

Μάθημα Θεωρίας Αριθμών

Ε.Μ.Ε

1. Να αποδειχθεί ότι δεν υπάρχει θετικός ακέραιος n έτσι ώστε οι αριθμοί $n+3$ και n^2+3n+3 να είναι ταυτόχρονα τέλειοι κύβιοι.

2. Να αποδειχθεί ότι για κάθε μη αρνητικό ακέραιο n ο αριθμός

$$A = 5^{5^{n+1}} + 5^{5^n} + 1$$

δεν είναι πρώτος.

3. Να αποδειχθεί ότι για οποιουδήποτε θετικούς ακέραιους a, b ο αριθμός

$$N = (36a + b)(36b + a)$$

δεν μπορεί να είναι δύναμη του 2.

4. Να λυθεί στους θετικούς ακέραιους η εξίσωση

$$x^{x+y} = y^{y-x}.$$

5. Ορίζουμε τους αριθμούς

$$T_n = 2^{2^n} + 1,$$

με $n \in \mathbb{N}^*$. Να αποδειχθεί ότι αν $m \neq n$ τότε οι αριθμοί T_m, T_n είναι σχετικά πρώτοι.

6. Να βρεθούν όλα τα ζεύγη ακεραίων (x, y) που είναι τέτοια, ώστε

$$x^6 + 3x^3 + 1 = y^4.$$

7. Να βρεθούν όλα τα ζεύγη μη-μηδενικών ακεραίων (x, y) που είναι τέτοια, ώστε

$$(x^2 + y)(x + y^2) = (x - y)^3.$$

8. Να προσδιορισθούν οι θετικοί ακέραιοι n για τους οποίους ο αριθμός

$$n^4 + 4^n$$

είναι πρώτος.

9. Να βρεθούν όλα τα ζεύγη ακεραίων (x, y) που είναι τέτοια, ώστε

$$x^3 + x^2y + xy^2 + y^3 = 8(x^2 + xy + y^2 + 1).$$

10. Αν οι θετικοί ακέραιοι x, y ικανοποιούν την σχέση

$$2x^2 + x = 3y^2 + y,$$

τότε να αποδειχθεί ότι οι αριθμοί $x - y$ και $2x + 2y + 1$ είναι τέλεια τετράγωνα.

Σιλουανός Μπραζίτικος

Λύσεις

1. Αν υποθέσουμε ότι και οι δύο αριθμοί είναι τέλειοι κύβοι, τότε τέλειος κύβος είναι και το γινόμενό τους. Το γινόμενό τους ισούται με

$$K = (n+3)(n^2+3n+3) = n^3 + 6n^2 + 12n + 9.$$

Παρατηρούμε όμως ότι

$$(n+2)^3 < K < (n+3)^3,$$

για κάθε θετικό ακέραιο n . Έπεται ότι ο K δεν μπορεί να είναι τέλειος κύβος. $\square$

2. Θέτουμε $5^{5^n} = x$. Τότε

$$A = x^5 + x + 1 = x^5 - x^2 + x^2 + x + 1 = (x^2 + x + 1)(x^3 - x^2 + 1).$$

Εύκολα βλέπουμε ότι καθεμιά παρένθεση είναι μεγαλύτερη του 1 για $5^{5^n} = x$ επομένως ο A δεν είναι πρώτος. $\square$

3. Έστω ότι

$$(1) \quad (36a+b)(36b+a) = 2^k,$$

για κάποιο ακέραιο $k \geq 1$. Υποθέτουμε ότι $d = (a, b)$ και γράφουμε $a = dx$, $b = dy$, με $(x, y) = 1$. Τότε η (1) δίνει ότι

$$d^2(36x+y)(36y+x) = 2^k.$$

Έπεται ότι ο d είναι δύναμη του 2. Επομένως μένει να λύσουμε την εξίσωση

$$(2) \quad (36x+y)(36y+x) = 2^s,$$

για κάποιο $s \geq 0$. Παρατηρούμε ότι ο s δεν μπορεί να είναι μηδέν. Επιπλέον $(36x+y, 36y+x) | 2^s$ άρα είναι κάποια δύναμη του δύο ή είναι ίσος με 1. Αν είναι κάποια δύναμη του 2, τότε $2|x$ και $2|y$, που είναι άτοπο. Επομένως ο $(36x+y, 36y+x) = 1$. Τότε η (2) συνεπάγεται ότι είτε ο $36x+y$ είτε ο $36y+x$ είναι ίσος με 1. Αυτό είναι άτοπο και το ζητούμενο έπεται. $\square$

4. Αν $y < x$ τότε προφανώς δεν έχουμε λύσεις. Αν $y = x$, τότε έχουμε τα ζεύγη λύσεων $(x, y) = (1, 1)$ και $(x, y) = (-1, -1)$.

Υποθέτουμε τώρα ότι $y > x$. Παρατηρούμε αρχικά ότι

$$p|x \Leftrightarrow p|y.$$

Έπεται ότι

$$x = p_1^{\alpha_1} \dots p_k^{\alpha_k} \text{ και } y = p_1^{\beta_1} \dots p_k^{\beta_k}.$$

Αντικαθιστώντας στην εξίσωση και χρησιμοποιώντας τη μοναδικότητα της παραγοντοποίησης στο $\mathbb{Z}$, συμπεραίνουμε ότι

$$\alpha_i(x+y) = \beta_i(y-x),$$

για κάθε $i = 1, \dots, k$. Έπεται ότι $\alpha_i < \beta_i$ και επομένως $x|y$. Γράφουμε $y = sx$. Αντικαθιστώντας στην αρχική εξίσωση παίρνουμε και ύστερα από τις απλοποιήσεις παίρνουμε

$$x^2 = s^{s-1}.$$

Από την τελευταία συμπεραίνουμε ότι είτε $s = t^2$, είτε $s - 1 = 2z$. Στην πρώτη περίπτωση έχουμε την οικογένεια λύσεων

$$(x, y) = (t^{t^2-1}, t^{t^2+1}), \quad t \in \mathbb{N}^*.$$

Στη δεύτερη περίπτωση έχουμε την οικογένεια λύσεων

$$(x, y) = ((2z + 1)^z, (2z + 1)^{z+1}), \quad s \in \mathbb{N}.$$

□

5. Παρατηρούμε ότι

$$\begin{aligned} T_n - 2 &= 2^{2^n} - 1 = (2^{2^{n-1}} - 1)(2^{2^{n-1}} + 1) \\ &= (2^{2^{n-2}} - 1)(2^{2^{n-2}} + 1)(2^{2^{n-1}} + 1) \\ &\dots \\ &= T_{n-1}T_{n-2} \dots T_1. \end{aligned}$$

Έπεται ότι αν κάποιος αριθμός d διαιρεί τον T_m και τον T_n τότε διαιρεί και το 2. Τότε πρέπει $d = 1$ γιατί οι T_n είναι περιττοί, που είναι και το ζητούμενο. □

6. Συμπληρώνοντας το τετράγωνο, γράφουμε την εξίσωση στη μορφή

$$\begin{aligned} \left(x^3 + \frac{3}{2}\right)^2 - \frac{5}{4} &= y^4 \Rightarrow \\ (2x^3 + 3)^2 - 4y^4 &= 5 \Rightarrow \\ (2x^3 + 3 - 2y^2)(2x^3 + 3 + 2y^2) &= 5. \end{aligned}$$

Προκύπτουν έτσι τέσσερα συστήματα

$$\begin{aligned} \begin{cases} 2x^3 - 2y^2 + 3 = 1, \\ 2x^3 + 2y^2 + 3 = 5, \end{cases} & \begin{cases} 2x^3 - 2y^2 + 3 = -1, \\ 2x^3 + 2y^2 + 3 = -5, \end{cases} \\ \begin{cases} 2x^3 - 2y^2 + 3 = 5, \\ 2x^3 + 2y^2 + 3 = 1, \end{cases} & \begin{cases} 2x^3 - 2y^2 + 3 = -5, \\ 2x^3 + 2y^2 + 3 = -1. \end{cases} \end{aligned}$$

Τελικά τα μοναδικά ζεύγη λύσεων είναι τα $(0, 1), (0, -1)$. □

7. Η εξίσωση είναι ισοδύναμη με την ακόλουθη

$$2y^2 + (x^2 - 3x)y + 3x^2 + x = 0.$$

Η παραπάνω έχει ακέραιες λύσεις αν και μόνο αν η διακρίνουσά της είναι τέλειο τέλειο τετράγωνο. Δηλαδή αν

$$\Delta = x(x + 1)^2(x - 8) = z^2,$$

για κάποιο μη αρνητικό ακέραιο z . Έπεται ότι για κάποιο μη αρνητικό ακέραιο w ισχύει

$$x(x - 8) = w^2 \Rightarrow (x - 4)^2 - w^2 = 16 \Rightarrow (x - w - 4)(x + w - 4) = 16.$$

Διακρίνοντας τις περιπτώσεις βρίσκουμε ότι τα ζεύγη λύσεων είναι

$$(x, y) \in \{(-1, -1), (8, -10), (9, -6), (9, -21)\}.$$

□

8. Αν $n = 1$, τότε ο αριθμός είναι πρώτος. Αν n είναι άρτιος τότε ο αριθμός είναι πολλαπλάσιο του 2 επομένως πρέπει $n = 2k + 1$. Τότε γράφουμε

$$\begin{aligned} n^4 + 4^n &= n^4 + 4^{2k+1} = n^4 + 4 \cdot 2^{4k} \\ &= n^4 + 4m^4 \\ &= n^4 + 4m^4 + (2mn)^2 - (2mn)^2 \\ &= (n^2 + 2m^2 - 2mn)(n^2 + 2m^2 + 2mn), \end{aligned}$$

όπου $m = 2^k$. Για $n > 1$ εύκολα βλέπουμε ότι κάθε παρένθεση είναι μεγαλύτερη του 1, άρα ο αριθμός δεν είναι πρώτος. Συνεπώς μοναδική λύση είναι η $n = 1$. □

9. Επειδή η εξίσωση είναι συμμετρική ως προς x, y θέτουμε $x + y = s$ και $xy = p$. Τότε αυτή παίρνει τη μορφή

$$s^3 - 2sp = 8s^2 - 8p + 8.$$

Από την τελευταία έπεται ότι ο s είναι άρτιος και γράφουμε $s = 2t$. Τότε παίρνουμε

$$2t^3 - tp = 8t^2 - 2p + 2$$

και λύνονοντας ως προς p παίρνουμε

$$p = \frac{2t^3 - 8t^2 - 2}{t - 2} = 2t^2 - 4t - 8 - \frac{18}{t - 2}.$$

Επομένως αφού p είναι ακέραιος, θα πρέπει $t - 2 \mid 18$. Εξετάζοντας τις 12 περιπτώσεις που προκύπτουν, έχουμε τελικά ότι τα μόνα ζεύγη λύσεων είναι $(x, y) \in \{(8, 2), (2, 8)\}$. □

10. Γράφουμε τη δοθείσα στη μορφή

$$\begin{aligned} 2x^2 - 2y^2 + x - y &= y^2 \Rightarrow \\ (3) \quad (x - y)(2x + 2y + 1) &= y^2. \end{aligned}$$

Θα βρούμε το μέγιστο κοινό διαιρέτη των $x - y$ και $2x + 2y + 1$. Έστω ένας πρώτος p που είναι κοινός διαιρέτης των $x - y$ και $2x + 2y + 1$. Τότε η (3) δίνει ότι $p \mid y$. Οπότε $p \mid x$ αλλά τότε πρέπει $p \mid 1$. Έπεται ότι δύο αυτοί αριθμοί είναι πρώτοι μεταξύ τους και έτσι πρέπει να είναι και οι δύο τέλεια τετράγωνα, που είναι και το ζητούμενο. Ενδιαφέρον παρουσιάζει το ερώτημα να βρεθούν όλοι οι ακέραιοι x, y που ικανοποιούν την (3). Για να δοθεί όμως απάντηση στο παραπάνω ερώτημα απαιτούνται εργαλεία ξεφεύγουν από τους σκοπούς της παρουσίασης. □

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 ».

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

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

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

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

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

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

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

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

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

$\exists$: 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 v (υπόλοιπο) τέτοιοι ώστε να ισχύει

$$\Delta = \pi \cdot \delta + v, \quad 0 \leq v < \delta$$

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

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

$$\alpha = \kappa \cdot \beta + v, \quad 0 \leq v < |\beta|.$$

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 $0, 1, \dots, n-1$. Άρα κάθε αριθμός α είναι της μορφής $k \cdot n, k \cdot n + 1, \dots, k \cdot n + (n-1)$. Ειδικά όταν $n = 2$ τότε τα δυνατά υπόλοιπα είναι 0, 1. Εάν $v = 0$ τότε ο $\alpha = 2k$ λέγεται **άρτιος**, ενώ εαν $v = 1$ τότε ο $\alpha = 2k + 1$ λέγεται **περιττός**.

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

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 **πολβλαπλάσιο** του b , και γράφουμε $b|a$ ή $a = \text{πολλ.}b$. Άρα

$$b|a \iff \exists k \in \mathbb{Z} \text{ τέτοιο ώστε } a = k \cdot b.$$

Παρατήρηση: Για να δηλώσουμε ότι ο ακέραιος b **δεν διαιρεί** τον ακέραιο a , γράφουμε $b \nmid a$ ή ισοδύναμα $a \neq \text{πολλ.}b$. 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) $a|b \iff -a|b \iff a|-b \iff |a| \mid |b|$
- (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 διααιρετότητας στο σύνολο των ακεραίων, είναι αρκετό να περιοριστούμε στο σύνολο των θετικών ακεραίων.

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

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 $a = -b$ (Δήλαδή $|a| = |b|$).

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 $k, k+1, \dots, k+(n-1)$, 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

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

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

Συνεπώς αφού το $4y$ είναι πολλ.4, θα έχουμε $x^2 + 4y = \text{πολλ.}4$ είτε $x^2 + 4y = \text{πολλ.}4 + 1$ αλλιώς $1995 = \text{πολλ.}4 + 3$ άρα η εξίσωση είναι αδύνατη¹.

□

Παράδειγμα 1.7 Να δείξετε ότι για κάθε φυσικό αριθμό n ισχύει

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

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 $9 \mid P(k)$ δηλαδή ότι $9 \mid 10^k + 3 \cdot 4^{k+2} + 5$. 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 $9 \mid P(k)$, η παρατήρηση της Πρότασης 1.1 δίνει ότι $9 \mid P(k+1)$. Συνεπώς ισχύει $9 \mid P(n)$ για κάθε $n \in \mathbb{N}$.

□

Παράδειγμα 1.8 Να δείξετε ότι για κάθε $n \in \mathbb{Z}$ ισχύει $4 \nmid n^2 + 2$.

Απόδειξη :

Ας υποθέσουμε, αντίθετα, ότι υπάρχει ακέραιος n τέτοιος ώστε $4 \mid n^2 + 2$. 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 $4 \mid n^2 + 2$, έπεται ότι $4 \mid 4k^2 + 2$, δηλαδή $4 \mid 2$, άτοπο.
- Εαν $n = 2k + 1$, όπου $k \in \mathbb{Z}$, τότε $n^2 + 2 = (2k + 1)^2 + 2 = 4k^2 + 4k + 3$. Επειδή όμως $4 \mid 4k^2 + 4k$, έπεται ότι $4 \mid 3$, άτοπο.

Άρα για κάθε $n \in \mathbb{Z}$ ισχύει $4 \nmid n^2 + 2$.

□

¹Φυσικά 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 $a_1, \dots, a_n$ ακέραιοι αριθμοί από τους οποίους ένας τουλάχιστον είναι $\neq 0$. Κάθε ακέραιος που διαιρεί καθένα από τους $a_1, \dots, a_n$ λέγεται **κοινός διαιρέτης** των $a_1, \dots, a_n$. Συμβολίζουμε με S το σύνολο των θετικών κοινών διαιρειτών των $a_1, \dots, a_n$. 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 $a_1, \dots, a_n$ και συμβολίζεται με $(a_1, \dots, a_n)$. Για κάθε $a \in \mathbb{Z}$, το σύνολο των θετικών διαιρειτών του a συμπίπτει με αυτό του $-a$. Επομένως ισχύει $(a_1, \dots, a_n) = (|a_1|, \dots, |a_n|)$, δηλαδή ο Μ.Κ.Δ. είναι ανεξάρτητος προσήμων. Επίσης, καθώς κάθε ακέραιος είναι διαιρέτης του 0, έχουμε $(0, a_1, \dots, a_n) = (a_1, \dots, a_n)$. Συνεπώς μπορούμε να υποθέσουμε ότι κανένας εκ των ακεραίων $a_1, \dots, a_n$ δεν είναι μηδέν.

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

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

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

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

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

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

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

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 Πρόσημα 1.1 δίνει $d|(a, b)$ απ' όπου $d|1$. Επομένως $d = 1$.

□

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

- (i) $(\lambda a_1, \dots, \lambda a_n) = |\lambda|(a_1, \dots, a_n)$,
- (ii) αν $(a_1, \dots, a_n) = d$, τότε $(\frac{a_1}{d}, \dots, \frac{a_n}{d}) = 1$,
- (iii) $(a_1, \dots, a_n) = (a_1 + k_2 a_2 + \dots + k_n a_n, a_2, \dots, a_n)$, όπου $k_2, \dots, k_n \in \mathbb{Z}$.

