εαν ήταν $b < 0$, τότε $(a, b) = (a, |b|)$, και εαν ήταν $b = 0$, τότε $(a, b) = |a|$. Θέτουμε $d := (a, b)$.

Από την Ευκλείδεια διαίρεση μπορούμε να βρούμε ακεραίους q και r τέτοιους, ώστε $a = q_0 b + r_0$ όπου $0 \leq r_0 < b$.

Ας σημειωθεί ότι $(a, b) = (b, r_0)$, επειδή $d \mid a$ και $d \mid b$, συνεπώς $d \mid r_0 = a - q_0 b$. Εάν οι b και r_0 είχαν κοινό διαιρέτη d' μεγαλύτερο του d, τότε το d' θα ήταν κοινός διαιρέτης των a και b, το οποίο θα ερχόταν σε αντίθεση με την επιλογή του d ως μέγιστου. Συνεπώς, $d = (b, r_0)$.

Μπορούμε να επαναλάβουμε τη διαίρεση, αυτή τη φορά με τα b και r_0. Συνεχίζοντας με τον ίδιο τρόπο διαδοχικά έχουμε

$$\begin{aligned} a &= q_0 b + r_0 \text{ όπου } 0 \leq r_0 < b \\ b &= q_1 r_0 + r_1 \text{ όπου } 0 \leq r_1 < r_0 \\ r_0 &= q_2 r_1 + r_2 \text{ όπου } 0 \leq r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 \text{ όπου } 0 \leq r_3 < r_2 \\ &\vdots \end{aligned}$$

Συνεπώς παίρνουμε μία φθίνουσα ακολουθία μη αρνητικών ακεραίων $b > r_0 > r_1 > r_2 > \ldots$, η οποία πρέπει να φτάνει καποια στιγμή στο 0. Ας υποθέσουμε ότι αυτό γίνεται στο n-οστό βήμα. Τότε $r_n = 0$ και ο αλγόριθμος τερματίζει. Μπορούμε πολύ εύκολα να γενικεύσουμε αυτό το επιχείρημα για να δείξουμε ότι $d = (r_{k-1}, r_k) = (r_k, r_{k+1})$ για $k = 0, 1, 2, \ldots$, όπου $r_{-1} = b$. Συνεπώς, $d = (r_{n-1}, r_n) = (r_{n-1}, 0) = r_{n-1}$.

Πιο συγκεκριμένα, ο Μ.Κ.Δ. είναι το ελάχιστο μη μηδενικό υπόλοιπο στον παραπάνω αλγόριθμο.

Ο παραπάνω αλγόριθμος μας δίνει κάτι παραπάνω εκτός από τον Μ.Κ.Δ. Δίνει ένα τρόπο για να εκφράσουμε τον Μ.Κ.Δ. d, ως γραμμικό συνδυασμό των a και b, ένα Θεώρημα γνωστό ως Λήμμα $Bezout$. (Θεώρημα 1.2). Ακολουθώντας την

αντίστροφη πορεία από την προηγούμενη, έχουμε

$$\begin{aligned} a - q_0 b &= r_0 \\ b - q_1 r_0 &= r_1 \\ r_0 - q_2 r_1 &= r_2 \\ r_1 - q_3 r_2 &= r_3 \\ &\vdots \\ r_{n-3} - q_{n-1} r_{n-2} &= r_{n-1} \\ r_{n-2} &= q_n r_{n-1} \end{aligned}$$

συνεπώς, αντικαθιστώντας κάθε υπόλοιπο r_k στην επόμενη εξίσωση παίρνουμε

$$\begin{array}{ccccc} b - q_1(a - q_0 b) & = & k_1 a + l_1 b & = & r_1 \\ (a - q_0 b) - q_2(k_1 a + l_1 b) & = & k_2 a + l_2 b & = & r_2 \\ (k_1 a + l_1 b) - q_3(k_2 a + l_2 b) & = & k_3 a + l_3 b & = & r_3 \\ & & \vdots & & \vdots \\ (k_{n-3} a + l_{n-3} b) - q_n(k_{n-2} a + l_{n-2} b) & = & k_{n-1} a + l_{n-1} b & = & r_{n-1} \end{array}$$

Παράδειγμα 1.12 *Να βρείτε τον Μ.Κ.Δ. των ακεραίων 391 και 323, κάνοντας χρήση του Ευκλειδείου Αλγόριθμου και να γράψετε τον Μ.Κ.Δ. ως γραμμικό συνδυασμό των 391 και 323.*

Λύση: *Είναι*

$$391 = 1 \cdot 323 + 68$$
$$323 = 4 \cdot 68 + 51$$
$$68 = 1 \cdot 51 + 17$$
$$51 = 3 \cdot 17 + 0.$$

Επομένως (391,323)=17. Στη συνέχεια θα βρούμε ακεραίους x, y έτσι, ώστε $17 = 391x + 323y$. Έχουμε

$$\begin{aligned} 17 &= 68 - 51 = 68 - (323 - 4 \cdot 68) = -323 + 5 \cdot 68 \\ &= -323 + 5(391 - 323) = 5 \cdot 391 - 6 \cdot 323 \end{aligned}$$

Επομένως $17 = 5 \cdot 391 + (-6) \cdot 323$.

Παράδειγμα 1.13 *Θα βρούμε του Μ.Κ.Δ. των $a = 756$ και $b = 595$. Στον παρακάτω πίνακα, το r χρησιμοποιείται για τα υπόλοιπα που εμφανίζονται από τις διαδοχικές διαιρέσεις, το q για την αντίστοιχη ακολουθία πηλίκων και οι στήλες των k, l είναι η αντίστοιχη ακολουθία των k_i και l_i που περιγράφεται παραπάνω. Συνεπώς,* $(756, 595) = 7$ *και μάλιστα* $37 \cdot 756 - 47 \cdot 595 = 7$.

r	q	k	l
756		1	0
595	1	0	1
161	3	1	-1
112	1	-3	4
49	2	4	-5
14	3	-11	14
7	2	37	-47
0			

1.5 Ελάχιστο Κοινό Πολλαπλάσιο (Ε.Κ.Π.)

Έστω $a_1, \ldots, a_n \in \mathbb{Z}$. Ένας ακέραιος μ καλείται **κοινό πολλαπλάσιο** των $a_1, \ldots, a_n$ εαν $a_1|\mu, \ldots, a_n|\mu$. Παρατηρούμε ότι εαν ένας από τους ακέραιους $a_1, \ldots, a_n$ είναι το 0, τότε το μοναδικό πολλαπλάσιο τους είναι το 0. Ας υποθέσουμε στη συνέχεια ότι οι ακέραιοι $a_1, \ldots, a_n$ είναι μη μηδενικοί. Ο φυσικός $|a_1 \cdots a_n|$ είναι ένα κοινό πολλαπλάσιο των $a_1, \ldots, a_n$. Επομένως, (λόγω της Πρότασης 1.2) το σύνολο των θετικών πολλαπλασίων των $a_1, \ldots, a_n$ είναι μη κενό, επομένως έχει ένα ελάχιστο στοιχείο. Το στοιχείο αυτό καλείται **Ελάχιστο Κοινό Πολλαπλάσιο (Ε.Κ.Π.)** των $a_1, \ldots, a_n$ και συμβολίζεται με $[a_1, \ldots, a_n]$. Καθώς το σύνολο των θετικών πολλαπλασίων των $a_1, \ldots, a_n$ είναι το ίδιο με εκείνο των $|a_1|, \ldots, |a_n|$, συμπεραίνουμε ότι $[a_1, \ldots, a_n] = [|a_1|, \ldots, |a_n|]$.

Πρόταση 1.6 *Έστω $a_1, \ldots, a_n$ μη μηδενικοί ακέραιοι. Ο θετικός ακέραιος m είναι το Ε.Κ.Π. των $a_1, \ldots, a_n$, αν και μόνο αν, έχουμε*

(*i*) $a_1|m, \ldots, a_n|m$,

(*ii*) *εαν μ είναι θετικός ακέραιος με $a_1|\mu, \ldots, a_n|\mu$, τότε $m|\mu$.*

Πρόταση 1.7 *Έστω $\lambda, a_1, \ldots, a_n$ μη μηδενικοί ακέραιοι. Ισχύουν τα εξής:*

(*i*) $[\lambda a_1, \ldots, \lambda a_n] = |\lambda|[a_1, \ldots, a_n]$,

(*ii*) *αν $[a_1, \ldots, a_n] = m$ τότε $\left(\frac{m}{a_1}, \ldots, \frac{m}{a_n}\right) = 1$.*

Πρόταση 1.8 *Έστω $a_1, \ldots, a_n$ μη μηδενικοί ακέραιοι με $n > 2$. Για κάθε k, $1 \leq k \leq n-2$ ισχύει*

$$[a_1, \ldots, a_n] = [a_1, \ldots, a_k, [a_{k+1}, \ldots, a_n]] .$$

Παρατήρηση: *Η παραπάνω Πρόταση ανάγει τον υπολογισμό του Ε.Κ.Π. πεπερασμένου πλήθους ακεραίων στον υπολογισμό του Ε.Κ.Π. δύο ακεραίων.*

1.6 Πρώτοι Αριθμοί

Ορισμός 1.2 *Ένας θετικός ακέραιος $p > 1$ καλείται **πρώτος** εαν οι μόνοι διαιρέτες του είναι οι ακέραιοι ± 1 και $\pm p$. Ένας πρώτος αριθμός που είναι διαιρέτης ενός ακέραιου m καλείται **πρώτος διαιρέτης** ή **πρώτος παράγοντας** του m. Ένας θετικός ακέραιος $n > 1$ που δεν είναι πρώτος, καλείται **σύνθετος**. Σε αυτή την περίπτωση υπάρχουν d, e τέτοιοι, ώστε*

$$n = d \cdot e \ \text{ και } \ 1 < d \leq e < n.$$

(Το 2 είναι ο μοναδικός άρτιος πρώτος αριθμός).

Πρόταση 1.9 *Κάθε ακέραιος αριθμός $a > 1$ έχει ένα τουλάχιστον πρώτο διαιρέτη.*

Παράδειγμα 1.14 *Να βρείτε όλους τους θετικούς ακεραίους n για τους οποίους οι αριθμοί $3n-4,\ 4n-5, 5n-3$ είναι όλοι πρώτοι αριθμοί.*

Λύση:

Το άθροισμα των 3 αριθμών είναι άρτιος, συνεπώς τουλάχιστον ένας από αυτούς είναι άρτιος. Ο μοναδικός άρτιος πρώτος είναι το 2. Μόνο οι $3n-4$ και $5n-3$ μπορεί να είναι άρτιοι. Λύνουτας λοιπόν τις εξισώσεις $3n-4=2$ και $5n-3=2$ παίρνουμε $n=2$ και $n=1$ αντίστοιχα. Μόνο για $n=2$ οι 3 παραπάνω αριθμοί είναι πρώτοι άρα είναι και η μοναδική λύση.

□

Παράδειγμα 1.15 *(AHSME 1976) Εαν οι p και q είναι πρώτοι και το τριώνυμο $x^2 - px + q = 0$ έχει διακεκριμένες θετικές ακέραιες ρίζες, να βρείτε τα p και q.*

Λύση:

Έστω x_1 και x_2 με $x_1 < x_2$, οι δύο διακεκριμένες θετικές ακέραιες ρίζες. Τότε $x^2 - px + q = (x - x_1)(x - x_2)$, το οποίο δίνει ότι $p = x_1 + x_2$ και $q = x_1 x_2$. Καθώς ο q είναι πρώτος, άρα $x_1 = 1$. Συνεπώς οι $q = x_2$ και $p = x_2 + 1$ είναι διαδοχικοί πρώτοι αριθμοί, άρα $q = 2$ και $p = 3$.

□

Παράδειγμα 1.16 *(ARML 2003) Να βρείτε το μεγαλύτερο διαιρέτη του αριθμού 1001001001 που δεν ξεπερνά το 10000.*

Λύση:

Έχουμε

$$1001001001 = 1001 \cdot 10^6 + 1001 = 1001 \cdot (10^6 + 1) = 7 \cdot 11 \cdot 13 \cdot (10^6 + 1).$$

Ας σημειωθεί ότι

$$x^6 + 1 = (x^2)^3 + 1 = (x^2 + 1)(x^4 - x^2 + 1).$$

Άρα $10^6+1 = 101 \cdot 9901$, *άρα* $1001001001 = 7 \cdot 11 \cdot 13 \cdot 101 \cdot 9901$. *Δεν είναι δύσκολο τώρα να ελέγξουμε ότι κανένας συνδυασμός των 7,11,13 και 101 δεν φτιάχνει γινόμενο που να ξεπερνά το 9901 και να είναι μικρότερο του 1000, άρα η απάντηση είναι 9901.*

□

Παράδειγμα 1.17 *Έστω* n *ένας θετικός ακέραιος. Να αποδειχθεί ότι ο* $3^{2^n}+1$ *διαιρείται από το* 2 *αλλά όχι από το* 4 [2].

Απόδειξη:

Καταρχήν, ο 3^{2^n} *είναι περιττός και ο* $3^{2^n}+1$ *είναι άρτιος. Επίσης,*

$$3^{2^n} = (3^2)^{2^{n-1}} = 9^{2^{n-1}} = (8+1)^{2^n}.$$

Από το διώνυμο του Νεύτωνα

$$(x+y)^m = x^m + \binom{m}{1}x^{m-1}y + \binom{m}{2}x^{m-2}y^2 + \cdots + \binom{m}{m-1}xy^{m-1} + y^m,$$

για $x=8,\ y=1$ *και* $m=2^{n-1}$, *όλοι οι όροι του αθροίσματος πλην του τελευταίου (που είναι* $y^m=1$*), είναι πολλαπλάσια του 8 (τα οποία είναι πολλαπλάσια του 4). Συνεπώς το υπόλοιπο του* 3^{2^n} *όταν διαιρεθεί με το* 4 *είναι ίσο με 1, και το υπόλοιπο του* $3^{2^n}+1$ *με το 4 είναι ίσο με 2.*

Παρατήρηση: *Φυσικά το παραπάνω πρόβλημα απλοποιείται εαν κάνουμε χρήση ισοτιμιών* $modulo\ 4$ *(βλέπε παρακάτω).*

□

Παράδειγμα 1.18 *Να βρεθεί το* n *έτσι ώστε* $2^n \| 3^{1024}-1$.

Λύση:

Η απάντηση είναι 12. Ας σημειώσουμε ότι $1024 = 2^{10}$ *και* $x^2-y^2 = (x-y)(x+y)$. *Τότε, έχουμε*

$$\begin{aligned} 3^{2^{10}}-1 &= \left(3^{2^9}+1\right)\left(3^{2^9}-1\right) = \left(3^{2^9}+1\right)\left(3^{2^8}+1\right)\left(3^{2^8}-1\right) \\ &= \cdots = \left(3^{2^9}+1\right)\left(3^{2^8}+1\right)\cdots\left(3^{2^1}+1\right)\left(3^{2^0}+1\right)(3-1) \end{aligned}$$

*Όμως από το παράδειγμα (*1.17*),* $2\|3^{2^k}+1$ *για θετικούς ακεραίους* k. *Συνεπώς η απάντηση είναι 9+2+1=12.*

□

[2] Δηλαδή $2\|3^{2^n}+1$.

Η ακόλουθη Πρόταση είναι πολύ χρήσιμη σε ασκήσεις στις οποίες χρειαζόμαστε την αναπαράσταση ενός πρώτου αριθμού.

Πρόταση 1.10 *Κάθε πρώτος αριθμός είναι είτε της μορφής $6k+1$ είτε της μορφής $6k+5$.*

Θεώρημα 1.3 *Το πλήθος των πρώτων είναι άπειρο.*

Απόδειξη: [3]

Ας υποθέσουμε ότι $p_1, \ldots, p_n$ είναι όλοι οι πρώτοι αριθμοί. Θεωρούμε τον αριθμό

$$A = p_1 \cdots p_n + 1.$$

Σύμφωνα με την Πρόταση 1.9, υπάρχει πρώτος p τέτοιος, ώστε $p|A$. Καθώς $p_1, \ldots, p_n$ είναι όλοι οι πρώτοι, έχουμε $p = p_j$ για κάποιο δείκτη j με $1 \leq j \leq n$. Επομένως $p|A$ και $p|p_1 \cdots p_n$ απ' όπου παίρνουμε $p|1$ που είναι άτοπο. Συνεπώς, το πλήθος των πρώτων είναι άπειρο.