Παράδειγμα 1.10 Εάν 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 $a_1, \dots, a_n$ μη μηδενικοί ακέραιοι με $n > 2$. Για κάθε $k, 1 \leq k \leq n - 2$ ισχύει

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

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. Εάν $a|bc$ 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

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

Απόδειξη :

Έστω ότι υπάρχουν τέτοιοι φυσικοί με τις ιδιότητες

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

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 γενικότητας, $b > 0$, 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 $a = q_0b + r_0$ όπου $0 \leq r_0 < b$.

Ας σημειωθεί ότι $(a, b) = (b, r_0)$, επειδή $d \mid a$ και $d \mid b$, συνεπώς $d \mid r_0 = a - q_0b$. 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

$$\begin{aligned} a &= q_0b + r_0 \text{ όπου } 0 \leq r_0 < b \\ b &= q_1r_0 + r_1 \text{ όπου } 0 \leq r_1 < r_0 \\ r_0 &= q_2r_1 + r_2 \text{ όπου } 0 \leq r_2 < r_1 \\ r_1 &= q_3r_2 + r_3 \text{ όπου } 0 \leq r_3 < r_2 \\ &\vdots \end{aligned}$$

Συνεπώς παίρνουμε μία φθίνουσα ακολουθία μη αρνητικών ακεραίων $b > r_0 > r_1 > r_2 > \dots$, η οποία πρέπει να φτάνει κάποια 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 $k = 0, 1, 2, \dots$, 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

$$\begin{aligned}
 a - q_0b &= r_0 \\
 b - q_1r_0 &= r_1 \\
 r_0 - q_2r_1 &= r_2 \\
 r_1 - q_3r_2 &= r_3 \\
 &\vdots \\
 r_{n-3} - q_{n-1}r_{n-2} &= r_{n-1} \\
 r_{n-2} &= q_n r_{n-1}
 \end{aligned}$$

συνεπώς, αντικαθιστώντας κάθε υπόλοιπο r_k στην επόμενη εξίσωση παίρνουμε

$$\begin{aligned}
 b - q_1(a - q_0b) &= k_1a + l_1b = r_1 \\
 (a - q_0b) - q_2(k_1a + l_1b) &= k_2a + l_2b = r_2 \\
 (k_1a + l_1b) - q_3(k_2a + l_2b) &= k_3a + l_3b = r_3 \\
 &\vdots \\
 (k_{n-3}a + l_{n-3}b) - q_n(k_{n-2}a + l_{n-2}b) &= k_{n-1}a + l_{n-1}b = r_{n-1}
 \end{aligned}$$

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

Λύση: Είναι

$$\begin{aligned}
 391 &= 1 \cdot 323 + 68 \\
 323 &= 4 \cdot 68 + 51 \\
 68 &= 1 \cdot 51 + 17 \\
 51 &= 3 \cdot 17 + 0.
 \end{aligned}$$

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

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

- (i) $a_1 | m, \dots, a_n | m$,
- (ii) εαν μ είναι θετικός ακέραιος με $a_1 | \mu, \dots, a_n | \mu$, τότε $m | \mu$.

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

- (i) $[\lambda a_1, \dots, \lambda a_n] = |\lambda| [a_1, \dots, a_n]$,
- (ii) αν $[a_1, \dots, a_n] = m$ τότε $\left(\frac{m}{a_1}, \dots, \frac{m}{a_n}\right) = 1$.

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

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

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. Λύνοντας 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) Εάν 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 αλλήλα 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

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

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 $2^n \parallel 3^{1024} - 1$.

Λύση:

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

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

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

□

²Δηλαδή $2 \parallel 3^{2^n} + 1$.

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 $p_1, \dots, p_n$ 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 $p_1, \dots, p_n$ 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 Εάν με p_n συμβολίσουμε τον 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, κανείς από τους οποίους δεν είναι πρώτος αριθμός.

Απόδειξη:

Αρκεί να θεωρήσουμε τους εξής n διαδοχικούς φυσικούς αριθμούς

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

Κανείς από τους αριθμούς αυτούς δεν είναι πρώτος, διότι για κάθε $m = 2, 3, \dots, n+1$, 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 άλγιο 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).

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

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

□

Η Πρόταση που ακολουθεί μας δίνει ένα τρόπο για να ελέγχουμε εάν 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 Εάν 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 εάν 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. Εάν $p|ab$ τότε $p|a$ ή $p|b$.

Γενίκευση: Έστω $a_1, \dots, a_n$ ακέραιοι $\neq 0, 1$ και p ένας πρώτος. Εάν $p|a_1 \cdots a_n$ 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, εάν a είναι ένας φυσικός > 1 , τότε υπάρχουν διαφορετικοί πρώτοι $p_1, \dots, p_k$ και φυσικοί $a_1, \dots, a_k > 0$ 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 τον a , αν και μόνο αν, $d = p_1^{\beta_1} \cdots p_k^{\beta_k}$ με $0 \leq \beta_i \leq a_i$ ($i = 1, \dots, k$).

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 $\frac{a^3 + 1}{b + 1}, \frac{b^3 + 1}{a + 1}$ 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 $p_i \neq q_j, \forall i = 1, 2, \dots, k$ και $j = 1, 2, \dots, l$ αληθά 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 $\frac{a^3 + 1}{b + 1} + \frac{b^3 + 1}{a + 1} \in \mathbb{N}$ 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 $a_1, \dots, a_n$ μη μηδενικοί ακέραιοι με

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

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

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

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

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

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

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

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

Πόρισμα 1.6 Έστω $a, b_1, \dots, b_n$ ($n \geq 2$) μη μηδενικοί ακέραιοι και οι $b_1, \dots, b_n$ πρώτοι μεταξύ τους ανά δύο. Εάν $b_1 | a, \dots, b_n | a$ 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 διαδοχικών 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 $a_1, \dots, a_n$ μη μηδενικοί ακέραιοι με

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

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

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

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

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

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

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 περισσότερων 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 (εάν 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 εν 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 ακραίους, **δεν ισχύει** ανάλογη σχέση με την παραπάνω. Δηλαδή γενικά, έχουμε

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

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 ». Εάν ο ακέραιος a δεν είναι ισοϋπόλοιπος 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

$$a \equiv b \pmod{n} \iff n \mid a - b$$

Άμεσες συνέπειες του ορισμού είναι οι επόμενες ιδιότητες.

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

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

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

Πόρισμα 2.2 (i) $a \equiv 0 \pmod{n} \iff n \mid a$,

(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) Εάν $a \equiv b \pmod{n}$ και $m \mid n$ τότε $a \equiv b \pmod{m}$,

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

(vi) Εάν 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. Εάν $a \equiv b \pmod{n}$ 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

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

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 προσθέτοντας 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 τον 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 $11|n + 7 \Leftrightarrow (n = 11k + 4 \text{ ή } n = 11k - 7)$ και αντικαθιστώντας το n στο $n^2 + 3n + 5$, το τελευταίο παίρνει τη μορφή $121\lambda + v$ με $0 < v < 121$ το οποίο είναι άτοπο.

□

Παράδειγμα 2.5 (ΕΜΕ 1997) Έστω a, b, c ακέραιοι αριθμοί τέτοιои, 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 $a, b, c \equiv 0, \pm 1 \pmod{3}$. Εάν και οι τρεις αφήνουν διαφορετικό υπόλοιπο στη διαίρεσή τους με το 3, τότε $a + b + c \equiv -1 + 0 + 1 = 0 \pmod{3}$ ενώ $(a - b)(b - c)(c - a) \not\equiv 0 \pmod{3}$. Εάν ακριβώς δύο είναι ισουπόλοιποι, χωρίς βλάβη της γενικότητας 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 γενικότητας 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 $a \equiv v \pmod{10^n}$ και $0 \leq v < 10^n$, τότε τα τελευταία n ψηφία του αριθμού a είναι το v με τόσα μηδενικά στην αρχή, όσα χρειάζονται ώστε το μήκος του αριθμού v 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 (EME 1988) Να βρεθούν τα δύο τελευταία ψηφία του αριθμού 2^{70} .

Λύση:

Τι 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.

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

επανάληψη ανά 20

04, 08, 26, 32 . . .

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 (κάποιον είδους) επαλήθευση μπορούμε να βρούμε το τελευταίο ψηφίο του ίδιου αριθμού χρησιμοποιώντας την περιοδικότητα του τελευταίου ψηφίου που είναι 4, $[2, 4, 8, 6]$, $2, 4, \dots$ 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

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

Λύση:

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

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

άρα

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

Έτσι,

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

□

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

$$\underbrace{a_n a_{n-1} a_{n-2} \dots a_4}_{A} 1994 = 10000A + 1994 = A(5 \cdot 1993 + 35) + 1993 + 1$$

$$\equiv 35 \cdot A + 1 \pmod{1993}$$

Για να είναι $35 \cdot A + 1 \equiv 0 \pmod{1993}$ θα πρέπει $35A + 1 = 1993k$, $k \in \mathbb{Z}$ δηλαδή $A = 57k - \frac{2k+1}{35}$ (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

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

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) Εάν 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 $11 \mid a_n$.

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

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

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

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

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

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 $a_1, \dots, a_n$ καλείται **πλήρες σύστημα υπολοίπων mod n** , εαν κάθε ένα από τα $a_1, \dots, a_n$ είναι ισοϋπόλοιπο με ένα και μόνο αριθμό του συνόλου $\{0, 1, \dots, n-1\}$ ⁵.

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

Μερικά συστήματα υπολοίπων $\bmod n$ που μπορούμε να διακρίνουμε αμέσως είναι τα εξής:

- (i) Ελάχιστο μη αρνητικό σύστημα υπολοίπων $\bmod n$: $\{0, 1, \dots, n-1\}$.
- (ii) Ελάχιστο θετικό σύστημα υπολοίπων $\bmod n$: $\{1, \dots, n\}$
- (iii) Πλήρες σύστημα των απόλυτα ελαχίστων υπολοίπων $\bmod n$:

- Για n περιττό είναι το σύνολο

$$\left\{ -\frac{n-1}{2}, \dots, -1, 0, 1, \dots, \frac{n-1}{2} \right\}$$

- και για n άρτιο, το σύνολο

$$\left\{ -\left(\frac{n}{2} - 1\right), \dots, -1, 0, 1, \dots, \frac{n}{2} \right\}$$

Παράδειγμα 2.13 Το σύνολο $S = \{14, 24, 9, -11, 34, 68, -21, 87\}$ είναι ένα πλήρες σύστημα υπολοίπων $\bmod 8$. Πραγματικά, έχουμε

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

Καθώς το σύνολο $\{0, 1, \dots, 7\}$ είναι ένα πλήρες σύστημα υπολοίπων $\bmod 8$ άρα το σύνολο S είναι επίσης ένα πλήρες σύστημα υπολοίπων $\bmod 8$.

□

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

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 $\{0, 1, \dots, n\}$ (με το 1).

□

Παράδειγμα 2.15 (EME 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 . Εάν $a = 7k$, τότε φανερά το γινόμενο είναι πολλαπλάσιο του 7. Όμοια εάν $a = 7k + 1, 7k - 1$ τότε $7|a - 1, 7|a + 1$ αντίστοιχα, άρα διαιρεί όλη την παράσταση. Εάν $a = 7k + 2$ ή $a = 7k - 3$ τότε ο $a^2 + a + 1$ είναι πολλαπλάσιο του 7 και τέλος εάν $a = 7k + 3$ 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 $\text{mod } 7$).

□

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

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 Εάν $0 < s < p$, 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 $1+2+\cdots+(p-1) = \frac{p(p-1)}{2}$, αρκεί να δείξουμε ότι

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

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

$$p(p-1) \mid (p-1)! - (p-1).$$

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

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

□

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 Εάν p είναι ένας πρώτος αριθμός και $a_1, \dots, a_n$ ακέραιοι αριθμοί, τότε ισχύει

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

Παράδειγμα 2.18 Εάν για το φυσικό αριθμό n ισχύει

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

να αποδειχθεί ότι $5 \mid n^2 + 1$.

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 $\frac{7 \cdot 1968^{1968} - 3 \cdot 68^{78}}{10}$ είναι ακέραιος.

Απόδειξη:

Αρκεί να δείξουμε ότι

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

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

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

Επίσης, έχουμε

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

οπότε

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

Δηλαδή

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

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

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

□

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

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

Άρα

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

οπότε

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

□

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 $p \nmid ab$ 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 $20p \mid 5^p - 4^p - 1$.

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

□

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

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

διαφείνεται από το p .

Απόδειξη:

Έχουμε

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

και το συμπέρασμα προκύπτει από το Μικρό Θεώρημα του Fermat⁶.

□

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 $n \equiv \pm 1, \pm 3, \pm 5, \pm 7 \pmod{16}$. Συνεπώς μπορούμε να βελτιώσουμε το αποτέλεσμα της άσκησης σε $p^4 \equiv 1 \pmod{240}$ για όλους τους πρώτους $p > 5$.

□

⁶Ας σημειωθεί ότι $(10, p) = 1$

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

$$n^2 - 1 \mid 2^{n!} - 1.$$

Απόδειξη :

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

□

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 $p \mid a^2 + ab + b^2$, 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 $p \mid a$, άτοπο.

□

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

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

□

Παράδειγμα 2.28 (Διεθνής Ολυμπιάδα Μαθηματικών 2005) Θεωρούμε την ακολουθία $a_1, a_2, \dots$ 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 $p \mid 6a_{p-2}$. 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** $ax \equiv b \pmod{n}$ οποιονδήποτε 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 $6x \equiv 1 \pmod{8}$ ($8 \nmid 6x - 1$, 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 απλοποιείται και έχουμε $2x \equiv 4 \pmod{6}$. Οι ακέραιοι $0, 1, 2, 3, 4, 5$ αποτελούν ένα πλήρες σύστημα υπολοίπων $\text{mod } 6$ 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 γίνονται αρκετά επίπονοι. Αυτός είναι και ο λόγος που θα μελετήσουμε αναλυτικότερα τις γραμμικές ισοτιμίες.

Ορισμός 2.4 Ονομάζουμε **αντίστροφο ενός αριθμού** $a \pmod{n}$ (αν υπάρχει) εκείνον τον 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 $3 \pmod{7}$ 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 απλοποιείται 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 $35 \pmod{102}$, 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: Εάν $(a, n) = 1$ τότε για να προσδιορίσουμε τον αντίστροφο του $a \pmod{n}$ 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 $a \pmod{n}$, είναι το $a^{r-1} \pmod{n}$. Συνεπώς εάν $(a, n) = 1$, 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 $7 \pmod{30}$ 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 $\text{ord}_{30}(7) = 4$ 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 $d = (a, n)$. Ειδικότερα, εάν ο ακέραιος x_0 επαληθεύει τη γραμμική ισοτιμία, τότε υπάρχουν ακριβώς d λύσεις οι

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

Παράδειγμα 2.32 Να υπολογίσετε τις λύσεις της γραμμικής ισοτιμίας

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

Λύση:

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

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 $0, 1, \dots, 10$ αποτελούν ένα πλήρες σύστημα υπολοίπων $\pmod{11}$. 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

$$a_1x \equiv b_1 \pmod{n_1}$$

$$\vdots$$

$$a_kx \equiv b_k \pmod{n_k}$$

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 $a \pmod{c}$ εννοούμε ότι έχει ως λύσεις όλους τους ακραίους που είναι ισοϋπόλοιποι με το $a \pmod{c}$. Δύο συστήματα καλούνται **ισοδύναμα** όταν έχουν το ίδιο σύνολο λύσεων.

Θεώρημα 2.6 (Κινέζικο Θεώρημα Υπολοίπων ή Θεώρημα Υπολοίπων του Νικόμα-χου) Έστω $b_1, \dots, b_k$ ακέραιοι και $n_1, \dots, n_k$ 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 $\text{mod } n_1 \cdots n_k$, 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

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

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 $\text{mod } 385$.

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

Έτσι, παίρνουμε τις γραμμικές ισοτιμίες

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

ή ισοδύναμα

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

οι οποίες έχουν τις λύσεις

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

αντίστοιχα. Επομένως, η λύση του συστήματος είναι

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

□

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

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 λύσεων 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 $\text{mod } 90$. 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

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

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 $d_i = (a_i, n_i)$, $i = 1, \dots, k$. Ας υποθέσουμε ότι $d_i | b_i$, $i = 1, \dots, k$. Τότε υπάρχουν $A_i, B_i, N_i \in \mathbb{Z}$ με $(A_i, N_i) = 1$ έτσι ώστε $a_i = d_i A_i$, $b_i = d_i B_i$, $n_i = d_i N_i$, $i = 1, \dots, k$. 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 $x \equiv C_i \pmod{N_i}$, $i = 1, \dots, k$. 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 $\text{mod } 455$. 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 *Brahmagupta*, 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 карабиού 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:

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

(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

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

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

¹⁰Η 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) εάν p πρώτος, τότε οι $\binom{p}{1}, \binom{p}{2}, \dots, \binom{p}{p-1}$ 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 $2^{10} = 1024$ διαφεθεί 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 Εάν 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

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

με

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

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) $\varphi(1) = 1$

¹¹Το σύμβολο $\#\{\dots\}$ συμβολίζει το πλήθος των στοιχείων του συνόλου $\{\dots\}$.

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

(iii) Η συνάρτηση φ είναι πολλαπλασιαστική δηλαδή εάν $(m, n) = 1$, 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) Εάν 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, εάν $n = p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l}$ 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 $n \in \mathbb{N} \setminus \{4\}$ 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

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

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 $(p_1-1), (p_2-1), \dots, (p_l-1)$. 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

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

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

$$n = p^k \quad \text{ή} \quad n = 2p^k.$$

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)

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

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 Εάν 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

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

□

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 (1η Λύση) την εξαιρετική λύση της συναδέλφου Ε. Μήτσιου που δημοσιεύθηκε τότε στο περιοδικό «Διάσταση» και κατόπιν (2η Λύση) κάνοντας 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

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

{ Εάν $k = 3l$ τότε η (1) γίνεται

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

{ Εάν $k = 3l + 1$ τότε $\eta(1)$ γίνεται

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

{ Εάν $k = 3l + 2$ τότε $\eta(1)$ γίνεται

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

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

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

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

{ Αν $k = 3l + 1$ τότε

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

άρα όχι $\pi\sigma\lambda.7$

{ Αν $k = 3l + 2$ τότε

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

άρα όχι $\pi\sigma\lambda.7$

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

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

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

2η 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 v , όπου $n = 6k + v$, $v = 0, 1, 2, 3, 4, 5$, θα χρειαστούν το πολύ 6 βήματα για να δούμε τα δυνατά υπόλοιπα των 2^n και 3^n με το 7.

$v = n \pmod{6}$	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 ότι 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 γραμμές 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⁾

¹³Σημειώστε 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.

¹⁴Προφανώς 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 ναδειχτεί 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 $n \not\equiv 0 \pmod{6}$ 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 $n \not\equiv 0 \pmod{p-1}$ 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.

Κατάρχην παρατηρούμε ότι

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

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

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

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

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 $p \mid [1^n + 2^n + \dots + (p-1)^n]$ 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:

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

¹⁶διότι 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 $n = 6k + v$, $v = 0, 1, \dots, 5$ και δείξτε (φανερό) ότι $v \neq 2, 3, 4$ 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 ότι 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:** $A = 3^p - (2^p + 1) = 3^p - (2 + 1)(2^{p-1} + 2^{p-2} + \dots + 2 + 1) \equiv 0 \pmod{3}$

(iii) **Με το p :** Από 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 $A \equiv 0 \pmod{7}$

¹⁷Θυμίζουμε ότι 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 διαιρετός του 6. Φτιάξτε λοιπόν τον αντίστοιχο πίνακα, όπως έγινε στα παραπάνω παραδείγματα, για να δείξετε ότι στις περιπτώσεις $p = 6k + 1, p = 6k + 5$ έχουμε ότι $A \equiv 0 \pmod{7}$. Δικαιολογείται λοιπόν με τα παραπάνω ο λόγος για τον οποίο χρειάστηκε να εργαστούμε $\pmod{6}$ και ο οποίος μας οδήγησε να καταλήξουμε στο (γενικό και πολύ χρήσιμο) Λήμμα 5.1.

□

Εισαγωγή στη Θεωρία Αριθμών για το Λύκειο

Σημειώσεις Προετοιμασίας για Μαθηματικούς Διαγωνισμούς

Ασκήσεις

Αλέξανδρος Γ. Συγκελάκης

ags@math.uoc.gr

Νοέμβριος 2012

1 Μαθηματική Επαγωγή

1.1 Ασκήσεις Α΄ Ομάδας

Άσκηση 1.1 Να αποδείξετε ότι για οποιοδήποτε φυσικό $n \geq 1$ ισχύει

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

Άσκηση 1.2 Να αποδείξετε ότι για οποιοδήποτε φυσικό $n \geq 1$ ισχύει

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Άσκηση 1.3 Να αποδείξετε ότι για οποιοδήποτε φυσικό $n \geq 1$ ισχύει

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2} \right)^2.$$

Άσκηση 1.4 Να αποδείξετε ότι για οποιοδήποτε φυσικό $n \geq 1$ ισχύει

$$1 + 3 + 5 + \cdots + (2n-1) = n^2.$$

Άσκηση 1.5 Να αποδείξετε ότι για οποιοδήποτε φυσικό $n \geq 1$ ισχύει

$$1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 = \frac{n(4n^2-1)}{3}.$$

Άσκηση 1.6 Να αποδείξετε ότι για οποιοδήποτε φυσικό $n \geq 1$ ισχύει

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n \cdot (n+1) = \frac{n(n+1)(n+2)}{3}.$$

Άσκηση 1.7 Να αποδείξετε ότι για οποιοδήποτε φυσικό $n \geq 1$ ισχύει

$$1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + 3 \cdot 4 \cdot 5 + \cdots + n \cdot (n+1) \cdot (n+2) = \frac{n(n+1)(n+2)(n+3)}{3}.$$

Να γενικεύσετε το αποτέλεσμα και να αποδείξετε τον ισχυρισμό σας.

Άσκηση 1.8 Να αποδείξετε ότι για οποιοδήποτε φυσικό $n \geq 1$ ισχύει

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{n \cdot (n+1)} = \frac{n}{n+1}.$$

Άσκηση 1.9 Να αποδείξετε ότι για οποιοδήποτε φυσικό $n \geq 1$ ισχύει

$$\frac{(n+1) \cdot (n+2) \cdots (2n)}{1 \cdot 3 \cdot 5 \cdots (2n-1)} = 2^n.$$

Άσκηση 1.10 Να αποδείξετε ότι για οποιοδήποτε φυσικό $n \geq 4$ ισχύει $3^n > n^2$.

Άσκηση 1.11 (i) Να αποδείξετε ότι για οποιοδήποτε $a > -1$ και οποιοδήποτε φυσικό $n \geq 1$, ισχύει $(1+a)^n \geq 1+na$.

(ii) Να αποδείξετε ότι για οποιοδήποτε φυσικό n ισχύει $2^n + 5^n + 7^n > 11n$.

Άσκηση 1.12 Να αποδείξετε ότι για οποιοδήποτε φυσικό $n \geq 2$ ισχύει

$$2 \cdot 2^1 + 3 \cdot 2^2 + 4 \cdot 2^3 + \cdots n \cdot 2^{n-1} = (n-1) \cdot 2^n.$$

Άσκηση 1.13 Να αποδείξετε ότι για οποιοδήποτε φυσικό n ισχύει

$$1^2 - 2^2 + 3^2 - 4^2 + \cdots + (-1)^{n-1} n^2 = (-1)^{n-1} \cdot \frac{n(n+1)}{2}.$$

Άσκηση 1.14 Να αποδείξετε ότι για οποιοδήποτε φυσικό n ισχύει

$$\frac{1^2}{1 \cdot 3} + \frac{2^2}{3 \cdot 5} + \frac{3^2}{5 \cdot 7} + \cdots + \frac{n^2}{(2n-1)(2n+1)} = \frac{n(n+1)}{2(2n+1)}.$$

Άσκηση 1.15 Να αποδείξετε ότι για οποιοδήποτε φυσικό $n \geq 1$ ο αριθμός

$$A_n = 2^{n+2} + 3^{2n+1}$$

είναι πολλαπλάσιο του 7.

Άσκηση 1.16 Να αποδείξετε ότι για οποιοδήποτε φυσικό $n \geq 1$ ο αριθμός

$$A_n = 2^{4n+1} - 2^{2n} - 1$$

είναι πολλαπλάσιο του 9.

Άσκηση 1.17 Να αποδείξετε ότι για οποιοδήποτε φυσικό $n \geq 1$ ο αριθμός

$$A_n = 10^n + 18n - 1$$

είναι πολλαπλάσιο του 27.

Άσκηση 1.18 Να αποδείξετε ότι για οποιοδήποτε φυσικό n ο αριθμός

$$A_n = 2^{4n} + 29^{2n+1}$$

είναι πολλαπλάσιο του 15.

1.2 Ασκήσεις Β' Ομάδας

Άσκηση 1.19 Να αποδείξετε ότι για οποιοδήποτε φυσικό $n \geq 3$ ισχύει $n^{n+1} > (n+1)^n$.

Άσκηση 1.20 Να αποδείξετε ότι εάν a, b, c είναι τα μήκη των πλευρών ορθογωνίου τριγώνου ABC με $\angle A = 90^\circ$, τότε $a^n > b^n + c^n$.

Άσκηση 1.21 Να αποδείξετε ότι για οποιοδήποτε φυσικό $n \geq 1$ και οποιουδήποτε πραγματικούς αριθμούς a, b ισχύει

$$(a+b)^n = C_n^n a^n b^0 + C_{n-1}^n a^{n-1} b^1 + C_{n-2}^n a^{n-2} b^2 + \cdots + C_2^n a^2 b^{n-2} + C_1^n a^1 b^{n-1} + C_0^n a^0 b^n,$$

όπου $C_k^n = \frac{n!}{k!(n-k)!}$ (Ορίζουμε $0! = 1$ και $k! = 1 \cdot 2 \cdot 3 \cdots k$ για κάθε $k \in \mathbb{N}^*$).

Άσκηση 1.22 Να αποδείξετε ότι για οποιοδήποτε φυσικό $n \geq 2$ ισχύει

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} > 2\sqrt{n+1} - 2.$$

Άσκηση 1.23 Να αποδείξετε ότι για οποιοδήποτε φυσικό $n \geq 2$ ισχύει

$$\frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} < \frac{3}{4}.$$

Άσκηση 1.24 Να αποδείξετε ότι για οποιοδήποτε φυσικό $n \geq 1$, ο αριθμός

$$(1 + \sqrt{2})^{2n} + (1 - \sqrt{2})^{2n}$$

είναι άρτιος ακέραιος και ο αριθμός

$$\frac{1}{\sqrt{2}} \left((1 + \sqrt{2})^{2n} - (1 - \sqrt{2})^{2n} \right)$$

είναι ακέραιος.

Άσκηση 1.25 Να αποδείξετε ότι για οποιοδήποτε φυσικό $n \geq 1$ ισχύει

$$\frac{1^2}{2^2} \cdot \frac{3^2}{4^2} \cdots \frac{(2n-1)^2}{(2n)^2} < \frac{1}{3n}.$$

Άσκηση 1.26 Δείξτε ότι για κάθε φυσικό n υπάρχουν n διαφορετικοί ανα δύο διαφéréτες του $n!$ των οποίων το άθροισμα είναι $n!$.

Άσκηση 1.27 Να αποδείξετε ότι εάν k περιττός τότε $2^{n+2} \mid k^{2^n} - 1$ για οποιοδήποτε φυσικό $n \geq 1$.

Άσκηση 1.28 Ισχύει ότι για οποιοδήποτε φυσικό n ο αριθμός $n^2 + n + 41$ είναι πρώτος ;

Άσκηση 1.29 Να αποδείξετε επαγωγικά ότι εάν ένα σύνολο περιέχει $n \geq 1$ στοιχεία, τότε τα υποσύνολά του είναι σε πλήθος 2^n .

2 Διαιρετότητα

2.1 Ασκήσεις Α΄ Ομάδας

Άσκηση 2.1 Να δείξετε ότι το άθροισμα και η διαφορά δύο περιττών αριθμών ή δύο άρτιων είναι πάντα άρτιος.

Άσκηση 2.2 Να βρεθεί το υπόλοιπο της διαίρεσης του $17^{50} + 33^{100}$ δια του 8.

Άσκηση 2.3 Να βρεθεί το υπόλοιπο της διαίρεσης του $25^{40} + 17^{30}$ δια του 8.

Άσκηση 2.4 Αν ο ακέραιος a δεν είναι πολλαπλάσιο του 5, να δείξετε ότι το υπόλοιπο της διαίρεσης του a^4 δια 5 είναι ίσο με 1. Κατόπιν να δείξετε ότι αν οι ακέραιοι a, b δεν είναι πολλαπλάσια του 5, τότε ο $a^4 - b^4$ είναι πολλαπλάσιο του 5.

Άσκηση 2.5 Να βρεθεί το τελευταίο ψηφίο του αριθμού

(i) 2^{2009}

(ii) 3^{1821}

(iii) 71^{1453}

(iv) 777^{333}

Άσκηση 2.6 Αν ο αριθμός n είναι φυσικός, να δείξετε ότι ο αριθμός $A = n(n^2 + 2)$ είναι πολλαπλάσιο του 3.

Άσκηση 2.7 Αν ο αριθμός n είναι φυσικός, να δείξετε ότι ο αριθμός $A = n(n^2 + 5)$ είναι πολλαπλάσιο του 6.

Άσκηση 2.8 Αν οι a, b είναι ακέραιοι και τέτοιοι ώστε ο αριθμός $a^2 + b^2$ να είναι πολλαπλάσιο του 3, να αποδείξετε ότι καθένας εκ των a, b είναι πολλαπλάσιο του 3.

Άσκηση 2.9 Αν για τρεις ακεραίους a, b, c ο αριθμός $a^2 + b^2 + c^2$ είναι πολλαπλάσιο του 5, να αποδείξετε ότι ένας τουλάχιστον από τους a, b, c είναι πολλαπλάσιο του 5.

Άσκηση 2.10 Αν οι a, b είναι ακέραιοι και τέτοιοι ώστε ο αριθμός $a^4 + b^4$ να είναι πολλαπλάσιο του 7, να αποδείξετε ότι καθένας εκ των a, b είναι πολλαπλάσιο του 7.

Άσκηση 2.11 Αν κανένας από τους ακεραίους a, b, c δεν είναι πολλαπλάσιος του 3, να δείξετε ότι ο αριθμός $a^2 + b^2 + c^2$ είναι πολλαπλάσιο του 3.

Άσκηση 2.12 Για ποιους ακεραίους k ο αριθμός $5k + 2$ είναι πολλαπλάσιο του 4 ;

Άσκηση 2.13 Βρείτε όλους τους 2-ψήφιους αριθμούς που έχουν ακριβώς 3 διαιρέτες.

Άσκηση 2.14 Βρείτε όλους τους φυσικούς που έχουν ακριβώς 4 διαιρέτες με την προϋπόθεση ότι το γινόμενο των διαιρετών τους είναι 225.

Άσκηση 2.15 Βρείτε όλους τους 4-ψήφιους που έχουν ακριβώς 5 διαιρέτες.

Άσκηση 2.16 Βρείτε όλα τα πολλαπλάσια του 10 που έχουν ακριβώς 6 διαιρέτες.

Άσκηση 2.17 Βρείτε το μικρότερο φυσικό αριθμό που έχει ακριβώς 42 διαιρέτες.

Άσκηση 2.18 Να δείξετε ότι δεν υπάρχουν 3-ψήφιοι φυσικοί που είναι πολλαπλάσια του 35 και οι οποίοι να έχουν ακριβώς 9 διαιρέτες.

Άσκηση 2.19 Βρείτε πρώτους αριθμούς x, y, z που είναι τέτοιοι ώστε ο αριθμός

$$n = 11^x \cdot 19^y \cdot 31^z,$$

να έχει ακριβώς 144 διαιρέτες.

Άσκηση 2.20 Βρείτε το φυσικό αριθμό της μορφής $n = 3^a \cdot 5^b \cdot 7^c$, αν ο $27n$ έχει 36 διαιρέτες περισσότερους από το n και ο $49n$ έχει 12 διαιρέτες περισσότερους από το n .

Άσκηση 2.21 Να βρείτε για ποιους ακераίους αριθμούς n ο αριθμός $n + 1$ διαιρεί τον $n^2 + 1$.

Άσκηση 2.22 Να βρείτε για ποιους ακεραίους αριθμούς $n \neq 3$ ο αριθμός $n - 3$ διαιρεί τον $n^3 - 3$.

Άσκηση 2.23 Να αποδείξετε ότι για οποιοδήποτε φυσικό $n \geq 1$ ο αριθμός $A = 2^n \cdot 5^n + 1988$ είναι πολλαπλάσιο του 18.

Άσκηση 2.24 Να αποδείξετε ότι για οποιοδήποτε φυσικό n ο αριθμός $A = n^5 - n$ είναι πολλαπλάσιο του 30.

Άσκηση 2.25 Εάν ο αριθμός $3a + 5b$ είναι πολλαπλάσιο του 17 για κάποιους ακεραίους a, b τότε να αποδείξετε ότι και ο αριθμός $4a + b$ είναι πολλαπλάσιο του 17. Ισχύει το αντίστροφο ;

Άσκηση 2.26 Εάν ο αριθμός $5a + 7b$ είναι πολλαπλάσιο του 31 για κάποιους ακεραίους a, b τότε να αποδείξετε ότι και ο αριθμός $11a + 3b$ είναι πολλαπλάσιο του 31.

Άσκηση 2.27 Αποδείξτε το κριτήριο διαιρετότητας του 3 και του 9.

Άσκηση 2.28 Βρείτε τον αριθμό x ώστε ο αριθμός $\overline{2x5}$ να είναι πολλαπλάσιο του 3 (αντίστοιχα του 9).

Άσκηση 2.29 Δείξτε ότι η διαφορά δύο διαδοχικών κύβων είναι πάντα περιττός.

Άσκηση 2.30 Βρείτε το τελευταίο ψηφίο του 7^{2009} .

Άσκηση 2.31 Να δείξετε ότι ο αριθμός $A = 2007^{2009} + 2008^{2010} + 2009^{2011}$ είναι πάντα πολλαπλάσιο του 15.