□

Πρόταση 1.11 *Εαν με p_n συμβολίσουμε του n-οστό πρώτο αριθμό, τότε ισχύει (η απόδειξη με επαγωγή)*

$$p_n \leq 2^{2^{n-1}}.$$

Παράδειγμα 1.19 *Για κάθε φυσικό αριθμό $n > 1$ υπάρχουν n διαδοχικοί φυσικοί αριθμοί, καυείς από τους οποίους δεν είναι πρώτος αριθμός.*

Απόδειξη:

Αρκεί να θεωρήσουμε τους εξής n διαδοχικούς φυσικούς αριθμούς

$$(n+1)! + 2,\ (n+1)! + 3,\ \cdots, (n+1)! + (n+1).$$

Καυείς από τους αριθμούς αυτούς δεν είναι πρώτος, διότι για κάθε $m = 2, 3, \cdots, n+1$, ο αριθμός $(n+1)! + m$ διαιρείται δια του m [4].

Παρατήρηση: *Από το παραπάνω παράδειγμα προκύπτει ότι υπάρχουν όσο μεγάλα κενά πρώτων αριθμών θέλουμε, στο σύνολο των φυσικών αριθμών.*

Ωστόσο, ανοικτό παραμένει το ερώτημα αν μπορούμε με κάποιο άλλο τρόπο (εκτός από εξαντλητικό ψάξιμο) να βρούμε τους μικρότερους διαδοχικούς αριθμούς που να έχουν το επιθυμητό κενό. Αυτή είναι εύλογη ερώτηση αν αναλογιστούμε ότι το παραγοντικό μεγαλώνει πολύ πολύ γρήγορα. Να αναφέρουμε ότι π.χ. με τον παραπάνω τρόπο για να προσδιορίσουμε 5 διαδοχικούς σύνθετους αριθμούς μπορούμε να πάρουμε τους αριθμούς 6!+2, 6!+3, 6!+4, 6!+4, 6!+6 δηλαδή τους αριθμούς 722, 723, 724, 725, 726. Όμως οι 5 πρώτοι διαδοχικοί φυσικοί αριθμοί που συναντάμε είναι οι 24,25,26,27,28 (ασφαλώς πολύ πολύ μικρότεροι από εκείνους που προκύπτουν με την παραπάνω μέθοδο).

[3] Πρόκειται για μία πολύ όμορφη απόδειξη η οποία οφείλεται στον Ευκλείδη και την οποία παραθέτουμε για ιστορικούς λόγους.

[4] Επίσης οι αριθμοί $(n+1)! - (n+1), \ldots, (n+1)! - 3, (n+1)! - 2$ είναι αποδεκτοί.

□

Η Πρόταση που ακολουθεί μας δίνει ένα τρόπο για να ελέγχουμε εαν ένας φυσικός αριθμός είναι πρώτος.

Πρόταση 1.12 *Κάθε σύνθετος φυσικός αριθμός $a > 1$, έχει ένα τουλάχιστον πρώτο διαιρέτη p, με $p \leq \sqrt{a}$.*

Πόρισμα 1.4 *Εαν ένας φυσικός αριθμός $a > 1$ δεν διαιρείται από κανένα πρώτο p, με $p \leq \sqrt{n}$, τότε ο αριθμός a είναι πρώτος.*

Παράδειγμα 1.20 *Θα εξετάσουμε έαν ο ακέραιος 383 είναι πρώτος. Έχουμε $19 < \sqrt{383} < 20$. Οι πρώτοι που είναι ≤ 19 είναι οι 2,3,5,7,11,13,17 και 19. Κανένας από αυτούς δεν διαιρεί το 383. Επομένως ο αριθμός 383 είναι πρώτος.*

Πρόταση 1.13 *Έστω a, b ακέραιοι $\neq 0, 1$ και p ένας πρώτος. Εαν $p|ab$ τότε $p|a$ ή $p|b$.*

Γενίκευση: *Έστω $a_1, \ldots, a_n$ ακέραιοι $\neq 0, 1$ και p ένας πρώτος. Εαν $p|a_1 \cdots a_n$ τότε $p|a_m$ για κάποιο δείκτη m ($1 \leq m \leq n$).*

Το ακόλουθο Θεώρημα είναι ένα από τα σημαντικότερα της Θεωρίας Αριθμών και είναι γνωστό ως το **Θεμελιώδες Θεώρημα της Αριθμητικής**.

Θεώρημα 1.4 *(**Θεμελιώδες Θεώρημα της Αριθμητικής**) Κάθε φυσικός $a > 1$ αναλύεται σε γινόμενο πρώτων κατά ένα και μόνο τρόπο, αν παραβλέψουμε την τάξη των παραγόντων στο γινόμενο.*

Ορισμός 1.3 *Σύμφωνα με το παραπάνω Θεώρημα, εαν a είναι ένας φυσικός > 1, τότε υπάρχουν διαφορετικοί πρώτοι $p_1, \ldots, p_k$ και φυσικοί $a_1, \ldots, a_k > 0$ έτσι, ώστε*

$$a = p_1^{a_1} \cdots p_k^{a_k}.$$

*Η παραπάνω γραφή του a θα καλείται **πρωτογενής ανάλυση** του a.*

Πρόταση 1.14 *Έστω a ένας φυσικός > 1 και $a = p_1^{a_1} \cdots p_k^{a_k}$ η πρωτογενής του ανάλυση. Ο φυσικός αριθμός d διαιρεί του a, αν και μόνο αν, $d = p_1^{\beta_1} \cdots p_k^{\beta_k}$ με $0 \leq \beta_i \leq a_i$ ($i = 1, \ldots, k$).*

Παράδειγμα 1.21 *(Ευκλείδης 1995) Να προσδιορίσετε όλα τα ζευγάρια φυσικών αριθμών x, y που ικανοποιούν την εξίσωση $x^2 = y^2 + 2y + 9$.*

Λύση:

$x^2 = y^2 + 2y + 9 \Leftrightarrow x^2 - (y+1)^2 = 8 \Leftrightarrow (x - y - 1)(x + y + 1) = 8$. *Οι αριθμοί $x - y, x + y$ είναι είτε και οι δύο άρτιοι είτε και οι δύο περιττοί, αν όμως ήταν άρτιοι τότε οι αριθμοί $x - y - 1, x + y + 1$ θα ήταν περιττοί με γινόμενο περιττό, άτοπο. Άρα $x - y$ περιττός και $x + y$ περιττός. Μάλιστα αφού ο $x + y + 1$ είναι θετικός πρέπει $x - y - 1$ θετικός. Άρα $(x - y - 1, x + y + 1) = (2, 4)$ ή $(4, 2)$ απ' όπου παίρνουμε και τη μοναδική λύση $(x, y) = (3, 0)$.*

□

Παράδειγμα 1.22 *(Ευκλείδης 1997) Οι φυσικοί αριθμοί* a, b $(a, b \in \mathbb{N}^*)$ *είναι τέτοιοι, ώστε*

$$\frac{a^3+1}{b+1} + \frac{b^3+1}{a+1} \in \mathbb{N}.$$

Να αποδείξετε ότι κάθε ένα από τα κλάσματα $\dfrac{a^3+1}{b+1}, \dfrac{b^3+1}{a+1}$ *είναι φυσικοί.*

Απόδειξη :

Έστω $(a+1, b+1) = d$. *Τότε* $a+1 = d \cdot p_1 p_2 \cdots p_k$ *και* $b+1 = d \cdot q_1 q_2 \cdots q_l$, *όπου* p_i, q_j *πρώτοι με* $p_i \neq q_j$, $\forall i = 1, 2 \ldots, k$ *και* $j = 1, 2, \ldots, l$ *αλλά όχι κατ' ανάγκη οι* p_i *διαφορετικοί μεταξύ τους ούτε οι* q_j *μεταξύ τους.*

Έχουμε διαδοχικά

$$\begin{aligned}
\frac{a^3+1}{b+1} + \frac{b^3+1}{a+1} &= \frac{(a+1)(a^2-a+1)}{b+1} + \frac{(b+1)(b^2-b+1)}{a+1} \\
&= \frac{d \cdot p_1 p_2 \cdots p_k (a^2-a+1)}{d \cdot q_1 q_2 \cdots q_l} + \frac{d \cdot q_1 q_2 \cdots q_l (b^2-b+1)}{d \cdot p_1 p_2 \cdots p_k} \\
&= \frac{p_1^2 p_2^2 \cdots p_k^2 (a^2-a+1) + q_1^2 q_2^2 \cdots q_l^2 (b^2-b+1)}{q_1 q_2 \cdots q_l p_1 p_2 \cdots p_k} \in \mathbb{N}
\end{aligned}$$

Εφόσον τα q_j *διαιρούν τον αριθμό* $q_1^2 q_2^2 \cdots q_l^2 (b^2-b+1)$ *και το άθροισμα*

$$p_1^2 p_2^2 \cdots p_k^2 (a^2-a+1) + q_1^2 q_2^2 \cdots q_l^2 (b^2-b+1),$$

θα διαιρούν και τη διαφορά τους δηλαδή τον αριθμό $p_1^2 p_2^2 \cdots p_k^2 (a^2-a+1)$. *Όμως τα* q_j *δεν διαιρούν τον αριθμό* $p_1^2 p_2^2 \cdots p_k^2$ *άρα τα* q_j *διαιρούν τον* a^2-a+1 *δηλαδή*

$$\begin{aligned}
\frac{a^2-a+1}{q_1 q_2 \cdots q_l} \in \mathbb{N} &\Rightarrow \frac{d(a^2-a+1)}{d \cdot q_1 q_2 \cdots q_l} \in \mathbb{N} \\
&\Rightarrow \frac{d(a^2-a+1)}{b+1} \in \mathbb{N} \\
&\Rightarrow p_1 p_2 \cdots p_k \cdot \frac{d(a^2-a+1)}{b+1} \in \mathbb{N} \\
&\Rightarrow \frac{(a+1)(a^2-a+1)}{b+1} \in \mathbb{N} \\
&\Rightarrow \frac{a^3+1}{b+1} \in \mathbb{N}
\end{aligned}$$

και εφόσον $\dfrac{a^3+1}{b+1} + \dfrac{b^3+1}{a+1} \in \mathbb{N}$ *άρα* $\frac{b^3+1}{a+1} \in \mathbb{N}$.

□

1.7 Εφαρμογές στον Μ.Κ.Δ. και στο Ε.Κ.Π

Πρόταση 1.15 *Έστω $a_1, \ldots, a_n$ μη μηδενικοί ακέραιοι με*

$$|a_1| = p_1^{a_{11}} \cdots p_k^{a_{1k}}, \ldots, |a_n| = p_1^{a_{n1}} \cdots p_k^{a_{nk}}$$

όπου $p_1, \ldots, p_k$ είναι πρώτοι και a_{ij} φυσικοί αριθμοί ($i = 1, \ldots, n, \quad j = 1, \ldots, k$). Τότε

$$(a_1, \ldots, a_n) = p_1^{d_1} \cdots p_k^{d_k},$$

όπου $d_j = \min\{a_{1j}, \ldots, a_{nj}\}$ $(j = 1, \ldots, k)$.

Πόρισμα 1.5 *Έστω $a_1, \ldots, a_n$ μη μηδενικοί ακέραιοι και $m \in \mathbb{N}$. Τότε*

$$(a_1^m, \ldots, a_n^m) = (a_1, \ldots, a_n)^m.$$

Πρόταση 1.16 *Έστω $a, b_1, \cdots, b_n$ ($n \geq 2$) μη μηδενικοί ακέραιοι και οι $b_1, \cdots, b_n$ πρώτοι μεταξύ τους ανά δύο. Τότε*

$$(a, b_1, \ldots, b_n) = (a, b_1) \cdots (a, b_n).$$

Πόρισμα 1.6 *Έστω $a, b_1, \ldots, b_n$ ($n \geq 2$) μη μηδενικοί ακέραιοι και οι $b_1, \ldots, b_n$ πρώτοι μεταξύ τους ανά δύο. Εαν $b_1|a, \ldots, b_n|a$ τότε $b_1 \cdots b_n|a$.*

Παράδειγμα 1.23 *Έστω n ένας περιττός ακέραιος > 1. Να δείξετε ότι*

$$24|n(n^2 - 1).$$

Απόδειξη:

Ο ακέραιος $A = n(n^2 - 1) = (n - 1)n(n + 1)$ είναι γινόμενο τριών διαδιχικών ακεραίων συνεπώς είναι πολλαπλάσιο του 3 άρα $3|A$. Επειδή ο ακέραιος n είναι περιττός > 1, υπάρχει $k \in \mathbb{N}$ με $k \neq 0$ έτσι, ώστε $n = 2k + 1$. Οπότε

$$A = 4k(k + 1)(2k + 1).$$

Ένας από τους φυσικούς $k, k + 1$ είναι άρτιος άρα $8|A$. Τέλος, καθώς $(3, 8) = 1$, το πόρισμα (3.1) δίνει το ζητούμενο $24|A$.

□

Πρόταση 1.17 *Έστω $a_1, \ldots, a_n$ μη μηδενικοί ακέραιοι με*

$$|a_1| = p_1^{a_{11}} \cdots p_k^{a_{1k}}, \ldots, |a_n| = p_1^{a_{n1}} \cdots p_k^{a_{nk}}$$

όπου $p_1, \ldots, p_k$ είναι πρώτοι και a_{ij} φυσικοί αριθμοί ($i = 1, \ldots, n, j = 1, \ldots, k$). Τότε

$$[a_1, \ldots, a_n] = p_1^{c_1} \cdots p_k^{c_k},$$

όπου $c_j = \max\{a_{1j}, \ldots, a_{nj}\}$ $(j = 1, \ldots, k)$.

Πόρισμα 1.7 *Έστω $a_1, \ldots, a_n$ μη μηδενικοί ακέραιοι και $m \in \mathbb{N}$. Τότε*

$$[a_1^m, \ldots, a_n^m] = [a_1, \ldots, a_n]^m.$$

Παράδειγμα 1.24 *Οι προτάσεις $(1.15), (1.17)$ είναι πολύ χρήσιμες για την εύρεση του Μ.Κ.Δ. και Ε.Κ.Π. δύο ή περισσοτέρων φυσικών στην περίπτωση που γνωρίζουμε την πρωτογενή τους ανάλυση. Για τον Μ.Κ.Δ. αρκεί να πάρουμε το γινόμενο όλων των πρώτων που εμφανίζονται στην πρωτογενή ανάλυση κάθε αριθμού υψωμένο στη μικρότερη δύναμη (εαν κάποιος πρώτος δεν εμφανίζεται στην πρωτογενή ανάλυση του αριθμού, τότε θεωρούμε ότι εμφανίζεται με εκθέτη 0, συνεπώς αυτός ο εκθέτης είναι και ο μικρότερος που εμφανίζεται για τον ευ λόγω πρώτο). Για το Ε.Κ.Π. αρκεί να πάρουμε το γινόμενο όλων των πρώτων που εμφανίζονται στην πρωτογενή ανάλυση κάθε αριθμού υψωμένο στη μεγαλύτερη δύναμη. Έτσι, ο Μ.Κ.Δ. των αριθμών $49000 = 2^3 \cdot 5^3 \cdot 7^2$, $36400 = 2^4 \cdot 5^2 \cdot 7 \cdot 13$, $27500 = 2^2 \cdot 5^4 \cdot 11$ είναι $2^2 \cdot 5^2 \cdot 7^0 \cdot 11^0 \cdot 13^0 = 100$. ενώ το Ε.Κ.Π. των ίδιων είναι $2^4 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 = 70070000$.*

Πρόταση 1.18 *Έστω a, b δύο μη μηδενικοί ακέραιοι. Τότε*

$$(a, b) \cdot [a, b] = |ab|.$$

Παρατήρηση: *Για περισσότερους από δύο ακεραίους,* ***δεν ισχύει*** *ανάλογη σχέση με την παραπάνω. Δηλαδή γενικά, έχουμε*

$$(a_1, \ldots, a_n) \cdot [a_1, \ldots, a_n] \neq |a_1 \cdots a_n| \quad \textbf{για} \quad n > 2.$$

Για παράδειγμα, $(6, 8, 10) \cdot [6, 8, 10] = 2 \cdot 120 = 240 \neq 480 = 6 \cdot 8 \cdot 10$.

2 Ισοτιμίες

2.1 Ορισμός και βασικές Ιδιότητες

Ορισμός 2.1 *Έστω n ένας ένας θετικός ακέραιος. Δύο ακέραιοι a, b λέγονται* ***ισοϋπόλοιποι*** *με μέτρο n, όταν διαιρούμενοι με το n αφήνουν το ίδιο υπόλοιπο. Τότε γράφουμε ότι*

$$a \equiv b \pmod{n}$$

και διαβάζουμε «a ισοϋπόλοιπο με το b μόντουλο n». Εαν ο ακέραιος a δεν είναι ισουπόλοιπος με τον b μόντουλο n, γράφουμε

$$a \not\equiv b \pmod{n}$$

.