Άσκηση 2.32 Δείξτε ότι για κάθε $n \in \mathbb{N}$ ο αριθμός $A = 5^{2n+3} \cdot 9^{n+2} + 3^{2n+1} \cdot 25^{n+1}$ είναι πολλαπλάσιο του 17.

Άσκηση 2.33 Δείξτε ότι ο αριθμός $A = 63^n + 7^{n+1} \cdot 3^{2n+1} - 21^n \cdot 3^{n+2}$ είναι πολλαπλάσιο του 13.

Άσκηση 2.34 Βρείτε τους θετικούς ακέραιους x, y που είναι τέτοιοι ώστε $45 \mid \overline{4xy}$.

Άσκηση 2.35 Να αποδειχθεί ότι δεν υπάρχει ακέραιος αριθμός n που να ικανοποιεί την ισότητα

$$n(n-1) + (n-1)(n+1) + n(n+1) + 3n^5 = 3000000.$$

(Διαγωνισμός «Ο Θαλής» 1996)

Άσκηση 2.36 Να δείξετε ότι $n^2 \mid (n+1)^n - 1$.

Άσκηση 2.37 Αν ο n είναι περιττός φυσικός, τότε να δείξετε ότι $\frac{n(n+1)}{2} \mid n!$.

Άσκηση 2.38 Αν $\frac{n(n+1)}{2} \nmid n!$, τότε ο $n+1$ είναι πρώτος.

Άσκηση 2.39 Να δείξετε ότι $1897 \mid 2903^n - 803^n - 464^n + 261^n$.

Άσκηση 2.40 Να δείξετε ότι $1001 \mid 1^{2009} + 2^{2009} + \dots + 1000^{2009}$.

Άσκηση 2.41 Να δείξετε ότι ο αριθμός $A = 3 + 3^2 + 3^3 + \dots + 3^{1986}$ είναι πολλαπλάσιο του 156.

Άσκηση 2.42 Να δείξετε ότι για $\forall 1$ ο αριθμός $A = 15^{n+1} + 3^{n+1} + 5 \cdot 3^{n+2}$ είναι πολλαπλάσιο του 27.

Άσκηση 2.43 Να δείξετε ότι ο αριθμός $\underbrace{111 \dots 1}_{91 \text{ άσσοι}}$ είναι σύνθετος.

Άσκηση 2.44 Να δείξετε ότι $5 \mid 1^{99} + 2^{99} + 3^{99} + 4^{99}$.

Άσκηση 2.45 Να δείξετε ότι αν a, b ακέραιοι με $ab \neq 1$ τότε ο αριθμός $a^4 + 4b^4$ είναι σύνθετος.

Άσκηση 2.46 Να δείξετε ότι $100 \mid 11^{10} - 1$.

Άσκηση 2.47 (i) Να δείξετε ότι δεν υπάρχει ακέραιος αριθμός n τέτοιος ώστε ο $n^3 + 3n$ να είναι περιττός.

(ii) Να δείξετε ότι δεν υπάρχουν ακέραιοι αριθμοί x, y τέτοιοι ώστε

$$5x^3 - 4y^2 - 6xy + 15x + 6y - 5 = 0.$$

(Διαγωνισμός «Ο Θαλής» 1996)

Άσκηση 2.48 Είναι γνωστό ότι ο αριθμός 27000001 έχει ακριβώς 4 γνήσιους διαιρέτες. Να βρείτε το άθροισμά τους.

Άσκηση 2.49 Να δείξετε ότι εαν $a^3 \mid b^2$ τότε $a \mid b$. Εαν $a^2 \mid b^3$ τότε μπορούμε να βγάλουμε σαν συμπέρασμα ότι $a \mid b$;

Άσκηση 2.50 Να αποδείξετε ότι το τελευταίο μη μηδενικό ψηφίο του $n!$ είναι πάντα άρτιο για $n \geq 2$.

Άσκηση 2.51 Να βρεθεί η μεγαλύτερη δύναμη του 15 που διαιρεί το $60!$.

Άσκηση 2.52 Σε πόσα μηδενικά λήγει ο αριθμός $169!$;

Άσκηση 2.53 Σε πόσα μηδενικά λήγει ο αριθμός $\frac{500!}{200!}$;

Άσκηση 2.54 (i) Πόσοι ακέραιοι μεταξύ του 500 και του 2000 διαιρούνται και από το 3 αβηλά και από το 7 ;

(ii) Πόσοι ακέραιοι μεταξύ του 500 και του 2000 διαιρούνται από το 3 ή από το 7 ;

(iii) Πόσοι ακέραιοι μεταξύ του 500 και του 2000 δεν διαιρούνται από το 3 ή από το 7 ;

Άσκηση 2.55 Μια παλιά και δυσδιάκριτη απόδειξη γράφει ότι 36 κοτόπουλα αγοράστηκαν αντί του ποσού $x73.9y$ •. Λαμβάνοντας υπόψη ότι καθένα κοτόπουλο κοστίζει λιγότερο από 10 •, να βρεθούν τα ψηφία που λείπουν.

Άσκηση 2.56 Ο 7-ψήφιος αριθμός $72x20y2$ όπου οι x, y είναι ψηφία, διαιρείται από το 72. Ποιές είναι οι δυνατές τιμές που μπορούν να πάρουν τα x, y ;

Άσκηση 2.57 Υποθέτουμε ότι ο 792 διαιρεί τον ακέραιο που έχει δεκαδική αναπαράσταση $13xy45z$. Να βρεθούν τα ψηφία x, y, z .

2.2 Ασκήσεις Β' Ομάδας

Άσκηση 2.58 Να αποδείξετε ότι αν $n \geq 3$ περιττός φυσικός, τότε ο αριθμός $2^n + 1$ είναι σύνθετος.

Άσκηση 2.59 Να δείξετε ότι ο αριθμός $\underbrace{111 \dots 1}_{n \text{ άσσοι}} 2 \underbrace{111 \dots 1}_{n \text{ άσσοι}}$ είναι σύνθετος για κάθε $n \in \mathbb{N}^*$.

(Διαγωνισμός «Ο Ευκλείδης» 1997)

Άσκηση 2.60 Σε τετραγωνισμένο χαρτί 50×50 τοποθετούμε τους αριθμούς $1, 2, 3, \dots, 2500$. Να εξετάσετε εάν είναι δυνατό να τοποθετήσουμε τους αριθμούς αυτούς έτσι ώστε το άθροισμα των στοιχείων κάθε γραμμής και κάθε στήλης να είναι:

(i) περιττός αριθμός.

(ii) αριθμός μη διαιρετός από το 5.

(Διαγωνισμός «Ο Θαλής» 1997)

Άσκηση 2.61 Να αποδείξετε ότι εάν ο φυσικός αριθμός $n > 4$ είναι σύνθετος, τότε

$$n | (n-1)!$$

Άσκηση 2.62 Να αποδείξετε ότι για κάθε n σύνθετο με $n > 4$ ισχύει $2n | (n-1)!$ (JBMO 2006)

Άσκηση 2.63 Βρείτε τους θετικούς ακέραιους που ικανοποιούν την εξίσωση

$$9(x^2 + y^2 + 1) + 2(3xy + 2) = 2005.$$

(JBMO 2005)

Άσκηση 2.64 Για τους ακέραιους x, y ισχύει ότι $x^3 + y^3 + (x+y)^3 + 30xy = 2000$. Να δείξετε ότι $x + y = 10$. (JBMO 2000)

Άσκηση 2.65 Καλούμε έναν αριθμό ημιπρώτο, εάν είναι σύνθετος αλλήλα όχι διαιρετός από τους 2, 3 και 5. Οι τρεις μικρότεροι είναι οι 49, 77, 91. Υπάρχουν 168 πρώτοι αριθμοί που είναι μικρότεροι του 1000. Πόσοι ημιπρώτοι είναι μικρότεροι του 1000;

Άσκηση 2.66 Έστω $n = 2^{31} \cdot 3^{19}$. Πόσοι θετικοί διαιρέτες του n^2 είναι μικρότεροι του n αλλήλα δε διαιρούν το n ;

Άσκηση 2.67 Να βρεθούν οι θετικοί ακέραιοι k για τους οποίους ο αριθμός $k^{\frac{1}{k-7}}$ είναι ακέραιος.

Άσκηση 2.68 Να αποδείξετε ότι υπάρχουν τουλάχιστον 5 ζευγάρια από διαδοχικούς θετικούς ακέραιους τέτοιους ώστε το άθροισμα των τετραγώνων των αριθμών σε κάθε ζευγάρι διαιρεί τον αριθμό $2^{2006} + 1$. (**BMO Shortlist 2006**)

Άσκηση 2.69 Έστω $A = \{0, 1, 2, \dots, n\}$ όπου $n \in \mathbb{N}$. Έστω S το σύνολο των τριάδων (a_1, a_2, a_3) όπου $a_1, a_2, a_3 \in A$ για τις οποίες $|a_1 - a_2| = |a_2 - a_3|$. Να βρεθεί ο αριθμός των στοιχείων του συνόλου S (**BMO Shortlist 2006**)

Άσκηση 2.70 Να βρεθούν όλες οι τριάδες (m, n, p) θετικών ρητών αριθμών που είναι τέτοιες ώστε οι αριθμοί $m + \frac{1}{np}$, $n + \frac{1}{pm}$, $p + \frac{1}{mn}$ να είναι ακέραιοι. (**BMO 2006**)

Άσκηση 2.71 Να αποδείξετε ότι ο αριθμός $2(2006m^2 + 2007mn + 2008n^2)$ με m, n θετικούς ακέραιους δεν είναι ποτέ τέλειο τετράγωνο ακέραιου. (**Παραβλητική Θέματος διαγωνισμού «Ο Αρχιμήδης» 1994**).

Άσκηση 2.72 Να αποδείξετε ότι για κάθε φυσικό αριθμό n , υπάρχει φυσικός αριθμός k τέτοιος ώστε

$$\sqrt{k + 2006^n} + \sqrt{k} = \left(\sqrt{2007} + 1\right)^n.$$

(**Παραβλητική Θέματος 2ης Προκριματικής Φάσης 1997**)

Άσκηση 2.73 Να αποδείξετε ότι η εξίσωση $(x - y)^3 + (y - z)^3 + (z - x)^3 = 30$ δεν έχει ακέραιες λύσεις. (**1η Προκριματική Φάση 1997**)

Άσκηση 2.74 Να βρείτε τους θετικούς ακέραιους (x, y) που είναι τέτοιοι ώστε $y|x^2 + 1$ και $x^2|y^3 + 1$.

(**Μεσογειακός 2002**)

Άσκηση 2.75 Μπορούμε να φτιάξουμε μία ακολουθία από n διαδοχικούς σύνθετους αριθμούς για οποιοδήποτε n ;

Άσκηση 2.76 Να βρεθούν όλοι οι θετικοί ακέραιοι n που είναι τέτοιοι ώστε ο $n!$ να λήγει σε ακριβώς 40 μηδενικά.

Άσκηση 2.77 Αν N είναι ένας αριθμός του οποίου το δεκαδικό ανάπτυγμα έχει 3^n ίδια ψηφία, να αποδείξετε ότι $3^n | N$.

Άσκηση 2.78 Να αποδείξετε ότι ο αριθμός $1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}$ δεν είναι ακέραιος για οποιαδήποτε τιμή του ακέραιου $n > 1$.

3 Τέλειες δυνάμεις ακεραίων

3.1 Ασκήσεις Α΄ Ομάδας

Άσκηση 3.1 Να δείξετε ότι για $n \geq 1$ ο αριθμός $\underbrace{111 \dots 1}_{2n \text{ άσσοι}} - \underbrace{222 \dots 2}_{n \text{ 2-άρια}}$ είναι τετράγωνο ακεραίου.

Άσκηση 3.2 Να δείξετε ότι για κάθε $n \geq 1$, ο αριθμός $\underbrace{444 \dots 4}_n \underbrace{888 \dots 8}_{n-1 \text{ 8-άρια}} 9$ είναι τέλειο τετράγωνο ακεραίου.

Άσκηση 3.3 Να βρεθούν όλα τα δυνατά υπόλοιπα που μπορεί να αφήσει ένα τέλειο τετράγωνο όταν διαιρεθεί με το 13.

Άσκηση 3.4 Να δείξετε ότι η εξίσωση $4x^3 - 7y^3 = 2003$ δεν έχει ακέραιες λύσεις.

Άσκηση 3.5 Να δείξετε ότι η εξίσωση $x^3 + y^4 = 7$ δεν έχει ακέραιες λύσεις.

Άσκηση 3.6 Να αποδείξετε ότι η εξίσωση $x^2 - 4x - 19^{96} - 96^{19} - 2000 = 0$ δεν έχει ακέραια λύση.

Άσκηση 3.7 Αν οι αριθμοί $a, a + d, a + 2d$ είναι πρώτοι > 3 , να δείξετε ότι $6 \mid d$. **(Διαγωνισμός «Ο Θαλής» 1997)**

Άσκηση 3.8 Να αποδείξετε ότι στο σύνολο $\{11, 111, 1111, \dots\}$ δεν υπάρχουν τέλεια τετράγωνα.

Άσκηση 3.9 Να βρείτε όλους τους πρώτους p που είναι τέτοιοι ώστε ο $17p + 1$ να είναι τέλειο τετράγωνο ακεραίου.

Άσκηση 3.10 Να αποδείξετε ότι εαν $(a, b) = 1$ και το γινόμενο $ab = 1$ είναι μία τέλεια k -δύναμη, τότε να αποδείξετε ότι κάθε ένα από τα a, b είναι τέλεια k -δύναμη.

Άσκηση 3.11 (i) Έστω a, b, c θετικοί ακέραιοι. Να δείξετε ότι εάν οι ab, bc, ac είναι τέλειοι κύβοι τότε κάθε ένας από τους a, b, c είναι τέλειος κύβος.

(ii) Να εξετάσετε τί συμβαίνει εάν στο προηγούμενο ερώτημα έχουμε τέλεια k -δύναμη για k οποιοδήποτε ακέραιο αντί για τέλειο κύβο.

Άσκηση 3.12 Υποθέτουμε ότι οι $q_1, q_2, \dots, q_n$ είναι περιττοί πρώτοι αριθμοί. Μπορεί ο αριθμός $N = (q_1 q_2 \dots q_n)^2 + 1$ να είναι τέλειο τετράγωνο;

Άσκηση 3.13 Να αποδείξετε ότι οποιοσδήποτε αριθμός της μορφής $4k + 3$ δεν μπορεί να γραφτεί σαν άθροισμα δύο τετραγώνων.

Άσκηση 3.14 Να αποδείξετε ότι η εξίσωση $x^2 - 2y^2 = 10$ δεν έχει ακέραιες λύσεις.

Άσκηση 3.15 Να δείξετε ότι εάν ο n έχει περιττό πλήθος διαιρετών τότε ο n είναι τέλειο τετράγωνο.

Άσκηση 3.16 Εάν ένας αριθμός n γραφτεί σαν άθροισμα κάποιων ακεραίων τότε το άθροισμα των κύβων αυτών των ακεραίων είναι ισότιμο με $n \pmod{6}$.

3.2 Ασκήσεις Β' Ομάδας

Άσκηση 3.17 Να βρεθούν όλοι οι φυσικοί n για τους οποίους η παράσταση

$$A = n^4 + 4n^3 + 5n^2 + 6n$$

είναι τέλειο τετράγωνο φυσικού. **(Διαγωνισμός «Ο Αρχιμήδης» 1997)**

Άσκηση 3.18 Να αποδείξετε ότι η ισοτιμία $x^2 \equiv -1 \pmod{p}$ έχει λύση με p πρώτο αριθμό, αν και μόνο αν ο p είναι της μορφής $p = 4k + 1$ για κάποιο ακέραιο αριθμό k .

Άσκηση 3.19 Εάν ο p είναι πρώτος τότε να δείξετε ότι ο αριθμός $A = 7p + 3^p - 4$ δεν είναι τέλειο τετράγωνο ακεραίου. **(JBMO 2007)**

Άσκηση 3.20 Να δείξετε ότι ο αριθμός

$$A = \underbrace{111 \dots 1}_{1997 \text{ άσσοι}} \underbrace{222 \dots 2}_{1997 \text{ δυνάρια}} 5$$

είναι τέλειο τετράγωνο ακεραίου. **(JBMO 1998)**

Άσκηση 3.21 Να βρεθούν οι ακέραιοι $n \geq 1$ ώστε ο $n^2 + 3^n$ να είναι τέλειο τετράγωνο. **(JBMO 2000)**

Άσκηση 3.22 Έστω n θετικός ακέραιος. Ένας αριθμός A έχει $2n$ ψηφία καθένα από τα οποία είναι το 4 και ένας αριθμός B έχει n ψηφία καθένα από τα οποία είναι το 8. Να δείξετε ότι ο αριθμός $A + 2B + 4$ είναι τέλειο τετράγωνο ακεραίου. **(JBMO 2003)**

Άσκηση 3.23 Αν οι θετικοί ακέραιοι x, y είναι τέτοιτοι ώστε οι αριθμοί $3x + 4y$ και $4x + 3y$ να είναι τέλεια τετράγωνα, να δείξετε ότι οι αριθμοί x, y είναι και οι δύο πολλαπλάσια του 7.

Άσκηση 3.24 Να αποδείξετε ότι για οποιουσδήποτε θετικούς ακεραίους a, b ο αριθμός $(36a + b)(a + 36b)$ δεν είναι δύναμη του 2.

Άσκηση 3.25 Να αποδείξετε ότι το τετράγωνο περιττού αριθμού είναι πάντοτε της μορφής $8n + 1$.

Άσκηση 3.26 Να προσδιορίσετε τον πρώτο αριθμό p που είναι τέτοιος ώστε η παράσταση $A = 1 + p + p^2 + p^3 + p^4$ είναι τέλειο τετράγωνο ακεραίου.

Εφαρμογές

- (i) Αν οι a, b, c, m είναι ακέραιοι να αποδείξετε ότι ο αριθμός $a^2 + b^2 + c^2$ δεν είναι ποτέ της μορφής $8m + 7$.
- (ii) Να δείξετε ότι η παράσταση $2^n + 3^n + 4^n$ δεν είναι ποτέ τέλειο τετράγωνο ακεραίου για $n > 1$ και περιττό.
- (iii) Εάν οι a, b, c είναι ακέραιοι με $a^2 = b^2 + c^2$ τότε να δείξετε ότι $4|b$ ή $4|c$.
- (iv) Να αποδείξετε ότι η εξίσωση $2^m - 1 = x^n$ δεν έχει ακέραιες λύσεις αν $m, n > 1$.
- (v) Να αποδείξετε ότι για a, n φυσικούς, η παράσταση

$$A = (a + 1)^n + (a + 2)^n + (a + 3)^n + (a + 4)^n$$

δεν είναι ποτέ τέλειο τετράγωνο ακεραίου.

- (vi) Αν οι αριθμοί $a_1, a_2, \dots, a_{1998}$ είναι φυσικοί και ικανοποιούν την ισότητα

$$a_1^2 + a_2^2 + \dots + a_{1997}^2 = a_{1998}^2,$$

να αποδείξετε ότι δύο τουλάχιστον από αυτούς είναι άρτιοι. **(JBMO 1998)**

- (vii) Να αποδείξετε ότι η εξίσωση $3x^2 - y^2 = 5^z$ δεν έχει ακέραιες λύσεις.

Άσκηση 3.27 Να αποδείξετε ότι το τετράγωνο οποιουδήποτε ακεραίου είναι της μορφής $3m$ ή $3m + 1$.

Εφαρμογές

- (i) Να αποδείξετε ότι το άθροισμα τριών διαδοχικών ακεραίων δεν μπορεί να είναι τέλειο τετράγωνο.

- (ii) Να δείξετε ότι η παράσταση $2^n + 3^n + 4^n$ δεν είναι ποτέ τέλειο τετράγωνο ακεραίου για n άρτιο.
- (iii) Εάν a, b, c ακέραιοι με $a^2 = b^2 + c^2$, τότε $3|bc$.
- (iv) Να αποδείξετε ότι η εξίσωση $3x^2 - y^2 = 1998$ δεν έχει ακέραιες λύσεις.
- (v) Να αποδείξετε ότι για οποιοδήποτε ακέραιο n , ο αριθμός $A = (n-1)^3 + n^3 + (n+1)^3$ είναι πολλαπλάσιο του 9.
- (vi) Να αποδείξετε ότι το άθροισμα των κύβων εννέα διαδοχικών ακεραίων διαιρείται από το 27.

Άσκηση 3.28 Να αποδείξετε ότι το τετράγωνο οποιουδήποτε ακεραίου είναι της μορφής $5m$ ή $5m \pm 1$.

Εφαρμογές

- (i) Εάν a, b, c ακέραιοι με $a^2 = b^2 + c^2$ τότε $5|abc$.
- (ii) Να αποδείξετε ότι η εξίσωση $x^2 - 5y^2 = 200$ δεν έχει ακέραιες λύσεις.
- (iii) Για $n > 3$ φυσικό, ο αριθμός $S_n = \sum_{k=1}^n k!$ δεν είναι ποτέ τέλειο τετράγωνο ακεραίου.
- (iv) Εάν οι a, b είναι ακέραιοι τέτοιοι ώστε $5|a^4 + b^4$, τότε να δείξετε ότι $5^4|a^4 + b^4$.
- (v) Να αποδείξετε ότι η εξίσωση $x^2 + xy + y^2 = 5z^2$ δεν έχει λύση στους ακεραίους.

Άσκηση 3.29 Να αποδείξετε ότι ο κύβος οποιουδήποτε ακεραίου είναι της μορφής $7m$ ή $7m \pm 1$.

Εφαρμογές

- (i) Να αποδείξετε ότι η εξίσωση $x^3 + y^3 = 2006$ δεν έχει ακέραιες λύσεις.
- (ii) Για $n > 1$ φυσικό, ο αριθμός $S_n = \sum_{k=1}^n k!$ δεν είναι ποτέ τέλειος κύβος ακεραίου.
- (iii) Να αποδείξετε ότι η παράσταση $A = 1^n + 2^n + 3^n + 4^n$ δεν είναι ποτέ τέλειος κύβος ακεραίου.
- (iv) Να αποδείξετε ότι η παράσταση $A = 1 + 2^n + 2^{2n}$ δεν είναι ποτέ τέλειος κύβος ακεραίου.
- (v) Να αποδείξετε ότι η εξίσωση $19x^3 - 84y^2 = 1984$ δεν έχει λύσεις στους ακεραίους **(Ρωσία 1984)**.

(vi) Να αποδείξετε ότι η παράσταση $A = 2^n + 3^n + 5^n + 6^n$ δεν είναι ποτέ τέλειος κύβος ακεραίου.

(vii) Εάν οι αριθμοί a, b, c είναι ακέραιοι τέτοιοι ώστε $7|a^3 + b^3 + c^3$ τότε $7|abc$.

Άσκηση 3.30 Να αποδείξετε ότι ο κύβος οποιουδήποτε ακεραίου είναι της μορφής $9m$ ή $9m \pm 1$.

Εφαρμογές

(i) Να αποδείξετε ότι το άθροισμα των τετραγώνων τριών διαδοχικών ακεραίων δεν είναι ποτέ τέλειος κύβος ακεραίου.

(ii) Να αποδείξετε ότι η εξίσωση $x^3 + y^3 + z^3 = 2003$ δεν έχει ακέραιες λύσεις.

(iii) Εάν οι αριθμοί a, b, c είναι ακέραιοι τέτοιοι ώστε $9|a^3 + b^3 + c^3$ τότε $3|abc$.

(iv) Να αποδείξετε ότι υπάρχουν άπειροι ακέραιοι που δε γράφονται σαν άθροισμα τριών τέλειων κύβων ακεραίων αριθμών.

(v) Να αποδείξετε ότι ο αριθμός 123456 καθώς και οποιοσδήποτε 6-ψήφιος προκύπτει από την αντιμετάθεση των ψηφίων του, δεν είναι τέλειος κύβος ακεραίου.

(vi) Εάν οι αριθμοί a, b, c είναι ακέραιοι τέτοιοι ώστε $3^2|a^3 + b^3 + c^3$ να αποδείξετε ότι $3^6|a^3 + b^3 + c^3$.

(vii) Να βρεθούν όλοι οι θετικοί ακέραιοι a, b, c που είναι τέτοιοι ώστε $a^3 + b^3 + c^3 = 2001$.
(JBMO 2001)

Άσκηση 3.31 Να αποδείξετε ότι το γινόμενο οποιουδήποτε τεσσάρων διαδοχικών ακεραίων δεν είναι ποτέ τέλειο τετράγωνο ¹

Άσκηση 3.32 (i) Να αποδείξετε ότι κανένας αριθμός της μορφής $8k+7$ όπου k ακέραιος, δεν μπορεί να γραφτεί σαν άθροισμα τριών τετραγώνων.

(ii) Να κάνετε χρήση του παραπάνω αποτελέσματος για να δείξετε ότι κανένας αριθμός της μορφής $4^m(8k+7)$ όπου m θετικός ακέραιος και k ακέραιος, δεν μπορεί να γραφτεί σαν άθροισμα τριών τετραγώνων.

Άσκηση 3.33 Να βρείτε το μικρότερο θετικό ακέραιο n που είναι τέτοιος ώστε ο $\frac{n}{3}$ να είναι τέλειος κύβος, ο $\frac{n}{5}$ να είναι τέλεια πέμπτη δύναμη και ο $\frac{n}{7}$ να είναι τέλεια έβδομη δύναμη.

¹Στην πραγματικότητα αυτό είναι μερικό αποτέλεσμα ενός γενικότερου πολύ ισχυρού θεωρήματος που οφείλεται στους Erdos και Selfridge (1975) σύμφωνα με το οποίο το γινόμενο οποιονδήποτε διαδοχικών ακεραίων δεν είναι ποτέ τέλεια k - δύναμη για οποιονδήποτε $k \geq 2$.

Άσκηση 3.34 Να εξετάσετε εάν υπάρχουν θετικές ακέραιες τιμές του x ώστε οι παραστάσεις

$$(i) -5^x + 5^5 + 5^x$$

$$(ii) 2^4 + 2^7 + 2^x$$

να γίνονται τέλεια τετράγωνα. **(Διαγωνισμός «Ο Αρχιμήδης» 1995)**

4 Μέγιστος Κοινός Διαιρέτης και Ελάχιστο Κοινό Πολλαπλάσιο

4.1 Ασκήσεις Α΄ Ομάδας

Άσκηση 4.1 Για οποιουσδήποτε μη μηδενικούς ακραίους a, b , να δείξετε ότι

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

Άσκηση 4.2 Αν a, b, c φυσικοί και $(a, b, c)[a, b, c] = abc$ να δείξετε ότι

$$(a, b) = (b, c) = (c, a) = 1.$$

Άσκηση 4.3 Για οποιουσδήποτε φυσικούς a, b, c να αποδειχθούν οι ισότητες:

$$(i) (a, [b, c]) = [(a, b), (a, c)],$$

$$(ii) [a, (b, c)] = ([a, b], [a, c]).$$

Άσκηση 4.4 Για οποιουσδήποτε μη μηδενικούς ακραίους a, b, c να δείξετε ότι

$$([a, b], [b, c], [c, a]) = [(a, b), (b, c), (c, a)].$$

Άσκηση 4.5 Αν οι φυσικοί m, n είναι πρώτοι μεταξύ τους, να δείξετε ότι

$$(m^2 + n^2, m + n) \in \{1, 2\}.$$

Άσκηση 4.6 Δείξτε ότι $(15n^2 + 8n + 6, 30n^2 + 21n + 13) = 1$ για κάθε n φυσικό.

Άσκηση 4.7 Έστω a, b, c φυσικοί αριθμοί τέτοιοι ώστε η παράσταση

$$K = \frac{a+1}{b} + \frac{b+1}{c} + \frac{c+1}{a}$$

είναι φυσικός. Να αποδείξετε ότι $(a, b, c) \leq \sqrt[3]{ab + bc + ca}$.

Άσκηση 4.8 Να αποδείξετε ότι το κλάσμα $\frac{n^4 + 3n^2 + 1}{n^3 + 2n}$ είναι ανάγωγο για κάθε $n \in \mathbb{Z}^*$.

Άσκηση 4.9 Έστω a, b, c, d θετικοί ακέραιοι με $b \neq d$. Να δείξετε ότι εάν τα κλάσματα $\frac{a}{b}$ και $\frac{c}{d}$ είναι ανάγωγα τότε η παράσταση $\frac{a}{b} + \frac{c}{d}$ δεν είναι ακέραιος.

Άσκηση 4.10 Να δείξετε ότι οι αριθμοί $n! + 1$ και $(n + 1)! + 1$ είναι πρώτοι μεταξύ τους.

Άσκηση 4.11 Εάν $(a, b) = 1$ τότε να δείξετε ότι $(a + b, a - b) = 1$ ή 2 .

Άσκηση 4.12 Να αποδείξετε ότι για οποιοδήποτε φυσικό αριθμό n , τα παρακάτω ζεύγη αριθμών είναι αριθμοί πρώτοι μεταξύ τους:

(i) $6n + 5$ και $7n + 6$,

(ii) $10n + 3$ και $15n + 4$,

(iii) $4 \cdot 7^n + 3$ και $5 \cdot 7^n + 4$.

Άσκηση 4.13 Εάν $(a, b) = 1$ και $c|a + b$, να δείξετε ότι $(a, c) = (b, c) = 1$.

Άσκηση 4.14 Να δείξετε ότι εάν $(b, c) = 1$ και $m|b$ τότε $(m, c) = 1$.

Άσκηση 4.15 Με τον Ευκλείδειο Αλγόριθμο βρείτε το $(93, 51)$ καθώς επίσης και ακεραίους a, b που είναι τέτοιοι ώστε $93a + 51b = (93, 51)$.

Άσκηση 4.16 Βρείτε τους φυσικούς a, b που είναι τέτοιοι ώστε $a + b = 1089$ και $(a, b) = 121$.

Άσκηση 4.17 Βρείτε τους φυσικούς a, b που είναι τέτοιοι ώστε $ab = 1600$ και

$$[a, b] = 4 \cdot (a, b).$$

Άσκηση 4.18 Βρείτε τους φυσικούς a, b με $a < b$ που είναι τέτοιοι ώστε $[a, b] - (a, b) = 34$.

Άσκηση 4.19 Εάν τοποθετήσουμε τους μαθητές ενός σχολείου σε σειρές 2, 3, 4, 5 ή 6 μαθητών τότε περισσεύει κάθε φορά ένας μαθητής αλλιώς εάν τους τοποθετήσουμε σε σειρά των 7, τότε όλες οι σειρές είναι πλήρεις και δεν περισσεύει κανένας μαθητής. Να βρείτε τον ελάχιστο αριθμό μαθητών που μπορεί να έχει το σχολείο.

Άσκηση 4.20 Να δείξετε ότι εάν b θετικός ακέραιος τότε ακριβώς (b, n) από τους αριθμούς $n, 2n, 3n, \dots, bn$ είναι πολλαπλάσια του b .

Άσκηση 4.21 Ποιός είναι ο ελάχιστος θετικός ρητός αριθμός που μπορεί να εκφραστεί στη μορφή $\frac{x}{30} + \frac{y}{36}$ με x, y ακεραίους;

4.2 Ασκήσεις Β' Ομάδας

Άσκηση 4.22 Για οποιουδήποτε φυσικούς a, m, n με $a \geq 2$, να δείξετε ότι

$$(a^m - 1, a^n - 1) = a^{(m,n)} - 1.$$

Άσκηση 4.23 Ο αριθμός $A_n = 2^{3n} + 3^{6n+2} + 5^{6n+2}$ ορίζεται για $n = 0, 1, 2, \dots, 1999$. Να βρείτε το μέγιστο κοινό διαιρέτη των αριθμών $A_0, A_1, A_2, \dots, A_{1999}$. **(JBMO 1999)**

Άσκηση 4.24 Έστω m, n θετικοί ακέραιοι τέτοιοι ώστε $[m, n] + (m, n) = m + n$. Να δείξετε ότι ένας από τους δύο αριθμούς είναι διαιρετός από τον άλλο. **(Ρωσία 1995)**

Άσκηση 4.25 Να αποδείξετε ότι το κλάσμα $\frac{21n+4}{14n+3}$ είναι ανάγωγο για κάθε $n \in \mathbb{Z}$. **(IMO 1959)**

Άσκηση 4.26 Το άθροισμα δύο θετικών ακεραίων είναι ίσο με 5432 και το ελάχιστο κοινό πολλαπλάσιό τους είναι 223020. Να βρείτε τους δύο αριθμούς.

Άσκηση 4.27 Εάν $(a, b) = 10$ να βρείτε όλες τις πιθανές τιμές που παίρνει το (a^3, b^4) .

Άσκηση 4.28 Ας υποθέσουμε ότι ο n είναι θετικός ακέραιος και έχει r διακεκριμένους πρώτους διαιρέτες. Να δείξετε ότι υπάρχουν 2^r διατεταγμένα ζεύγη (x, y) πρώτων μεταξύ τους ακεραίων τέτοια ώστε $xy = n$.

5 Πρώτοι αριθμοί και τα βασικά θεωρήματά τους

5.1 Ασκήσεις Α' Ομάδας

Άσκηση 5.1 Να βρεθούν όλοι οι πρώτοι αριθμοί της μορφής $n^3 - 1$ με $n > 1$.

Άσκηση 5.2 Να βρεθούν οι τιμές του n για τις οποίες ο αριθμός $n^4 + 4$ είναι πρώτος.

Άσκηση 5.3 Να δείξετε ότι αν ο αριθμός p είναι περιττός πρώτος και

$$\frac{a}{b} = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1},$$

τότε $p \mid a$.

Άσκηση 5.4 Να δείξετε ότι αν ο αριθμός $a^n - 1$, $1 < a \in \mathbb{N}$ είναι πρώτος τότε $a = 2$ και ο n είναι επίσης πρώτος. (Πρώτοι αυτής της μορφής ονομάζονται πρώτοι του **Mersenne**)

Άσκηση 5.5 Ας υποθέσουμε ότι οι p και $p+2$ είναι πρώτοι αριθμοί με $p > 3$. Να αποδείξετε ότι το άθροισμά τους διαιρείται από το 12.