Για παράδειγμα $10 \equiv 2 \pmod 4$, $11 \equiv -15 \pmod{13}$ *ενώ* $-7 \not\equiv -11 \pmod 5$.

Θεώρημα 2.1

$$\boxed{a \equiv b \pmod{n} \iff n|a-b}$$

Άμεσες συνέπειες του ορισμού είναι οι επόμενες ιδιότητες.

Πόρισμα 2.1 (i) $a \equiv a \pmod n$ ***(ανακλαστική ιδιότητα)***.

(ii) *Εαν* $a \equiv b \pmod n$, *τότε* $b \equiv a \pmod n$ ***(συμμετρική ιδιότητα)***.

(iii) *Εαν* $a \equiv b \pmod n$ *και* $b \equiv c \pmod n$, *τότε* $a \equiv c \pmod n$ ***(μεταβατική ιδιότητα)***.

Πόρισμα 2.2 (i) $a \equiv 0 \pmod n \Leftrightarrow n|a$,

(ii) *Ο ακέραιος a είναι άρτιος, αν και μόνο αν,* $a \equiv 0 \pmod 2$,

(iii) *Ο ακέραιος a είναι περιττός, αν και μόνο αν,* $a \equiv 1 \pmod 2$,

(iv) *Εαν* $a \equiv b \pmod n$ *και* $m|n$ *τότε* $a \equiv b \pmod m$,

(v) *Για κάθε ζεύγος ακεραίων a, b ισχύει* $a \equiv b \pmod 1$,

(vi) *Εαν το υπόλοιπο της διαίρεσης του a με το n είναι v, τότε* $a \equiv v \pmod n$.

Πρόταση 2.1 *Έστω $a, b, c, d \in \mathbb{Z}$ και $f(x)$ ένα πολυώνυμο με ακέραιους συντελεστές. Εαν* $a \equiv b \pmod n$ *και* $c \equiv d \pmod n$, *τότε*

(i) $a + c \equiv b + d \pmod n$ *και* $ac \equiv bd \pmod n$,

(ii) $a^m \equiv b^m \pmod n$, *για κάθε* $m \in \mathbb{N}$,

(iii) $f(a) \equiv f(b) \pmod{n}$.

Πρόταση 2.2 *Έστω $a, b, k \in \mathbb{Z}$ με $k \neq 0$ και $d = (n, k)$. Τότε*

$$ka \equiv kb \pmod{n} \Longleftrightarrow a \equiv b \pmod{\frac{n}{d}}.$$

Οι ισοτιμίες εμφανίζονται πολύ συχνά στη καθημερινή μας ζωή.

Για παράδειγμα, ο ωροδείκτης των ρολογιών δείχνει την ώρα $modulo$ 12 και ο χιλιομετρικός δείκτης των αυτοκινήτων δείχνει τα χιλιόμετρα που έχουμε διανύσει $modulo$ 100.000. Έτσι, όταν η ώρα είναι 18, το ρολόι δείχνει 6, που είναι το υπόλοιπο της διαίρεσης του 18 με το 12, και όταν ένα αυτοκίνητο έχει διανύσει συνολικά 245.000 Km, ο χιλιομετρικός δείκτης δείχνει 45.000 Km, που είναι το υπόλοιπο της διαίρεσης του 245.000 με το 100.000.

Ερώτηση: Μήπως μπορείτε να βρείτε τί μέρα θα είναι η 217η ημέρα του χρόνου εαν η πρώτη μέρα ήταν Δευτέρα; Ποιό μέτρο ($modulo$) χρησιμοποιήσατε για να το βρείτε; Μήπως τελικά έχουν πολλές εφαρμογές οι ισοτιμίες στην καθημερινή μας ζωή;

Παράδειγμα 2.1 *Να υπολογίσετε το υπόλοιπο της διαίρεσης του αριθμού $A = 13^{23}27^{41}$ με το 8.*

Λύση:

Είναι

$$13^2 = 169 \equiv 9 \equiv 1 \pmod{8}.$$

Επομένως

$$13^{23} = 13^{2\cdot 11+1} = 13 \cdot (13^2)^{11} \equiv 13 \equiv 5 \pmod{8}.$$

Επίσης $27 \equiv 3 \pmod{8}$, *απ' όπου* $27^2 \equiv 9 \equiv 1 \pmod{8}$. *Επομένως*

$$27^{41} = 27^{2\cdot 20+1} = 27 \cdot (27^2)^{20} \equiv 27 \equiv 3 \pmod{8}.$$

Άρα $A \equiv 15 \equiv 7 \pmod{8}$ *και επομένως υπάρχει* $a \in \mathbb{Z}$ *τέτοιο, ώστε* $A = 8a + 7$. *Συνεπώς το ζητούμενο υπόλοιπο είναι ο αριθμός 7.*

□

Παράδειγμα 2.2 *Να δείξετε ότι* $2222^{5555} + 5555^{2222} \equiv 0 \pmod{7}$.

Απόδειξη:

Ισχύει $2222 \equiv 3 \pmod{7}$ *και* $5555 \equiv 4 \pmod{7}$.

Άρα $2222^{5555} + 5555^{2222} \equiv 3^{5555} + 4^{2222} \pmod{7}$.

Επίσης

$$3^{5555} = (3^5)^{1111} = (-2)^{1111} = -2^{1111} \pmod{7}$$

και

$$4^{2222} = (4^2)^{1111} \equiv 2^{1111} \pmod{7}$$

και προσθέτωντας τις τελευταίες, παίρνουμε αυτό που θέλουμε.

□

Παράδειγμα 2.3 *Αν $\lambda \in \mathbb{N}$, να αποδειχθεί ότι ο αριθμός $A = \sqrt[4]{5\lambda + 3}$ είναι άρρητος.*

Απόδειξη:

Έστω a τυχαίος ακέραιος. Τότε όπως είναι γνωστό $a \equiv 0, 1, 2, 3, 4 \pmod 5$ άρα $a^2 \equiv 0, 1, 4 \pmod 5$ και τελικά $a^4 \equiv 0, 1 \pmod 5$.

Επειδή $5\lambda + 3 \equiv 3 \pmod 5$, συμπεραίνουμε ότι ο $5\lambda + 3$ δεν έχει τη μορφή a^4 με $a \in \mathbb{Z}$. Άρα ο A είναι άρρητος. (Είναι $A^4 = 5\lambda + 3 \equiv 3 \pmod 5$, άτοπο).

Άσκηση: *(Μολδαβία 1997) Να αποδείξετε ότι ο αριθμός $a = \sqrt{5n^2 + 10}$ είναι άρρητος για κάθε $n \in \mathbb{Z}$.*

□

Παράδειγμα 2.4 *(Βουλγαρία) Να αποδείξετε ότι ο 121 δεν διαιρεί του αριθμό $n^2 + 3n + 5$ για κάθε τιμή του $n \in \mathbb{Z}$.*

Απόδειξη:

Ας υποθέσουμε ότι $121|n^2+3n+5$. Τότε $11|n^2+3n+5$. Έτσι $n^2+3n+5 \equiv 0 \equiv 33 \pmod{11}$. Άρα $n^2 + 3n - 28 \equiv 0 \pmod{11} \Leftrightarrow 11|(n-4)(n+7) \Leftrightarrow 11|n-4$ ή $11|n+7 \Leftrightarrow (n = 11k+4$ ή $n = 11k-7)$ και αντικαθιστώντας το n στο n^2+3n+5, το τελευταίο παίρνει τη μορφή $121\lambda + \upsilon$ με $0 < \upsilon < 121$ το οποίο είναι άτοπο.

□

Παράδειγμα 2.5 *(ΕΜΕ 1997) Έστω a, b, c ακέραιοι αριθμοί τέτοιοι, ώστε*

$$(a-b)(b-c)(c-a) = a+b+c.$$

Να αποδείξετε ότι ο αριθμός $a + b + c$ διαιρείται με το 27.

Απόδειξη:

Προφανώς για τους a, b, c ισχύει ότι $a, b, c \equiv 0, \pm 1 \pmod 3$. Εαν και οι τρεις αφήνουν διαφορετικό υπόλοιπο στη διαίρεσή τους με το 3, τότε $a + b + c \equiv -1 + 0 + 1 = 0 \pmod 3$ ενώ $(a-b)(b-c)(c-a) \not\equiv 0 \pmod 3$. Εαν ακριβώς δύο είναι ισουπόλοιποι, χωρίς βλάβη της γενικότητος έστω οι a, b τότε $a - b \equiv 0 \pmod 3$ άρα $(a-b)(b-c)(c-a) \equiv 0 \pmod 3$ ενώ $a + b + c \not\equiv 0 \pmod 3$. Συνεπώς οι a, b, c είναι ισουπόλοιποι $mod 3$. Τότε $a - b \equiv b - c \equiv c - a \equiv 0 \pmod 3$, άρα $(a-b)(b-c)(c-a) \equiv 0 \pmod{27}$. Όμως $(a-b)(b-c)(c-a) = a+b+c$ άρα η προηγούμενη ισότητα δίνει $a + b + c \equiv 0 \pmod{27}$ που είναι και το ζητούμενο.

□

Παράδειγμα 2.6 *(Ευκλείδης 1995) Να προσδιορίσετε τους πρώτους αριθμούς p, q για τους οποίους ο αριθμός $p^{p+1} + q^{q+1}$ είναι πρώτος.*

Λύση:

Εαν p, q και οι δύο άρτιοι ή και οι δύο περιττοί, τότε ο αριθμός $p^{p+1} + q^{q+1}$ είναι άρτιος > 2 άρα όχι πρώτος. Άρα ο ένας είναι το 2 και ο άλλος είναι περιττός. Άρα χωρίς βλάβη της γενικότητος μπορούμε να υποθέσουμε ότι $p = 2$ και $q \equiv 0, 1, -1 \pmod 3$ και περιττός. Εαν $q \equiv 1 \pmod 3$, τότε $p^{p+1} + q^{q+1} \equiv 8 + 1 \equiv 0 \pmod 3$, άτοπο. Εαν $q \equiv -1 \pmod 3$, τότε $p^{p+1} + q^{q+1} \equiv 8 + 1 \equiv 0 \pmod 3$ (διότι q περιττός άρα $q + 1$ άρτιος), άτοπο. Τέλος, εαν $q \equiv 0 \pmod 3$ τότε επειδή ο q είναι πρώτος άρα $q = 3$ κι έτσι $p^{p+1} + q^{q+1} = 89$ που είναι πρώτος. Άρα η μοναδική δεκτή λύση είναι $p = 2,\ q = 3$ (ή $p = 3,\ q = 2$).

□

Παράδειγμα 2.7 *(Αρχιμήδης 1994) Για ποιές τιμές του λ έχει το πολυώνυμο $x^3 + 1995x^2 - 1994x + \lambda$ και τις τρεις ρίζες ακέραιες;*

Λύση:

Έστω ότι το πολυώνυμο έχει τρεις ρίζες ακέραιες τις ρ_1, ρ_2, ρ_3. Τότε από τους τύπους $Vieta$ έχουμε

$$A = \rho_1 + \rho_2 + \rho_3 = -1995 \equiv 0 \pmod 3 \quad (1)$$

και

$$B = \rho_1\rho_2 + \rho_2\rho_3 + \rho_3\rho_1 = -1994 \equiv 1 \pmod 3.$$

Λόγω της (1) έχουμε:

$\rho_1, \rho_2, \rho_3 \equiv 0 \pmod 3$ *ή* $\rho_1, \rho_2, \rho_3 \equiv 1 \pmod 3$ *ή* $\rho_1, \rho_2, \rho_3 \equiv -1 \pmod 3$ *ή* $\rho_1 \equiv 0 \pmod 3,\ \rho_2 \equiv 1 \pmod 3,\ \rho_3 \equiv -1 \pmod 3$ *(Οι υπόλοιπες περιπτώσεις είναι ισοδύναμες). Οπότε το B θα είναι $B \equiv 0 \pmod 3$ ή $B \equiv -1 \pmod 3$, αδύνατο αφού $B \equiv 1 \pmod 3$. Άρα δεν υπάρχει λ έτσι ώστε το πολυώνυμο να έχει τρεις ρίζες ακέραιες.*

□

Βασική Παρατήρηση - Τελευταίο Ψηφίο Αριθμού: Έαν $a \equiv \upsilon \pmod{10^n}$ και $0 \leq \upsilon < 10^n$, τότε τα τελευταία n ψηφία του αριθμού a είναι το υ με τόσα μηδενικά στην αρχή, όσα χρειάζονται ώστε το μήκος του αριθμού υ να είναι ίσο με n. Για παράδειγμα, επειδή $99^{2007} + 3 \equiv (-1)^{2007} + 3 = 2 \pmod{10^2}$, άρα ο αριθμός $99^{2007} + 3$ τελειώνει σε 02.

□

Παράδειγμα 2.8 *(ΕΜΕ 1988) Να βρεθούν τα δύο τελευταία ψηφία του αριθμού 2^{70}.*

Λύση:

Τί κάνουμε για να βρούμε για παράδειγμα το 2^{24} από το 2^{23}; Πολλαπλασιάζουμε το 2^{23} επί 2. Και αφού μας ενδιαφέρουν μόνο τα δύο τελευταία ψηφία πολλαπλασιάζουμε το 2 με αυτά και αν προκύψουν περισσότερα κρατάμε μόνο τα δύο. Έτσι,

υψώνοντας διαδοχικά και κρατώντας μόνο τα δύο τελευταία ψηφία, παίρνουμε την εξής ακολουθία τελευταίων ψηφίων.

$$02, \underbrace{[04, 08, 16, 32, 64, 28, 56, 12, 24, 48, 96, 92, 84, 68, 36, 72, 44, 88, 76, 52]}_{\text{επανάληψη ανά 20}},$$

$04, 08, 26, 32 \ldots$

Παρατηρούμε λοιπόν ότι τα δύο τελευταία ψηφία ξαναεμφανίζονται με περίοδο 20. Γράφοντας

$$2^{70} = (2^{20})^3 \cdot 2^{10},$$

συμπεραίνουμε ότι τα δύο τελευταία ψηφία του 2^{70} θα είναι τα ίδια με εκείνα του 2^{10}, άρα το 24.

Παρατήρηση: Για (κάποιου είδους) επαλήθευση μπορούμε να βρούμε το τελευταίο ψηφίο του ίδιου αριθμού χρησιμοποιώντας την περιοδικότητα του τελευταίου ψηφίου που είναι $4, [2, 4, 8, 6], 2, 4, \ldots$ και έτσι

$$2^{70} = (2^4)^{17} \cdot 2^2.$$

Το τελευταίο ψηφίο του 2^{70} θα είναι το ίδιο με εκείνο του 2^2 δηλαδή το 4.

□

Άσκηση: (Αρχιμήδης 1989) Να βρεθούν τα δύο τελευταία ψηφία του αριθμού 6^{1989}.