Άσκηση 5.6 Να κάνετε χρήση της ισότητας $640 = 5 \cdot 2^7$ για να αποδείξετε ότι ο αριθμός Fermat $F_5 = 2^{2^5} + 1$ διαιρείται από το 641.

Άσκηση 5.7 Βρείτε έναν ακέραιο n με $0 \leq n \leq 16$ που είναι τέτοιος ώστε

$$3^{100} \equiv n \pmod{17}.$$

Άσκηση 5.8 Ποιό είναι το (ελάχιστο θετικό) υπόλοιπο της διαίρεσης του 55^{142} με το 143 ;

Άσκηση 5.9 Να δείξετε ότι για οποιοδήποτε μη αρνητικό ακέραιο αριθμό n , ο αριθμός $A = 3^{6n} - 2^{6n}$ διαιρείται από το 35.

Άσκηση 5.10 Υποθέτουμε ότι ο αριθμός p είναι πρώτος και ότι ισχύει $a^p + b^p = c^p$. Να αποδείξετε ότι $p | a + b - c$.

Άσκηση 5.11 Εάν p, q διακεκριμένοι περιττοί πρώτοι αριθμοί έτσι ώστε $p-1 | q-1$. Εάν $(a, pq) = 1$, να δείξετε ότι $a^{q-1} \equiv 1 \pmod{pq}$.

Άσκηση 5.12 Κάνοντας χρήση του θεωρήματος του Fermat να δείξετε ότι κάθε πρώτος $p > 5$ διαιρεί άπειρους αριθμούς της μορφής $999 \dots 9$ (δηλαδή αριθμούς που στη δεκαδική τους αναπαράσταση περιέχουν μόνο το ψηφίο 9).

Άσκηση 5.13 (i) Να αποδείξετε ότι υπάρχουν άπειροι ακέραιοι n για τους οποίους ο αριθμός $n! - 1$ είναι σύνθετος.

(ii) Να αποδείξετε ότι υπάρχουν άπειροι ακέραιοι n για τους οποίους ο αριθμός $n! + 1$ είναι σύνθετος.

Άσκηση 5.14 Να δείξετε ότι εάν ο p είναι πρώτος και $1 \leq n \leq p-1$, τότε

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

Άσκηση 5.15 Ας υποθέσουμε ότι $2^{n-1} \equiv 1 \pmod{n}$. Εάν $N = 2^n - 1$, να δείξετε ότι $2^{N-1} \equiv 1 \pmod{N}$.

Άσκηση 5.16 Να αποδείξετε ότι το τελευταίο ψηφίο της τέταρτης δύναμης οποιουδήποτε ακεραίου αριθμού που δε διαιρείται από το 2 ή το 5 είναι το 1.

Άσκηση 5.17 Να βρείτε τα δύο τελευταία ψηφία της δεκαδικής αναπαράστασης του 9^{9^9} .

Άσκηση 5.18 Να δείξετε ότι εάν ο $p > 3$ είναι πρώτος τότε ο αριθμός $p^2 - 1$ είναι πάντα πολλαπλάσιο του 24.

Άσκηση 5.19 Να δείξετε ότι εάν ο αριθμός $2^m + 1$ είναι πρώτος (m φυσικός) τότε το m είναι δύναμη του 2.

Άσκηση 5.20 Να δείξετε ότι όλοι οι αριθμοί του Fermat με τάξη μεγαλύτερη από 1 (δηλαδή οι αριθμοί $F_n = 2^{2^n} + 1$ με $n > 1$), έχουν τελευταίο ψηφίο το 7.

Άσκηση 5.21 Για ποιες τιμές του n ισχύει $\phi(n) = n - 2$;

Άσκηση 5.22 Να αποδείξετε ότι εάν d, n ακέραιοι τέτοιοι ώστε $d|n$, τότε $\phi(d)|\phi(n)$.

Άσκηση 5.23 Να αποδείξετε ότι $\phi(n) = \phi(2n)$ όταν το n είναι περιττός.

Άσκηση 5.24 Εάν n άρτιος τότε $\phi(n) = \frac{n}{2}$ αν και μόνο αν $n = 2^k$ για κάποιο ακέραιο $k \geq 1$.

5.2 Ασκήσεις Β' Ομάδας

Άσκηση 5.25 Να βρεθούν όλοι οι ακέραιοι $n \geq 1$ για τους οποίους ο $n^4 + 4^n$ είναι πρώτος.

Άσκηση 5.26 (i) Να βρεθεί ένας κλειστός τύπος για το γινόμενο

$$P = (1 + 2^{2^0}) (1 + 2^{2^1}) (1 + 2^{2^2}) \cdots (1 + 2^{2^n})$$

(ii) Κάνοντας χρήση του παραπάνω τύπου, να δείξετε ότι για όλους τους θετικούς ακέραιους n ισχύει $2^{2^n} + 1 \mid 2^{2^{2^n}+1} - 2$.

Άσκηση 5.27 Αν με p_n συμβολίζουμε τον n -οστό πρώτο αριθμό, να δείξετε ότι

$$(i) \quad p_n \leq p_1 \cdots p_{n-1} + 1 \text{ για } n \geq 2,$$

$$(ii) \quad p_{n-1} \geq n + 2 \text{ για } n \geq 5,$$

$$(iii) \quad p_{n-1} \geq 2n + 2 \text{ για } n \geq 10,$$

$$(iv) \quad p_n \leq 2^{2^{n-1}} \text{ για κάθε } n.$$

Άσκηση 5.28 Καλούμε έναν αριθμό n τέλει εάν το άθροισμα των θετικών ακεραίων διαιρετών του (μαζί με το 1 και το n) ισούται με $2n$. Να βρείτε όλους τους τέλει αριθμούς n που είναι τέτοιοι ώστε οι αριθμοί $n - 1$ και $n + 1$ να είναι πρώτοι αριθμοί. **(JBO 2006)**

Άσκηση 5.29 Να βρείτε όλους τους πρώτους αριθμούς p που είναι τέτοιοι ώστε ο αριθμός $p^2 + 11$ να έχει ακριβώς 6 διαφορετικούς διαιρέτες (συμπεριλαμβανομένου του 1 και του ίδιου του αριθμού).

Άσκηση 5.30 Έστω p πρώτος και $1 \leq k \leq p-1$ ακέραιος. Να δείξετε ότι

$$\binom{p-1}{k} \equiv (-1)^k \pmod{p}.$$

Άσκηση 5.31 Εάν ο p είναι πρώτος τότε να εξετάσετε εάν ο αριθμός

$$N = p^{1997} + 1997^p + 1998^{1997+p}$$

είναι πρώτος. **(Διαγωνισμός «Ο Θαλής» 1997)**

Άσκηση 5.32 (i) Να αποδείξετε ότι οποιοσδήποτε θετικός ακέραιος της μορφής $4k+3$ έχει ένα πρώτο διαιρέτη της ίδιας μορφής.

(ii) Κάνοντας χρήση του παραπάνω αποτελέσματος και μιμούμενος την απόδειξη του Ευκλείδη, να δείξετε ότι υπάρχουν άπειροι πρώτοι της μορφής $4k+3$.

Άσκηση 5.33 Εάν p πρώτος αριθμός της μορφής $4k+3$ (k φυσικός), να αποδείξετε ότι αν $x, y \in \mathbb{Z}$ και $p|x^2 + y^2$, τότε $p|x$ και $p|y$. **(3η Προκριματική Φάση 1996)**

Άσκηση 5.34 Να αποδείξετε ότι εάν ο n είναι ακέραιος τότε και ο $A = \frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$ είναι ακέραιος.

Άσκηση 5.35 (i) Έστω a ακέραιος, u, v θετικοί ακέραιοι και $m > 1$ έτσι ώστε $a^u \equiv 1 \pmod{m}$ και $a^v \equiv 1 \pmod{m}$ τότε $a^d \equiv 1 \pmod{m}$, όπου $d = (u, v)$.

(ii) Να δείξετε ότι εάν $n|2^n - 1$ τότε $n = 1$.

Άσκηση 5.36 (i) Να αποδείξετε το αντίστροφο του θεωρήματος Wilson: Εάν $m > 1$ και ο m δεν είναι πρώτος, τότε $(m-1)! \not\equiv -1 \pmod{m}$.

(ii) [Ισχυρότερο από το (i)] Εάν $m > 4$ σύνθετος τότε $(m-1)! \equiv 0 \pmod{m}$.

(iii) Να βρείτε όλους τους ακεραίους $n > 1$ που είναι τέτοιοι ώστε $n(n+1)|(n-1)!$.

Άσκηση 5.37 Να δείξετε ότι για οποιοδήποτε πρώτο p και οποιοδήποτε ακέραιο a , ο αριθμός $a^p + (p-1)!a$ διαιρείται από το p .

Άσκηση 5.38 Να δείξετε ότι εάν οι αριθμοί $n, n+2$ είναι πρώτοι τότε

$$4[(n-1)! + 1] + n \equiv 0 \pmod{n(n+2)}.$$

Άσκηση 5.39 (Liouville 1856) Εάν ο p είναι κάποιος από τους πρώτους 2, 3 ή 5 τότε ο αριθμός $(p-1)! + 1$ είναι τέλεια δύναμη πρώτου. Να δείξετε ότι αυτό δεν ισχύει για $p > 5$ δείχνοντας τα παρακάτω:

- (i) Εάν $p > 5$ τότε $(p-1)^2 \mid (p-1)!$.
- (ii) Εάν ο αριθμός $(p-1)! + 1$ είναι τέλεια δύναμη πρώτου τότε είναι δύναμη του πρώτου p (και όχι κάποιου τυχαίου).
- (iii) Εάν $(p-1)! + 1 = p^k$ για κάποιο ακέραιο k τότε $p-1 \mid p^{k-1} + p^{k-2} + \dots + p + 1$. Αυτό μπορεί να συμβαίνει μόνο εάν $p-1 \mid k$ και τότε η εξίσωση $(p-1)! + 1 = p^k$ είναι αδύνατη.

Άσκηση 5.40 (i) Να δείξετε ότι εάν ο αριθμός p είναι πρώτος και $p \nmid a$ τότε ο αριθμός ba^{p-2} είναι λύση της ισοτιμίας $ax \equiv b \pmod{p}$. Να χρησιμοποιήσετε αυτή την τεχνική για να λύσετε την ισοτιμία $5x \equiv 4 \pmod{17}$.

- (ii) Προσαρμόστε την ιδέα του ερωτήματος (i) ώστε να βρείτε τη λύση της ισοτιμίας $ax \equiv b \pmod{n}$ όταν $(a, n) = 1$ και το n δεν είναι απαραίτητα πρώτος αριθμός. Χρησιμοποιήστε αυτό τον τρόπο για να λύσετε την ισοτιμία $5x \equiv 4 \pmod{42}$.

Άσκηση 5.41 (i) Ας υποθέσουμε ότι $(a, m) = 1$ και $n \mid t\phi(m) + 1$ για κάποιο ακέραιο t . Να αποδείξετε ότι η ισοτιμία $x^n \equiv a \pmod{m}$ έχει μοναδική λύση την a^k όπου $k = \frac{t\phi(m) + 1}{n}$.

- (ii) Χρησιμοποιώντας το προηγούμενο ερώτημα να λύσετε τις ισοτιμίες

- $x^{11} \equiv 3 \pmod{68}$,
- $x^{13} \equiv 7 \pmod{68}$,
- $x^{23} \equiv 5 \pmod{68}$.

Άσκηση 5.42 (i) Υποθέτουμε ότι ο m είναι σύνθετος αλλήλα ότι $a^{m-1} \equiv 1 \pmod{m}$, όπου $a \not\equiv 1 \pmod{m}$. Να κάνετε χρήση του θεωρήματος Euler και της άσκησης 5.35(i) για να δείξετε ότι $a^d \equiv 1 \pmod{m}$ για κάποιο κατάλληλο διαιρέτη d του $n-1$.

- (ii) Να κάνετε χρήση του προηγούμενου ερωτήματος για να δείξετε ότι εάν υπάρχει a τέτοιο ώστε $a^{m-1} \equiv 1 \pmod{m}$ αλλήλα $a^{\frac{m-1}{p}} \not\equiv 1 \pmod{m}$, για οποιοδήποτε πρώτο διαιρέτη p του $m-1$, τότε ο m είναι πρώτος.

Άσκηση 5.43 (i) Υποθέστε ότι $a = 2^k b$ όπου ο b είναι περιττός. Εάν $\phi(x) = a$, να δείξετε ότι ο x έχει το πολύ k διακεκριμένους περιττούς πρώτους παράγοντες.

- (ii) Να κάνετε χρήση του προηγούμενου ερωτήματος για να χαρακτηρίσετε εκείνους τους ακέραιους n για τους οποίους το $\phi(n)$ δεν είναι διαιρετό από το 4.

Άσκηση 5.44 (i) Να αποδείξετε ότι δεν υπάρχει ακέραιος n για τον οποίο $\phi(n) = 14$.

- (ii) Να αποδείξετε ότι δεν υπάρχει ακέραιος n τέτοιος ώστε $\phi(n) = 2 \cdot 7^k$, όπου $k \geq 1$ ακέραιος (χρησιμοποιήστε την άσκηση 5.43(ii) και μετά αποδείξτε ότι ο αριθμός $2 \cdot 7^k + 1$ δεν είναι ποτέ πρώτος).

- (iii) Να βρείτε κι άλλες περιπτώσεις στις οποίες το διπλάσιο ενός περιττού αριθμού δεν μπορεί να είναι ίσο με το $\phi(n)$ για κάποιο φυσικό αριθμό n .

6 Ισοτιμίες

6.1 Ασκήσεις Α΄ Ομάδας

Άσκηση 6.1 Να βρεθεί το υπόλοιπο του 6^{1987} με το 37.

Άσκηση 6.2 Να αποδείξετε ότι δεν υπάρχουν ακέραιοι x, y τέτοιοι ώστε $x^2 - 5y^2 = 2$.

Άσκηση 6.3 Να βρεθεί το τελευταίο ψηφίο του αριθμού 7^{7^7} .

Άσκηση 6.4 Να δείξετε ότι κάθε χρόνος (κανονικός ή δίσεκτος) έχει πάντα τουλάχιστον μία Τρίτη και 13.

Άσκηση 6.5 Να βρεθούν άπειροι ακέραιοι αριθμοί n τέτοιοι ώστε $7 \mid 2^n + 27$.

Άσκηση 6.6 Εάν k θετικός ακέραιος τότε να δείξετε ότι $2^k - 5 \not\equiv 1 \pmod{7}$.

Άσκηση 6.7 Να βρεθεί (το ελάχιστο θετικό) υπόλοιπο της διαίρεσης του αριθμού

$$1! + 2! + \cdots + 100!$$

με το 45.

Άσκηση 6.8 Να αποδείξετε ότι για εαν ο $p \geq 5$ είναι πρώτος τότε ο αριθμός $p^2 + 2$ είναι σύνθετος.

Άσκηση 6.9 Να αποδείξετε ότι ο αριθμός $2^{2^n} + 5$ είναι σύνθετος για οποιαδήποτε τιμή του θετικού ακεραίου n .

Άσκηση 6.10 Να αποδείξετε ότι ο αριθμός $n^3 + 11n + 1$ δε διαιρείται από κανένα από τους αριθμούς 2, 3, 5, 7 για οποιοδήποτε ακέραιο n .

6.2 Ασκήσεις Β' Ομάδας

Άσκηση 6.11 Να αποδείξετε ότι οι αριθμοί $n(n-1)$ και $(n+1)^2$ έχουν διαφορετικό άθροισμα ψηφίων. (Διαγωνισμός «Ο Ευκλείδης» 1997)

Άσκηση 6.12 Εάν $a \equiv b \pmod{n}$, να δείξετε ότι $a^n \equiv b^n \pmod{n^2}$. Ισχύει το αντίστροφο ;

Άσκηση 6.13 Για κάθε θετικό ακέραιο n ορίζουμε $a_n = 1^1 + 2^2 + 3^3 + \dots + n^n$. Να αποδείξετε ότι υπάρχουν άπειρες τιμές του n για τις οποίες ο a_n είναι περιττός και σύνθετος αριθμός.

Άσκηση 6.14 Υπάρχει ζεύγος φυσικών x και y για τους οποίους ισχύει:

$$(i) \quad x^3 + y^4 = 2^{2003};$$

$$(ii) \quad x^3 + y^4 = 2^{2005};$$

Άσκηση 6.15 Να αποδείξετε ότι δεν υπάρχουν ρητοί αριθμοί x, y, z τέτοιοι ώστε

$$x^2 + y^2 + z^2 + 3(x + y + z) + 5 = 0.$$

Άσκηση 6.16 Για ποιες τιμές του λ το πολυώνυμο $x^3 + 1995x^2 - 1994x + \lambda$ έχει και τις τρεις ρίζες του ακέραιες ; (Διαγωνισμός «Ο Αρχιμήδης» 1994)

Άσκηση 6.17 Να αποδείξετε ότι ο αριθμός $n^2 + n + 9$ δε διαιρείται με το 25 για οποιοδήποτε $n \in \mathbb{Z}$.

Άσκηση 6.18 Να αποδείξετε ότι οποιοσδήποτε ακέραιος x ικανοποιεί τουλάχιστον μία από τις ισοτιμίες $x \equiv 0 \pmod{2}$, $x \equiv 0 \pmod{3}$, $x \equiv 1 \pmod{4}$, $x \equiv 3 \pmod{8}$, $x \equiv 7 \pmod{12}$, $x \equiv 23 \pmod{24}$.

Άσκηση 6.19 Είναι το σύνολο $\{1^2, 2^2, 3^2, \dots, m^2\}$ πλήρες σύστημα υπολοίπων mod m ;

Άσκηση 6.20 Έστω p πρώτος. Να αποδείξετε ότι $\binom{2p}{p} \equiv 2 \pmod{p}$.

Άσκηση 6.21 Έστω n θετικός ακέραιος με $n \neq 1, 2, 3, 4, 6$. Να αποδείξετε ότι υπάρχουν ακέραιοι a και b με $1 < a < n-1$ και $1 < b < n-1$ τέτοιοι ώστε $ab \equiv -1 \pmod{n}$.

7 Διοφαντικές Εξισώσεις

7.1 Ασκήσεις Α' Ομάδας

Άσκηση 7.1 Να λυθεί στους ακεραίους η εξίσωση $3x + 5y = 2$.

Άσκηση 7.2 Να λυθεί στους ακεραίους η εξίσωση $543312x + 65340y = 1188$.

Άσκηση 7.3 Υπάρχουν θετικοί ακέραιοι x, y τέτοιοι ώστε $x^3 = 2^y + 15$;

Άσκηση 7.4 Να προσδιορίσετε όλους τους ακεραίους x, y που ικανοποιούν την εξίσωση $x^2 = y^2 + 2y + 9$.

Άσκηση 7.5 Να βρεθούν όλοι οι φυσικοί $a, b, c \geq 1$ με

$$\frac{1}{ab} + \frac{1}{bc} + \frac{1}{ca} = 1.$$

Άσκηση 7.6 Αν x, y ακέραιοι με $0 \leq x, y \leq 100$, να λύσετε την εξίσωση

$$|x + y - 2| + |3x - 2y + 1| + 3x - 2y + 1 = 0.$$

(Διαγωνισμός «Ο Θαλής» 1996)

Άσκηση 7.7 Να βρεθούν οι θετικές ακέραιες λύσεις της εξίσωσης $x^3 - y^3 = xy + 61$.
(Ολυμπιάδα Ρωσίας)

Άσκηση 7.8 Να λυθεί η εξίσωση $p - x^4 = 4$ όπου p πρώτος και x ακέραιος.

7.2 Ασκήσεις Β' Ομάδας

Άσκηση 7.9 Να λυθεί στους ακεραίους η εξίσωση $x^2(y - 1) + y^2(x - 1) = 1$. **(Ολυμπιάδα Πολωνίας)**

Άσκηση 7.10 Εάν p, q πρώτοι, να λύσετε την εξίσωση $\frac{1}{x} + \frac{1}{y} = \frac{1}{pq}$ στους θετικούς ακεραίους.

Άσκηση 7.11 Να βρεθούν τα ζεύγη ακεραίων x, y που ικανοποιούν την εξίσωση

$$x^3 + y^3 = (x + y)^2.$$

Άσκηση 7.12 Να λυθεί στους θετικούς ακεραίους η εξίσωση

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{3}{5}.$$

Άσκηση 7.13 Να βρεθούν οι θετικοί ακέραιοι x, y, z που ικανοποιούν την εξίσωση

$$\left(1 + \frac{1}{x}\right) \left(1 + \frac{1}{y}\right) \left(1 + \frac{1}{z}\right) = 2.$$

Άσκηση 7.14 Να δείξετε ότι η εξίσωση $a^2 + b^2 = c^2 + 3$ έχει άπειρες ακέραιες λύσεις.

Άσκηση 7.15 Υπάρχουν λύσεις της εξίσωσης $x!y! = z!$ στους φυσικούς $x, y, z > 5$;

Άσκηση 7.16 Δίνεται ο αριθμός $x = \sqrt[3]{2 + \sqrt{5}} + \sqrt[3]{2 - \sqrt{5}}$. Να εξετάσετε εάν είναι ρητός.

Άσκηση 7.17 Να λυθεί στο σύνολο των ακεραίων x, y το σύστημα των εξισώσεων

$$\begin{cases} x^2 + y^2 + z^2 = 155, & (1) \\ x + y + z = 21, & (2) \end{cases}$$

(Διαγωνισμός «Ο Ευκλείδης» 1996)

Άσκηση 7.18 Να λύσετε στους θετικούς ακεραίους x, y, z την εξίσωση $2^x + 3^y = z^2$.

Άσκηση 7.19 Να δείξετε ότι η εξίσωση

$$(x+1)^2 + (x+2)^2 + \cdots + (x+2001)^2 = y^2$$

δεν έχει ακέραιες λύσεις.

Άσκηση 7.20 Να βρείτε όλα τα ζεύγη πρώτων αριθμών (p, q) που είναι τέτοια ώστε

$$p^3 - q^5 = (p+q)^2.$$

(Ολυμπιάδα Ρωσίας)

Άσκηση 7.21 Να δείξετε ότι η εξίσωση $x^5 - y^2 = 4$ δεν έχει ακέραια λύση. **(BMO 1998)**

Άσκηση 7.22 Να βρεθούν όλοι οι πρώτοι αριθμοί p για τους οποίους το σύστημα

$$\begin{cases} p+1 = 2x^2, & (1) \\ p^2+1 = 2y^2, & (2) \end{cases}$$

έχει λύση στους ακεραίους x, y .

Άσκηση 7.23 Να δείξετε ότι εάν το n είναι θετικός ακέραιος τέτοιος ώστε η εξίσωση

$$x^3 - 3xy^2 + y^3 = n$$

να έχει λύση στους ακεραίους (x, y) , τότε έχει τουλάχιστον 3 λύσεις. Να δείξετε επίσης ότι η εξίσωση δεν έχει ακέραια λύση όταν $n = 2891$. **(IMO 1982)**

Άσκηση 7.24 Να λύσετε στους θετικούς ακέραιους την εξίσωση $3^x - 5^y = z^2$. **(BMO 2009)**

Άσκηση 7.25 Να αποδείξετε ότι δεν υπάρχουν ακέραιοι x, y, z όχι όλοι μηδέν και τέτοιοι ώστε να έχουμε $x^2 + y^2 = 3z^2$.

Άσκηση 7.26 Να βρεθούν οι φυσικοί αριθμοί x, y που είναι τέτοιοι ώστε

$$1! + 2! + 3! + \cdots + x! = y^2.$$

Άσκηση 7.27 Αν οι συντελεστές της εξίσωσης $ax^2 + bx + c = 0$, $a \neq 0$ είναι ακέραιοι περιττοί αριθμοί, να δείξετε ότι οι ρίζες της εξίσωσης δεν είναι ρητοί αριθμοί.

Άσκηση 7.28 Να προσδιορίσετε τις ακέραιες λύσεις (αν υπάρχουν) της εξίσωσης

$$14x^{12} - 11y^{12} + 3z^{12} - 8w^{12} = 1997^{1996}.$$

(1η Προκριματική Φάση 1997)

Άσκηση 7.29 Να αποδείξετε ότι:

(i) Υπάρχουν ακέραιοι a, b, c που είναι τέτοιοι ώστε $a^2 + b^2 - 8c = 9$.

(ii) Δεν υπάρχουν ακέραιοι a, b, c που είναι τέτοιοι ώστε $a^2 + b^2 - 8c = 6$.

(2η Προκριματική Φάση 1997)

Άσκηση 7.30 Να βρεθούν όλες οι ακέραιες λύσεις της εξίσωσης

$$\frac{13}{x^2} + \frac{1996}{y^2} = \frac{z}{1997}.$$

(Διαγωνισμός «Ο Αρχιμήδης» 1997)

Βιβλιογραφία

- [1] Δ. Πουλάκης, *Θεωρία Αριθμών, Μία σύγχρονη θεώρηση της κλασικής Θεωρίας Αριθμών*, Θεσσαλονίκη 1998.
- [2] Κ. Λάκκη, *Θεωρία Αριθμών*, Θεσσαλονίκη 1991.
- [3] Κ. Λάκκη, Γ. Τζίτζι, *Ασκήσεις Θεωρίας Αριθμών*, Θεσσαλονίκη 1991.
- [4] *Περιοδικό «Διάσταση»*, Εκδόση του Παραρτήματος Κεντρικής Μακεδονίας της ΕΜΕ.
- [5] *Σημειώσεις από το αρχείο διαγωνισμών της Ε. Μήτσιου*.
- [6] Μ. Στεργίου, *Ολυμπιάδες Μαθηματικών, Μαθηματικοί Διαγωνισμοί Α' Λυκείου*, Εκδόσεις Σαββάλα 2003.
- [7] Θ. Ν. Καζαντζή, *Θεωρία Αριθμών*, Εκδόσεις Μαθηματική Βιβλιοθήκη, Β' Έκδοση (1997).
- [8] T. Andreescu, D. Andrica, Z. Feng, *104 Number Theory Problems, From the Training of the USA IMO Team*, Birkhäuser 2007.

Μάθημα Θεωρίας Αριθμών

Ε.Μ.Ε

1. Γράφουμε στις σειρές τους διψήφιους αριθμούς από το 19 ως το 80. Ο αριθμός που προκύπτει διαιρείται με 1980;

2. Να εξετασθεί αν έχει λύση η εξίσωση

$$p^2 + q^3 = r^4$$

όταν οι p, q, r είναι πρώτοι αριθμοί.

3. Συμβολίζουμε με $S(n)$ το άθροισμα των ψηφίων του θετικού ακεραίου n . Να βρείτε φυσικούς αριθμούς n, m τέτοιους ώστε

$$n + S(n) = 1980 \text{ και } m + S(m) = 2013.$$

4. Ένα σύνολο A αποτελείται από ακεραίους αριθμούς και έχει ως ελάχιστο στοιχείο το 1 και ως μέγιστο το 100. Κάθε στοιχείο του A , εκτός του 1, είναι ίσο με το άθροισμα δύο (μπορεί και ίσων) αριθμών οι οποίοι ανήκουν στο A . Μεταξύ όλων των συνόλων A που ικανοποιούν τις παραπάνω συνθήκες να βρεθεί αυτό με το ελάχιστο πλήθος στοιχείων.

5. Να αποδειχθεί ότι ένας φυσικός δεν μπορεί να γράφεται ταυτόχρονα ως γινόμενο δύο διαδοχικών φυσικών αλλά και ως γινόμενο τεσσάρων διαδοχικών φυσικών.

6. Να βρεθούν όλοι οι φυσικοί αριθμοί που είναι ίσοι με το τετράγωνο του πλήθους των διαιρετών τους.

7. Για ποιες τιμές του φυσικού αριθμού n ο αριθμός

$$A = 3^{2n+1} - 2^{2n+1} - 6^n$$

είναι σύνθετος;

8. Να λυθεί στους φυσικούς η εξίσωση

$$x^3 - y^3 = xy + 61.$$

9. Το γινόμενο n ακεραίων αριθμών είναι ίσο με n ενώ το άθροισμά τους είναι ίσο με μηδέν. Να αποδειχθεί ότι $4 \mid n$.

10. Αν οι x, y είναι διαφορετικοί μεταξύ τους θετικοί ακέραιοι, να αποδειχθεί ότι ο αριθμός

$$A = \frac{(x+y)^2}{x^3 + xy^2 - x^2y - y^3}$$

δεν είναι ακέραιος.

Λύσεις

1. Γράφουμε αρχικά $1980 = 2^2 \cdot 3^2 \cdot 5 \cdot 11$. Ο δοσμένος αριθμός προφανώς διαιρείται με το 4, αφού το τελευταίο διψήφιο του τμήμα διαιρείται με 4. Επιπλέον διαιρείται με 5. Θα χρησιμοποιήσουμε ότι ένας αριθμός διαιρείται με το 9 και το 11 αν το άθροισμα των διψήφίων τμημάτων του διαιρούνται με το 9 και το 11 (εξηγήστε γιατί αρκεί και αυτό;). Έχουμε:

$$19 + 20 + \dots + 80 = (1 + 2 + \dots + 80) - (1 + 2 + \dots + 18) = \frac{80 \cdot 81}{2} - \frac{18 \cdot 19}{2} = 9 \cdot 11 \cdot 31.$$

και το ζητούμενο έπεται.

2. Γράφουμε την εξίσωση στη μορφή

$$q^3 = r^4 - p^2 = (r^2 - p)(r^2 + p).$$

Όμως $r^2 + p > r^2 - p$ οπότε έχουμε τις εξής περιπτώσεις:

- $r^2 - p = q$ και $r^2 + p = q^2$. Τότε η δεύτερη δίνει

$$p = q^2 - r^2 = (q - r)(q + r),$$

οπότε αφού $q + r > q - r$ θα έχουμε ότι $q + r = p$ και $q - r = 1$. Η δεύτερη δίνει ότι $q = 3$, $r = 2$ που όμως δίνει άτοπο στην αρχική.

- $r^2 - p = 1$ και $r^2 + p = q^3$. Τότε η πρώτη δίνει

$$p = (r - 1)(r + 1)$$

οπότε $r + 1 = p$ και $r - 1 = 1$ οπότε $r = 2$, $p = 3$ που πάλι δίνει άτοπο.

3. Θα βρούμε ένα n ώστε να ισχύει το πρώτο και η διαδικασία για το δεύτερο είναι παρόμοια. Το $S(n)$ παίρνει τη μεγαλύτερη τιμή όταν ο αριθμός έχει όσο το δυνατόν πιο πολλά 9. Επιπλέον $1000 < n < 1980$. Οπότε η μέγιστη τιμή λαμβάνεται ότι $n = 1979$ όπου τότε $S(n) = 26$. Αφού $n + S(n) = 1980$, θα πρέπει $n \geq 1980 - 26 = 1954$. Με δοκιμές τώρα βρίσκουμε ότι $n = 1962$.

Όμοια βρίσκουμε $m = 2010$.

4. Έστω ότι οι δεδομένοι αριθμοί είναι οι

$$k_1 = 1 \leq k_2 \leq \dots \leq k_n = 100.$$

Από τη συνθήκη ότι κάθε αριθμός γράφεται σαν άθροισμα δύο άλλων έχουμε

$$2k_i \geq k_{i+1},$$

από όπου

$$k_i \leq 2^{i-1} \text{ για κάθε } i = 1, 2, \dots, n.$$

Ειδικότερα έχουμε ότι $2^{n-1} \geq 100$ από όπου $n \geq 8$. Αν όμως $n = 8$ τότε εύκολα βλέπουμε ότι $k_7 = 50$ και $2k_5 = 25$ που είναι άτοπο. Άρα $n \geq 9$. Παράδειγμα σε αυτή την περίπτωση είναι το σύνολο

$$\{1, 2, 3, 5, 10, 20, 25, 50, 10\}.$$

5. Θέλουμε ουσιαστικά να δείξουμε ότι η εξίσωση

$$(1) \quad n(n+1) = m(m+1)(m+2)(m+3),$$

είναι αδύνατη στους φυσικούς. Πράγματι γράφουμε

$$m(m+1)(m+2)(m+3) = (m^2 + 3m)(m^2 + 3m + 2) = (m^2 + 3m)^2 + 2(m^2 + 3m),$$

οπότε προσθέτοντας 1 και στα δύο μέλη της (1) παίρνουμε

$$n^2 + n + 1 = (m^2 + 3m + 1)^2.$$

Όμως ο αριθμός $n^2 + n + 1$ δεν είναι ποτέ τέλειο τετράγωνο όταν ο n είναι θετικός ακέραιος αφού

$$n^2 < n^2 + n + 1 < (n+1)^2.$$

6. Έστω ότι ο αριθμός $n = m^2$ έχει $m > 1$ διαφορετικούς διαιρέτες. Τότε επειδή είναι τέλειο τετράγωνο, το πλήθος των διαιρετών του είναι περιττό, άρα $m = 2k+1$. Τότε όμως ο n είναι περιττός και έχει k διαιρέτες μικρότερους από m . Έπεται ότι ο n έχει διαιρέτη κάθε περιττό μικρότερο του $2k+1$. Οπότε

$$2k-1 \mid n = (2k+1)^2 = 4 + (2k-1)(2k+3).$$

Έπεται ότι $2k-1 \mid 4$ άρα $k = 1$ και $n = 9$.

7. Θα θέσουμε για ευκολία

$$3^n = a \text{ και } 2^n = b.$$

Τότε η παράσταση γράφεται

$$\begin{aligned} A &= 3a^2 - 2b^2 - ab \\ &= 2(a-b)(a+b) + a(a-b) \\ &= (a-b)(3a+2b) \\ &= (3^n - 2^n)(3^{n+1} + 2^{n+1}) \end{aligned}$$

Οπότε ο αριθμός A είναι σύνθετος εκτός της περίπτωσης $n = 1$.