Παράδειγμα 2.9 *(Ολυμπιάδα Καναδά) Να βρεθεί το τελευταίο ψηφίο του αριθμού*

$$\underbrace{7^{7^{7^{\cdot^{\cdot^{\cdot^{7}}}}}}}_{1001\ 7-\text{άρια}}$$

Λύση:

Αρχικά παρατηρούμε ότι $7^4 \equiv 1 \pmod{10}$. *Επίσης, αφού*

$$7^{2k} \equiv 1 \pmod 4 \ \textit{και}\ 7^{2k+1} \equiv 3 \pmod 4$$

άρα

$$a := \underbrace{7^{7^{7^{\cdot^{\cdot^{\cdot^{7}}}}}}}_{1000\ 7-\text{άρια}} \equiv 3 \pmod 4 \ \textit{συνεπώς}\ a = 3k+4,\ k \in \mathbb{Z}.$$

Έτσι,

$$\underbrace{7^{7^{7^{\cdot^{\cdot^{\cdot^{7}}}}}}}_{1001\ 7-\text{άρια}} = 7^a = 7^{4k+3} = 7^3 \cdot (7^4)^k \equiv 7^3 \equiv 3 \pmod{10}.$$

□

Παράδειγμα 2.10 *(ΕΜΕ 1994) Να αποδείξετε ότι υπάρχουν φυσικοί αριθμοί που τα 4 τελευταία ψηφία τους είναι 1994 και διαιρούνται με το 1993.*

Απόδειξη:

Ο αριθμός αυτός είναι της μορφής

$$\begin{aligned}\overline{\underbrace{a_n a_{n-1} a_{n-2} \ldots a_4}_{A}\,1994} &= 10000A + 1994 = A(5 \cdot 1993 + 35) + 1993 + 1 \\ &\equiv 35 \cdot A + 1 \pmod{1993}\end{aligned}$$

Για να είναι $35 \cdot A + 1 \equiv 0 \pmod{1993}$ *θα πρέπει* $35A + 1 = 1993k,\ k \in \mathbb{Z}$ *δηλαδή* $A = 57k - \dfrac{2k+1}{35}$ (1) *δηλαδή πρέπει το* $2k+1$ *να είναι πολλαπλάσιο του 35. Για* $k = 17$ *έχουμε* $A = 968$. *Ο αριθμός λοιπόν 9681994 είναι πολλαπλάσιο του 1993. Υπάρχουν άπειροι τέτοιοι αριθμοί αφού η* (1) *έχει άπειρες λύσεις.*

□

Παράδειγμα 2.11 *Να αποδείξετε ότι για κάθε* $n \in \mathbb{N}$ *ισχύει*

$$17 | 3^{4n+2} + 2 \cdot 4^{3n+1}.$$

Απόδειξη:

Έχουμε $3^4 = 81 \equiv 13 \pmod{17}$. *Επομένως*

$$3^{4n+2} = 9 \cdot 81^n \equiv 9 \cdot 13^n \pmod{17}.$$

Επίσης $4^3 = 64 \equiv 13 \pmod{17}$, *οπότε* $4^{3n+1} = 4 \cdot (4^3)^n \equiv 4 \cdot 13^n \pmod{17}$. *Άρα*

$$3^{4n+2} + 2 \cdot 4^{3n+1} \equiv 9 \cdot 13^n + 8 \cdot 13^n = 17 \cdot 13^n \equiv 0 \pmod{17}.$$

Παρατήρηση: *Το παραπάνω πρόβλημα μπορεί να επιλυθεί και με τη μέθοδο της μαθηματικής επαγωγής.*

□

Παράδειγμα 2.12 *(Βαλκανιάδα 1990) Εαν* a_n *ακολουθία με* $a_1 = 1$, $a_2 = 3$ *και* $a_{n+2} = (n+3)a_{n+1} - (n+2)a_n$, *να βρεθούν τα* n *για τα οποία* $11 | a_n$.

Λύση:

$$\begin{aligned} a_{n+2} - a_{n+1} &= (n+2)(a_{n+1} - a_n) \\ a_{n+1} - a_n &= (n+1)(a_n - a_{n-1}) \\ &\vdots \\ a_3 - a_2 &= 3(a_2 - a_1) \\ a_2 - a_1 &= 2 \end{aligned}$$

Με πολλαπλασιασμό κατά μέλη των παραπάνω ισοτήτων προκύπτει ότι

$$a_{n+2} - a_{n+1} = (n+2)!$$

Αφού $a_1 = 1, a_2 = 3, a_3 = 9$ *άρα ο 11 δεν τους διαιρεί. Επίσης* $a_4 = 33$ *άρα* $11|a_4$. $a_5 = a_4 + 5!$ *και* $11 \nmid 5!$ *άρα* $11 \nmid a_5$. *Ομοίως* $11 \nmid a_6$ *και* $11 \nmid a_7$.

$$\begin{aligned} a_8 &= a_4 + 5! + 6! + 7! + 8! = a_4 + 5!(1 + 6 + 6 \cdot 7 + 6 \cdot 7 \cdot 8) \\ &= a_4 + 5!(7 \cdot 7 + 6 \cdot 7 \cdot 8) = a_4 + 5!7 \cdot 55, \end{aligned}$$

άρα $11|a_8$. *Πολύ εύκολα παίρνουμε* $11 \nmid a_9$ *ενώ* $11|a_{10}$ *αφού*

$$a_{10} = a_8 + 9! + 10! = a_8 + 9!(1 + 10).$$

$$a_{11} = a_{10} + 11!, \quad \textit{άρα} \ \ 11|a_{11}.$$

Για κάθε $n \in \mathbb{N}$ *με* $n \geq 11$ *ισχύει* $11|n!$ *συνεπώς* $11|a_n$ *αφού*

$$a_n = a_{10} + 11! + 12! + \cdots + n!$$

Τελικά, $11|a_n$ *εαν* $n = 4, n = 8$ *και* $n \geq 10$.

□

Θα συμπληρώσουμε την Πρόταση 1.10 με μερικές ακόμη βασικές προτάσεις γραμμένες με ισοτιμίες

Πρόταση 2.3 ***(Βασική Πρόταση)***

(*i*) *Αν ο* $p \neq 3$ *είναι πρώτος τότε* $p^2 \equiv 1 \pmod 3$.

(*ii*) *Αν ο* $p \neq 2$ *είναι πρώτος τότε* $p^2 \equiv 1 \pmod 8$.

(*iii*) *Αν ο* $p > 3$ *είναι πρώτος τότε* $p^2 \equiv 1 \pmod{12}$.

(*iv*) *Για κάθε πρώτο* $p > 3$ *ισχύει ότι* $p \equiv \pm 1 \pmod 6$ *(Αναδιατύπωση της Πρότασης* 1.10*).*

2.2 Συστήματα υπολοίπων

Ορισμός 2.2 *Ένα σύνολο* n *ακεραίων* $a_1, \ldots, a_n$ *καλείται* ***πλήρες σύστημα υπολοίπων*** $modn$, *εαν κάθε ένα από τα* $a_1, \ldots, a_n$ *είναι ισοϋπόλοιπο με ένα και μόνο αριθμό του συνόλου* $\{0, 1, \ldots, n-1\}$ [5].

[5] Δηλαδή τα $a_1, \ldots, a_n$ θα μπορούσαμε να τα θεωρήσουμε ως τα δυνατά υπόλοιπα της διαίρεσης ενός ακεραίου με το n αντί των $\{0, 1, \ldots, n-1\}$.

Μερικά συστήματα υπολοίπων $modn$ που μπορούμε να διακρίνουμε αμέσως είναι τα εξής:

(i) Ελάχιστο μη αρνητικό σύστημα υπολοίπων $modn$: $\{0, 1, \ldots, n-1\}$.

(ii) Ελάχιστο θετικό σύστημα υπολοίπων $modn$: $\{1, \ldots, n\}$

(iii) Πλήρες σύστημα των απόλυτα ελαχίστων υπολοίπων $modn$:

- Για n περιττό είναι το σύνολο
$$\left\{-\frac{n-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{n-1}{2}\right\}$$
- και για n άρτιο, το σύνολο
$$\left\{-\left(\frac{n}{2}-1\right), \ldots, -1, 0, 1, \ldots, \frac{n}{2}\right\}$$

Παράδειγμα 2.13 *Το σύνολο $S = \{14, 24, 9, -11, 34, 68, -21, 87\}$ είναι ένα πλήρες σύστημα υπολοίπων $mod8$. Πραγματικά, έχουμε*

$14 \equiv 6 \pmod 8$, $24 \equiv 0 \pmod 8$, $9 \equiv 1 \pmod 8$, $-11 \equiv 5 \pmod 8$,
$34 \equiv 2 \pmod 8$, $68 \equiv 4 \pmod 8$, $-21 \equiv 3 \pmod 8$, $87 \equiv 7 \pmod 8$.

Καθώς το σύνολο $\{0, 1, \ldots, 7\}$ είναι ένα πλήρες σύστημα υπολοίπων $mod8$ άρα το σύνολο S είναι επίσης ένα πλήρες σύστημα υπολοίπων $mod8$.

□

Παράδειγμα 2.14 *Το σύνολο $T = \{1, 2^2, 3^2, \ldots, n^2\}$ δεν είναι πλήρες σύστημα υπολοίπων $modn$.*

Απόδειξη:

Καθώς $(n-1)^2 - 1 = n^2 - 2n$, έχουμε $(n-1)^2 \equiv 1 \pmod n$ και επομένως δύο διαφορετικά στοιχεία του συνόλου T (τα $(n-1)^2$ και το 1) είναι ισουπόλοιπα με το ίδιο στοιχείο του συνόλου $\{0, 1, \ldots, n\}$ (με το 1).

□

Παράδειγμα 2.15 *(ΕΜΕ 1990) Να αναλυθεί σε γινόμενο η παράσταση $a^7 - a$. Αν ο a είναι φυσικός αριθμός, η παράσταση αυτή είναι πάντοτε διαιρετή με το 42.*

Απόδειξη:

$a^7 - a = a(a^6 - 1) = a(a^3 - 1)(a^3 + 1) = a(a-1)(a+1)(a^2 + a + 1)(a^2 - a + 1)$. *Εαν a φυσικός τότε $a, a+1$ διαδοχικοί φυσικοί άρα ο ένας είναι πολλαπλάσιο του 2. Επίσης $a-1, a, a+1$ τρεις διαδοχικοί φυσικοί άρα ο ένας είναι πολλαπλάσιο του 3 και επειδή $(2, 3) = 1$ έχουμε $6|a(a-1)(a+1)$. Επίσης $(6, 7) = 1$ άρα αρκεί να δείξουμε ότι η παράσταση είναι διαιρετή από το 7. Διακρίνουμε περιπτώσεις για*

το a. Εαν $a = 7k$, τότε φανερά το γινόμενο είναι πολλαπλάσιο του 7. Όμοια εαν $a = 7k + 1, 7k - 1$ τότε $7|a - 1, 7|a + 1$ αντίστοιχα, άρα διαιρεί όλη την παράσταση. Εαν $a = 7k+2$ ή $a = 7k-3$ τότε ο a^2+a+1 είναι πολλαπλάσιο του 7 και τέλος εαν $a = 7k + 3$ ή $a = 7k - 2$ ο $a^2 - a + 1$ είναι πολλαπλάσιο του 7. (Να υπενθυμίσουμε ότι το σύνολο $\{-3, -2, -1, 0, 1, 2, 3\}$ είναι ένα πλήρες σύστημα υπολοίπων $mod 7$).

□

Πρόταση 2.4 *Έστω $\{x_0, x_1, \ldots, x_{n-1}\}$ ένα πλήρες σύστημα υπολοίπων $mod n$ και $a, b \in \mathbb{Z}$ με $(a, n) = 1$. Τότε το σύνολο $\{ax_0 + b, \ldots, ax_{n-1} + b\}$ αποτελεί ένα πλήρες σύστημα υπολοίπων $mod n$.*

2.3 Θεώρημα Wilson - Θεωρήματα Fermat και Euler

Το παρακάτω Θεώρημα δίνει μία ικανή και αναγκαία συνθήκη για να είναι ένας φυσικός p πρώτος.

Θεώρημα 2.2 ***(Θεώρημα του Wilson)*** *Ένας ακέραιος $p > 1$ είναι πρώτος, αν και μόνο αν, ισχύει*

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

Πόρισμα 2.3 *Για κάθε πρώτο αριθμό p ισχύει*

$$(p-2)! \equiv 1 \pmod{p}.$$

Παράδειγμα 2.16 *Εαν $0 < s < p$, όπου p πρώτος αριθμός, να αποδειχθεί ότι ισχύει*

$$(s-1)!(p-s)! + (-1)^{s-1} \equiv 0 \pmod{p}.$$

Απόδειξη:

Για $s = 1$ η Πρόταση είναι αληθής λόγω του θεωρήματος Wilson. Υποθέτουμε ότι ισχύει

$$(s-2)!(p-(s-1))! + (-1)^{s-2} \equiv 0 \pmod{p}$$

οπότε

$$\begin{aligned}
& (s-2)!(p-s+1)! + (-1)^{s-2} \equiv 0 \pmod{p} \\
\Rightarrow\ & (s-2)!(p-s)!(p-s+1) + (-1)^{s-2} \equiv 0 \pmod{p} \\
\Rightarrow\ & (s-2)!(p-s)!p - (s-2)!(p-s)!(s-1) + (-1)^{s-2} \equiv 0 \pmod{p} \\
\Rightarrow\ & -(s-2)!(s-1)(p-s)! + (-1)^{s-2} \equiv 0 \pmod{p} \\
\Rightarrow\ & (s-1)!(p-s)! - (-1)^{s-2} \equiv 0 \pmod{p} \\
\Rightarrow\ & (s-1)!(p-s)! + (-1)^{s-1} \equiv 0 \pmod{p}
\end{aligned}$$

άρα η Πρόταση ισχύει για κάθε s με $0 < s < p$.

Παρατήρηση: *Η Πρόταση ισχύει και για $s = p$. Πράγματι,*

$$(p-1)!0! + (-1)^{p-1} = (p-1)! + 1 \equiv 0 \pmod{p}.$$

□

Πρόταση 2.5 *Έστω p ένας περιττός πρώτος. Τότε*

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 = \begin{cases} -1 \pmod{p}, \text{αν } p \equiv 1 \pmod{4} \\ 1 \pmod{p}, \text{αν } p \equiv 3 \pmod{4} \end{cases}$$

Παράδειγμα 2.17 *Έστω p πρώτος > 2. Να δείξετε ότι*

$$(p-1)! \equiv p-1 \pmod{1+2+\cdots+(p-1)}.$$

Απόδειξη:

Καθώς $1+2+\cdots+(p-1) = \dfrac{p(p-1)}{2}$, αρκεί να δείξουμε ότι

$$\frac{p(p-1)}{2} | (p-1)! - (p-1).$$

Από το Θεώρημα Wilson, έχουμε $(p-1)! \equiv -1 \pmod{p}$, απ' όπου $p|(p-1)!+1$ και επομένως $p|(p-1)! - (p-1)$. Επίσης, $(p-1)! - (p-1) = (p-1)\left((p-2)! - 1\right)$, απ' όπου $p-1|(p-1)! - (p-1)$. Επειδή $(p, p-1) = 1$ παίρνουμε

$$p(p-1)|(p-1)! - (p-1).$$

Καθώς ο πρώτος p είναι περιττός, έπεται ότι ο αριθμός $(p-1)/2$ είναι ακέραιος και κατά συνέπεια ισχύει

$$\frac{p(p-1)}{2} | (p-1)! - (p-1).$$

□

Από τα σπουδαιότερα θεωρήματα της στοιχειώδους Θεωρίας Αριθμών είναι το ακόλουθο, που είναι γνωστό ως Μικρό Θεώρημα του Fermat

Θεώρημα 2.3 ***(Θεώρημα Fermat)*** *Έστω p ένας πρώτος και a ένας ακέραιος με $p \nmid a$. Τότε*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Πόρισμα 2.4 *Έστω p ένας πρώτος. Τότε για κάθε $a \in \mathbb{Z}$ ισχύει*

$$a^p \equiv a \pmod{p}.$$

Πρόταση 2.6 *Εαν p είναι ένας πρώτος αριθμός και $a_1, \ldots, a_n$ ακέραιοι αριθμοί, τότε ισχύει*

$$(a_1 + \cdots + a_n)^p \equiv a_1^p + \cdots + a_n^p \pmod{p}.$$

Παράδειγμα 2.18 *Εαν για το φυσικό αριθμό n ισχύει*

$$5 \nmid n-1,\ 5 \nmid n,\ 5 \nmid n+1,$$

να αποδειχθεί ότι $5|n^2+1$.

Απόδειξη:

Επειδή $5 \nmid n$, απ' το Μικρό Θεώρημα του Fermat, ισχύει

$$n^4 \equiv 1 \pmod{5} \Rightarrow (n-1)(n+1)(n^2+1) \equiv 0 \pmod{5}$$

οπότε, επειδή $5 \nmid n-1,\ 5 \nmid n+1$ έχουμε το ζητούμενο.

□

Η ακόλουθη γενίκευση του (μικρού) θεωρήματος του Fermat είναι γνωστό ως Θεώρημα Euler.

Θεώρημα 2.4 ***(Θεώρημα Euler)*** *Έστω n ένας φυσικός > 1 και a ένας ακέραιος τέτοιος, ώστε $(a, n) = 1$. Τότε*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Παράδειγμα 2.19 *Να υπολογίσετε το υπόλοιπο της διαίρεσης του 10^{6k+4}, όπου $k \in \mathbb{N}$, με το 7.*

Λύση:

Καθώς $(10, 7) = 1$, το Θεώρημα Fermat δίνει $10^6 \equiv 1 \pmod{7}$, απ' όπου $10^{6k} \equiv 1 \pmod{7}$. Επίσης

$$10^4 \equiv 3^4 = 9^2 \equiv 2^2 = 4 \pmod{7}.$$

Άρα

$$10^{6k+4} \equiv 4 \pmod{7}$$

και επομένως το ζητούμενο υπόλοιπο είναι το 4.

□

Παράδειγμα 2.20 *Να δείξετε ότι ο αριθμός $\dfrac{7 \cdot 1968^{1968} - 3 \cdot 68^{78}}{10}$ είναι ακέραιος.*

Απόδειξη:

Αρκεί να δείξουμε ότι

$$10 | 7 \cdot 1968^{1968} - 3 \cdot 68^{78}.$$

Το Θεώρημα του Fermat δίνει $3^4 \equiv 1 \pmod{5}$. Επομένως

$$1968^{1968} \equiv 3^{1968} = \left(3^4\right)^{492} \equiv 1 \pmod{5}.$$

Επίσης, έχουμε

$$68^{78} \equiv 3^{78} = 9 \cdot \left(3^4\right)^{19} \equiv 9 \equiv 4 \pmod{5},$$

οπότε

$$7 \cdot 1968^{1968} - 3 \cdot 68^{78} \equiv 7 - 3 \cdot 4 = -5 \equiv 0 \pmod{5}.$$

Δηλαδή

$$5 | 7 \cdot 1968^{1968} - 3 \cdot 68^{78}.$$

Καθώς ο ακέραιος $7 \cdot 1968^{1968} - 3 \cdot 68^{78}$ είναι άρτιος και $(2, 5) = 1$ παίρνουμε

$$10 | 7 \cdot 1968^{1968} - 3 \cdot 68^{78}.$$

□

Παράδειγμα 2.21 *Να δείξετε ότι για κάθε ακέραιο n ισχύει*

$$2730|n^{13}-n.$$

Απόδειξη:

Η πρωτογενής ανάλυση του 2730 είναι $2730 = 2\cdot 3\cdot 5\cdot 7\cdot 13$. Καθώς οι ακέραιοι $2,3,5,7,13$ είναι πρώτοι μεταξύ τους ανά δύο αρκεί να δείξουμε ότι καθένας απ' αυτούς διαιρεί τον $n^{13}-n$.

Παρατηρούμε ότι αν ο n είναι άρτιος τότε και ο $n^{13}-n$ είναι άρτιος. Επίσης, εαν ο n είναι περιττός, τότε ο $n^{13}-n$ είναι άρτιος. Άρα για κάθε $n\in\mathbb{Z}$ ισχύει $2|n^{13}-n$. Από το Πόρισμα (2.4) έχουμε ότι για κάθε $n\in\mathbb{Z}$ ισχύουν

$$n^3\equiv n \pmod 3,\ n^5\equiv n \pmod 5,\ n^7\equiv n \pmod 7, n^{13}\equiv n \pmod{13}.$$

Άρα

$$\begin{aligned} n^{13} &\equiv n\cdot\left(n^3\right)^4 \equiv n\cdot n^4 = n^3\cdot n^2 \equiv n^3\equiv n \pmod 3\\ n^{13} &\equiv n^3\cdot\left(n^5\right)^2 \equiv n^3\cdot n^2 = n^5\equiv n \pmod 5\\ n^{13} &\equiv n^6\cdot n^7 \equiv n^6\cdot n = n^7\equiv n \pmod 7 \end{aligned}$$

οπότε

$$3|n^{13}-n,\ \ 5|n^{13}-n,\ \ 7|n^{13}-n,\ \ 13|n^{13}-n.$$

□

Παράδειγμα 2.22 *Έστω p πρώτος. Να αποδείξετε ότι $p|ab^p-ba^p$ για όλους τους ακεραίους a,b.*

Απόδειξη:

Ας σημειώσουμε αρχικά ότι $ab^p-ba^p = ab(b^{p-1}-a^{p-1})$.

Εαν $p|ab$ τότε $p|ab^p-ba^p$, ενώ εαν $p\not| ab$ τότε $(p,a)=(p,b)=1$ συνεπώς από το Μικρό Θεώρημα του Fermat έχουμε $b^{p-1}\equiv a^{p-1}\equiv 1 \pmod p$. Άρα $p|b^{p-1}-a^{p-1}$ που δίνει ότι $p|ab^p-ba^p$ και έτσι σε κάθε περίπτωση $p|ab^p-ba^p$.

□

Παράδειγμα 2.23 *(Εσωτερικός Διαγωνισμός Ε.Μ.Ε. 1995) Εαν p πρώτος αριθμός με $p>3$, να αποδείξετε ότι $20p|5^p-4^p-1$.*

Απόδειξη:

Εαν $p = 5$ τότε το αποτέλεσμα ισχύει. Έστω λοιπόν $p \geq 7$. Τότε $5^p - 4^p - 1 \equiv 0 - (-1)^p - 1 = 0 \pmod 5$
$5^p - 4^p - 1 \equiv 1^p - 0 - 1 = 0 \pmod 4$
και τέλος, λόγω του Πορίσματος 2.4, *παίρνουμε* $5^p \equiv 5 \pmod p$ *και* $4^p \equiv 4 \pmod p$ *άρα* $5^p - 4^p - 1 \equiv 5 - 4 - 1 = 0 \pmod p$ *και επειδή* $(4, 5, p) = 1$ *παίρνουμε ότι* $20p|5^p - 4^p - 1$.

Άσκηση: *(2ος Εσωτερικός διαγωνισμός Ε.Μ.Ε. 1989) Εαν p πρώτος να αποδείξετε ότι* $42p|3^p - 2^p - 1$. *(Υπόδειξη: Για να δείξετε ότι* $7|3^p - 2^p - 1$, *χρησιμοποιήστε την Πρόταση* 1.10*).*

□

Παράδειγμα 2.24 *Έστω $p \geq 7$ ένας πρώτος. Να αποδείξετε ότι ο αριθμός*

$$\underbrace{11\ldots1}_{p-1 \ \text{μονάδες}}$$

διαιρείται από το p.

Απόδειξη:

Έχουμε

$$\underbrace{11\ldots1}_{p-1 \ \text{μονάδες}} = \frac{10^{p-1} - 1}{9}$$

και το συμπέρασμα προκύπτει από το Μικρό Θεώρημα του Fermat [6].

□

Παράδειγμα 2.25 *Έστω p ένας πρώτος με $p > 5$. Να αποδείξετε ότι* $p^8 \equiv 1 \pmod{240}$.

Απόδειξη:

Η πρωτογενής ανάλυση του 240 είναι $240 = 2^4 \cdot 3 \cdot 5$. *Από το Μικρό Θεώρημα του Fermat, έχουμε* $p^2 \equiv 1 \pmod 3$ *και* $p^4 \equiv 1 \pmod 5$. *Επειδή ένας θετικός ακέραιος είναι πρώτος προς το* 2^4 *αν και μόνο αν είναι περιττός* $\phi(2^4) = 2^3$ *και έτσι λόγω του θεωρήματος Euler, έχουμε* $p^8 \equiv 1 \pmod{16}$. *Συνεπώς* $p^8 \equiv 1 \pmod m$ *για* $m = 3, 5, 16$ *των οποίων το Ε.Κ.Π. είναι το 240 και έτσι* $p^8 \equiv 1 \pmod{240}$.

Παρατήρηση: *Δεν είναι δύσκολο να δούμε ότι* $n^4 \equiv 1 \pmod{16}$ *για* $n \equiv \pm1, \pm3, \pm5, \pm7 \pmod{16}$. *Συνεπώς μπορούμε να βελτιώσουμε το αποτέλεσμα της άσκησης σε* $p^4 \equiv 1 \pmod{240}$ *για όλους τους πρώτους* $p > 5$.

□

[6] Ας σημειωθεί ότι $(10, p) = 1$

Παράδειγμα 2.26 *Να αποδείξετε ότι για κάθε άρτιο θετικό ακέραιο n ισχύει*

$$n^2 - 1 | 2^{n!} - 1.$$

Απόδειξη:

Θέτουμε $m = n + 1$. Θέλουμε τότε να δείξουμε ότι $m(m-2)|2^{(m-1)!} - 1$. Επειδή $\phi(m)|(m-1)!$, έχουμε $2^{\phi(m)} - 1 | 2^{(m-1)!} - 1$ και από το Θεώρημα του Euler έχουμε $m|2^{\phi(m)} - 1$. Έτσι, προκύπτει ότι $m|2^{(m-1)!} - 1$. Όμοια, $m-2|2^{(m-1)!} - 1$ και επειδή ο m είναι περιττός, παίρνουμε $(m, m-2) = 1$ άρα το ζητούμενο αποτέλεσμα.

□

Παράδειγμα 2.27 *Έστω p ένας πρώτος της μορφής $3k+2$ που διαιρεί το a^2+ab+b^2 για κάποιους ακεραίους a, b. Αποδείξτε ότι οι a, b είναι και οι δύο διαιρετοί από το p.*

Απόδειξη:

Ας υποθέσουμε ότι ο p δεν διαιρεί το a. Επειδή $p|a^2 + ab + b^2$, άρα ο p διαιρεί και το $a^3 - b^3 = (a-b)(a^2 + ab + b^2)$ συνεπώς $a^3 \equiv b^3 \pmod{p}$. Άρα

$$a^{3k} \equiv b^{3k} \pmod{p} \quad (1)$$

Συνεπώς ο p δεν διαιρεί ούτε το b. Από το Μικρό Θεώρημα του Fermat έχουμε $a^{p-1} \equiv b^{p-1} \equiv 1 \pmod{p}$, ή

$$a^{3k+1} \equiv b^{3k+1} \pmod{p} \quad (2)$$

Επειδή ο p είναι πρώτος προς το a, και λόγω των (1), (2) παίρνουμε $a \equiv b \pmod{p}$. Το τελευταίο σε συνδυασμό με το $a^2 + ab + b^2 \equiv 0 \pmod{p}$ δίνει $3a^2 \equiv 0 \pmod{p}$. Έτσι, αφού $p \neq 3$ άρα $p|a$, άτοπο.

□

Με όμοιο τρόπο όπως την παραπάνω να λύσετε την επόμενη, θέμα της 3ης Προκαταρτικής Φάσης της 13ης Εθνικής Μαθηματικής Ολυμπιάδας του 1996.

Άσκηση: Έστω p πρώτος αριθμός της μορφής $4k + 3$ ($k \in \mathbb{N}$). Εαν $x, y \in \mathbb{Z}$ και $p|x^2 + y^2$, να αποδείξετε ότι $p|x$ και $p|y$.

□

Παράδειγμα 2.28 *(Διεθνής Ολυμπιάδα Μαθηματικών 2005) Θεωρούμε την ακολουθία $a_1, a_2, \ldots$ που ορίζεται με τον τύπο*

$$a_n = 2^n + 3^n + 6^n - 1$$

για όλους τους θετικούς ακεραίους n. Να βρείτε όλους τους θετικούς ακέραιους που είναι πρώτοι προς όλους τους όρους της ακολουθίας.

Λύση:

Η απάντηση είναι μόνο το 1. Αρκεί να δείξουμε ότι κάθε πρώτος p διαιρεί το a_n για κάποιο θετικό ακέραιο n. Ας σημειωθεί ότι οι $p = 2$ και $p = 3$ διαιρούν τον $a_2 = 48$.

Ας υποθέσουμε τώρα ότι $p \geq 5$. Τότε από το Μικρό Θεώρημα του Fermat έχουμε $2^{p-1} \equiv 3^{p-1} \equiv 6^{p-1} \equiv 1 \pmod{p}$. Τότε

$$3 \cdot 2^{p-1} + 2 \cdot 3^{p-1} + 6^{p-1} \equiv 3 + 2 + 1 \equiv 0 \pmod{6}$$

δηλαδή $6(2^{p-2} + 3^{p-2} + 6^{p-2} - 1) \equiv 0 \pmod{p}$, δηλαδή $p | 6a_{p-2}$. Επειδή $(p, 6) = 1$, άρα ο a_{p-2} διαιρείται από το p όπως το θέλαμε.

□

2.4 Γραμμικές Ισοτιμίες

Ορισμός 2.3 *Έστω n ένας φυσικός > 1 και a, b δύο ακέραιοι. Μία ισοτιμία της μορφής*

$$ax \equiv b \pmod{n},$$

όπου x προσδιοριστέος ακέραιος, καλείται ***γραμμική ισοτιμία****. Λέμε ότι ο ακέραιος x_0 επαληθεύει ή πληροί την παραπάνω γραμμική ισοτιμία αν*

$$ax_0 \equiv b \pmod{n}.$$

Παρατήρηση: *Σε αυτή την περίπτωση, κάθε ακέραιος y με $x_0 \equiv y \pmod{n}$, επαληθεύει επίσης τη γραμμική ισοτιμία. Έτσι, θα καλούμε* ***λύση της ισοτιμίας*** $ax \equiv b \pmod{n}$ *οποιουδήποτε ακέραιο y με $x_0 \equiv y \pmod{n}$ όπου x_0 μία οποιαδήποτε λύση της αρχικής ισοτιμίας ή όπως λέμε ένας* ***αντιπρόσωπος*** *του συνόλου των λύσεων. Φυσικά, υπάρχουν και ισοτιμίες οι οποίες δεν έχουν καμία λύση. Π.χ. η $6x \equiv 1 \pmod{8}$ ($8|6x-1$, άτοπο αφού $6x-1$ περιττός).*

Παράδειγμα 2.29 *Να προσδιορίσετε τις λύσεις της γραμμικής ισοτιμίας $2x \equiv 10 \pmod{6}$.*

Λύση:

Καθώς $10 \equiv 4 \pmod{6}$, η γραμμική ισοτιμία απλουστεύεται και έχουμε $2x \equiv 4 \pmod{6}$. Οι ακέραιοι 0, 1, 2, 3, 4, 5 αποτελούν ένα πλήρες σύστημα υπολοίπων $mod 6$ κι έτσι παρατηρούμε τα εξής:

$$2 \cdot 0 = 0 \not\equiv 4 \pmod{6}, \quad 2 \cdot 1 = 2 \not\equiv 4 \pmod{6}, \quad 2 \cdot 2 \equiv 4 \pmod{6}$$

$$2 \cdot 3 = 6 \not\equiv 4 \pmod{6}, \quad 2 \cdot 4 = 8 \not\equiv 4 \pmod{6}, \quad 2 \cdot 5 = 10 \equiv 4 \pmod{6}.$$

Επομένως οι λύσεις είναι οι $x \equiv 2, 5 \pmod{6}$.

Παρατήρηση: *Παρατηρούμε ότι η μέθοδος αυτή που χρησιμοποιήσαμε στο παραπάνω παράδειγμα δεν είναι εύκολο να εφαρμοστεί για τον προσδιορισμό των λύσεων μιας γραμμικής ισοτιμίας με μεγάλο n διότι οι υπολογισμοί γίνουται αρκετά επίπονοι. Αυτός είναι και ο λόγος που θα μελετήσουμε αναλυτικότερα τις γραμμικές ισοτιμίες.*

Ορισμός 2.4 *Ονομάζουμε* ***αντίστροφο ενός αριθμού*** $a \ mod n$ *(αν υπάρχει) εκείνον του ακέραιο b για τον οποίο ισχύει $ab \equiv 1 \pmod{n}$. Τον συμβολίζουμε με a^{-1} ή με $\frac{1}{a}$.*

Για παράδειγμα ο αντίστροφος του 3 $mod 7$ είναι το 5 διότι $3 \cdot 5 \equiv 1 \pmod{7}$.

Πρόταση 2.7 *Έστω $a \in \mathbb{Z}$ με $a \neq 0$. Τότε υπάρχει το αντίστροφο του a, αν και μόνο αν, $(a, n) = 1$.*

Πρόταση 2.8 *Έστω $(a, n) = 1$. Τότε η γραμμική ισοτιμία $ax \equiv b \pmod{n}$ έχει ακριβώς μία λύση.*

Παράδειγμα 2.30 *Να υπολογίσετε τις λύσεις της γραμμικής ισοτιμίας* $137x \equiv 4 \pmod{102}$

Λύση:

Καθώς $137 \equiv 35 \pmod{102}$, *η γραμμική ισοτιμία απλουστεύεται και έχουμε* $35x \equiv 4 \pmod{102}$. *Με τον αλγόριθμο του Ευκλείδη βρίσκουμε ότι* $(102, 35) = 1$ *(άρα η παραπάνω ισοτιμία έχει μοναδική λύση) και συγκεκριμένα ότι* $-12 \cdot 102 + 35 \cdot 35 = 1$. *Επομένως* $35 \cdot 35 \equiv 1 \pmod{102}$. *Συνεπώς ο αντίστροφος του 35* $mod 102$, *είναι ο εαυτός του και έτσι, πολλαπλασιάζοντας και τα δύο μέλη της ισοτιμίας* $35x \equiv 4 \pmod{102}$ *με 35, παίρνουμε* $x \equiv 4 \cdot 35 \equiv 38 \pmod{102}$.

□

Παρατήρηση: Εαν $(a, n) = 1$ τότε για να προσδιορίσουμε τον αντίστροφο του a $mod n$ μπορούμε να δουλέψουμε και ως εξής: Έστω r ένας θετικός ακέραιος έτσι ώστε $a^r \equiv 1 \pmod{n}$ (π.χ. $r = \phi(n)$). Τότε το αντίστροφο του a $mod n$, είναι το a^{r-1} $mod n$. Συνεπώς εαν $(a, n) = 1$, τότε η λύση της γραμμικής ισοτιμίας $ax \equiv b \pmod{n}$ είναι η $x \equiv ba^{r-1} \pmod{n}$.