8. Θέλοντας να χρησιμοποιήσουμε την ταυτότητα Euler πολλαπλασιάζουμε με 27 και αφαιρούμε 1 και από τα δύο μέλη οπότε η εξίσωση γράφεται

$$(3x)^3 + (-3y)^3 + (-1)^3 - 3(3x)(-3y)(-1) = 1642.$$

Κάνοντας χρήση της ταυτότητας του Euler η παραπάνω γράφεται ως

$$(3x - 3y - 1)(9x^2 + 9y^2 + 1 + 9xy + 3x - 3y) = 2 \cdot 823.$$

Ο όρος της δεύτερης παρένθεσης είναι μεγαλύτερος από αυτόν της πρώτης και επίσης ο πρώτος όρος δεν μπορεί να ισούται με 1, άρα έχουμε

$$3x - 3y - 1 = 2 \quad \text{και} \quad 9x^2 + 9y^2 + 1 + 9xy + 3x - 3y = 823.$$

Εύκολα λύνοντας το παραπάνω σύστημα (με αντικατάσταση) βρίσκουμε ότι λύση είναι η $(x, y) = (6, 5)$.

9. Αν όλοι οι αριθμοί είναι περιττοί τότε πρέπει n περιττός (από το γινόμενο), αλλά τότε έχουμε περιττό πλήθος περιττών ίσο με 0, άτοπο.

Αν ακριβώς ένας είναι άρτιος, τότε n άρτιος οπότε οι υπόλοιποι $n - 1$ είναι περιττοί και το άθροισμά τους είναι επίσης περιττό γιατί το πλήθος τους, που είναι $n - 1$, είναι περιττός. Και πάλι η σχέση με το άθροισμα δίνει άτοπο, άρα $4 \mid n$.

10. Για τον παρονομαστή γράφουμε

$$x^3 + xy^2 - x^2y - y^3 = (x - y)(x^2 + y^2).$$

Αφού ο A είναι ακέραιος, θα πρέπει

$$x^2 + y^2 \mid (x + y)^2 = x^2 + y^2 + 2xy.$$

Οπότε

$$x^2 + y^2 \mid 2xy.$$

Όμως ξέρουμε ότι

$$x^2 + y^2 \geq 2xy$$

οπότε πρέπει $x = y$, που είναι άτοπο.

Σιλουανός Μπραζιτικός

Μάθημα Θεωρίας Αριθμών

Ε.Μ.Ε

1. Να αποδειχθεί ότι κάθε θετικός ακέραιος αριθμός $n \geq 6$, μπορεί να γραφεί στη μορφή

$$n = a^2 + b^2 - c^2,$$

όπου οι a, b, c είναι θετικοί ακέραιοι.

2. Να αποδειχθεί ότι για κάθε ακέραιο $n \geq 2$ υπάρχει ένας θετικός ακέραιος ο οποίος μπορεί να γραφεί ως άθροισμα k τέλειων τετραγώνων για κάθε $2 \leq k \leq n$.

3. Θεωρούμε έναν φυσικό αριθμό $n > 1$ και έναν πρώτο αριθμό p που είναι τέτοιος ώστε

$$n \mid p - 1 \text{ και } p \mid n^3 - 1.$$

Να αποδειχθεί ότι ο $4p - 3$ είναι τέλειο τετράγωνο.

4. Να αποδειχθεί ότι υπάρχουν άπειροι θετικοί ακέραιοι n τέτοιοι ώστε

$$S(3^n) \geq S(3^{n+1}),$$

όπου με $S(a)$ συμβολίζουμε το άθροισμα των ψηφίων του a στη δεκαδική αναπαράσταση.

5. Να αποδειχθεί ότι στο επίπεδο δεν μπορούμε να βρούμε ένα άπειρο σύνολο μη συνευθειακών σημείων ώστε ανά δύο τα σημεία να έχουν ακέραια απόσταση.

6. Να αποδειχθεί ότι κάθε φυσικός αριθμός μπορεί να γραφεί ως άθροισμα αριθμών της μορφής $2^a 3^b$ ώστε κανείς προσθετέος να μην διαιρεί κάποιον άλλο.

7. Να βρεθούν όλοι οι θετικοί ακέραιοι n ώστε να υπάρχουν $k \geq 2$ θετικοί ρητοί αριθμοί $a_1, a_2, \dots, a_k$ που να ικανοποιούν

$$a_1 + \dots + a_k = a_1 \dots a_k = n.$$

8. Να βρεθούν όλες οι συναρτήσεις $f : \mathbb{N}^* \mapsto \mathbb{N}^*$ που είναι τέτοιες ώστε

$$m^2 + f(n) \mid (f(m))^2 + n,$$

για κάθε $m, n \in \mathbb{N}^*$.

9. Να βρεθούν όλες οι 1-1 συναρτήσεις $f : \mathbb{N} \mapsto \mathbb{N}$ που είναι τέτοιες ώστε

$$f(f(n)) \leq \frac{n + f(n)}{2},$$

για κάθε $n \in \mathbb{N}$.

1. Αρχικά παρατηρούμε ότι κάθε αριθμός που δεν είναι της μορφής $4k+2$ μπορεί να γραφεί στη μορφή xy όπου οι x, y είναι είτε και οι δύο άρτιοι είτε και οι δύο περιττοί. Οπότε κάθε τέτοιος αριθμός γράφεται στη μορφή

$$xy = \left(\frac{x+y}{2}\right)^2 - \left(\frac{x-y}{2}\right)^2.$$

Παίρνουμε τώρα έναν τυχαίο φυσικό $n \geq 6$. Αν αυτός δεν είναι της μορφής $4k+3$ τότε ο $n-1$ δεν είναι της μορφής $4k+2$ οπότε από τα παραπάνω θα έχουμε ότι θα υπάρχουν x, y που είναι και οι δύο άρτιοι ή και οι δύο περιττοί, ώστε

$$n-1 = \left(\frac{x+y}{2}\right)^2 - \left(\frac{x-y}{2}\right)^2,$$

οπότε

$$n = 1 + \left(\frac{x+y}{2}\right)^2 - \left(\frac{x-y}{2}\right)^2,$$

που είναι το ζητούμενο.

Αν τώρα ο n είναι της μορφής $4k+3$ τότε ο αριθμός $p-2^2$ δεν είναι της μορφής $4k+2$ άρα θα υπάρχουν x, y που είναι και οι δύο άρτιοι ή και οι δύο περιττοί, ώστε

$$n-2^2 = \left(\frac{x+y}{2}\right)^2 - \left(\frac{x-y}{2}\right)^2,$$

οπότε

$$n = 2^2 + \left(\frac{x+y}{2}\right)^2 - \left(\frac{x-y}{2}\right)^2,$$

που είναι το ζητούμενο.

2. Θα χρησιμοποιήσουμε επαγωγή στο n . Όταν $n = 2$ τότε παίρνουμε επιλέγουμε για παράδειγμα τον αριθμό 25. Αυτός είναι τέλειο τετράγωνο και γράφεται και σαν άθροισμα δύο τετραγώνων αφού

$$25 = 5^2 = 3^2 + 4^2.$$

Ας υποθέσουμε τώρα ότι για τον $n-1$ υπάρχει φυσικός x που γράφεται ως άθροισμα $2, 3, \dots, n-1$ τετραγώνων. Από την άσκηση 1, θα έχουμε ότι ο x γράφεται στη μορφή

$$x = a^2 + b^2 - c^2.$$

Θεωρούμε τον αριθμό

$$A = x + c^2.$$

Τότε αυτός είναι άθροισμα $3, 4, \dots, n$ τετραγώνων, αλλά επιπλέον $A = a^2 + b^2$ οπότε ολοκληρώνεται η επαγωγή.

3. Έχουμε ότι

$$p \mid n^3 - 1 = (n-1)(n^2 + n + 1).$$

Από την πρώτη σχέση όμως έχουμε ότι $n \leq p-1$, άρα αναγκαστικά

$$(1) \quad p \mid n^2 + n + 1.$$

Και πάλι από την πρώτη σχέση έχουμε ότι υπάρχει θετικός ακέραιος k ώστε

$$p = nk + 1.$$

Αντικαθιστώντας στην (1) έχουμε ότι

$$nk + 1 \mid n^2 + n + 1.$$

Έπεται ότι

$$nk + 1 \mid kn^2 + kn + k = (kn + 1)(n + 1) - n + k - 1,$$

από όπου συμπεραίνουμε ότι

$$nk + 1 \mid k - n - 1.$$

Όμως είναι εύκολο να δούμε ότι $kn + 1 > k - n - 1$, οπότε αναγκαστικά πρέπει

$$k = n + 1.$$

Τότε

$$4p - 3 = 4n(n + 1) + 1 = (2n + 1)^2,$$

και έχουμε το ζητούμενο.

4. Υποθέτουμε το αντίθετο. Τότε υπάρχει ένας φυσικός N ώστε για κάθε $n \geq N$, να έχουμε

$$S(3^{n+1}) > S(3^n).$$

Όμως για $n \geq 2$, έχουμε ότι

$$9 \mid S(3^{n+1}) \text{ και } 9 \mid S(3^n),$$

οπότε

$$S(3^{n+1}) \geq S(3^n) + 9.$$

Εφαρμόζοντας την τελευταία σχέση διαδοχικά παίρνουμε ότι για κάθε $n \geq N$,

$$S(3^{n+1}) \geq S(3^N) + 9(n - N + 1).$$

Το πλήθος των ψηφίων του 3^{n+1} είναι το πολύ

$$\log_{10} 3^{n+1} + 1.$$

Καθένα από αυτά τα ψηφία είναι μικρότερο ή ίσο του 9, άρα

$$S(3^{n+1}) \leq 9(\log_{10} 3^{n+1} + 1).$$

Οπότε θα έχουμε ότι

$$9(\log_{10} 3^{n+1} + 1) \geq 9(n - N + 1),$$

ή ισοδύναμα

$$N + \log_{10} 3 \geq n(1 - \log_{10} 3).$$

Η τελευταία όμως δίνει άτοπο για n αρκετά μεγάλο.

5. Θεωρούμε τρία μη συνευθειακά σημεία A, B, C από το σύνολο και έστω P άλλο ένα σημείο. Θετούμε

$$k = \max\{AB, BC\}.$$

Τότε σύμφωνα με τη συνθήκη ο k είναι θετικός ακέραιος και επιπλέον από την τριγωνική ανισότητα έχουμε

$$|PA - PB| \leq k \text{ και } |PB - PC| \leq k.$$

Οι παραπάνω απόλυτες τιμές είναι θετικοί ακέραιοι επομένως μπορούν να πάρουν το πολύ $k+1$ τιμές οι καθεμιά. Έπεται ότι το P μπορεί να ανήκει σε $k+1$ υπερβολές που ορίζονται από τα A, B και σε $k+1$ υπερβολές που ορίζονται από τα B, C . Οπότε για το P έχουν ως δυνατές επιλογές τα σημεία τομής αυτών των υπερβολών τα οποία όμως είναι το πολύ $4(k+1)^2$ οπότε δεν μπορεί το σύνολο να έχει άπειρα στοιχεία.

6. Θα δουλέψουμε με ισχυρή επαγωγή στο n . Για $n = 1$ γράφουμε $1 = 2^0 \cdot 3^0$ και για $n = 2$, γράφουμε $2 = 2^1 \cdot 3^0$. Υποθέτουμε ότι ισχύει για κάθε ακέραιο μικρότερο του n και θα δείξουμε τον ισχυρισμό για το n .

- Αν n άρτιος τότε ο $n/2$ είναι ακέραιος μικρότερος από τον n άρα γράφεται στη μορφή

$$n/2 = \sum 2^i 3^j,$$

όπου κανείς όρος δεν διαιρεί κάποιον άλλο, οπότε

$$n = \sum 2^{i+1} 3^j,$$

όπου κανείς όρος δεν διαιρεί κάποιον άλλο.

- Αν n περιττός τότε θεωρούμε τον ακέραιο k για τον οποίο ισχύει $3^k \leq n < 3^{k+1}$. Θεωρούμε τον αριθμό $n - 3^k/2$. Αυτός είναι ακέραιος, άρα από την επαγωγική υπόθεση γράφεται στη μορφή

$$n - 3^k/2 = \sum 2^i 3^j,$$

όπου κανείς όρος δεν διαιρεί κάποιον άλλο, οπότε

$$n = \sum 2^{i+1} 3^j + 3^k,$$

όπου κανείς όρος δεν διαιρεί τον άλλο, αφού για τους πρώτους το έχουμε από την επαγωγή και επίσης όλοι πλέον είναι άρτιοι εκτός από τον τελευταίο και $3^k > 3^i$, οπότε η επαγωγή ολοκληρώνεται.

7.

- Θεωρούμε πρώτα την περίπτωση που ο n είναι σύνθετος. Τώρα γράφεται στη μορφή $n = p_1 p_2$. Επιπλέον παρατηρούμε ότι $p_1 + p_2 \leq n$ οπότε μπορούμε να επιλέξουμε $a_1 = p_1$, $a_2 = p_2$ και οι υπόλοιποι να είναι $(n - p_1 - p_2)$ άσσοι. Στην περίπτωση που $p_1 + p_2 = n$, τότε $n = 4$ όπου παίρνουμε $p_1 = p_2 = 2$.
- Στην περίπτωση που ο n είναι πρώτος, επιλέγουμε

$$a_1 = \frac{n}{2}, a_2 = 4, a_3 = \frac{1}{2}$$

και τα υπόλοιπα a_k ίσα με 1. Οι μόνοι αριθμοί που δεν καλύπτουμε σε αυτή την περίπτωση είναι αυτοί για τους οποίους ισχύει

$$\frac{n}{2} + 4 + \frac{1}{2} > n \implies n < 9.$$

Οπότε μένει να εξετάσουμε ξεχωριστά τους αριθμούς

$$n = 1, 2, 3, 5, 7.$$

- Για $n = 1$, θεωρούμε $a_1 a_2 \dots a_k = 1$. Τότε από την ανισότητα AM-GM, έχουμε

$$a_1 + a_2 + \dots + a_k \geq k \sqrt[k]{1} > 1$$

για $k \geq 2$. Επομένως η περίπτωση $n = 1$ είναι αδύνατη.

- Αν $n = 2$, θεωρούμε $a_1 a_2 \dots a_k = 2$. Όμοια με παραπάνω έχουμε

$$a_1 + a_2 + \dots \geq k \sqrt[k]{2} > 2$$

για $k \geq 2$, οπότε και αυτή η περίπτωση είναι αδύνατη.

- Αν $n = 3$, θεωρούμε $a_1 a_2 \dots a_k = 3$. Όμοια με πριν

$$a_1 + a_2 + \dots \geq k \sqrt[k]{3} > 3.$$

για $k \geq 2$. Οπότε και αυτή η περίπτωση είναι αδύνατη.

- Αν $n = 5$, τότε δουλεύοντας όμοια με παραπάνω μένει να ελέγξουμε μόνο την περίπτωση $k = 2$. Τότε $a_1 + a_2 = 5$ και $a_1 a_2 = 5$. Αυτό το σύστημα όμως δεν έχει λύσεις άρα και η περίπτωση $n = 5$ είναι αδύνατη.
- Αν $n = 7$, τότε μπορούμε να επιλέξουμε τους αριθμούς

$$a_1 = \frac{9}{2}, \quad a_2 = \frac{4}{3}, \quad a_3 = \frac{7}{6}.$$

Οπότε ο n μπορεί να είναι οποιοσδήποτε θετικός ακέραιος μεγαλύτερος του 3 με μόνη εξαίρεση το 5.

8. Θέτουμε αρχικά όπου n και m το 1 και παίρνουμε

$$f(1) + 1 \mid f(1)^2 + 1 = f(1)(f(1) + 1) - f(1) + 1,$$

οπότε

$$f(1) + 1 \mid f(1) - 1 = f(1) + 1 - 2$$

άρα

$$f(1) + 1 \mid 2$$

οπότε $f(1) = 1$. Θέτοντας τώρα όπου m το 1 παίρνουμε

$$1 + f(n) \mid 1 + n$$

από όπου

$$(2) \quad f(n) \leq n.$$

Όμως αν θέσουμε όπου n το 1 παίρνουμε

$$m^2 + 1 \leq f^2(m) + 1$$

από όπου

$$(3) \quad m^2 \leq f^2(m) \implies m \leq f(m).$$

Από τις (2) και (3) έχουμε ότι $f(n) = n$ για κάθε θετικό ακέραιο n .

9. Δείχνουμε πρώτα ότι δεν υπάρχει φυσικός n ώστε $f(n) < n$. Πράγματι αν κάτι τέτοιο ισχύει τότε από την αρχική παίρνουμε

$$f(f(n)) < \frac{n+n}{2} = n.$$

Επαγωγικά δείχνουμε ότι

$$(4) \quad f^{(k)}(n) < n$$

για κάθε θετικό ακέραιο k , όπου με

$$f^{(k)}(n)$$

συμβολίζουμε την k σύνθεση της f με τον εαυτό της. Έπεται ότι θα υπάρχουν δύο θετικοί ακέραιοι $k_1 > k_2$ ώστε

$$f^{(k_1)}(n) = f^{(k_2)}(n).$$

Τότε λόγω του ότι η f είναι 1-1, θα έχουμε

$$f^{(k_1-k_2)}(n) = n,$$

το οποίο όμως είναι άτοπο λόγω της (4). Επομένως

$$f(n) \geq n$$

για κάθε φυσικό αριθμό n . Τότε η αρχική δίνει

$$f(n) \leq f(f(n)) \leq \frac{n+f(n)}{2},$$

από όπου

$$f(n) \leq n$$

για κάθε φυσικό αριθμό n . Έπεται ότι $f(n) = n$.

Σιλουανός Μπραζιτικός