Παράδειγμα 2.31 *Θα λύσουμε τη γραμμική ισοτιμία* $7x \equiv 8 \pmod{30}$.

Λύση:

Καθώς $(7, 30) = 1$, *η γραμμική ισοτιμία έχει μοναδική λύση. Έχουμε* $7^{\phi(30)} \equiv 1 \pmod{30}$. *Όμως* $\phi(30) = 8$ *άρα η τάξη του 7* $mod 30$ [7], *διαιρεί το* $\phi(30) = 8$. *Δοκιμάζοντας παίρνουμε* $7^2 = 49 \equiv 19 \equiv -11 \pmod{30}$ *και* $7^4 \equiv (-11)^2 = 121 \equiv 1 \pmod{30}$. *Άρα* $ord_{30}(7) = 4$ *και έτσι, πολλαπλασιάζοντας και τα δύο μέλη της γραμμικής ισοτιμίας με* 7^3 *παίρνουμε*

$$x \equiv 7^3 8 \equiv (-77)8 \equiv (-17)8 \equiv 13 \cdot 8 = 104 \equiv 14 \pmod{30}.$$

□

Θεώρημα 2.5 *Η γραμμική ισοτιμία* $ax \equiv b \pmod{n}$ *έχει λύση αν και μόνο αν* $d|b$ *όπου* $d = (a, n)$. *Ειδικώτερα, εαν ο ακέραιος* x_0 *επαληθεύει τη γραμμική ισοτιμία, τότε υπάρχουν ακριβώς* d *λύσεις οι*

$$x \equiv x_0, x_0 + \frac{n}{d}, x_0 + 2\frac{n}{d}, \ldots, x_0 + (d-1)\frac{n}{d} \pmod{n}$$

Παράδειγμα 2.32 *Να υπολογίσετε τις λύσεις της γραμμικής ισοτιμίας*

$$21x \equiv 6 \pmod{33}.$$

Λύση:

[7] Εαν $(a, n) = 1$ τότε **τάξη** του a $mod n$ ονομάζουμε τον ελάχιστο ακέραιο r για τον οποίο ισχύει $a^r \equiv 1 \pmod{n}$. Την συμβολίζουμε με $ord_n(a)$ και αποδεικνύεται (πολύ εύκολα) ότι $ord_n(a)|\phi(n)$.

Έχουμε $(21, 33) = 3$ *και* $3|6$. *Σύμφωνα με το παραπάνω Θεώρημα, η ισοτιμία έχει 3 λύσεις. Ένας ακέραιος* x *επαληθεύει την παραπάνω ισοτιμία αν και μόνο αν* $7x \equiv 2 \pmod{11}$. *Οι ακέραιοι 0,1,...,10 αποτελούν ένα πλήρες σύστημα υπολοίπων* $mod 11$. *Δοκιμάζουμε καθένα από αυτούς στην παραπάνω γραμμική ισοτιμία και διαπιστώνουμε ότι ο* 5 *την επαληθεύει. Άρα μοναδική λύση της ισοτιμίας* $7x \equiv 2 \pmod{11}$ *είναι η* $x \equiv 5 \pmod{11}$. *Ο 5 επαληθεύει και την* $21x \equiv 6 \pmod{33}$. *Επομένως, σύμφωνα με το παραπάνω Θεώρημα οι λύσεις της ισοτιμίας* $21x \equiv 6 \pmod{33}$ *είναι οι* $x \equiv 5, 16, 27 \pmod{33}$.

□

Παράδειγμα 2.33 *Να υπολογίσετε τις λύσεις της ισοτιμίας*

$$2086x \equiv -1624 \pmod{1729}.$$

Λύση:

Καθώς $2086 \equiv 357 \pmod{1729}$ *και* $-1624 \equiv 105 \pmod{1729}$, *μπορούμε να απλοποιήσουμε τη γραμμική ισοτιμία και έτσι έχουμε* $357x \equiv 105 \pmod{1729}$. *Με τον αλγόριθμο του Ευκλείδη παίρνουμε ότι* $(357, 1729) = 7$ *καθώς επίσης ότι* $7 = 19 \cdot 1729 - 92 \cdot 357$. *Οπότε* $-92 \cdot 357 \equiv 7 \pmod{1729}$. *Πολλαπλασιάζοντας και τα δύο μέλη της ισοτιμίας με 15 παίρνουμε* $(-92 \cdot 15) \cdot 357 \equiv 105 \pmod{1729}$. *Σύμφωνα με το παραπάνω Θεώρημα οι 7 λύσεις της γραμμικής ισοτιμίας είναι οι εξής*

$$x \equiv 349, 596, 843, 1090, 1337, 1584, 102 \pmod{1729}.$$

□

2.5 Συστήματα γραμμικών ισοτιμιών

Ορισμός 2.5 *Καλούμε* ***λύση*** *του συστήματος*

$$a_1 x \equiv b_1 \pmod{n_1}$$

$$\vdots$$

$$a_k x \equiv b_k \pmod{n_k}$$

κάθε ακέραιο που επαληθεύει ***κάθε μία*** *από τις γραμμικές ισοτιμίες. Για παράδειγμα, μία λύση του συστήματος* $3x \equiv 9 \pmod{10}$, $2x \equiv 1 \pmod{5}$ *είναι ο ακέραιος 3. Ένα σύστημα ενδέχεται να μην έχει λύση, ακόμη και στην περίπτωση, όπου κάθε μία από τις γραμμικές ισοτιμίες που το αποτελούν έχει λύση. Όταν λέμε ότι ένα σύστημα έχει λύση την* $a \bmod c$ *εννοούμε ότι έχει ως λύσεις όλους τους ακεραίους που είναι ισοϋπόλοιποι με το* $a \bmod c$. *Δύο συστήματα καλούνται* ***ισοδύναμα*** *όταν έχουν το ίδιο σύνολο λύσεων.*

Θεώρημα 2.6 ***(Κινέζικο Θεώρημα Υπολοίπων ή Θεώρημα Υπολοίπων του Νικόμαχου)*** *Έστω $b_1, \ldots, b_k$ ακέραιοι και $n_1, \ldots, n_k$ φυσικοί > 1, πρώτοι μεταξύ τους ανά δύο. Τότε το σύστημα γραμμικών ισοτιμιών*

$$\begin{aligned} x &\equiv b_1 \pmod{n_1} \\ x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ x &\equiv b_k \pmod{n_k} \end{aligned}$$

έχει μοναδική λύση $mod n_1 \cdots n_k$, την οποία βρίσκουμε ως εξής:

Ορίζουμε $N_j = n_1 \cdots n_{j-1} n_{j+1} \cdots n_k$ και βρίσκουμε την λύση M_j της ισοτιμίας $N_j x \equiv 1 \pmod{n_j}$ [8] *(είτε με τον Ευκλείδειο αλγόριθμο είτε με απλές δοκιμές εαν οι αριθμοί είναι μικροί). Τότε η λύση του συστήματος είναι η $x_0 \pmod{n_1 \cdots n_k}$, όπου*

$$x_0 = b_1 N_1 M_1 + \cdots + b_k N_k M_k.$$

Παράδειγμα 2.34 *Να λυθεί το σύστημα*

$$x \equiv 2 \pmod{5},\ x \equiv 3 \pmod{7},\ x \equiv 4 \pmod{11}.$$

Λύση:

Επειδή οι ακέραιοι $5, 7, 11$ είναι πρώτοι μεταξύ τους ανά δύο, σύμφωνα με το Κινέζικο Θεώρημα Υπολοίπων, το παραπάνω σύστημα έχει μοναδική λύση $mod 385$.

$$N_1 = 7 \cdot 11 = 77,\ N_2 = 5 \cdot 11 = 55,\ N_3 = 5 \cdot 7 = 35.$$

Έτσι, παίρνουμε τις γραμμικές ισοτιμίες

$$77x \equiv 1 \pmod{5},\ 55x \equiv 1 \pmod{7},\ 35x \equiv 1 \pmod{11},$$

ή ισοδύναμα

$$2x \equiv 1 \pmod{5},\ 6x \equiv 1 \pmod{7},\ 2x \equiv 1 \pmod{11},$$

οι οποίες έχουν τις λύσεις

$$x \equiv 3 \pmod{5},\ x \equiv 6 \pmod{7},\ x \equiv 6 \pmod{11},$$

αντίστοιχα. Επομένως, η λύση του συστήματος είναι

$$x_0 \equiv 77 \cdot 3 \cdot 2 + 55 \cdot 6 \cdot 3 + 35 \cdot 6 \cdot 4 = 2292 \equiv 367 \pmod{385}.$$

□

[8] καθώς οι φυσικοί $n_1, \ldots, n_k$ είναι πρώτοι μεταξύ τους ανά δύο έχουμε $(N_j, n_j) = 1$ για $j = 1, \ldots, k$, άρα η ισοτιμία έχει μοναδική λύση $mod n_j$.

Μία γενίκευση του Κινέζικου Θεωρήματος Υπολοίπων είναι η παρακάτω

Θεώρημα 2.7 *Το σύστημα γραμμικών ισοτιμιών*

$$\begin{aligned} x &\equiv b_1 \pmod{n_1} \\ x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ x &\equiv b_k \pmod{n_k} \end{aligned}$$

έχει λύση, αν και μόνο αν, $(n_i, n_j)|b_i - b_j$ *για κάθε* i, j *με* $i \neq j$*. Αν* x_0 *είναι μία λύση του συστήματος, τότε το σύνολο λύσεών του είναι η* $x_0 \pmod{[n_1 \cdots n_k]}$.

Στα παρακάτω παραδείγματα φαίνεται και ο τρόπος με τον οποίο επιλύουμε τα γραμμικά συστήματα με τη βοήθεια του παραπάνω θεωρήματος.

Παράδειγμα 2.35 *Να λυθεί το σύστημα των ισοτιμιών*

$$x \equiv 1 \pmod{15}, \quad x \equiv 7 \pmod{18}.$$

Λύση:

Έχουμε $(15, 18) = 3$ *και* $3|1 - 7$*. Επίσης* $[15, 18] = 90$*. Οπότε, σύμφωνα με το παραπάνω Θεώρημα το σύστημα έχει μοναδική λύση* $mod 90$*. Αρκεί λοιπόν, να προσδιορίσουμε μία λύση του για να έχουμε όλο το σύνολο λύσεων.*

Θέτουμε στη δεύτερη γραμμική ισοτιμία $x = 1 + 15y$ *και παίρνουμε*

$$1 + 15y \equiv 7 \pmod{18}.$$

Επομένως $15y \equiv 6 \pmod{18}$ *απ' όπου* $5y \equiv 2 \pmod{6}$*. Εύκολα διαπιστώνουμε ότι ο* 4 *επαληθεύει την παραπάνω ισοτιμία. Συνεπώς η μοναδική λύση του συστήματος είναι η*

$$x = 1 + 15 \cdot 4 \equiv 61 \pmod{90}.$$

□

Παράδειγμα 2.36 *Να λυθεί το σύστημα των ισοτιμιών*

$$x \equiv 3 \pmod{8}, \quad x \equiv 11 \pmod{20}, \quad x \equiv 1 \pmod{15}.$$

Λύση:

Έχουμε $(8, 20) = 4,\ (8, 15) = 1,\ (15, 20) = 5$ *και* $4|3 - 11,\ 1|3 - 1,\ 5|1 - 11$*. Επίσης* $[8, 20, 15] = 120$*. Άρα σύμφωνα με το παραπάνω Θεώρημα προκύπτει ότι το σύστημα έχει μοναδική λύση* $\pmod{120}$.

Θεωρούμε το σύστημα των δύο πρώτων γραμμικών ισοτιμιών

$$x \equiv 3 \pmod{8}, \quad x \equiv 11 \pmod{20}, \quad [8, 20] = 40.$$

Θέτουμε $x = 3 + 8y$ *στη δεύτερη ισοτιμία και έχουμε*

$$3 + 8y \equiv 11 \pmod{20},$$

απ' όπου

$$y \equiv 1 \pmod{5},$$

άρα

$$x \equiv 3 + 8 = 11 \pmod{40}.$$

Άρα το αρχικό μας σύστημα είναι ισοδύναμο με το σύστημα

$$x \equiv 11 \pmod{40}, \quad x \equiv 1 \pmod{15}.$$

Θέτουμε $x = 11 + 40y$ *στη δεύτερη ισοτιμία και παίρνουμε*

$$11 + 40y \equiv 1 \pmod{15}.$$

Οπότε $y \equiv 2 \pmod{3}$. *Άρα η ζητούμενη λύση είναι*

$$x \equiv 11 + 2 \cdot 40 = 91 \pmod{120}.$$

□

Όμως το Θεώρημα 2.7 δε μας βοηθάει για να λύνουμε συστήματα της μορφής

$$a_i x \equiv b_i, \quad i = 1, \ldots, k.$$

Ας θεωρήσουμε λοιπόν το σύστημα των γραμμικών ισοτιμιών

$$a_1 x \equiv b_1 \pmod{n_1}$$

$$\vdots$$

$$a_k x \equiv b_k \pmod{n_k}.$$

Για να έχει το σύστημα αυτό λύση, πρέπει κάθε μία από τις γραμμικές ισοτιμίες να έχει λύση, που ισοδυναμεί με τις σχέσεις $d_i | b_i$ όπου $d_i = (a_i, n_i), \quad i = 1, \ldots, k$. Ας υποθέσουμε ότι $d_i | b_i, \quad i = 1, \ldots, k$. Τότε υπάρχουν $A_i, B_i, N_i \in \mathbb{Z}$ με $(A_i, N_i) = 1$ έτσι ώστε $a_i = d_i A_i, \; b_i = d_i B_i, \; n_i = d_i N_i, \quad i = 1, \ldots, k$. Οπότε το παραπάνω σύστημα είναι ισοδύναμο με το εξής

$$A_1 x \equiv B_1 \pmod{N_1}$$

$$\vdots$$

$$A_k x \equiv B_k \pmod{N_k}.$$

Καθώς $(A_i, N_i) = 1$, η γραμμική ισοτιμία $A_i x \equiv B_i \pmod{N_i}$ έχει μοναδική λύση την $x \equiv C_i \pmod{N_i}$, $i = 1, \ldots, k$. Έτσι, το αρχικό μας σύστημα είναι ισοδύναμο με το σύστημα

$$\begin{aligned} x &\equiv C_1 \pmod{N_1} \\ &\vdots \\ x &\equiv C_k \pmod{N_k}. \end{aligned}$$

το οποίο μπορούμε να μελετήσουμε με τις μεθόδους, που περιγράψαμε στα προηγούμενα.

Παράδειγμα 2.37 *Να λυθεί το σύστημα των ισοτιμιών*

$$8x \equiv 4 \pmod{20}, \quad 15x \equiv 10 \pmod{35}, \quad 9x \equiv 12 \pmod{39}.$$

Λύση:

Έχουμε $(8, 20) = 4,\ (15, 35) = 5,\ (9, 39) = 3$. *Καθώς* $4|4,\ 5|10,\ 3|12$, *κάθε μία από τις γραμμικές ισοτιμίες του συστήματος έχει λύση. Το σύστημα είναι ισοδύναμο με το εξής*

$$2x \equiv 1 \pmod{5}, \quad 3x \equiv 2 \pmod{7}, \quad 3x \equiv 4 \pmod{13}.$$

Οι λύσεις των γραμμικών ισοτιμιών δίνουν το σύστημα

$$x \equiv 3 \pmod{5}, \quad x \equiv 3 \pmod{7}, \quad x \equiv 10 \pmod{13}.$$

Οι ακέραιοι $5, 7, 13$ *είναι πρώτοι μεταξύ τους ανά δύο. Επομένως το σύστημα έχει μοναδική λύση* $mod 455$. *Θα λύσουμε πρώτα το σύστημα*

$$x \equiv 3 \pmod{5}, \quad x \equiv 3 \pmod{7}.$$

Παρατηρούμε ότι ο 3 είναι μία λύση του συστήματος. Επειδή $(5, 7) = 1$, *η (μοναδική) λύση του συστήματος είναι η* $x \equiv 3 \pmod{35}$. *Συνεπώς το αρχικό σύστημα είναι ισοδύναμο με το σύστημα*

$$x \equiv 3 \pmod{35}, \quad x \equiv 10 \pmod{13}.$$

Για να το λύσουμε θέτουμε $x = 3 + 35y$ *στη δεύτερη γραμμική ισοτιμία και έχουμε* $3 + 35y \equiv 10 \pmod{13}$, *απ' όπου* $9y \equiv 7 \pmod{13}$. *Εύκολα διαπιστώνουμε ότι η λύση αυτής της γραμμικής ισοτιμίας είναι η* $y \equiv 8 \pmod{13}$ *και επομένως η λύση του συστήματος είναι η*

$$x \equiv 3 + 8 \cdot 35 = 283 \pmod{455}.$$

□

Ασκηση 1: (Πρόβλημα του $Branmagupta$, 7ος αιώνας μ.Χ.) Όταν παίρνουμε αυγά από ένα καλάθι ανά 2,3,4,5,6 κάθε φορά, τότε μένουν αντίστοιχα : 1,2,3,4,5 αυγά στο καλάθι. Όταν όμως παίρνουμε ανά 7 δεν μένει κανένα. Να υπολογισθεί ο ελάχιστος αριθμός αυγών που πρέπει να περιέχει το καλάθι.

Ασκηση 2: (Το πρόβλημα του κινέζου μάγειρα) Σ' ένα πλιάτσικο 17 πειρατές αρπάζουν ένα μπαούλο γεμάτο χρυσές λίρες (ίσης αξίας). Αποφασίζουν να τις μοιραστούν σε ίσα μέρη και να δώσουν το υπόλοιπο στον κινέζο μάγειρα του καραβιού τους. Σ' αυτόν αντιστοιχούν 3 λίρες. Σε μία ναυμαχία σκοτώνονται έξι από αυτούς. Στο μάγειρα αντιστοιχούν τότε 4 λίρες. Κατόπιν σε ένα ναυάγιο σώζονται μόνο έξι απ' αυτούς, το μπαούλο και ο μάγειρας. Στο μάγειρα αντιστοιχούν τότε 5 λίρες. Κατόπιν ο μάγειρας δηλητηριάζει τους πειρατές και παίρνει το μπαούλο. Πόσες λίρες τουλάχιστον περιέχει το μπαούλο;

3 Το μικρό Θεώρημα του Fermat και η γενίκευσή του

Θεώρημα 3.1 *Εάν p πρώτος και a ένας φυσικός αριθμός τότε:*

(i) $a^p \equiv a \pmod{p}$

(ii) *(Το μικρό θεώρημα του Fermat) εάν $(a,p)=1$ τότε*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Απόδειξη:

Σχόλιο: Υπάρχουν πολλές αποδείξεις του μικρού Θεωρήματος του Fermat . Επιλέξαμε αυτή η οποία χτίζει βήμα-βήμα την απόδειξη και είναι μέσα στις δυνατότητες ενός μαθητή με ενδιαφέρον για τα μαθηματικά.

(i) Θα κάνουμε χρήση της μαθηματικής επαγωγής. Για $a=1$ ισχύει τετριμμένα. Ας υποθέσουμε ότι $p|a^p-a$. Θα αποδείξουμε ότι $p|(a+1)^p-(a+1)$.

Απ'τον τύπο του διωνύμου του Newton [9], έχουμε

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a + 1.$$

Συνεπώς

$$(a+1)^p - a^p - 1 = \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a.$$

Όμως το p διαιρεί το δεξί μέλος [10] άρα και το αριστερό. Συνδιάζοντας αυτό με την επαγωγική υπόθεση, έχουμε ότι

$$p \mid [(a+1)^p - a^p - 1] + (a^p - a) = (a+1)^p - (a+1).$$

(ii) Προφανώς από το (i) έχουμε $p \mid a^p - a \Rightarrow p \mid a(a^{p-1}-1)$ που σε συνδιασμό με το $(a,p)=1$ δίνει το ζητούμενο

$$p \mid a^{p-1} - 1.$$

[9] $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.

[10] Η απόδειξη αυτού αφήνεται ως άσκηση στους αναγνώστες. Τα δύο βήματα που χρειάζονται για την απόδειξη είναι:

(a) Το γινόμενο n διαδοχικών ακεραίων διαιρείται από το $n!$ και

(b) εαν p πρώτος, τότε οι $\binom{p}{1}, \binom{p}{2}, \ldots, \binom{p}{p-1}$ διαιρούνται από το p.

□

Παράδειγμα 3.1 (i) *Αφού* $(2, 11) = 1$ *και ο* 11 *είναι πρώτος, θα είναι* $2^{11-1} \equiv 1 \pmod{11}$. *Πράγματι όταν το* $2^{10} = 1024$ *διαιρεθεί με το* 11, *αφήνει υπόλοιπο* 1.

(ii) *Με μεγαλύτερα νούμερα: π.χ. οι αριθμοί* $2^3 * 5 * 11^2 = 4840$ *και* 101 *είναι πρώτοι μεταξύ τους και αφού ο* 101 *είναι πρώτος, έχουμε* $4840^{100} \equiv 1 \pmod{101}$.

□

Πόρισμα 3.1 *Εαν* p *πρώτος και* a *ένας φυσικός αριθμός με* $(a, p) = 1$, *και* d *είναι ο μικρότερος εκθέτης για τον οποίο ισχύει*

$$a^d \equiv 1 \pmod{p}$$

τότε $d \mid p - 1$.

Η απόδειξη αφήνεται ως άσκηση στους αναγνώστες.

□

4 Η συνάρτηση του Euler

Για δοσμένο φυσικό αριθμό $n \geq 1$, συμβολίζουμε με $\varphi(n)$ το πλήθος των φυσικών αριθμών των μικρότερων ή ίσων του n που είναι πρώτοι προς τον n. Με αυτό τον τρόπο ορίσαμε μία συνάρτηση

$$\varphi : \mathbb{N} \to \mathbb{N}$$

με

$$\varphi(n) = \sharp\{k \in \mathbb{N} \backslash k \leq n \ \text{ και } \ (a, n) = 1\}^{(11)}.$$

Παράδειγμα 4.1 $\varphi(9) = 6$ *διότι οι* 6 *αριθμοί* $1, 2, 4, 5, 7, 8$ *είναι μικρότεροι και πρώτοι προς το* 9.

□

Ιδιότητες της συνάρτησης Euler

(i) $\varphi(1) = 1$

[11] Το σύμβολο $\sharp\{\ldots\}$ συμβολίζει το πλήθος των στοιχείων του συνόλου $\{\ldots\}$.

(ii) Είναι φανερό ότι εάν $n = p$ πρώτος, τότε $\varphi(p) = p - 1$ καθώς όλοι οι αριθμοί οι μικρότεροι του p, δηλαδή οι $1, 2, \ldots, p-1$, είναι πρώτοι προς τον p.

(iii) Η συνάρτηση φ είναι πολλαπλασιαστική δηλαδή εαν $(m, n) = 1$, τότε

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$$

(Για παράδειγμα $\varphi(21) = \varphi(3 \cdot 7) = \varphi(3) \cdot \varphi(7) = (3-1) \cdot (7-1) = 12$).

(iv) Εαν p πρώτος, τότε

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$$

[Απλά λογαριάστε το πλήθος των αριθμών που είναι μικρότεροι ή ίσοι του p^k και είναι πρώτοι προς τον p^k (ή αντίθετα, αφαιρέστε τα πολλαπλάσια του p τα οποία σε πλήθος είναι p^{k-1})].

(v) Γενικά, εαν $n = p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l}$ η ανάλυση του n σε πρώτους (διακεκριμένους μεταξύ τους) παράγοντες, χρησιμοποιήστε την ιδιότητα (iii) για να δείξετε ότι:

$$\begin{aligned} \varphi(n) &= p_1^{k_1-1}(p_1-1) \cdot p_2^{k_2-1}(p_2-1) \cdots p_l^{k_l-1}(p_l-1) \\ &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_l}\right) \\ &= n\prod_{i=1}^{l}\left(1-\frac{1}{p_i}\right) \end{aligned}$$

□

Παράδειγμα 4.2 *Είναι*

$$\begin{aligned} \varphi(1200) &= \varphi(2^2 \cdot 3^4 \cdot 5^2) = 1200\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) \\ &= 1200 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 320 \end{aligned}$$

Άρα με αυτό τον τρόπο βρήκαμε, με πολύ απλό τρόπο, ότι το πλήθος των φυσικών που είναι μικρότεροι απ'το 1200 *και πρώτοι προς αυτόν είναι* 320.

□

Παράδειγμα 4.3 (i) *Να αποδειχθεί ότι οι φυσικοί αριθμοί* $n \in \mathbb{N}\backslash\{4\}$ *για τους οποίους ισχύει* $\varphi(n) \equiv 2 \pmod 4$ *είναι είτε της μορφής* $n = p^k$ *είτε της μορφής* $n = 2p^k$, *όπου* $k \in \mathbb{N}$ *και ο* p *ένας πρώτος με* $p \equiv 3 \pmod 4$.

(ii) *Να αποδειχθεί ότι δεν υπάρχει φυσικός αριθμός* n *με* $\varphi(n) = 14$.

Λύση:

(i) *Θα δείξουμε ότι στην ανάλυση του* n *σε πρώτους αριθμούς, δε γίνεται να υπάρχουν περισσότεροι από δύο διακεκριμένοι πρώτοι αριθμοί οι οποίοι να είναι* ≥ 3. *Γι'αυτό, ας υποθέσουμε αντίθετα, ότι*

$$n = p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l}, \;\; p_i \geq 3 \; \forall i = 1, \ldots, l \;\; \textit{και} \;\; l \geq 2.$$

Τότε

$$\varphi(n) = p_1^{k_1 - 1}(p_1 - 1) p_2^{k_2 - 1}(p_2 - 1) \cdots p_l^{k_l - 1}(p_l - 1)$$

Όμως, καθώς $l \geq 2$, *υπάρχουν τουλάχιστον* 2 *άρτιοι παράγοντες μεταξύ των* $(p_1 - 1), (p_2 - 1), \ldots, (p_l - 1)$. *Άρα* $\varphi(n) \equiv 0 \pmod 4$, *άτοπο.*

Άρα

$$n = 2^r p^k.$$

Εαν $r \geq 3$ *(*$r \neq 2$ *διότι* $n \neq 4$*) , τότε*

$$\varphi(n) = 2^{r-1} p^{k-1}(p - 1) \equiv 0 \pmod 4, \;\; \textit{άτοπο.}$$

Άρα, $r = 0, 1$ *(*$r \neq 2$ *διότι* $n \neq 4$*) συνεπώς*

$$n = p^k \;\; \textit{ή} \;\; n = 2p^k.$$

Έμεινε να δείξουμε ότι $p \equiv 3 \pmod 4$. *Εαν αντίθετα ήταν* $p \equiv 1 \pmod 4$[12], *τότε θα είχαμε (και στις δύο περιπτώσεις για τον* n*)*

$$\varphi(n) = p^k(p - 1) \equiv 0 \pmod 4, \;\; \textit{άτοπο.}$$

Έτσι αποδείχθηκε η ζητούμενη.

(ii) *Πρόκειται για άμεση εφαρμογή του πρώτου ερωτήματος.*

□

Δεν σταματάνε όμως εδώ οι πολύ σημαντικές εφαρμογές της συνάρτησης του Euler . Υπάρχουν πολλές ακόμη εφαρμογές και σπουδαία θεωρήματα που την χρησιμοποιούν. Κλείνουμε αυτή την παράγραφο με το Θεώρημα του Euler , χωρίς απόδειξη (καθώς υπάρχει σε πολλά κλασσικά βιβλία Θεωρίας Αριθμών), το οποίο αποτελεί γενίκευση του μικρού Θεωρήματος του Fermat .

Θεώρημα 4.1 *(Θεώρημα Euler) Εαν* a *είναι φυσικός πρώτος προς τον* n *τότε ισχύει*

$$a^{\varphi(n)} \equiv 1 \pmod n.$$

Παρατήρηση: Εαν $n = p$, τότε παίρνουμε το μικρό Θεώρημα του Fermat .

[12] Προφανώς αφού $p \neq 2$, άρα p περιττός οπότε δεν γίνεται να είναι $p \equiv 0, 2 \pmod 4$

Παράδειγμα 4.4 *Επειδή* $\varphi(9) = 6$, *και* $(9, 4) = 1$ *έχουμε ότι* $4^6 \equiv 1 \pmod 9$.

Πόρισμα 4.1 *Εαν* a *είναι φυσικός πρώτος προς τον* n, *και* $k \equiv l \pmod{\varphi(n)}$, *τότε*

$$a^k \equiv a^l \pmod n.$$

Απόδειξη:

Ας υποθέσουμε χωρίς βλάβη της γενικότητας ότι $k \geq l$. Τότε λόγω της $k \equiv l \pmod{\varphi(n)}$, συμπεραίνουμε ότι υπάρχει ακέραιος π τέτοιος ώστε $k = \pi\varphi(n) + l$ άρα, λόγω και του θεωρήματος του Euler , έχουμε

$$a^k = a^l \left(a^{\varphi(n)}\right)^l \equiv a^l \cdot 1^l \equiv a^l \pmod n$$

□

5 Εφαρμογή του Θεωρήματος Euler σε μία κατηγορία ασκήσεων

Ας δώσουμε μερικές ασκήσεις και τον τρόπο με τον οποίο μπορούμε να εργαστούμε ώστε να τις λύσουμε μεθοδικά και εύκολα με τα παραπάνω εφόδια .

Μία άσκηση της 6ης Εθνικής Μαθηματικής Ολυμπιάδας του 1989 ήταν:

Παράδειγμα 5.1 *Για ποιές τιμές του* $n \in \mathbb{N}$ *ο αριθμός* $1^n + 2^n + 3^n$ *διαιρείται με το* 7 ;

Σχόλιο: *Θα παρουσιάσουμε αρχικά (*1*η Λύση) την εξαιρετική λύση της συναδέλφου Ε. Μήτσιου που δημοσιεύθηκε τότε στο περιοδικό «Διάσταση» και κατόπιν (*2*η Λύση) κάνουτας χρήση της παραπάνω θεωρίας.*

1η Λύση (Ε. Μήτσιου)

Για $n = 1$ *η δοθείσα παράσταση δεν διαιρείται με το* 7, *για* $n = 2$ *διαιρείται με το* 7 *και για* $n = 3$ *δεν διαιρείται με το* 7.

- *Για* $n = 2k$ *έχουμε*

$$1^{2k} + 2^{2k} + 3^{2k} = 1 + 4^k + 9^k = 1 + 4^k + \pi o\lambda.7 + 2^k = \pi o\lambda.7 + 1 + 2^k + 4^k \quad (1)$$

{ *Εάν* $k = 3l$ *τότε η* (1) *γίνεται*

$$\begin{aligned} \pi o\lambda.7 + 1 + 2^{3l} + 4^{3l} &= \pi o\lambda.7 + 1 + 8^l + 64^l \\ &= \pi o\lambda.7 + 1 + \pi o\lambda.7 + 1^l + \pi o\lambda.7 + 1^l \\ &= \pi o\lambda.7 + 3 \end{aligned}$$

{ *Εάν* $k = 3l + 1$ *τοτε η* (1) *γίνεται*

$$\begin{aligned} \pi o\lambda.7 + 1 + 2^{3l+1} + 4^{3l+1} &= \pi o\lambda.7 + 1 + 2 \cdot 8^l + 1 \cdot 64^l \\ &= \pi o\lambda.7 + 1 + 2(\pi o\lambda.7 + 1^l) \\ &+ 4(\pi o\lambda.7 + 1^l) \\ &= \pi o\lambda.7 + 1 + 2 + 4 = \pi o\lambda.7 \end{aligned}$$

{ *Εάν* $k = 3l + 2$ *τοτε η* (1) *γίνεται*

$$\begin{aligned} \pi o\lambda.7 + 1 + 2^{3l+2} + 4^{3l+2} &= \pi o\lambda.7 + 1 + 4 \cdot 8^l + 16 \cdot 64^l \\ &= \pi o\lambda.7 + 1 + \pi o\lambda.7 + 4 \cdot 1^l \\ &+ \pi o\lambda.7 + 16 \cdot 1^l \\ &= \pi o\lambda.7 + 1 + 4 + 16 = \pi o\lambda.7 \end{aligned}$$

Άρα εάν $n = 2k$, *τότε πρέπει* $k = 3l + 1$ *ή* $k = 3l + 2$, *δηλαδή* $n = 6l + 2$ *ή* $n = 6l + 4$.

- *Για* $n = 2k + 1$ *έχουμε*

$$\begin{aligned} 1^{2k+1} + 2^{2k+1} + 3^{2k+1} &= 1 + 2 \cdot 4^k + 3 \cdot 9^k = 1 + 2 \cdot 4^k + \pi o\lambda.7 + 3 \cdot 2^k \\ &= \pi o\lambda.7 + 2(1 + 2^k + 4^k) + 2^k - 1 \end{aligned}$$

Βρήκαμε ότι αν $k = 3l + 1$ *ή* $k = 3l + 2$, *τότε* $1 + 2^k + 4^k = \pi o\lambda.7$, . *Θα εξετάσουμε το* $2^k - 1$ *για* $k = 3l + 1$ *ή* $k = 3l + 2$.

{ *Αν* $k = 3l + 1$ *τότε*

$$2^k - 1 = 2^{3l+1} - 1 = 2 \cdot 8^l - 1 = \pi o\lambda.7 + 2 \cdot 1^l - 1 = \pi o\lambda.7 + 1$$

άρα όχι $\pi o\lambda.7$

{ *Αν* $k = 3l + 2$ *τότε*

$$2^k - 1 = 2^{3l+2} - 1 = 4 \cdot 8^l - 1 = \pi o\lambda.7 + 4 \cdot 1^l - 1 = \pi o\lambda.7 + 3$$

άρα όχι $\pi o\lambda.7$

Άρα το $2^k - 1$ *είναι* $\pi o\lambda.7$ *για* $k = 3l$ *γιατί*

$$2^{3l} - 1 = 8^l - 1 = \pi o\lambda.7 + 1^l - 1 = \pi o\lambda.7$$

όμως τότε το $1^k + 2^k + 4^k$ *δεν είναι* $\pi o\lambda.7$. *Άρα τελικά πρέπει ο* n *να είναι* $\pi o\lambda.2$ *και όχι* $\pi o\lambda.3$, *δηλαδή πρέπει* $n = 6k + 2$ *ή* $n = 6k + 4$ *ή αλλιώς* $n = 6k \pm 2$.

2**η Λύση** *Αφού το* 7 *είναι πρώτος αριθμός και* $(7,2) = 1 = (7,3)$*, από το Μικρό Θεώρημα του Fermat ισχύει ότι*

$$2^{7-1} \equiv 1 \pmod 7 \text{ οπότε } 2^6 \equiv 1 \pmod 7$$

$$3^{7-1} \equiv 1 \pmod 7 \text{ οπότε } 3^6 \equiv 1 \pmod 7$$

Άρα, το υπόλοιπο του 2^n *με το* 7*, θα επαναλαμβάνεται το πολύ κάθε* 6 *βήματα και μάλιστα το βήμα της επανάληψης (Πόρισμα* 3.1*), θα είναι διαιρέτης του* 6 [13] *(δηλαδή* $1, 2, 3, 6$*). Όμοια και για το υπόλοιπο της διαίρεσης του* 3^n *με το* 7*. Αυτό που μένει λοιπόν να κάνουμε για να δούμε εποπτικά τα παραπάνω, είναι ένας απλός πίνακας δυνάμεων για να βρούμε το* $1^n + 2^n + 3^n$ *για τις διάφορες τιμές του* υ*, όπου* $n = 6k + \upsilon$*,* $\upsilon = 0, 1, 2, 3, 4, 5$*, θα χρειαστούν το πολύ* 6 *βήματα για να δούμε τα δυνατά υπόλοιπα των* 2^n *και* 3^n *με το* 7*.*

$\upsilon = n \pmod 6$	0	1	2	3	4	5	*επανάληψη ανα*
$1^n \pmod 7$	1	1	1	1	1	1	1
$2^n \pmod 7$	1	2	4	1	2	4	3
$3^n \pmod 7$	1	3	2	6	4	5	6
$1^n + 2^n + 3^n \pmod 7$	3	6	0	1	0	3	–

Τώρα φαίνεται καθαρά από τον παραπάνω πίνακα οτι ο αριθμός $1^n + 2^n + 3^n$ *είναι πολλαπλάσιο του* 7*, όταν το* n *έχει τη μορφή* $n = 6k + 2$ *ή* $6k + 4$*. (Ή ακόμη, ότι ο αριθμός* $1^n + 2^n + 3^n$*, διαιρούμενος με το* 7 *δεν αφήνει ποτέ υπόλοιπο* $2, 4, 5$*.)*

□

Η μέθοδος αυτή μπορεί να εφαρμοστεί και για πολυπλοκότερα προβλήματα τα οποία, όπως το παρακάτω, που χωρίς συγκεκριμένη στρατηγική, είναι δύσκολο να επιλυθούν.

Παράδειγμα 5.2 *Να βρεθούν όλα τα δυνατά υπόλοιπα της διαίρεσης του αριθμού* $A = 2 \cdot 3^n + 3 \cdot 7^{n+1} + 5^{3n+1} - 7$ *δια του* 11*.*

Λύση

Σχόλιο: Απλά θα προσαρμόσουμε τα δεδομένα στον πίνακα προσθέτοντας δύο ακόμη γραμμες για το $n+1$ και το $3n+1$ που εμφανίζονται ως εκθέτες στη δοθείσα παράσταση.

Αφού $(11,3) = (11,7) = (11,5) = 1$, ο ρυθμός επανάληψης των $3^n, 7^n, 5^n$ θα είναι διαιρέτης του $\varphi(11) = 10$ (δηλαδή η επανάληψη τώρα θα είναι είτε ανά $1, 2, 5$ ή 10) και έτσι ο αντίστοιχος πίνακας γίνεται [14]

[13] Σημειώστε πόσο φυσιολογικά έρχεται τώρα, ότι οι περιπτώσεις που πρέπει να πάρουμε για το n, είναι ως προς το υπόλοιπο που αφήνει όταν διαιρεθεί με το 6, κάτι που φαίνεται και στην 1η λύση.

[14] Προφανώς δεν χρειάζονται οι γραμμές των $3^n \pmod{11}, 5^n \pmod{11}, 7^n \pmod{11}$ απλά μπαίνουν για να γίνει μια πρώτη σύγκριση.

$n \pmod{10}$	0	1	2	3	4	5	6	7	8	9	επανάληψη ανα
$n+1 \pmod{10}$	1	2	3	4	5	6	7	8	9	0	–
$3n+1 \pmod{10}$	1	4	7	0	3	6	9	2	5	8	–
$3^n \pmod{11}$	1	3	9	5	4	1	3	9	5	4	5
$2 \cdot 3^n \pmod{11}$	2	6	7	10	8	2	6	7	10	8	5
$7^n \pmod{11}$	1	7	5	2	3	10	4	6	9	8	10
$3 \cdot 7^{n+1} \pmod{11}$	10	4	6	9	8	1	7	5	2	3	10
$5^n \pmod{11}$	1	5	3	4	9	1	5	3	4	9	5
$5^{3n+1} \pmod{11}$	5	9	3	1	4	5	9	3	1	4	5
A	10	1	9	2	2	1	4	8	6	8	–

Συμπεραίνουμε ότι εαν ο n είναι της μορφής $n = 10k+2$, τότε όταν ο A διαιρεθεί με το 11, αφήνει υπόλοιπο 1. Έτσι, είναι έτοιμη μία (απαιτητική) άσκηση που μπορεί να δειχτεί πλέον με επαγωγή:

Άσκηση: Να αποδειχθεί ότι εαν το τελευταίο ψηφίο του αριθμού n είναι το 2, τότε ο A αφήνει υπόλοιπο 1 όταν διαιρεθεί με το 11.

□

Σχόλια:

1. Ασκήσεις όπως η παραπάνω αποδεικνύονται με επαγωγή εαν γνωρίζουμε όμως το αποτέλεσμα της διαίρεσης με τον αριθμό. Για παράδειγμα παίρνω μία άσκηση από το βιβλίο του αείμνηστου Θ.Ν. Καζαντζή, Θεωρία Αριθμών, Β΄ Έκδοση, Εκδόσεις Μαθηματική Βιβλιοθήκη, Θεσσαλονίκη 1998.

   Άσκηση Να δείξετε ότι εαν n φυσικός ≥ 1 τότε η παράσταση $2^{4n+1} - 2^{2n} - 1$ διαιρείται από το 9. Κατασκευάζοντας τον αντίστοιχο πίνακα, θα διαπιστώσουμε ότι αφού $(2, 9) = 1$ και $\varphi(9) = 6$, τα υπόλοιπα της διαίρεσης του 2^n με το 9 θα επαναλαμβάνονται ανά αριθμό που είναι διαιρέτης του 6. Μπορεί για το συγκεκριμένο παράδειγμα (που η λύση με επαγωγή είναι πολύ εύκολη), η διαδικασία κατασκευής του πίνακα να είναι επίπονη, αλλά φανταστείτε ότι θα μπορούσατε με διάφορες δοκιμές να ανακαλύψετε μία τόσο συμμετρικά φτιαγμένη άσκηση!

2. Με τον παραπάνω τρόπο μπορείτε να κατασκευάσετε τις δικές σας ασκήσεις όπως την ακόλουθη που κατασκεύασα πριν από λίγο καιρό πειραματιζόμενος μπροστά στον υπολογιστή με την παραπάνω μέθοδο:

Άσκηση 1: Να δείξετε ότι εαν $n \neq 0 \pmod{6}$ τότε

$$1^n + 2^n + 3^n + 4^n + 5^n + 6^n \equiv 0 \pmod{7}.$$

Η λύση της είναι αρκετά απλή εαν κατασκευάσετε τον γνωστό πίνακα και αφήνεται ως άσκηση.

□

Ως γενίκευση αυτής της παρατήρησης μου γεννήθηκε το ερώτημα εαν ισχύει γενικά και το έθεσα ως προβληματισμό στο Forum [15]:

Άσκηση 2: Εαν $n \neq 0 \pmod{(p-1)}$ τότε

$$\sum_{i=1}^{p-1} i^n \equiv 0 \pmod{p}$$

Λύση: Λύση σε αυτό το πρόβλημα έδωσε (με εξαιρετικό τρόπο) ο Στέλιος, την οποία παραθέτω παρακάτω για να την απολαύσετε.

Κατάρχήν παρατηρούμε ότι

$$\begin{aligned} p^{n+2} &= p + \binom{n+2}{1}\left[1+2+\cdots+(p-1)\right] \\ &+ \binom{n+2}{2}\left[1^2+2^2+\cdots+(p-1)^2\right] \\ &+ \cdots + \binom{n+2}{n+1}\left[1^{n+1}+2^{n+1}+\cdots+(p-1)^{n+1}\right] \end{aligned}$$

Άρα αν $p \mid [1^k + 2^k + \cdots + (p-1)^k]$ για κάθε $k = 1, 2, \cdots, n$, όπου $n \in \{1, 2, \cdots, (p-3)\}$, τότε $p \mid [(n+2)(1^{n+1} + 2^{n+1} + \cdots + (p-1)^{n+1})]$

και επειδή $n \in \{1, 2, \cdots, (p-3)\}$ θα ισχύει ότι ο p δεν διαιρεί το $(n+2)$. Συνεπώς $p \mid [1^{n+1} + 2^{n+1} + \cdots + (p-1)^{n+1}]$.

Επαγωγικά λοιπόν αποδεικνύουμε ότι επειδή $p \mid [1+2+\cdots+(p-1)] = \dfrac{p(p-1)}{2}$ θα ισχύει ότι $p \mid [1^k + 2^k + \cdots + (p-1)^k]$ για κάθε $k = 1, 2, \cdots, (p-2)$

και αφού $a^{(p-1)m+u} \equiv (a^{p-1})^m a^u \equiv a^u \pmod{p}$ για κάθε a με $(a, p) = 1$ [16]

προκύπτει ότι $p \mid [1^n + 2^n + \cdots + (p-1)^n]$ για κάθε $n \in \mathbb{N}^*$ με $n \not\equiv 0 \pmod{p-1}$, όπου p πρώτος μεγαλύτερος του 2.

Σχόλιο: Στη βιβλιογραφία, έμαθα αργότερα, αναφέρεται ως Θεώρημα Chevalley-Warning του οποίου η απόδειξη δεν γίνεται συνήθως με στοιχειώδη τρόπο αφού τα μέσα που διαθέτει η Θεωρία Ομάδων, είναι πολύ ισχυρά και βγάζουν το επιθυμητό αποτέλεσμα της άσκησης σε δύο γραμμές. Αυτή όμως είναι και η αξία της λύσης του Στέλιου. Ότι με στοιχειώδη μέσα αποδεικνύει αυτή την Πρόταση.

□

Ακολουθεί μία πάρα πολύ καλή άσκηση από Μαθηματικό Διαγωνισμό με την οποία τελειώνουμε το άρθρο. Πριν δώσουμε την εκφώνηση δίνουμε ένα πολύ βασικό Λήμμα:

[15] $www.mathlinks.ro/Forum/viewtopic.php?t = 112234$

[16] διότι από το Μικρό Θεώρημα του Fermat ισχύει ότι $a^{p-1} \equiv 1 \pmod{p}$ αν $(a, p) = 1$

Λήμμα 5.1 *Κάθε πρώτος αριθμός $p > 3$, είναι της μορφής $6k+1$ ή $6k+5$ (Πάρτε ένα οποιοδήποτε φυσικό αριθμό n. Τότε $n = 6k + \upsilon,\ \upsilon = 0, 1, \ldots, 5$ και δείξτε (φανερό) ότι $\upsilon \neq 2, 3, 4$ εαν n πρώτος)*

Παράδειγμα 5.3 *(2ος Εσωτερικός Διαγωνισμός ΕΜΕ 1989)*

Να αποδειχθεί ότι εαν p πρώτος, τότε $42p \mid 3^p - 2^p - 1$.

Απόδειξη:

Αφού $42p = 2\cdot 3\cdot 7\cdot p$ άρα αρκεί να δείξουμε οτι ο $A = 3^p - 2^p - 1$ είναι πολλαπλάσιο των πρώτων αριθμών $2, 3, 7, p$ [17]

(i) **Με το 2:** *Φανερά ο A είναι άρτιος άρα $A \equiv 0 \pmod 2$.*

(ii) **Με το 3:** $A = 3^p - (2^p + 1) = 3^p - (2 + 1)(2^{p-1} + 2^{p-2} + \cdots + 2 + 1) \equiv 0 \pmod 3$

(iii) **Με το p:** *Απ'το Θεώρημα $3.1(i)$ έχουμε*

$$3^p \equiv 3 \pmod p \ \text{ και } \ 2^p \equiv 2 \pmod 2$$

Άρα

$$A = 3^p - 2^p - 1 \equiv 3 - 2 - 1 = 0 \pmod p.$$

(iv) **Με το 7:**

Σύμφωνα λοιπόν με το Λήμμα 5.1, κάθε πρώτος αριθμός είναι της μορφής $p = 6k + 1$ ή $p = 6k + 5$.

- *Εαν $p = 6k + 1$ τότε λόγω του Μικρού Θεωρήματος του Fermat , αφού $(2, 7) = 1$, είναι*

  $$2^6 \equiv 1 \pmod 7 \ \text{ άρα } \ 2^{6k} \equiv 1 \pmod 7 \ \text{ άρα } \ 2^{6k+1} \equiv 2 \pmod 7$$

  Όμοια, αφού $(3, 7) = 1$ έχουμε ότι

  $$3^{6k+1} \equiv 3 \pmod 7$$

  και έτσι

  $$A = 3^p - 2^p - 1 \equiv 3 - 2 - 1 = 0 \pmod 7$$

- *Εαν $p = 6k + 5$ τότε λόγω όμοια όπως παραπάνω έχουμε*

  $$2^{6k+5} \equiv 2^5 = 32 \equiv 4 \pmod 7$$

  και

  $$3^{6k+5} \equiv 3^5 = 243 \equiv 5 \pmod 7$$

  Άρα τελικά

  $$A = 3^p - 2^p - 1 \equiv 5 - 4 - 1 = 0 \pmod 7$$

  Σε κάθε περίπτωση λοιπόν έχουμε $A \equiv 0 \pmod 7$

[17] Θυμίζουμε οτι εάν p, q είναι δύο διακεκριμένοι πρώτοι αριθμοί και n φυσικός, με $p \mid n$ και $q \mid n$ τότε $p \cdot q \mid n$.

Σχόλιο: *Παρατηρήστε ότι* $(2,7) = 1 = (3,7)$ *και* $\varphi(7) = 6$ *άρα τα υπόλοιπα της διαίρεσης των* 2^k *και* 3^k *με το* 7*, σύμφωνα με όσα είπαμε παραπάνω, επαναλαμβάνονται ανά έναν αριθμό ο οποίος είναι διαιρέτης του* 6*. Φτιάξτε λοιπόν τον αντίστοιχο πίνακα, όπως έγινε στα παραπάνω παραδείγματα, για να δείξετε ότι στις περίπτωσεις* $p = 6k+1, p = 6k+5$ *έχουμε ότι* $A \equiv 0 \pmod 7$*. Δικαιολογείται λοιπόν με τα παραπάνω ο λόγος για τον οποίο χρειάστηκε να εργαστούμε* $\mod 6$ *και ο οποίος μας οδήγησε να καταλήξουμε στο (γενικό και πολύ χρήσιμο) Λήμμα* 5.1.

□